Науково-дослідний інститут інформатики і права
Національної академії правових наук України
Національна бібліотека України імені В. І. Вернадського

КІБЕРБЕЗПЕКА В ІНФОРМАЦІЙНОМУ СУСПІЛЬСТВІ

Інформаційно-аналітичний дайджест

№ 10 (жовтень)

Київ – 2019

Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О.Довгань; упоряд. О.Довгань, Л.Литвинова, С.Дорогих; Науково-дослідний інститут інформатики і права НАПрН України; Національна бібліотека України ім. В.І.Вернадського. – К., 2019. – №10 (жовтень) . – 121с.

Заснований Науково-дослідним інститутом інформатики і права Національної академії правових наук України та Національною бібліотекою України імені В.І. Вернадського у 2017 р. Видається щомісяця. Відповідальний редактор О. Довгань. Упорядники О. Довгань, Л.Литвинова, С.Дорогих. Дизайн обкладинки С.Дорогих.

Аналітичний дайджест покликаний надати інформацію з питань кібербезпеки, що є надзвичайно актуальними в контексті розвитку інформаційного суспільства, зростання кіберзлочинності, використання засобів кібертероризму у гібрідних війнах та необхідності розбудови системи забезпечення кібернетичної безпеки України відповідно до визначених стратегічних напрямків з урахуванням тенденцій розвитку кіберпростору, сучасних викликів та загроз його безпеці. Призначення дайджесту – ознайомлення широкого кола фахівців у сфері кібербезпеки, а також і всіх користувачів, які цікавляться цією проблематикою, з інформаційними джерелами мережі Інтернет та новими надходженнями до фондів НБУВ (монографії, автореферати дисертацій, підручники, збірники наукових праць, матеріали міжнародних конференцій, статті з періодичних видань), що висвітлюють сучасні проблеми кібербезпеки в Україні та за кордоном.

Ознайомитися з літературою із фондів НБУВ та онлайновими інформаційними ресурсами можна за адресою: проспект Голосіївський, 3, м. Київ, 03039.

ЗМІСТ

Стан кібербезпеки в Україні 4
Національна система кібербезпеки 15
Правове забезпечення кібербезпеки в Україні 17
Кібервійна проти України 20
Боротьба з кіберзлочинністю в Україні 21
Міжнародне співробітництво у галузі кібербезпеки 22
Світові тенденції в галузі кібербезпеки 26
Сполучені Штати Америки 30
Країни ЄС 33
Китай 34
Російська Федерація та країни ЄАЕС 36
Інші країни 37
Протидія зовнішній кібернетичній агресії 42
Створення та функціонування кібервійськ 47
Кіберзахист критичної інфраструктури 47
Захист персональних даних 50
Кіберзлочинність та кібертероризм 54
Діяльність хакерів та хакерські угруповування 67
Вірусне та інше шкідливе програмне забезпечення 79
Операції правоохоронних органів та судові справи проти кіберзлочинців ... 91
Технічні аспекти кібербезпеки 95
Виявлені вразливості технічних засобів та програмного забезпечення 98
Технічні та програмні рішення для протидії кібернетичним загрозам 107
Нові надходження до Національної бібліотеки України імені В.І. Вернадського 118

«У питанні кіберзахисту Україна просувається на міжнародній арені, але все ж існують фактори, які уповільнюють цей рух. Про такі тенденції в кулуарах форуму Legal Cybersecutiry Forum розповів УНН перший заступник голови Державної служби спеціального зв'язку та захисту інформації України Олександр Чаузов.

"Я згадував про міжнародні рейтинги, оцінка дуже проста: ми піднімаємося по цих щаблях, що дає нам сподіватися, що ми рухаємося в потрібному напрямку – якщо ми не стоїмо на місці, ми розвиваємось", - зазначив він.

Зі слів Чаузова, Україна наразі займає 26 місце у державному індексі кібербезпеки.

"Глобальний індекс кібербезпеки – 54 місце зі 180 країн. А були на 4 пункти нижче (у 2017 році)", - додав він.

На думку Чаузова, швидкість розвитку українського кіберзахисту має бути більша.

"Але, якщо ви подивитесь на те, по яких критеріях відбувається оцінка, то Держспецзв'язку 98% того, що треба було зробити в кібербезпеці, зробила. Є інші суб'єкти, які свою діяльність роблять недобре", - сказав співрозмовник.

…які саме це суб'єкти, він повідомив, що Україна, за результатами огляду стану кібербезпеки від 21 вересня 2017 року, не провела жодної військової кібероперації.

На питання про те, хто відповідає за їх проведення, Чаузов повідомив: Міністерство оборони України. Водночас, з його слів, є й інші недоліки, які заважають покращенню роботи з кіберзахисту…

"Стосовно фінансування, виходячи з законодавчих норм: у нас за захист інформації відповідає власник. Наприклад, якщо є якийсь державний орган, то я не можу йому нав'язувати, я прописую правила у вигляді нормативних документів. На жаль, ситуація така, що деякі державні органи нехтують законодавством. Купляють, наприклад, олівці, а не вкладають гроші у власну кібербезпеку, в інформаційну безпеку, технічний захист інформації. Звісно, вони, скажімо так – пам'ятаєте була передача — "слабое звено", які тягнуть нас донизу. І вони є областю вразливості держави. Тобто, через них ця проблема може розповсюдитися на всіх інших", - розповів співрозмовник.

На питання про те, чи вистачає кадрів Державній службі спеціального зв'язку та захисту інформації, Чаузов відповів, що це не українська, це – всесвітня проблема.

"Зараз є так звана воронка, коли держава вкладає кошти в фахівців державних органів, готує їх, а потім комерційні структури перекупають їх за більші гроші, потім інша комерційна структура – ще за більші гроші викупає у свого конкурента або сусіда, і відбувається іноді так, що фахівець на слуху не має достатніх знань, але через те, що його перекупають, у нього зносить дах і він думає, що він суперфахівець. Хоча для цього треба постійно розвиватися, підтверджувати кваліфікацію.

Для цього ми, Держспецзв’язку, розробило питання підготовки кадрів і аудиту їх знань. Найближчим часом нормативна база з цього питання буде проведена через ВР, через Кабмін. Побачимо це", - зазначив він.

Говорячи про атаки російських хакерів на українські інформаційні ресурси, Чаузов додав, що "вони не поодинокі в цьому".

"Є країни, агресивно облаштовані проти суспільства… Такий підхід у людей. Наше основне завдання – кіберзахист. Є питання кібербезпеки – це завдання СБУ, і кіберзахисту – це наше завдання. Ми робимо все для того, щоб убезпечити український інформаційний ресурс від таких негативних впливів", - сказав заступник голови Держспецзв’язку.» ***(Саша Картер. У Держспецзв'язку дали оцінку кіберзахисту державних органів України // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/exclusive/1827709-u-derzhspetszvyazku-dali-otsinku-kiberzakhistu-derzhavnikh-organiv-ukrayini). 02.10.2019).***

***

«У Міністерстві енергетики та захисту довкілля провели донорську конференцію з кібербезпеки з метою залучення міжнародної донорської допомоги для того, щоб забезпечити енергетичну безпеку України.

Під час заходу було відзначено, що Україна ухвалила низку актів, які регулюють питання кібербезпеки. Позитивними кроками стало прийняття Закону «Про основні засади забезпечення кібербезпеки України» та Національної стратегії кібербезпеки на період до 2020 року для виконання своїх міжнародних зобов’язань. Водночас потрібні зусилля для продовження роботи в цьому напрямку.

Учасники конференції приділили увагу аналізу прогалин нормативно-правової бази сектору кібербезпеки України. Зокрема, йшлося про необхідність відрегулювати національне законодавство відповідно до міжнародних зобов’язань, унормувати термінологію, прийняти низку правил щодо вимог і процедур аудиту інформаційної безпеки об’єктів критичної інфраструктури тощо.

На думку експертів, Україна потребує оновлення Стратегії кібербезпеки, термін дії якої спливає у 2020 році, та розроблення Стратегії кібербезпеки на 2020-2025 роки.

Було запропоновано також розробити стратегію комунікацій щодо кіберінцидентів, яка сприятиме обміну інформацією між стейкхолдерами, а також прийняти закон про державно-приватне партнерство у сфері кібербезпеки.

Обговорили поточний стан кібербезпеки та проекти, впровадження яких потребує першочергового вирішення, за участю фахівців з інформаційних технологій ДП «НЕК «УКРЕНЕРГО», ДП «НАЕК «ЕНЕРГОАТОМ», ПрАТ «УКРГІДРОЕНЕРГО».

У заході взяли участь заступник Міністра інфраструктури України Олександра Клітіна, представники Служби безпеки України, Держспецзв'язку, Європейської Комісії, Енергетичного Співтовариства ЄС, Посольства Великої Британії в Україні, Посольства Канади в Україні, Посольства США в Україні, IFES Україна, Бюро Європи та Євразії USAID, Атлантичної ради та НАТО, представники ГО «Міжнародний університет кібербезпеки, Світового Банку в Україні, Європейського Банку Реконструкції та Розвитку, Європейського

Інвестиційного Банку, Місії USAID в Україні, DAI, Інституту стратегічних досліджень при Президентові України.» ***(Визначено пріоритетні завдання для зміцнення кібербезпеки в енергетиці // Євроінтеграційний портал (https://eu-ua.org/novyny/vyznacheno-priorytetni-zavdannya-dlya-zmicnennya-kiberbezpeky-v-energetyci). 11.10.2019).***

***

«Гучна піар-кампанія Індастріал Інновейшн Груп, яка начебто допомагає привести Україну до цифрового майбутнього, насправді може спричинити глобальний витік даних з баз і реєстрів до країни-агресора. Хто ж лобіює інтереси сумнівної компанії? Спробувала дізнатись команда «СтопКору».

«Я думаю, що ця ситуація може призвести до того, що це розв'яже руки російським спецслужбам на території України. І ми неодноразово зможемо ще побачити, якщо таке станеться, викрадення на території України та фізичний вплив на території України, розправи», – вважає ветеран АТО Олександр Золотнюк.

Варто зауважити ще один важливий момент: захист персональної інформації поки що законодавчо врегульований досить слабко.

Як наголошує заступник голови Комітету ВР з питань цифрової трансформації Олександр Федієнко, у захисті персональних даних необхідно доопрацювати деякі законодавчі ініціативи та закони для того, щоб унеможливити у майбутньому використання цих реєстрів, а найголовніше – запровадити відповідну кримінальну відповідальність для посадових осіб, які відповідають за ті реєстри.

Проте після цього виникає низка логічних запитань: чому Україні нав'язують id-картку приватної фірми, якщо наявна – більш захищена і вже має чіп, куди незабаром записуватимуть цифровий електронний підпис.

Чому на ринок хочуть випустити фірму, керівництво якої раніше фігурувало у багатомільярдній корупційній афері? І, нарешті, чому нікого не бентежать зв'язки цієї компанії з Росією?» ***(Паспортна афера: хто підставляє Україну під масштабну кібератаку з боку країни-агресора // Politica.com.ua (http://politica.com.ua/pasportna-afera-xto-pidstavlyaye-ukra%d1%97nu-pid-masshtabnu-kiberataku-z-boku-kra%d1%97ni-agresora/). 10.10.2019).***

***

«Компания ELKO Ukraine сообщает о подписании дистрибьюторского контракта с Bufferzone и расширении портфеля инновационных решений в сфере кибербезопасности. Основная задача Bufferzone заключается в защите конечных точек ИТ-инфраструктуры организаций любого уровня. Как показывает практика мировых реализаций, данное решение демонстрирует высокую эффективность в процессе защиты предприятий от вирусов-вымогателей, атак «нулевого дня», фишинга, целевых кибератак и других угроз нового поколения.

Многие организации вместо внедрения современных средств защиты просто ограничивают действия своих сотрудников – блокируют интернет-соединение, вносят в черные списки те или иные веб-ресурсы, запрещают использование внешних носителей. Некоторые компании обучают персонал, как «правильно» вести себя при работе с электронной почтой и вложениями. Однако, все эти

действия не исключают риски человеческого фактора, при которых работник может загрузить нежелательное вложения, перейти на подозрительный сайт или использовать зараженный вирусом внешний носитель.

Именно для таких сценариев и используется решение Bufferzone, которое с одной стороны дает возможность пользователям работать, как им удобно, а с другой – позволяет свести к минимуму связанные с этим риски. Решение Bufferzone изолируют потенциально вредоносный контент, помещая его в виртуальный контейнер, где приложения и данные отделены от внутренних ресурсов компьютера, таких как: память, реестр и системные файлы. Далее вредоносный контент очищается и удаляется. При этом, с точки зрения конечного пользователя, все происходит абсолютно прозрачно и не требует дополнительных действий.» ***(ELKO Ukraine предлагает партнерам решения кибербезопасности Bufferzone // Компьютерное Обозрение (https://ko.com.ua/elko_ukraine_predlagaet_partneram_resheniya_kiberbezopasnosti_bufferzone_130445). 10.10.2019).***

***

«Члены украинской Ассоциации руководителей подразделений IT-безопасности CISO (Chief Information Security Officer) активно обсуждают создание в Украине отдельного центра по обмену информацией о киберугрозах.

В нашей стране есть два органа, которые должны заниматься информированием о киберугрозах — Ситуационный центр обеспечения кибербезопасности департамента контрразведывательной защиты интересов государства в сфере информбезопасности (ДКИБ) СБУ и CERT-UA в Госспецсвязи. Однако они стоят на службе преимущественно у государства, тогда как у частного бизнеса эта ниша пуста. В итоге на данный момент в Украине нет такой организации, которая бы собирала данные по атакам, анализировала их, выдавала рекомендации по защите, а в идеале еще бы и сама содержала собственных специалистов по реагированию.

В ассоциации киберэкспертов сейчас уже насчитывается более 20 участников, из которых порядка 15 действующие CISO, однако консолидировать интересы всех CISO — задачка непростая. Как говорит создатель Ассоциации CISO, украинский IT-бизнесмен Александр Кардаков, технически первым шагом будет создание единой технологической платформы для сбора, аналитики и обмена данными об угрозах. Это первичная инициатива, которая, по его словам, обеспечит радикальное повышение уровня осведомленности участвующих в создании такой платформы игроков.

Система позволит оперативно получить точное описание поведения зловреда и, соответственно, признаки, по которым его можно идентифицировать у себя в корпоративной сети, даже если антивирус его “прозевает”. Нынешняя стадия — определение участников новой платформы обмена информацией о киберугрозах.

Сейчас подразделения кибербезопасности в крупных компаниях получают рассылки об угрозах из широко известных международных источников, таких как Cisco Talos, IBM X-Force и другие. Но они, как правило, имеют глобальный, а не локализованный характер. В условиях, в которых мы находимся, этого

недостаточно. Возможность быстро обнаружить киберугрозу, “заточенную” под Украину, которая ещё “не светилась” нигде в мире имеет если не первостепенное, то очень важное значение.

“Нам нужно чувствовать подход следующего Petya еще на подготовительных стадиях. И если все участники Ассоциации сообща будут наблюдать за потенциальными угрозами, то будет больше шансов увидеть надвигающуюся атаку”, — подчеркнул Александр Кардаков…

Еще одним потенциально интересным сегментом является отслеживание сканирований, которые проводят хакеры для определения слабых мест в защите периметра организаций. Если будет возможность постоянно отслеживать такую разведку, то станет реальным не только “чистить” трафик от информационного мусора, но и вовремя распознать уникальные источники сканирований, которые раньше нигде ни для кого не проявлялись и могут говорить о подготовке целевой кибератаки.

Возможных “точек контроля” гораздо больше, так что единая база о реальных угрозах в разных компаниях, пригодится всем, кто хоть как-то присутствует в киберпространстве. Авторы идеи отмечают, что уже сейчас можно организовать систему для обмена такими данными за счет минимальных вложений.

По мнению участников Ассоциации нет смысла “изобретать велосипед”, а нужно максимально использовать передовой международный опыт. В качестве опорной точки был принят опыт Израиля, так как в этой воюющей стране что государство, что частные корпорации тоже оказались в ситуации, когда среда, в которой им приходится работать, является, мягко говоря, недоброжелательной.

Под киберопекой членов Ассоциации CISO на сегодня около более 100 000 компьютеров и 50 000 других устройств — это не меньше, чем в госорганах нашей страны. Первыми участниками центра по обмену киберугрозами могут стать коммерческий центр управления кибербезопасностью, созданный украинской компанией Октава Киберзахист, а также подразделения кибербезопасности мобильных операторов. Так, CISO Vodafone Ukraine Алексей Лукин в общем и целом поддерживает идею, при этом он против того, чтобы такой центр выстраивался на базе государственной структуры. По его словам, Vodafone уже обменивается данными об угрозах, например, с Киевстаром.» ***(Сергей Кулеш. Крупные украинские компании хотят создать единый центр по обмену киберугрозами, который поможет объединить усилия и ловить хакеров вместе // ООО «ХОТЛАЙН» (https://itc.ua/news/krupnye-ukrainskie-kompanii-hotyat-sozdat-edinyj-czentr-po-obmenu-kiberugrozami-kotoryj-pomozhet-obedinit-usiliya-i-lovit-hakerov-vmeste/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+itc-ua+%28ITC.ua%29). 09.10.2019).***

***

«Министерство юстиции Украины и Министерство цифровой трансформации спустя неделю объяснили «техническим сбоем» и «человеческим фактором» исчезновение из Единого портала открытых данных публичной истории изменений записей в ЕГР (данных о предыдущих

владельцах, бенефициарах юридических лиц, предыдущих местах регистрации юридических лиц и т.д.). Часть данных уже возвращена….

Напомним, ещё 3 октября из Единого портала открытых данных (data.gov.ua) была удалена вся историю публикации открытых данных Единого государственного реестра юридических лиц, физических лиц-предпринимателей и общественных формирований (ЕГР). 3 октября в 10-04 авторизованный пользователь со стороны распорядителя данных (Минюста) под ником «s-hudchenko» удалил ресурс 15-UFOP.zip из набора данных «Единый государственный реестр юрлиц, физических лиц-предпринимателей и общественных формирований», а затем, в 10-07, добавил файл с таким же названием (15-UFOP.zip), но уже "обновленный" – без истории изменений, которая позволяет исследовать связи, предотвращать рейдерство, извещать кредиторов, улучшать сервисы частного сектора, а также является практически единственным доказательством того, что из ЕГР что-то незаконно удалялось/добавлялось…

В Минцифры объяснили отсутствие информации о сбое тем, что проблема возникла на стороне Минюста, однако только сегодня утром Минцифры передало бэкапы удаленной информации.

– Каждое ведомство является распорядителем информации и имеет ответственное лицо, которое публикует и обновляет данные на портале по закону. При обновлении такой информации ответственным со стороны Минюста произошел сбой, что привело к удалению информации. Но это не критично, поскольку есть резервные копии – соответственно, вся информация будет восстановлена и возвращена на портал, что уже, собственно, происходит, – объяснили в Минцифры.

В Министерстве юстиции о сбое также сообщили только вечером 9 октября, «забыв» указать в опубликованной информации, собственно, дату сбоя. При этом в Минюсте сообщили, что существующий функционал портала открытых данных не предусматривает возможности восстановления истории обновления наборов данных:

– При обновлении набора данных из Единого государственного реестра юридических лиц, физических лиц-предпринимателей и общественных формирований на Едином государственном веб-портале открытых данных возник технический сбой, в результате которого на указанном ресурсе вместо необходимого файла набора данных системой было отражено URL-ссылку на сам файл. Техническим специалистом были осуществлены попытки исправления данной ситуации. В то же время, существующий технический инструментарий ресурса не позволил отменить операции, которые могли привести к потере истории обновления набора данных. Вместе с тем Министерством юстиции обеспечено размещение актуального набора данных на портале. Существующий функционал портала не предусматривает возможность восстановления истории обновление наборов данных, – объясняют в Минюсте.

Как сообщают в Минюсте, там обратились к техническому администратору Единого государственного веб-портала открытых данных с вопросом о возможных путей решения проблемы:

– Минюстом будут приняты все необходимые меры с целью исправления сложившейся ситуации. Также сообщаем, что на сайте Министерства обновления указанного набора данных осуществлялось в штатном режиме.

Пока неизвестно, когда будут восстановлены все потерянные данные.» ***(Владимир Кондрашов. Власти объяснили исчезновение открытых данных ЕГР технической ошибкой // Internetua (http://internetua.com/vlasti-ob-yasnili-iscseznovenie-otkrytyh-dannyh-egr-tehnicseskoi-oshibkoi). 10.10.2019).***

***

«Представители команды программного обеспечения M.E.Doc не опубликовали признание и отчет об исправлении обнаруженной уязвимости одного из серверов…

Как стало известно, спикер Украинского киберальянса, участник объединения RUH8, известный в сети под ником Шон Таунсенд, обнаружил у M.E.Doc уязвимый сервер и в рамках responsible disclosure (ответственное раскрытие информации) сообщил об этом представителям компании. Однако те не выполнили обещания и публично не отчитались о обнаруженной уязвимости и её закрытии.

…спикеру УКА предлагали 500 долларов США за найденную уязвимость, но тот отказался, попросив только опубликовать пост с признанием уязвимости. Но в M.E.Doc этого не сделали. В результате, спустя более недели после закрытия «дыры» Шон Таунсенд сам опубликовал подробную информацию об уязвимости

– Честно говоря, я редко встречаюсь с настолько упорным сопротивлением реальности. Компания, преступное разгильдяйство которой, позволило россиянам провести одну из самых разрушительных кибер-атак современности, по-прежнему не сделала для себя никаких выводов и продолжает работать в том же самом неподражаемом стиле. Если даже после NotPetya их сервер получилось взломать за две трахнутых минуты, то Медок в кассовом аппарате – прямая угроза национальной безопасности, – резюмирует спикер УКА…» ***(Владимир Кондрашов. M.E.Doc упорно замалчивает проблемы уязвимости своего сервера // Internetua (http://internetua.com/m-e-doc-uporno-zamalcsivaet-problemy-uyazvimosti-svoego-servera). 07.10.2019).***

***

«Директор Департамента информационно-коммуникационных технологий Киевской городской государственной администрации Юрий Назаров угрожает тюрьмой этичным хакерам, обнаружившим ряд уязвимостей на сервисе авторизации Единой учетной записи киевлянина KyivID (id.kyivcity.gov.ua) и, собственно, Официальном портале Киева (kyivcity.gov.ua)…

Поводом для угроз послужил пост в Facebook спикера Украинского киберальянса, украинского этичного хакера, известного в сети под ником Шон Таунсенд. Он в рамках флешмоба #fuckresponsibledisclosure опубликовал информацию об уязвимости столичного ресурса. На сайте оказалась возможность реализовать content spoofing – подмену содержимого веб-страницы для того, чтобы пользователь, переходя по ссылке на якобы доверенный ресурс (в данном случае –

сайт столичных властей), верил, что он просматривает подлинное содержание по требуемому адресу, когда на самом деле это не так.

Также выяснилось, что около месяца с момента сообщения об уязвимости остается открытой XSS – тип уязвимости программного обеспечения, который позволяет атакующему внедрить клиентский сценарий в web-страницы, просматриваемые другими пользователями.

Более того, оказалось, что существует ещё и уязвимость, позволяющая получить доступ к одному из серверов КГГА…

Практически сразу пост прокомментировал CEO компании FDI Ukraine Николай Козлов, который заявил, что «это все правится локально у человека и видно лишь ему» и порекомендовал активистам «заняться делом».

К слову, Николай Козлов ранее занимал должность CTO компании Kitsoft, которая является разработчиком официального портала Киева…

Спустя 4,5 часа после публикации Шона Таунсенда уязвимость content spoofing была исправлена и спустя какое-то время господин Назаров сообщил, что «готов слышать и реагировать» на замечания и предложения. Более того, чиновник поблагодарил «за конструктив» человека, от которого требовал контактные данные и которому грозил «компетентными органами» за несколько часов до этого…» ***(Владимир Кондрашов. Украинский чиновник угрожает тюрьмой хакерам из-за обнаруженной уязвимости // Internetua (http://internetua.com/ukrainskii-csinovnik-ugrojaet-tuarmoi-hakeram-iz-za-obnarujennoi-uyazvimosti). 04.10.2019).***

***

«Аттестат соответствия комплексной системы защиты информации защищенного узла интернет-доступа нужен в первую очередь самим провайдерам для защиты от возможных проблем в случае инцидентов.

Об этом на втором Legal Cybersecurity Forum заявил Первый заместитель Председателя Государственной службы специальной связи и защиты информации Украины Александр Чаузов, комментируя вопросы киберзащиты государственных учреждений…

– Есть два пути: каждый государственный орган может строить свою систему защиты, для того, чтобы обезопасить себя от уязвимостей (из вне), или услугу уже у тех провайдеров интернета, у кого такая защита есть. В начале этого пути у нас было всего 5 провайдеров, у которых была система защиты информации и аттестат соответствия. Сразу возникает вопрос «Зачем нужен этот аттестат соответствия?». Я отвечу: он нужен, в первую очередь, провайдеру. Если будет какая-то уязвимость, какие-то судебные тяжбы, если к тебе как к провайдеру придет киберполиция, а ты говоришь, что «у меня есть система», а она не оценена, то виновен ты; если же она оценена, то вопрос разворачивается в другую сторону. То есть, это средство защиты провайдеров в первую очередь и способ повышения уровня кибербезопасности в целом, – отметил первый зам главы ГСССЗИ.

По словам Александра Чаузова, на сегодняшний день уже 34 оператора/провайдера телекоммуникаций получили «добро» от Госспецсвязи…» ***(Владимир Кондрашов. Чиновник объяснил, зачем провайдерам КСЗИ // Internetua (http://internetua.com/chinovnik-ob-yasnil-zacsem-provaideram-kszi). 03.10.2019).***

***

«За последние пять лет в Украине количество киберпреступлений увеличилось более, чем в два раза. По большей части скачок преступности связан с вирусом «Петя» и с 2017 года количество информационных преступлений растет лавинообразно, сообщает онлайн-платформа «Опендатабот».

Как отмечается, от этих атак могут пострадать как граждане, так и компании, и государственный сектор. А объектом киберпреступников могут стать персональные данные, банковские счета, пароли и другую информацию, которая хранится в электронном виде.

Киберпреступления бывают очень разными:

направленные на завладение средствами;

направленные на завладение информацией (для собственного пользования или для продажи)

вмешательства в работу информационных систем (для преднамеренного повреждения за вознаграждение или через хулиганство)

распространения спама и вирусных программ.

«Увеличение количества таких преступлений в последние два года в значительной мере связано с тем, что постепенно штат сотрудников киберполиции все-таки расширяется и соответственно больше нарушается уголовных дел. Но, к сожалению, львиная доля таких дел или не доходит до суда, или разваливается в суде из-за плохого сбора доказательств следственными органами. В нашей стране совсем немного грамотных следователей и экспертов, которые могли бы квалифицированно, со всеми необходимыми доказательствами, довести до суда преступление этих категорий», - комментирует адвокат Максим Лазарев.

В «Опендатабот» отмечают, что в Украине в 2018 году зафиксировано 1070 таких преступлений, тогда как в 2016 по ним было открыто только 75 уголовных производств. Зконодательство предусматривает наказание по четырем статьям ККУ за информационные преступления.

«С начала 2015 года было возбуждено 4749 дел по ст. 361, а приговоров по ним вынесено только 113. Это может свидетельствовать и о низком проценте привлеченных к ответственности по этой статье, и о сложности расследования таких дел», - считает Виталий Собкович, управляющий партнер ЮК« Альянс Правовых Сил». ***(Ирина Дождева. Количество киберпреступлений в Украине выросло в два раза // ESGROUP (https://ubr.ua/ukraine-and-world/v-ukraine-vdvoe-vyroslo-kolichestvo-kiberprestuplenij-za-poslednie-pjat-let-3887584). 21.10.2019).***

***

«…убытки бизнеса от кибератак уже к 2021 году превысят 6 триллионов долларов, считают эксперты - участники Второго Международного форума «Кибербезопасность – защити свой бизнес», организованного в Киеве Торгово-промышленной палатой Украины при поддержке Совета Национальной Безопасности и Обороны.

В ходе работы форума, более 400 представителей бизнеса, учебных учреждений, центральных и местных органов власти, 30 профильных экспертов из США, Израиля, Германии и Украины обсуждали вопросы взаимодействия власти и

бизнеса, в частности, в деле создания Национальной экосистемы кибербезопасности.

Участники мероприятия особо акцентировали внимание на том, что обществу необходимо прививать концептуальное понимание новой кибернетической реальности.

Как подчеркнул вице-президент Киевской торгово-промышленной палаты, председатель Антикризисного центра кибернетической защиты бизнеса при ТПП Украины Владимир Коляденко, «нужно популяризировать киберзащиту, начиная со школы. Каждый год в учебных заведениях должен начинаться с уроков кибергигиены".

В ходе работы форума был подписан Меморандум о сотрудничестве между департаментом киберполиции Национальной полиции и Торгово-промышленной палатой Украины. «Государственно-частное партнерство является тем локомотивом, который способен значительно улучшить ситуацию в сфере кибербезопасности», отметил начальник департамента киберполиции.

Партнерами Форума выступили Google, Microsoft, Nokia, ЧАО «Институт информационных технологий», ПАО «Одескабель», компании «Dataway security», «10Guards», «Адамант», аналитический центр ЦОСЭР и другие.

В рамках Форума открылась и Первая Национальная выставка «Кибербезопасность-2019», которая стала уникальной площадкой для бизнес-промоций и налаживания деловых контактов.» ***(Миру срочно необходима реальная действенная система киберзащиты // Багнет (http://www.bagnet.org/news/tech/409713/miru-srochno-neobhodima-realnaya-deystvennaya-sistema-kiberzashchity). 21.10.2019).***

***

«Сотрудники одного из территориальных отделов Государственной исполнительной службы как минимум несколько лет пренебрегали элементарными нормами безопасности при работе с Единым государственным реестром исполнительных производств. Госисполнители хранили логины и пароли для входа в реестр на рабочем столе, не вынимали электронные ключи из рабочих ПК даже на ночь, а сами компьютеры ГИС находились в сети wi-fi, доступ к которой был у всех желающих. Пренебрежение безопасностью госисполнители объясняют сложными паролями и закрывающейся на ночь дверью в отдел.

Об этом в суде под присягой заявил один из действующих сотрудников Государственной исполнительной службы…

На днях Подольский райсуд Киева вынес оправдательный приговор в деле начальника отдела государственной исполнительной службы Оболонского районного управления юстиции в Киеве. По версии обвинения в декабре 2013-го года тогда ещё главный государственный исполнитель отдела ГИС Подольского райуправления юстиции несколько раз со своего служебного компьютера при помощи личного ключа электронной цифровой подписи насанкционированно вмешивался в работу Единого государственного реестра исполнительных производств, изменяя данные об исполнительном производстве на сумму 460 тысяч 902 гривны. Пикантности ситуации добавляет тот факт, что должником, согласно исполнительному производству, данные которого по версии следствия и менял

обвиняемый, являлся будущий начальник отдела ГИС Подольского райуправления юстиции. Сторона обвинения считала, что таким образом обвиняемый «сделал невозможным дальнейшее исполнение решения суда и фактически исключил данное лицо с ЕГРИП как должника в исполнительном производстве, что устранило лишние препятствия в назначении последнего на должность начальника в указанном отделе ГИС».

На суде обвиняемый не только не признал свою вину в совершении инкриминируемых ему преступлений, предусмотренных частями 1 и 3 статьи 362 УК Украины, но и заявил, что внести изменения в Единый реестр мог кто угодно, поскольку госисполнители систематически и осознанно нарушали правила работы с реестром и элементарные правила кибербезопасности.

Так в суде начальник отдела ГИС Оболонского РУ Юстиции рассказал, что в 2010-м или 2012-м году для выполнения функций государственного исполнителя, касающихся внесения сведений, изменений, составления процессуальных документов в системе Единого государственного реестра исполнительных производств, ему был выдан электронный ключ, содержащий текстовый файл из 60 символов, логин (8-10 латинских букв) и пароль – 10 латинских букв. По словам госисполнителя, работа с указанным ключом была очень неудобной, так как уходило много времени для каждого входа в реестр и при ошибке государственного исполнителя «хотя бы на одну букву или цифру», срабатывала система блокировки, делая невозможным вход в систему ЕГРИП на срок до одного рабочего дня.

– Следовательно, для того, чтобы оптимизировать время и облегчить работу, поскольку нагрузки были большие, как правило, государственные исполнители, в том числе и он, не извлекали электронных ключей, копировали и хранили текстовые файлы, логины и пароли на рабочие столы своих компьютеров, – цитирует приговор слова госисполнителя. – Также обвиняемый обратил внимание на то, что при таких обстоятельствах существовала опасность несанкционированного и незаконного доступа посторонних лиц в Единый государственный реестр исполнительных производств, и внесение любых изменений в том или ином исполнительном производстве.

Обвиняемый также предположил, что при существовавших в то время мерах безопасности против несанкционированного вмешательства в систему ЕГРИП, постороннее лицо, находясь даже не в кабинете того или иного исполнителя, а в коридоре, через сеть wi-fi, зайдя на компьютер государственного исполнителя и скопировав пароль, логин и текстовый файл, могло в дальнейшем на любом компьютере и в любом месте осуществить вход в систему реестра исполнительных производств. Доступ в отдел ГИС в Подольском районе Киева в приемные дни был свободным.

Подтвердил слова обвиняемого и на тот момент начальник ОГИС Подольского РУ Юстиции в Киеве (тот самый, в интересах которого, по версии следствия, и действовал обвиняемый). Он рассказал суду, что из-за очень сложного пароля и большой нагрузки на госисполнителей, цифровые ключи для доступа к реестру в течение рабочего дня никогда не вытягивались из системных блоков и, более того, оставались по окончании рабочего дня в компьютерах на следующий

день. Экс-начальник отдела ГИС заявил суду, что потребности в извлечении этих ключей не было, еще и потому, что входная дверь ОГИС Подольского районного управления юстиции в Киеве была закрыта и открывалась кодом, который знали только работники ОГИС.

Спустя почти шесть лет суд признал теперь уже руководителя отдела ГИС Оболонского райуправления юстиции невиновным в связи с недоказанностью его участия в совершении уголовных преступлений.

Напомним, «неудобные» ключи к реестру со «сложными» паролями, по словам обвиняемого, были выданы в 2010-м или 2012-м году и описанная участниками практика наплевательского отношения к безопасности существовала как минимум до инцидента, произошедшего в декабре 2013-го.» ***(Владимир Кондрашов. Украинские госисполнители нарушали все мыслимые правила кибербезопасности // Internetua (http://internetua.com/ukrainskie-gosispolniteli-narushali-vse-myslimye-pravila-kiberbezopasnosti). 22.10.2019).***

***

Національна система кібербезпеки

«…Начальник Київського управління кіберполіції Анатолій Скиба повідомив, що наразі кіберполіція має доступ до системи «Розумне місто» лише в 5 українських містах.

«Маючи доступ до системи, ми зможемо допомогти у виявленні вразливостей. У разі виявлення, наші спеціалісти зможуть допомогти у їх ліквідації», - відмітив Анатолій Скиба.

Він додав, що таким чином можливо максимально убезпечити систему від можливих сторонніх втручань у систему безпеки усього цього комплексу.

«Оскільки система «розумне місто» має такі великі можливості, зовнішнє втручання може надати зловмисникам необмежені можливості у використанні великого масиву даних. Це може становити серйозну загрозу безпеці громадян», - зазначив Анатолій Скиба.

Відтак, кіберполіція запропонувала допомогу у дослідженні системи безпеки «розумного міста». ***(Кіберполіція пропонує допомогу у дослідженні системи безпеки «розумного міста» // Кіберполіція України (https://cyberpolice.gov.ua/news/kiberpolicziya-proponuye-dopomogu-u-doslidzhenni-systemy-bezpeky-rozumnogo-mista-5705/). 01.10.2019).***

***

«Президент України Володимир Зеленський призначив Сергія Демедюка заступником секретаря Ради національної безпеки і оборони України.

Про це йдеться у президентському указі №765/2019 від 21 жовтня.

«Призначити Демедюка Сергія Васильовича заступником секретаря Ради національної безпеки і оборони України», – йдеться у тексті указу.

Додамо, генерал поліції третього рангу Демедюк Сергій Васильович раніше очолював Департамент кіберполіції НПУ.

В свою чергу, новий очільник РНБО, Данілов заявив, що потрібно забезпечити таку систему кіберзахисту, “щоб жоден агресор не мав можливості напасти на нашу країну”

Про це сказав секретар Ради національної безпеки і оборони України Олексій Данілов, виступаючи на Другому міжнародному форумі “Кібербезпека. Захисти свій бізнес” у Києві, передає пресслужба РНБО.

Данілов наголосив, що фахівці державного й приватного секторів мають спільно розробити потужну систему кіберзахисту України.

“Сьогодні кібербезпека є питанням номер один для кожної сучасної країни, – заявив він. – Наше завдання – в жодному разі не програти питання кібербезпеки України”.

За словами секретаря РНБО України, потрібно забезпечити таку систему кіберзахисту, “щоб жоден агресор не мав можливості напасти на нашу країну”.

Данілов зазначив, що військовослужбовці, які боронять нашу країну на передовій, і фахівці із захисту цифрового й інформаційного простору “виконують одне і те саме завдання”.

У коментарі журналістам секретар РНБО України повідомив, що ближчим часом планується розробити зміни до Стратегії кіберзахисту України, і у цій роботі Раді національної безпеки і оборони України допомагають фахівці як з профільних державних структур, так і представники приватного сектору…» ***(Ігор Нагорний. Зеленський зробив гучне призначення! Секретар РНБО не став мовчати // Корупція Інфо (https://korupciya.com/zelenskyj-zrobyv-guchne-pryznachennya-sekretar-rnbo-ne-stav-movchaty/). 22.10.2019).***

***

«Державна служба спеціального зв'язку та захисту інформації приступила до реалізації проекту з розгортання першого в Україні кіберполігона…

За словами заступника голови Держспецзв'язку Олександра Чаузова кіберплатформа призначена для тренування нових співробітників і забезпечення кібербезпеки держсектора.

Чиновник зазначив, що полігон стане «інструментом для боротьби з дефіцитом фахівців з кібербезпеки».

«Цей механізм (кіберполігон — ред.) Буде спочатку запущений в інтересах силових структур, а потім ми будемо» підтягувати «фахівців з об'єктів критичної інфраструктури, вчених, студентів і т. д», — додав Чаузов.» ***(В Україні відкриють перший кіберполігон // Високий Замок Online (https://wz.lviv.ua/news/399516-v-ukraini-vidkryiut-pershyi-kiberpolihon). 21.10.2019).***

***

«Сьогодні, 19 жовтня, наказом Голови Національної поліції України на посаду начальника Департаменту кіберполіції було призначено Олександра Гринчака. Його першим заступником призначено Сергія Кропиву.

Голова Національної поліції України Ігор Клименко повідомив, що найближчим часом підрозділ змінюватиметься та розвиватиметься…

Новопризначений очільник Департаменту кіберполіції розповів, що наразі вже створено концепцію вдосконалення підрозділу. Її основою залишатиметься якісний підбір кадрів та сучасний підхід до роботи…

Він висловив вдячність за довіру та запевнив у готовності до якісного виконання поставлених перед підрозділом завдань у протидії кіберзлочинності…» ***(У Кіберполіції представили нового керівника підрозділу // Офіційний сайт Національної поліції (https://www.npu.gov.ua/news/kiberzlochini/u-kiberpolicziji-predstavili-novogo-kerivnika-pidrozdilu/). 19.10.2019).***

***

«Президент України Володимир Зеленський призначив секретаря Ради національної безпеки і оборони Олексія Данілова керівником Національного координаційного центру кібербезпеки

Про це повідомляє офіційний сайт президента України.

Текст відповідного указу №771/2019 від 25 жовтня оприлюднено на сайті глави держави. Згідно з документом, Зеленський вніс зміни до указу президента від 7 червня 2016 року № 242. “На зміну статті 2 Указу Президента України від 7 червня 2016 року № 242 “Про Національний координаційний центр кібербезпеки” (зі зміною, внесеною Указом від 19 червня 2019 року № 415) призначити Данілова Олексія Мячеславовича – Секретаря Ради національної безпеки і оборони України – керівником Національного координаційного центру кібербезпеки”, – йдеться в указі, який набирає чинності з дня публікації.» ***(Секретар РНБО Данілов очолив Національний координаційний центр кібербезпеки // ТРК «ТВА» (https://tva.ua/2019/10/27/sekretar-rnbo-danilov-ocholyv-natsionalnyj-koordynatsijnyj-tsentr-kiberbezpeky/). 27.10.2019).***

***

Правове забезпечення кібербезпеки в Україні

«Кабинет Министров Украины до сих пор не принял распоряжение «Об утверждении плана мероприятий на 2019 год по реализации Стратегии кибербезопасности Украины». Соответствующий проект постановления на данный момент проходит этап согласования с заинтересованными органами власти…

Сегодня, 22 октября, на заседании Национальной комиссии, осуществляющей государственное регулирование в сфере связи и информатизации, НКРСИ без замечаний согласовала проект распоряжения Кабинета Министров Украины «Об утверждении плана мероприятий на 2019 по реализации Стратегии кибербезопасности Украины», направленный письмом Государственной службы специальной связи и защиты информации Украины.

На реплику присутствующего на заседании Нацкомиссии первого заместителя председателя Комиссии по вопросам науки и ИТ УСПП Олега Гусева о том, что утверждать план деятельности на 2019-й год в октябре этого года поздно, в НКРСИ лишь развели руками.

Стратегия кибербезопасности Украины была утверждена Советом национальной безопасности и обороны 27 января 2016-го года и введена в действие Указом Президента от 15 марта того же года. Целью Стратегии кибербезопасности Украины является создание условий для безопасного функционирования киберпространства, его использования в интересах личности, общества и государства…». ***(Владимир Кондрашов. Кабмин до сих пор не утвердил план реализации стратегии кибербезопасности на нынешний год // Internetua (http://internetua.com/kabmin-do-sih-por-ne-utverdil-plan-realizacii-strategii-kiberbezopasnosti-na-nyneshnii-god). 22.10.2019).***

***

«Офис эффективного регулирования (BRDO) работает над имплементацией в отечественное законодательство европейского Кодекса электронных коммуникаций. Разрабатываемый документ, помимо прочего, содержит ряд новых инструментов, которые определяют особенности обеспечения безопасности сетей, услуг и взаимоотношения поставщика электронных коммуникационных услуг с потребителями, другими субъектами рынка и государством в сфере киберзащиты.

Об этом на втором международном форуме «Кибербезопасность. Защити свой бизнес» сообщила эксперт сектора IT и Телеком BRDO Надежда Кострыба…

– BRDO сейчас разрабатывает проект Кодекса об электронных коммуникациях. Мы находимся на этапе обсуждения этого проекта с участниками рынка. Основные задачи документа – развитие высокоскоростных сетей и предоставление услуги широкополосного доступа к Интернету как универсальной услуги для всех потребителей на всей территории Украины. Эти задачи, конечно же, требуют эффективного правового регулирования вопросов, связанных с безопасностью, учитывая курс на «государство в смартфоне», защиту цифровых прав граждан, а также то, что мы идем к единому цифровому рынку с Европейским союзом, что также накладывает свои требования, – отметила эксперт BRDO. – Мы взяли за основу модель Европейского Кодекса электронных коммуникаций 2018-го года, в котором предусмотрен ряд инструментов для поставщиков услуг, операторов. Эти инструменты определяют, как должна обеспечиваться безопасность сетей и услуг, в частности – относительно к пользователям и другим участникам рынка.

По словам Надежды Кострыбы, это преимущественно «информационные инструменты». Так поставщики электронных коммуникационных услуг должны как социально значимую информацию предоставлять своим потребителям сведения о средствах защиты конфиденциальности (персональных данных) и средствах защиты от киберинцидентов. Также до начала предоставления услуги, как одно из условий её предоставления, потребитель должен быть проинформирован о типах защиты, которые поставщик услуг планирует применять при предоставлении соответствующей услуги.

– Также есть ряд требований при наступлении реальных угроз безопасности сетей или услуг: опять-таки потребителям должна предоставляться информация о том, какие средства могут быть ими применены в конкретном случае для обеспечения безопасности, а также ориентировочная стоимость соответствующих средств обеспечения безопасности, – отметила эксперт. – Другим участникам рынка оператор должен предоставлять информацию, которая позволяет идентифицировать инцидент.

Однако, по словам эксперта сектора IT и Телеком BRDO, основным инструментом обеспечения ИБ для операторов и провайдеров услуг является выполнение требований специальных законов в сфере кибербезопасности.

– Здесь, конечно, есть ещё ряд вопросов, над которыми нужно работать. Закон об основах обеспечения кибербезопасности не дает ответов на все вопросы. В частности, это касается тех средств защиты, которые применяются частным сегментом, который не отнесен к объектам критической инфраструктуры. Также есть вопросы об имплементации Директивы Европейского Парламента и Совета (ЕС) 1148 (от 6.08.2016) «О мерах для высокого общего уровня безопасности сетевых и информационных систем на территории Союза» в части, например, защиты цифровых услуг. Директива предусматривает отдельные средства защиты таких услуг как электронные торговые площадки, поисковые системы, услуги облачных вычислений. И эти мероприятия предусматривают как управление рисками, так и обязанность информирования государства об инцидентах, возникающих при предоставлении таких услуг, – подчеркнула Надежда Кострыба.

Отметила эксперт BRDO и необходимость усовершенствования уже существующих инструментов обеспечения кибербезопасности:

– От многих участников анализируемых нами рынков мы получали сигналы о том, что действующая на сегодня комплексная система защиты информации требует, скажем так, «усовершенствования». Те инструменты, которые есть сегодня у госдуарства для бизнеса, должны быть эффективнее и удобнее. Здесь для нас всех есть поле для деятельности.

К слову, разрабатываемый BRDO проект Кодекса электронных коммуникаций играет на том же поле, что и уже внесенный в Раду 15 октября законопроект №2264 «Об электронных коммуникациях». Проект закона №2264 также, согласно пояснительной записке, имплементирует положения европейского Кодекса и позволяет активно развиваться высоко конкурентному рынку интернет-доступа в стране. Вопрос также в том, кто будет вносить законопроект от BRDO в Раду, ведь профильный комитет ВРУ по вопросам цифровой трансформации стал инициаторами проекта закона 2264.» ***(Владимир Кондрашов. В BRDO рассказали, какие новшества кибербезопасности будут в проекте Кодекса электронных коммуникаций // Internetua (http://internetua.com/v-brdo-rasskazali-kakie-novshestva-kiberbezopasnosti-budut-v-proekte-kodeksa-elektronnyh-kommunikacii). 17.10.2019).***

***

«До кінця 2019 року в ЗСУ завершать формування Командування військ зв'язку та кібербезпеки та Командування сил підтримки, які дозволять позбавити Генштаб невластивих функцій…

Формування двох нових командувань відбувається у рамках приведення Генерального штабу та інших органів військового управління у відповідність до структури, прийнятої у штабах НАТО.

Загалом усі заходи стосовно переведення як Генерального штабу ЗС України на J-структуру, так і органів військового управління оперативної ланки на J (G, A, N)-структури будуть завершені до кінця 2020 року.

Водночас готуються пропозиції щодо внесення змін до нормативно-правових актів, які забезпечать введення протягом 2020 року окремих посад Головнокомандувача ЗС України та начальника Генерального штабу Збройних сил України, а також набуття Генеральним штабом ЗС України та іншими органами військового управління спроможностей у складі J (G, A, N)-структур.

Також планується впровадити нову, вдосконалену, організаційно-штатну структуру Об'єднаного оперативного штабу ЗСУ та продовжити подальшу його трансформацію в Командування об'єднаних сил (протягом 2020 року).

У рамках удосконалення систем управління основна увага приділяється питанням відокремлення функцій генерування від функції застосування. Матрицею Стратегічного оборонного бюлетеня України визначено строк виконання зазначеного завдання до кінця 2020 року. На цей час функції генерування вже покладено на командування видів і родів військ (сил) та частково – на Генштаб ЗСУ. Функцію застосування військ (сил) покладено на Об'єднаний оперативний штаб, який нині реалізує це в операції об'єднаних сил.

Водночас, відповідно до чинного законодавства за Генеральним штабом зберігається функція стратегічного керівництва силами оборони в разі повномасштабної агресії. За командувачами видів залишено повноваження з проведення видових операцій поза межами відповідальності командувача об'єднаних сил.

Важливий аспект – продовження автоматизації процесів оперативного (бойового) управління та адміністративної діяльності. Пріоритетами за цим напрямом є:

автоматизація процесів керівництва та управління військами;

управління авіацією та протиповітряною обороною;

автоматизація обліку особового складу та управління персоналом;

управління ракетними військами й артилерією;

управління веденням військової розвідки;

управління логістичним забезпеченням;

управління оборонними ресурсами.

Для прискорення процесу автоматизації в Управлінні розвитку автоматизації ЗСУ та ГУЗІС нині переглядають усі дослідно-конструкторських роботи з метою, по-перше, виключити паралельну розробку різними колективами одних і тих самих функцій в загальній системі, а по-друге – не випустити з поля зору жодну з дійсно

перспективних і сучасних розробок, зокрема й волонтерських. Також до кінця поточного року планується суттєво збільшити потужність сил та засобів впровадження автоматизації, особливо польових: це пришвидшить перехід армії на нові стандарти й технології.» ***(Владислав Христофоров. В Збройних силах формують два нові командування // Національний промисловий портал (https://uprom.info/news/vpk/v-zbrojnyh-sylah-formuyut-dva-novi-komanduvannya/). 13.10.2019).***

***

«Хакеры взломали Facebook-страницу Чрезвычайного и Полномочного Посла Украины в Республике Австрия Александра Щербы…

На данный момент страница Александра Щербы удалена.

Как стало известно, несколько часов назад Чрезвычайный и Полномочный Посол Украины в Республике Австрия Александр Щерба на собственной странице в Facebook написал, что его аккаунт в соцсети был скомпрометирован. Дипломат также опубликовал скриншот, подтверждающий это, – злоумышленникам удалось изменить почту, к которой привязан FB-аккаунт посла. Спустя несколько минут, страница посла была удалена, но пользователи успели сохранить опубликованный дипломатом скриншот.

По данным пользователей, которым удалось ознакомиться с публикацией Александра Щербы до её удаления, в своём посте на Facebook тот писал о том, что аккаунт был взломан не смотря на использование двухфакторной аутентификации для входа.» ***(Владимир Кондрашов. Хакеры взломали Facebook-страницу посла Украины в Австрии // Internetua (http://internetua.com/hakery-vzlomali-facebook-stranicu-posla-ukrainy-v-avstrii). 22.10.2019).***

***

Боротьба з кіберзлочинністю в Україні

«…Працівники Слобожанського управління кіберполіції встановили причетність… 29-річного мешканця Харкова. Чоловік з 2018 року займався зламом віддалених серверів для подальшого продажу отриманої незаконним шляхом інформації.

Для залучення клієнтів, він розміщував на спеціалізованих сайтах та форумах оголошення щодо продажу доступів до віддалених серверів. Для оплати таких послуг використовувалися російські електронні платіжні системи…

За даним фактом триває досудове розслідування, кваліфіковане за ч. 2 ст. 361 (Несанкціоноване втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку) КК України. Зловмиснику загрожує до 6 років ув’язнення…» ***(Кіберполіція викрила хакера у зламі більше двох тисяч комп’ютерів українців // Кіберполіція України (https://cyberpolice.gov.ua/news/kiberpolicziya-vykryla-xakera-u-zlami-bilshe-dvox-tysyach-kompyuteriv-ukrayinczіv-4967/0. 04.10.2019).***

***

«…Працівники кіберполіції спільно зі слідчими Головного слідчого управління Національної поліції України, за процесуального керівництва Генеральної прокуратури України, викрили масштабний сервіс для масової розсилки електронних повідомлень.

Встановлено, що усі роботи сервісу проводилися виключно на замовлення зацікавлених клієнтів. За допомогою цього ресурсу можливо було купити активовані облікові записи у великій кількості до різноманітних поштових ресурсів, соціальних мереж, платіжних систем тощо. При цьому, продавалися і верифіковані облікові записи, вартість яких була значно більшою.

Такі послуги використовувалися зазвичай для здійснення анонімної масової розсилки повідомлень про нібито виграш автомобіля (грошей), сплати неіснуючого боргу тощо. Більше, сервіс надавав змогу своїм клієнтам здійснювати спам-розсилки та реєструвати акаунти на різноманітних ресурсах, що потребують для реєстрації номер телефону із подальшою верифікацією (соціальні мережі, електронна пошта тощо).

Для захисту своїх мереж та анонімізації зловмисники використовували VPN та TOR сервіси.

Поліцейські провели обшуки у шести містах України: Києві, Одесі, Львові, Миколаєві, Рівному та Херсоні. У цих містах знаходилися будинки, гаражні бокси, квартири та орендовані офіси, які зловмисники використовували для протиправної діяльності. За результатами обшуків вилучено обладнання, яке використовувалося для ведення такої діяльності. Техніку направлено на експертизу.

Досудове розслідування триває у межах раніше розпочатого кримінального провадження за ст.189 (Вимагання), ст.258 (Терористичний акт), ст.259 (Завідомо неправдиве повідомлення про загрозу безпеці громадян, знищення чи пошкодження об'єктів власності) КК України. Проводяться заходи щодо притягнення до відповідальності осіб, що причетні до організації такої діяльності.» ***(Кіберполіція припинила діяльність масштабного сервісу для реєстрації різних акаунтів у месенджерах, соцмережах та поштових сервісах // Кіберполіція України (https://cyberpolice.gov.ua/news/kiberpolicziya-prypynyla-diyalnist-masshtabnogo-servisu-dlya-reyestracziyi-riznyx-akauntiv-u-mesendzherax-soczmerezhax-ta-poshtovyx-servisax-8596/). 01.10.2019).***

***

Міжнародне співробітництво у галузі кібербезпеки

«Міністр цифровий трансформації Михайло Федоров хоче співпрацювати з корпорацією Google аби посилити кібербезпеку в Україні. Спільно з пошуковиком він хоче навчити членів Кабінету міністрів кіберграмотності.

Федоров наголосив, що деякі чиновники не розуміють навіть базові речі щодо кібербезпеки, передає видання tech.liga.net.

"Дуже важливе питання, яке я називаю "цифровою ментальністю". Дуже багато чиновників не розуміють базові речі кібербезпеки. Тому ми плануємо спільно з Google провести низку освітніх заходів для нашого Кабміну, для того, щоб його члени мали ці базові знання. Це називається в нашій сфері "кібергігієна", – передає міністр.

Він також додав, що подібні заходи нині потрібно проводити по всій країні. Це є однією з амбітних цілей його міністерства – навчити 6 мільйонів людей цих базових навик та умінь. І це має відбутись протягом найближчих кількох років.

Міністр наголосив, що лише така "цифрова ментальність" чиновників та усіх українців загалом зможе створити кібербезпеку на базовому рівні.» ***(Федоров хоче співпрацювати з Google щодо кібербезпеки в Україні // Телеканал новин «24» (https://24tv.ua/techno/fedorov_hoche_spivpratsyuvati_z_google_shhodo_kiberbezpeki_v_ukrayini_n1213236). 02.10.2019).***

***

«…Девять стран планируют присоединиться в ближайшее время к работе Центра киберзащиты НАТО в Таллине. Об этом в пятницу заявил руководитель центра, полковник Яак Тариэн.

По его словам… в процессе присоединения к Центру в данный момент находятся Словения, Хорватия, Черногория, Швейцария и Япония. Кроме того, Австралия, Ирландия, Канада и Люксембург заявили о намерении присоединиться к работе этой организации в будущем, добавил Тариэн.

«Понимание государствами серьезности тематики кибербезопасности за последние два-три года значительно изменилось, – сказал Яак Тариэн. — Большое изменение состоит в том, как государства осмысливают и как говорят о проблемах кибербезопасности. Очевидно, что об опасностях в этой сфере хотят говорить все чаще и что реальные шаги по усилению международного сотрудничества считают важными. О международной актуальности темы свидетельствует и постоянно растущее число членов расположенного в Эстонии центра по сотрудничеству в сфере кибероборонь»…» ***(Евгений Радченко. Центр киберзащиты НАТО расширяется: подробности // Независимый Регион (https://nr2.com.ua/sobytiya/2019/10/06/centr-kiberzashity-nato-rasshiriaetsia-podrobnosti/). 06.10.2019).***

***

«21 жовтня, відбулася зустріч Міністра оборони України Андрія Загороднюка з естонською делегацією на чолі з Міністром оборони Естонської Республіки паном Юрі Луйком…

В ході зустрічі Міністр оборони України подякував естонській стороні за послідовну та незмінну підтримку територіальної цілісності та незалежності України, а також за значну допомогу у посиленні спроможностей українських Збройних Сил, яку надає Уряд Естонії.

«Естонія є надійним партнером та другом України. Це країна, яка підтримує нас як політично, так і в сфері оборони. Ми сподіваємося на посилення оборонного співробітництва між нашими країнами», – зазначив Андрій Загороднюк.

Основною темою зустрічі стало обговорення питань двостороннього співробітництва між міністерствами оборони України та Естонії у сферах організації територіальної оборони та кібербезпеки. Андрій Загороднюк акцентував увагу на важливості вивчення та обміну досвідом Естонії із зазначених питань…

Сторони зауважили на необхідності обміну досвідом, враховуючи спільні виклики та загрози, які стоять перед обома країнами…» ***(Україна та Естонія співпрацюватимуть у сферах кібербезпеки, реабілітації військових та реформуванні військової освітии // Євроінтеграційний портал (https://eu-ua.org/novyny/ukrayina-ta-estoniya-spivpracyuvatymut-u-sferah-kiberbezpeky-reabilitaciyi-viyskovyh-ta). 22.10.2019).***

***

«Секретар Ради національної безпеки і оборони Олексій Данілов і посол Японії в Україні Такаші Кураі провели зустріч, під час якої обговорили, зокрема, можливості поглиблення співпраці між Україною та Японією у сфері кібербезпеки та екології…

Данілов, як зазначається, подякував Японії за послідовну політику щодо підтримки суверенітету та територіальної цілісності нашої країни і підтримку, яку надає Японія Україні за різними напрямами.

Він також висловив впевненість, що візит Президента Україна Володимира Зеленського до Японії стане черговим важливим кроком на шляху поглиблення діалогу між нашими державами.

Крім того, сторони обмінялися думками щодо розвитку безпекової ситуації у глобальному та регіональному вимірах, обговорили найбільш актуальні питання двостороннього порядку денного та домовилися щодо подальших кроків…

У свою чергу Кураі висловив підтримку реформам у секторі безпеки та оборони, започаткованим командою Президента…» ***(Ясамін Мохаммад. Україна та Японія обговорили поглиблення співпраці у сфері кібербезпеки // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1830704-ukrayina-ta-yaponiya-obgovorili-pogliblennya-spivpratsi-u-sferi-kiberbezpeki). 18.10.2019).***

***

«Під час зустрічі президента України Володимира Зеленського з генеральним секретарем Організації Північноатлантичного альянсу (НАТО) Єнсом Столтенбергом було досягнуто домовленості про допомогу Україні в розмірі 40 млн євро.

Про це повідомив генсек НАТО на спільному брифінгу з українським президентом після засідання комісії Україна-НАТО, який транслював телеканал ZIK.

"НАТО продовжує надавати Україні практичну допомогу. Сьогодні ми переглянули наш комплексний пакет допомоги Україні. Через 10 трастових фондів

союзники НАТО і партнери виділили більше 40 млн євро для підтримки України", - зазначив Столтенберг.

Гроші передбачені для бойового командування, кібербезпеки та медичної реабілітації…» ***(НАТО виділило Україні 40 млн євро на кібербезпеку та реабілітацію // Західна інформаційна корпорація (https://zik.ua/news/2019/10/31/nato_dalo_ukraini_40_mln_ievro_na_kiberbezpeku_ta_reabilitatsiyu_1680711). 31.10.2019).***

***

«Представники Європейського Союзу висловили зацікавленість в досвіді України у боротьбі з гібридними загрозами, особливо в контексті виборів. Про це заявили голова Представництва Європейського Союзу в Україні Матті Маасікас та голова Групи підтримки України Пітер Вагнер, передає УНН з посиланням на повідомлення пресслужби Представництва ЄС в Україні.

"ЄС висловлює солідарність з Україною під час підрахунку гібридних загроз і продовжує надавати свою підтримку в кібербезпеці та боротьбі з дезінформацією. Зокрема, зміцнення впевненості та підвищення обізнаності були ключовими елементами цієї підтримки перед та під час виборів 2019 року",- сказав голова Представництва Європейського Союзу в Україні Матті Маасікас під час конференції на тему "Дезінформація та кібербезпека під час виборів в Україні: засвоєні уроки та майбутні кроки", що відбулась 31 жовтня в Києві.

Він додав, що ЄС "використовуватиме позитивний досвід цієї співпраці у своїх майбутніх діях в Україні та за її межами".

"Оскільки військові гібридні загрози, як правило, посилюються в часи виборів, підтримка Європейського Союзу та Естонії для України була особливо важливою в 2019 році, коли відбулася не одна, а дві значні виборчі кампанії, президентська і парламентська", – прокоментував директор Естонського центру Східного партнерства Герт Анцу.

Повідомляється, що проект "Протидія виборчим кампаніям, пов'язаним з виборами та дезінформаційними кампаніями в Україні", реалізований Естонським центром Східного партнерства та CybExer Technologies, є частиною більш великих зусиль Європейського Союзу щодо підтримки стійкості України до кіберзагроз та дезінформації шляхом розбудови потенціалу структур безпеки України, відповідальних за запобігання та управління кіберзагрозами та зміцнення навичок представників місцевих ЗМІ у південних та східних регіонах України для виявлення та інформування громадськості про дезінформацію в кіберпросторі.

Пітер Вагнер, голова Групи підтримки України, додав, що "лише небагато країн стикаються з проблемами кібербезпеки, схожими на ті, що має Україна".

Він підкреслив, що "досвід України, особливо в контексті виборів, цікавий для інших країн Східного партнерства, а також для країн-членів ЄС"…» ***(Саша Картер. Досвід України в контексті виборів цікавий для країн-членів ЄС // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1833222-dosvid-ukrayini-v-konteksti-viboriv-tsikaviy-dlya-krayin-chleniv-yes). 31.10.2019).***

***

«Глава римо-католицької церкви Папа Франциск, виступаючи на конференції "Суспільне благо в цифровому сторіччі", що відбулася у Ватикані, звернувся до глав IT-компаній про наслідки аморального технологічного прогресу, який може призвести до занепаду соціуму…

"Видатні досягнення в області технології, особливо в штучному інтелекті, починають відігравати все більш значну роль у всіх областях людської діяльності", — заявив Папа Франциск.

Він також закликав громадськість до відкритого діалогу щодо цих питань. Понтифік попередив про небезпеку використання штучного інтелекту "для поширення думок та тенденційних помилкових даних, які можуть отруїти громадські дебати і навіть маніпулювати думками мільйонів людей.

Також понтифік попередив про можливі моральні проблеми, які можуть виникнути в результаті розвитку нових технологій.

"Якщо так званий технічний прогрес людства стане ворогом суспільного блага, це призведе до прискорбному регресу до якоїсь формі варварства, де панує право сильного", — сказав він.

Конференція була присвячена потенційним небезпекам поширення неправдивої інформації і таких технологій, як штучний інтелект і кібербезпеку. У заході брали участь теологи, науковці та керівники IT-компаній, зокрема, з-засновник Mozilla Мітчелл Бейкер, директор команди юристів з кібербезпеки з Facebook Гевін Корн, со-засновник LinkedIn Рейд Хоффман і старший віце-президент Western Digital Джим Уелш…» ***(Папа Римський виступає проти штучного інтелекту // Дзеркало тижня. Україна (https://dt.ua/WORLD/papa-rimskiy-vistupaye-proti-shtuchnogo-intelektu-325054_.html). 01.10.2019).***

***

«Компания Code42, профессионально занимающаяся защитой данных, на днях опубликовала глобальный отчет о состоянии кибербеопаности в 2019 году. Согласно этому отчету, Почти все сотрудники различных компаний хотя бы раз выносили за пределы своей работы информацию, которую выносить не следует.

…все идеи и прочая проприетарная информация являются цифровыми. Компании проделали хорошую работу, упростив процесс обмена информацией между сотрудниками. Для коммуникации на рабочем месте активно используются инструменты вроде Google Drive, Drop Box, Slack и электронной почты. Но проблема заключается в том, что эти же инструменты могут быть использованы для кражи ценных данных…

На цифровом рабочем месте люди и данные становятся все более подвижными. Количество традиционных рабочих мест сокращается. Все большие объемы работы производятся удаленно. Компании существенно экономят на офисах и зарплатах, позволяя своим людям работать через интернет или привлекая к работе внештатников. Но у этого есть своя цена.

“Несмотря на то, что многие компании используют традиционные инструменты профилактики, потери, утечки и кражи данных инсайдерами продолжают нарастать тревожными темпами. Группам информационной безопасности необходимо найти новые способы защиты данных. Без принятия срочных мер внутренние угрозы станут более разрушительными”, - говорится в исследовании.

Согласно отчету, 69% крупных организаций утверждают, что хотя бы раз сталкивались с кражей данных инсайдерами, несмотря на превентивные меры. Почти две трети опрошенных сотрудников признают, что принесли часть данных со своей прошлой работы на новое рабочее место. При этом большинство работников считают, что являются хозяевами результатов своей работы и имеют право распоряжаться ими на свое усмотрение.

…в прошлом году около 25% жителей США сменили работу. “Когда человек бросает одну работу, он часто идет работать на конкурента или начинает свое дело в похожей отрасли. Инсайдеры имеют больше доступа к информации, чем когда-либо. И у них гораздо меньше лояльности к своему работодателю…» ***(Исследование: Главная угроза для безопасности компании - это ее сотрудники // IGate (https://igate.com.ua/news/23984-issledovanie-glavnaya-ugroza-dlya-bezopasnosti-kompanii-ehto-ee-sotrudniki). 11.10.2019).***

***

«Ряд больших компаний, отвечающих за домены верхнего уровня и регистраторы доменных имен решили объединить усилия в борьбе против злоупотреблений в Системе доменных имен (DNS), разработав "Структуру борьбы со злоупотреблениями"

Каждая из компаний поделилась своим опытом по работе с нарушающим контентом, а целью этого было создание основополагающего документа для дальнейшего обсуждения в сообществе с участием заинтересованных сторон. В группу, создавшую документ, вошли Public Interest Registry, GoDaddy, Donuts, Tucows, Amazon Registry Services, Inc., Blacknight Solutions, Afilias, Name.com, Amazon Registrar, Inc., Neustar и Nominet UK.

«Компании, которые поучаствовали в создании документа, признают, что здоровье и безопасность DNS имеют важнейшее значение для доверия к Интернету и его безопасности. Также участники признали, что они играют важную, но зачастую неправильно понимаемую роль в качестве распорядителей этого общественного ресурса» — сказал сайту CircleID представитель группы. Группа рассматривает настоящий Документ как первый важный шаг в рамках более широких усилий сообщества по борьбе со злоупотреблениями в DNS…

«Пока проблема злоупотребления в DNS не будет решена, мы осознаем необходимость общего понимания того, как определить эти злоупотребления». Группа совместно определила злоупотребление DNS как пять широких категорий вредоносной активности: «вредоносные программы, бот-сети, фишинг, фарминг и спам (когда он служит механизмом доставки для других форм злоупотреблений в DNS)»…

«Несмотря на то, что у регистраторов и реестров есть только один грубый и непропорциональный инструмент для решения проблемы злоупотребления на

сайте [т.е. отключение всего доменного имени], мы считаем, что существуют настолько вопиющие формы нарушений, что сторона, заключившая договор, должна действовать, обязательно предоставляя конкретное и адекватное уведомление.

Например, даже если решения суда ещё нет, мы считаем, что домен или регистратор должны действовать, чтобы остановить следующие нарушения на веб-сайтах: (1) материалы о сексуальном насилии над детьми; (2) незаконные распространение опиоидов в интернете; (3) торговля людьми; (4) конкретные и правдоподобные призывы к насилию». ***(Ведущие игроки доменной индустрии объединились против киберпреступности // РосКомСвобода (https://roskomsvoboda.org/51065/). 21.10.2019).***

***

«Промышленное оборудование окажется в центре внимания в рамках следующего конкурса Pwn2Own. Впервые исследователям безопасности будет разрешено взламывать программное обеспечение и протоколы на Pwn2Own.

За 12 лет существования основными целями конкурса были браузеры и операционные системы. В последние несколько лет организаторы пополнили список объектов для взлома электрокарами Tesla и «умными» дисплеями Facebook Portal.

По словам организаторов проекта, в нынешнем году появятся пять категорий АСУ: сервер управления, сервер унифицированной архитектуры OPC, DNP3-шлюз, человеко-машинный интерфейс (HMI)/рабочая станция оператора и программное обеспечение Engineering Workstation (EWS).

Участники смогут свободно выбирать, какое из вышеперечисленного оборудования они хотят взломать. За успешное удаленное выполнение кода исследователи могут заработать $20 тыс., за раскрытие информации — $10 тыс., за вызов состояния отказа в обслуживании — $5 тыс. Призовой фонд конкурса составит более $250 тыс.

По словам организаторов, производители будут немедленно предупреждены обо всех уязвимостях, обнаруженных на предстоящем конкурсе Pwn2Own. Следующий Pwn2Own состоится на конференции по безопасности S4 ICS в Майами (США) 21-23 января 2020 года.» ***(На Pwn2Own впервые разрешат взломать промышленное оборудование // SecurityLab.ru (https://www.securitylab.ru/news/502101.php). 28.10.2019).***

***

«У Катовіце триває 5-й Європейський форум з кібербезпеки Cybersec - 2019.

З нагоди 5-го Європейського форуму кібербезпеки в Катовіце повідомлено про плани розширення міжнародної співпраці в сфері захисту даних. Безпека 5-го покоління мобільних мереж – це одна з головних тем цьогорічного Європейського форуму кібербезпеки CYBERSEC 2019 у Катовіце. У конференції беруть участь представники урядів, технологічних компаній, експерти та вчені з країн Європейського Союзу і США, — повідомляє polskieradio.pl

Як вважають організатори заходу, мережа 5G має ключове значення для розвитку держав. Тому, крім питання безпеки, експерти обговорюють вплив цієї технології на всю економіку, – сказав директор у справах просування і стратегічної співпраці в Інституті Костюшка Роберт Сюдак: «Буде запущена мережа 5G. Коли говорити про безпеку Інтернету речей або промисловості 4.0 – наступними роками все, мабуть, спиратиметься на передачу даних цією мережею».

Міністр цифризації Марек Заґурський звернув увагу, що зустріч у Катовіце є нагода обмінятися досвідом: «Так само, як очевидним є, що нам треба дедалі більше забезпечень, пов'язаних із кіберзагрозою, так само певним є те, що жодна держава не захиститься сама. Необхідною є співпраця».

Як додав міністр Марек Заґурський, польський уряд ухвалить Стратегію кібербезпеки на 2019-2024 роки. Цим документом передбачається, зокрема, розширення міжнародної співпраці в сфері захисту даних. 2020 року мережу 5G планується запустити принаймні в одному великому місті, а 2025 вона має бути розширена на всі найбільші агломерації.

Порівняно з дотеперішнім стандартом 4G, мережа 5G гарантує більш стабільний зв'язок, менше запізнення передачі даних та кращу швидкість мобільного Інтернету.» ***(Oksana Nagirna. Польський уряд ухвалить Стратегію кібербезпеки на 2019-2024 роки // Ukraiński informacyjny portal we Wrocławiu (https://inpoland.net.pl/novosti/polskijj-uryad-ukhvalit-strategiyu-kiberbezpeki-na-2019-2024-roki/). 30.10.2019).***

***

«Професор у сфері досліджень війни в королівському коледжі Лондона Лоуренс Фрідман розповів, що сьогодні кібератаки можуть бути як нападами дрібних хакерів, так і спробами цифрового штурму енергосистем та урядів країн.

Професор не виключив, що у майбутньому світ може побачити кібератаку, яку він назвав електронний Перл-Гарбор.

Фрідман вважає, що використовувати кібератаки особливо полюбляє Росія, оскільки продовжує сповідувати підхід командування.

– Це їхня культурна особливість та менталітет, але для цього у неї занадто слабкий фундамент. ВВП Росії – майже як ВВП Іспанії, у них серйозні проблеми з інфраструктурою, корупцією, тому цілком природно, що у намірах розширити джерела влади вона звернулася до кібервійни та інформаційних воєн, – сказав профессор…» ***(Світ чекає електронний Перл-Гарбор – професор про загрозу кібератак // ФАКТИ. ICTV (https://fakty.com.ua/ua/svit/20191031-svit-chekaye-elektronnyj-perl-garbor-profesor-pro-zagrozu-kiberatak/). 31.10.2019).***

***

«Адвокат президента США Дональда Трампа Рудольф Джуліані знайшов докази втручання України у вибори глави США 2016 року, про які заявляв ще у вересні. Джуліані опублікував фото доказів у мережі.

Відповідний допис з'явився на сторінці адвоката у соціальній мережі Twitter.

Так, Джуліані заявив про можливу змову між посадовими особами України й штабом передвиборної кампанії Хілларі Клінтон у 2016 році. Джуліані також оприлюднив електронне листування між представниками Національного комітету Демократичної партії США.

Джуліані показав листування між Алі Калупа (консультант DNC) і Луїсом Міранда (директором з комунікацій DNC) від 3 травня 2016 року, в якій вони обговорюють делегацію з 68 українських журналістів-розслідувачів, які приїхали в США на форум Open World Society.

Один з представників DNC повідомив, що познайомив журналістів з Майклом Ісикоффим, ймовірно, у справі Пола Манафорта (на той час голова передвиборчого штабу Дональда Трампа).

Зазначимо, що Джуліані отримав цю переписку з відкритої бази Wikileaks, документів, що були отримані завдяки кібератаці на сервери Демократичної партії США…» ***(Джуліані показав можливі докази втручання України у президентські вибори у США: фото // Znaj.ua (https://znaj.ua/politics/269199-dzhuliani-pokazav-mozhlivi-dokazi-vtruchannya-ukrayini-u-prezidentski-vibori-u-ssha-foto). 11.10.2019).***

***

«Подразделение кибербезопасности Министерства внутренней безопасности США требует внести в действующее законодательство поправки, которые дали бы ему право запрашивать у интернет-провайдеров информацию, позволяющую выявлять пользователей уязвимых систем.

Созданное менее года назад Агентство кибербезопасности и охраны инфраструктуры (Cybersecurity and Infrastructure Security Agency, CISA) хочет получить право на законных основаниях запрашивать у интернет-провайдеров контактную информацию владельцев уязвимых устройств и систем.

CISA, в чьи обязанности входит предупреждение правительственных и коммерческих организаций об уязвимостях, жалуется на отсутствие возможности уведомлять коммерческие компании о проблемах с безопасностью, поскольку выявить владельца проблемной системы можно далеко не всегда. Новые полномочия позволили бы CISA предупреждать об угрозах непосредственно владельцев уязвимых критических устройств (например, промышленных систем управления), пишет TechCrunch.

Согласно действующему законодательству США, интернет-провайдеры должны предоставлять доступ к данным абонентов только при наличии ордера, который может быть выдан федеральным органом даже без решения суда. CISA не имеет права выдавать ордеры на получение данных и поэтому вынуждено обращаться за ними к партнерским федеральным органам. Однако и здесь есть загвоздка, поскольку федеральные органы могут запрашивать данные только в

случае проведения уголовного расследования. Проблема заключается в том, что CISA должна предупреждать владельцев уязвимых систем, не зависимо от того, ведется ли расследование.» ***(Агентство кибербезопасности США требует права на получение данных абонентов у интернет-провайдеров // SecurityLab.ru (https://www.securitylab.ru/news/501697.php). 10.10.2019).***

***

«Співробітникам відділів Білого дому, що відповідають за IT та кібербезпеку, доручили активно виявляти і розслідувати витоки інформації. Про це повідомляє в п'ятницю новинний портал Axios в розпорядженні якого опинився внутрішній циркуляр…

"(Співробітники повинні) проводити захисні контрзаходи, відстежувати в цілодобовому режимі мережу і електронну пошту, активно ідентифікувати і розслідувати витоки такої чутливої інформації, як пересування і графік президента, що безпосередньо впливає на фізичну безпеку", — йдеться в документі від 1 червня. Крім того, в обов'язки відповідних відділів входить проведення для представників американського керівництва інструктажу про технічну обстановці в зарубіжних поїздках.

Двоє колишніх та один діючий співробітник відповідних підрозділів Білого дому розповіли виданню, що в їх завдання входило перегляд історії в браузерах працівників, те, які використовувалися програми, та чи дозволяють вони ідентифікувати тих, хто відкривав службові документи, зокрема графік президента. За відомостями видання, якщо раніше документи по електронній пошті приходили в форматі pdf, то тепер застосовується програма Microsoft Sharepoint, що надає відправнику можливість виявити тих, хто ознайомився з інформацією.

Джерела порталу вважають, що таким чином президент США Дональд Трамп намагається позбутися від персоналу, найнятого ще адміністрацією Барака Обами. Білий дім не став коментувати публікацію…» ***(Ілля Нежигай. Співробітникам IT-відділу Білого дому доручили активно виявляти витоки інформації // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1832170-spivrobitnikam-it-viddilu-bilogo-domu-doruchili-aktivno-viyavlyati-vitoki-informatsiyi). 26.10.2019).***

***

«Министерство внутренних дел США, контролирующее федеральное управление земельными ресурсами, приняло решение приостановить использование своего флота беспилотников, насчитывающий более 800 летательных аппаратов, из-за опасений шпионажа со стороны Китая и кибератак с помощью данных устройств.

Как сообщает издание The Wall Street Journal, каждый беспилотник, используемый МВД, произведен в Китае или оснащен комплектующими китайского производства. По словам министра внутренних дел Дэвида Бернхардта (David Bernhardt), дроны будут оставаться на земле, пока ведомство не завершит анализ угроз безопасности, которые они могут представлять.

«Министр Бернхардт пересматривает программу беспилотников Министерства внутренних дел. До тех пор, пока проверка не будет завершена,

министр запретил использовать дроны, изготовленные в Китае или произведенные из китайских компонентов, если они в настоящее время не используются в чрезвычайных ситуациях, таких как борьба с лесными пожарами, поиск и спасение пропавших, а также борьба со стихийными бедствиями, которые могут угрожать жизни или собственности», — сообщила пресс-секретарь МВД США Мелисса Браун (Melissa Brown).

Многие из дронов в настоящее время используются ведомством для борьбы с лесными пожарами, мониторинга плотин и наводнений, осмотра земель на предмет имущественного и экологического ущерба в результате эрозии и мониторинга исчезающих видов флоры и фауны. Власти опасаются, что беспилотники могут использоваться для передачи данных, включая фотографии и видео, о критической инфраструктуре страны, ставя ее под угрозу потенциальных кибератак.» ***(МВД США проверяет свои беспилотники из-за риска шпионажа со стороны Китая // SecurityLab.ru (https://www.securitylab.ru/news/502226.php). 31.10.2019).***

***

«Правительство США своими действиями ставит себя под угрозу взлома. Об этом сообщается во внутренней служебной записке, разосланной старшим директором по кибербезопасности Белого Дома Димитриосом Вастакисом (Dimitrios Vastakis).

Служебная записка, датированная 17 октября нынешнего года, вчера была опубликована на портале Axios…

По словам Вастакиса, принятое в июле решение о превращении Кабинета старшего директора по информационной безопасности (Office of the Chief Information Security Officer, OCISO) в Кабинет старшего директора по информации (Office of the Chief Information Officer, OCIO) «вызывает тревогу».

«Это значительный сдвиг в приоритетах высшего руководства, когда деловые операции и качество обслуживания ставится выше, чем безопасность президентской сети. У меня, как у специалиста по кибербезопасности, это вызывает тревогу», - сообщил Вастакис в служебной записке.

Документ был разослан после того, как десяток специалистов по кибербезопасности подали в отставку или были уволены из проекта, запущенного в 2014 году во времена Барака Обамы на волне взломов правительственных компьютеров. Целью проекта была защита систем Белого Дома от кибератак со стороны враждебных государств.

«Говорят, история повторяется. К сожалению, с учетом всего наблюдаемого мною в течение последних трех месяцев, я прогнозирую, что Белый Дом снова ставит себя под угрозу электронной компрометации», - подытожил Вастакис.

Помимо прочего, Вастакис сообщил в записке о решении подать в отставку. В качестве главной причины увольнения он назвал «основную тактику» нового руководства, которое «обычно враждебно относится к действующему персоналу OCISO». ***(Белый Дом США сам ставит себя под угрозу взлома // SecurityLab.ru (https://www.securitylab.ru/news/502015.php). 24.10.2019).***

***

«Євродепутати вважають за необхідне створити міжнародні правові рамки для надійного протистояння гібридним загрозам, включаючи кібератаки і дезінформацію.

Відповідну резолюцію Європарламент ухвалив 10 жовтня…

У документі депутати звернули увагу на «надзвичайно небезпечну природу російської пропаганди» і закликали Єврокомісію розробити «ефективну стратегію оперативного і надійного протидії російської дезінформації».

За резолюцію проголосували 469 євродепутатів, проти були 143, утрималися 47 парламентаріїв.

У Європарламенті стурбовані спробами вплинути на хід і результат виборів в країнах ЄС та сусідніх державах. Балканські країни, а також учасниці програми «Східне партнерство», зокрема, Грузія і Україна, як відзначається в резолюції, також стають об'єктами підриву «нормативних засад, принципів європейської демократії і суверенітету».

Таким країнам, вважає Європарламент, ЄС повинен надати конкретну допомогу: наприклад, підтримати незалежні засоби масової інформації.

У прийнятій резолюції Росію в черговий раз назвали «основним джерелом» дезінформації в Європі, але додали, що «підривне втручання» в суспільно-політичне життя країн ЄС здійснюють не тільки російські державні і недержавні організації. Так, у спробах послабити ЄС євродепутати також звинуватили Китай, Іран і Північну Корею.

На думку євродепутата Паскаля Дюрана з фракції «Оновити Європу», гроші, які виділяє ЄС на боротьбу з дезінформацією, мізерні в порівнянні з сумами, які витрачають інші країни на підривну діяльність в ЄС. Так, за його оцінками, одна тільки Росія виділила близько мільярда євро на пропагандистські кампанії у Франції та Італії. При цьому створена в ЄС робоча група зі стратегічних комунікацій (StratCom) для протидії пропаганді має бюджет всього в три мільйони євро на рік…» ***(Європарламент закликає створити ефективну стратегію протидії російській дезінформації // ДЕТЕКТОР МЕДІА (https://detector.media/infospace/article/171532/2019-10-13-evroparlament-zaklikae-stvoriti-efektivnu-strategiyu-protidii-rosiiskii-dezinformatsii/). 13.10.2019).***

***

«…Европейский месяц кибернетической безопасности является частью более широких усилий для развития и сохранения навыков людей в этой сфере, в исполнении долгосрочных превентивных мер и, таким образом - для создания безопасного Единого информационного рынка», - сказала еврокомиссар по вопросам цифровой экономики и общества Мария Габриэль.

Месяц кибербезопасности посвятят развитию базовых навыков предостережения, которые должны стать частью повседневного поведения каждого человека при контактах с высокотехнологичными устройствами.

"Развитие доверия, знаний, осведомленности и устойчивости являются решающими факторами, которые позволяют защититься от кибернетических угроз,

которые быстро меняются", - добавила Габриэль.» ***(Октябрь будет месяцем кибернетической безопасности // Gazeta.ua (https://gazeta.ua/ru/articles/science/_oktyabr-budet-mesyacem-kiberneticheskoj-bezopasnosti/930795). 01.10.2019).***

***

Китай

«…Жителей Китая обяжут сканировать лицо при покупке SIM-карт…

С первого декабря 2019 года, мобильные операторы Китая будут обязаны сканировать лица граждан при покупке SIM-карт. Соответствующее решение приняло Министерство промышленности и информационных технологий Китая.

В ведомстве заявили, что этот шаг должен «защитить законные права граждан в киберпространстве». Также пользователям смартфонов хотят запретить передавать свои номера мобильных другим пользователям…» ***(Евгений Радченко. Китайцев обяжут сканировать лицо при покупке SIM-карт // Независимый Регион (https://nr2.com.ua/tehnologii/2019/10/05/kitaicev-obiajyt-skanirovat-lico-pri-pokypke-sim-kart/). 05.10.2019).***

***

«Широко рекламируемое с января текущего года властями КНР приложение Xuexi Qiangguo («Изучай великую нацию»)… непосредственно пропагандирует «Мысль Си Цзиньпина» — теорию лидера компартии Китая о месте страны в мире и о её будущем. Правда, исследование немецкой фирмы по кибербезопасности «Cure53» показало, что, помимо обучающей функции, приложение следит за пользователями.

Для этого существуют бэкдоры, специально оставленные разработчиками, чтобы другие приложения могли легко видеть данные, которые хранит «Изучай великую нацию”. Исследователи отмечают, что если на смартфоне есть ещё одно государственное приложение кроме названного, оно может легко воровать данные у «Xuexi Qiangguo» и отправлять их куда следует. Среди данных — мультимедиа, сообщения, контакты и история поиска.

Но удивительным нюансом стало то, что приложение после установки получает права суперпользователя на смартфоне и может не только следить за местоположением, но ещё записывать и даже совершать звонки от имени пользователя. Приложение получает root-права без каких-либо запросов, благодаря оставленным бэкдорам, а пользователь даже не подозревает, на какие операции оно способно.

По данным исследователей, приложение «Изучай великую нацию» имеет права суперпользователя на 100 миллионах устройств. В настоящее время оно является самым загружаемым в Китае приложением в App Store, превосходя такие социальные сервисы, как WeChat и TikTok.» ***(Самое популярное приложение в Китае шпионит за гражданами // РосКомСвобода (https://roskomsvoboda.org/50812/). 14.10.2019).***

***

«Исследователи из компании Crowdstrike рассказали об одной из крупных киберпреступных операций, в которую были вовлечены сотрудники Министерства государственной безопасности Китая, хакеры и исследователи безопасности, а также сотрудники компаний по всему миру.

Целью данной операции было заполучить интеллектуальную собственность для сокращения технологического разрыва Китая в авиационной промышленности, и помочь китайскому государственному авиационно-космическому производителю Comac построить собственный авиалайнер — самолет C919 для конкуренции с такими компаниями, как Airbus и Boeing. Скоординированная многолетняя вредоносная кампания систематически атаковала иностранные компании, поставляющие компоненты для самолета C919. Как утверждают исследователи, конечная цель заключалась в заполучении интеллектуальной собственности, необходимой для производства всех компонентов C919 внутри Китая.

По словам исследователей, Министерство государственной безопасности КНР поручило Бюро Цзянсу осуществить данные атаки, а оно, в свою очередь, поручило двум ведущим сотрудникам координировать процесс. Один отвечал за киберпреступную команду, в то время как другой нанимал инсайдеров, работающих в авиационных и аэрокосмических компаниях.

В период с 2010 по 2015 год злоумышленники атаковали разные компании и взломали системы таких поставщиков для C919, как Ametek, Honeywell, Safran, Capstone Turbine, GE и пр.

Согласно обвинительному заключению Министерства юстиции США, ответственными за совершение атак были киберпреступники, которых вербовало Бюро Цзянсу. Им было поручено взломать целевые сети, где они обычно развертывали вредоносные программы, такие как Sakula, PlugX и Winnti, и использовать их для поиска конфиденциальной информации и ее передачи на удаленные серверы. В тех редких случаях, когда преступники не могли взломать сеть, второй сотрудник Бюро Цзянсу нанимал гражданина Китая, работающего на целевую компанию, и использовал его для установки Sakula в сети жертвы, обычно через USB-носители.

Киберпреступная группировка, получившая название Turbine Panda, совершила ошибку, когда атаковала таких крупных поставщиков, как Anthem и Управление кадровой службы США. Атаки привлекли внимание правительства США, позволив обнаружить вредоносную кампанию. Первыми были рассекречены инсайдеры, поскольку они не имели защиты от правительства Китая. Далее был обнаружен создатель вредоносного ПО Sakula по имени Ю, который вскоре был арестован во время участия в конференции по безопасности в Лос-Анджелесе.

Исследователи предполагают, что атаки на иностранные авиационные фирмы будут продолжаться в будущем, поскольку самолет Comac C919 не является тем результатом, которого ожидало китайское правительство. В настоящее время предпринимаются усилия по созданию модели C929.» ***(К производству китайского самолета C919 были привлечены киберпреступники // SecurityLab.ru (https://www.securitylab.ru/news/501766.php). 15.10.2019).***

***

«Российские военные провели тестирование специальных программ для защиты каналов связи АСУ «Акация», «Андромеда» и ЕСУ-ТЗ. Разработанное антивирусное ПО будет отслеживать несанкционированный доступ вредоносов, обнаруживать место вторжения и выявлять посторонние файлы. Также оно предупреждает оператора о кибератаке и предлагает несколько вариантов перенастройки сети и пути решения проблемы.

Оборудование АСУ состоит из сервера с собственным ПО, защищенных ноутбуков, шифрующих устройств и средств связи. Для передачи информации в основном используются спутниковые каналы и каналы радиосвязи. Хотя современные АСУ, как правило, физически не связаны с интернетом, злоумышленник может внедриться в них, взломав каналы передачи информации.

«Ретранслируемый сигнал может быть перехвачен. Поэтому его нужно защищать. Наиболее уязвимыми являются Wi-Fi-сигналы, которые также используются военными. Для проникновения в них достаточно взломать пароль. Правда, чтобы перехватить такой сигнал, к передатчику нужно максимально близко подобраться — примерно на 50 м. В то же время в сигналы радиосвязи можно внедриться с помощью электронных средств, которые устанавливаются на разведывательных самолетах», — отметил военный эксперт Дмитрий Болтенков.

Первые испытания армейского антивируса успешно прошли в ходе учений «Центр-2019». Разработки позволяют не только обеспечивать безопасность софта, но и обнаруживают место вторжения в программное обеспечение, находят повреждённые фалы, а также предлагают несколько вариантов решения проблемы, включая возможности перенастройки сети для защиты от атак извне.

АСУ позволяют организовать взаимодействие войск, командных пунктов, штабов, тыловых подразделений. Система обеспечивает передачу необходимой для управления войсками информации в реальном времени.» ***(Армейский антивирус для защиты каналов связи // РосКомСвобода (https://roskomsvoboda.org/51565/). 31.10.2019).***

***

«Зарубежные спецслужбы ведут работу по выявлению слабых мест в информационной системе России, чтобы совершать массированные кибератаки, заявил секретарь Совета безопасности Николай Патрушев на совещании в Омске:

«Основными целями для оказания вредоносного воздействия остаются объекты критической информационной инфраструктуры <…>, что создает реальные угрозы национальной безопасности».

Иностранные спецслужбы выискивают уязвимости в информационной инфраструктуре России для совершения массовых кибератак — Патрушев

Он отметил, что во всех регионах Сибири «организовано подключение информационных ресурсов органов государственной власти к российскому государственному сегменту сети Интернет, при этом сам российский

государственный сегмент в силу своей ориентированности на государственный сектор является привлекательной целью для компьютерных атак и деструктивных воздействий».

«Уже в этом году <…> зафиксировано более 1,7 млн вредоносных воздействий на информационные ресурсы органов власти субъектов Федерации Сибирского федерального округа. По плотности вредоносных компьютерных воздействий округ занимает третье место в стране», — заметил Патрушев.

«Несмотря на то что в целом необходимые условия <…> созданы, количество нарушений требований безопасности информации остается значительным. <…> Прежде всего это относится к таким важным сферам, как транспорт, связь и энергетика», — пояснил он. По мнению секретаря Совбеза, в этих областях, в частности, недостаточно эффективно идет переход на отечественное программное обеспечение.» ***(Патрушев: иностранные спецслужбы намерены ударить по IT-уязвимостям РФ // РосКомСвобода (https://roskomsvoboda.org/51319/). 25.10.2019).***

***

Інші країни

«Администрация ресторанов и других мест общественного пользования с бесплатным доступом к Wi-Fi должна хранить данные об активности пользователей в Сети в течение 90 дней. Как пояснил министр цифровой экономики Таиланда Буддхипонгсэ Пуннаканта, это необходимо на случай, если данные понадобятся для проведения уголовного расследования.

«Магазины и кафе с бесплатным Wi-Fi должны хранить информацию в течение 90 дней, для того чтобы при необходимости правоохранительные органы могли запросить ее в рамках статьи 26-й Закона о компьютерных преступлениях», - приводит слова министра тайское издание Khao Sod.

Буддхипонгсэ Пуннаканта упомянул раздел недавно обновленного закона о киберпреступлениях, обязывающего интернет-провайдеров хранить трафик своих пользователей. Кафе, рестораны и магазины, нарушающие требование законодательства, понесут наказание, отметил министр.» ***(Власти Таиланда обязали кафе с бесплатным Wi-Fi хранить данные пользователей // SecurityLab.ru (https://www.securitylab.ru/news/501674.php). 09.10.2019).***

***

«Юридические и дипломатические органы Ирана готовятся подать в суд на США за кибератаки. Руководитель Организации гражданской обороны Ирана генерал Голам Реза Джалали сообщил, что США создали киберугрозы и неоднократно осуществляли атаки на Иран. По его словам, Штаты понесут юридическую ответственность за свои действия, и судебные органы Ирана совместно с Министерством иностранных дел уже занимаются этим вопросом.

Как сообщает издание Tasnim, Организация гражданской обороны Ирана предприняла целый ряд шагов по укреплению возможностей Ирана в области

кибероборонны. К примеру, за последние шесть месяцев было проведено более 120 учений, и 70% из них были направлены на разработку тактик обороны против кибератак на критическую инфраструктуру…» ***(Иран подаст в суд на США за кибератаки // SecurityLab.ru (https://www.securitylab.ru/news/501604.php). 07.10.2019).***

***

«Когда правительства всё большего числа стран размышляют о рисках работы с зарубежными поставщиками сетей 5G, все взгляды прикованы к Швейцарии, которая одной из первых приняла на вооружение эту технологию. Займёт ли она более жёсткую позицию, наложив ограничения на участие в цепочке поставок 5G таких иностранных поставщиков, как Huawei, или отдаст решение этого вопроса на волю рынка?

Согласно мрачному, но не слишком надуманному сценарию, хакер может атаковать антенну 5G, отправив вредоносные сигналы миллионам подключённых к ней устройств. Это приведёт к коллапсу в работе транспортной системы и энергосистемы и парализует города. Ситуация быстро распространится на сети других стран, вызывая масштабную атаку на глобальную сеть Интернет.

Этот сценарий показывает, что при всех преимуществах, которые может обеспечить возможность тотального подключения в сетях 5G, с использованием этой технологии также обостряются проблемы безопасности. Обнародованная на прошлой неделе оценка риска кибербезопасности 5G во всех странах ЕС подтвердила это, показав, что зависимость критически важных услуг от сетей 5G означает, что масштабный сбой в их работе может иметь особо тяжкие последствия.

«Любые технологические изменения несут в себе и новые возможности, и новые риски», - говорит Флориан Эглофф (Florian Egloff), старший научный сотрудник Центра изучения проблем безопасности при Швейцарской высшей технической школе Цюриха (ETH Zürich).

Поскольку ни одна швейцарская компания не имеет достаточных средств для обеспечения инфраструктуры, необходимой для сети 5G, страна, по его словам, «должна полагаться «на иностранных поставщиков технологий, если хочет внедрить технологию 5G»…

В случае с 5G тем иностранным провайдером, который способен за разумную цену производить все элементы сети 5G «в нужном объёме и необходимого качества», оказался китайский телекоммуникационный гигант Huawei.

Данный факт вызвал в других странах опасения, что китайское правительство будет использовать это обстоятельство для кибершпионажа, и в итоге были приняты различные правительственные меры - от прямых запретов со стороны США и Австралии до внесения предложений о новых протоколах безопасности в Европейском союзе.

Эти соображения нашли отклик и в Швейцарии. В начале 2019 года несколько швейцарских политиков выступили с предостережениями о рисках работы с Huawei.

Швейцария развернула сотни антенн 5G, что делает её одним из мировых пионеров в использовании этой технологии.

Всем трём крупнейшим швейцарским операторам связи - Salt, Sunrise и Swisscom – выдано разрешение на размещение антенн 5G по всей Конфедерации, и все они используют оборудование Huawei в своих сетях стационарной и мобильной связи. Sunrise также заключила контракт с Huawei на предоставление лицензионных технологий для сети 5G.

Швейцарское правительство заявляет, что относится к проблемам безопасности очень серьёзно, однако признает, что его руки отчасти связаны.

Представитель Федерального ведомства связи (Bundesamt für Kommunikation - BAKOM) сообщил swissinfo.ch, что «в соответствии с существующей правовой базой правительство не может влиять на то, каких поставщиков оборудования выбирают операторы сетей»…

Итак, кто же несёт ответственность за обеспечение безопасности 5G? Хотя национальная безопасность и входит в компетенцию правительства, законодательство не всегда идёт в ногу с быстрыми изменениями в мире технологий.

Например, пересмотренный швейцарский «Закон о телекоммуникациях» включает специальную статью о кибербезопасности, призывающую компании бороться с любыми несанкционированными манипуляциями с их телекоммуникационным оборудованием.

Однако ни в этом законе, ни в последней редакции «Закона о защите данных» не упоминаются потенциальные угрозы, таящиеся в контрактах с зарубежными поставщиками программного или аппаратного обеспечения.

«Федеральный "Закон о телекоммуникациях" был разработан на том этапе, когда вопроса об использовании иностранных провайдеров ещё не было в повестке дня», - говорит Флориан Рот (Florian Roth), адвокат, специализирующийся в области телекоммуникационного права в цюрихской фирме Walder Wyss.

Существует также ряд не имеющих обязательную юридическую силу рекомендаций по безопасности, которые были составлены ещё в 2009 году.

По словам Рота, новая швейцарская стратегия в области кибербезопасности остаётся довольно расплывчатой, и частные компании вынуждены сами решать, какие меры принять, поскольку в самой стратегии они пока чётко не определены.

Рот отмечает, что такой подход типичен для швейцарских регулирующих органов. «Это очень прагматично. Регуляторы зачастую передоверяют участникам рынка принятие решений о том, какие меры являются адекватными», что возлагает большую ответственность за целостность сети на операторов связи.

В настоящее время для таких компаний не существует связывающих их юридическими обязательствами правил, касающихся использования оборудования иностранных поставщиков. Они также не имеют налагаемой законом обязанности сообщать о нарушениях системы безопасности, если такие нарушения не приводят к серьёзным сбоям в оказании услуг или в работе сети.

Ситуация может измениться с реализацией пересмотренного швейцарского «Закона о защите данных», но не ясно, когда он вступит в силу.

Как Swisscom, так и Sunrise сообщили swissinfo.ch, что они проводят оценку рисков поставщиков, а также регулярно отслеживают потенциальные угрозы и сообщают о них правительству.

Крупнейший швейцарский оператор связи Swisscom, контрольный пакет акций которого принадлежит государству, также заявил, что у него во всех контрактах и со всеми поставщиками есть положения о выходе из сделки. Условия сотрудничества также включают временные рамки, которые обычно пересматриваются и повторно определяются в процессе тендера через каждые 5-10 лет. Компания также регулярно публикует отчёты о состоянии кибербезопасности…

Однако эксперты по кибербезопасности говорят, что этих мер может быть недостаточно. Один большой вопрос связан с так называемыми «чёрными ходами» (бэкдорами) или скрытыми точками удалённого доступа, которые можно использовать для получения контроля над устройством.

В отчёте ЕС говорится, что, поскольку сети 5G будут в значительной степени основаны на программном обеспечении, существенные дефекты защиты могут упростить для хакеров злонамеренное включение бэкдоров в программы и затруднить их обнаружение.

Согласно приложению к статье «Закона о телекоммуникациях» о кибербезопасности, правительство не решается призвать поставщиков телекоммуникационных услуг проверять физический доступ и бэкдоры в аппаратном и программном обеспечении.

Представитель BAKOM сказал swissinfo.ch, что это условие было опущено в основном из-за сомнений в его осуществимости, поскольку его выполнение «зачастую невозможно для телекоммуникационных компаний, так как компьютер клиента находится у него дома или в каком-то другом месте»…

Реальность того, что инфраструктура 5G будет зависеть от иностранных поставщиков, вынуждает страны мира принимать превентивные меры. В то время как США и Австралия пошли дальше всех, занеся Huawei в чёрный список, ЕС обдумывает другие тактики, чтобы нивелировать потенциальные риски, не портя отношения с конкретными поставщиками.

Великобритания призвала операторов работать с поставщиками оборудования и технологий над проверкой надёжности и расширять контроль над некоторыми поставщиками с высоким уровнем риска. Франция обсуждает предложение, согласно которому операторы связи должны будут получать официальное разрешение премьер-министра на свои проекты сетей 5G.

Отдельные операторы при подписании контрактов с Huawei также ведут себя довольно осторожно. Норвежский телекоммуникационный провайдер Telia только что объявил, что для развёртывания сетей 5G выбрал Ericsson вместо Huawei. Правительство поспешно заявило, что не давало компании приказа отклонить предложение Huawei.

Компания Huawei неоднократно заявляла, что она скорее закроется, чем станет шпионить по заказу китайского правительства, предложив заключить «Соглашение о запрете шпионажа» правительствам нескольких стран. Например, недавно такое предложение было сделано Польше.

Ожидается, что ЕС также согласует меры по смягчению рисков кибербезопасности к концу этого года…

На данный момент швейцарское правительство, похоже, использует выжидательный подход, следя за тем, что первым сделает Евросоюз.

По словам Флориана Рота, при рассмотрении вопроса об ужесточении мер по контролю над кибербезопасностью в этом секторе регулирующие органы также должны взвесить защиту конфиденциальности личных данных и конкуренцию на рынке. Существует также проблема налаживания отношений с Китаем - одним из важнейших торговых партнёров Швейцарии.

В целом, по мнению Флориана Эглоффа из ETH Zürich, правительство Швейцарии достаточно серьёзно относится к опасениям в отношении безопасности каналов поставок.

В последнем отчёте о кибербезопасности, опубликованном в апреле этого года, отмечается, что в стране идёт общая дискуссия о том, как выбраться из положения «зависимости от двух фактических технологических гигантов - США и Китая». Правительство также объявило о создании профессионального рабочего центра по вопросам кибербезопасности.

Но проблемы на самом деле огромны как со стратегической, так и с технической точки зрения. Исследование, проведённое Центром исследований проблем безопасности при ETH Zürich, показало, что по-прежнему сохраняется двусмысленность в деталях отношений с частным сектором и у компаний нет стимулов для того, чтобы заниматься вопросами национальной безопасности…» ***(Джессика Дэвис Плюсс (Jessica Davis Plüss), Джи Гуо Цендер (Jie Guo Zehnder). 5G тестирует пределы кибербезопасности в Швейцарии // SWI swissinfo.ch (http://www.swissinfo.ch/rus/%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C_5g-%D1%82%D0%B5%D1%81%D1%82%D0%B8%D1%80%D1%83%D0%B5%D1%82-%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D1%8B-%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D0%B8-%D0%B2-%D1%88%D0%B2%D0%B5%D0%B9%D1%86%D0%B0%D1%80%D0%B8%D0%B8/45302906?utm_source=multiple&utm_campaign=swi-rss&utm_medium=rss&utm_content=o). 18.10.2019).***

***

«Норвежская нефтегазовая и металлургическая компания Norsk Hydro в третьем квартале подтвердила $3,6 млн страхового возмещения как частичную компенсацию убытков вследствие кибератаки в марте 2019 года.

Согласно пресс-релизу Norsk Hydro, компания имеет надежную систему киберстрахования с признанными страховщиками, и объемы дальнейшей компенсации застрахованных убытков будут после «подтверждения их достоверности».

Ранее интернет ресурс УкрСтрахование сообщал, что Norsk Hydro 19 марта приостановила часть своего производства и перешла на ручное управление после блокировки хакерами основных систем компании. Тогда в компании отказалась платить хакерам выкуп в обмен на разблокировку систем.

Вследствие инцидента первоначальный ущерб Norsk Hydro оценивался в $40 млн, затем эта сумма несколько раз пересматривалась, увеличившись сначала до $52 млн, а после – до $69 млн.

В пресс-релизе от 23 октября говорится: «Финансовые последствия кибератаки оцениваются в 550-650 миллионов норвежских крон ($60-71 млн) в первом полугодии с ограниченным финансовым эффектом в третьем квартале». ***(Norsk Hydro получила частичное страховое возмещение после массивной кибератаки // УкрСтрахование (https://www.ukrstrahovanie.com.ua/news/norsk-hydro-poluchila-chastichnoe-strahovoe-vozmeshhenie-posle-massivnoj-kiberataki). 23.10.2019).***

***

Протидія зовнішній кібернетичній агресії

«…"Для ситуации киберконфликта не существует общепринятого понимания и оценки его масштабов и того, каким образом его можно связать с традиционными военными операциями", - пишет в колонке "Can Cyberwarfare Be Regulated?" политолог Джозеф Най, бывший председатель Национального совета разведслужб США. "Кибероперации, которые одна сторона считает допустимой игрой, другая сторона может воспринимать совсем иначе." По мнению эксперта, такое положение может привести к неуправляемому раскручиванию спирали конфликта, если он возникнет.

Най напоминает, что десять лет назад Соединенные Штаты использовали вместо бомб киберсаботаж для уничтожения иранских объектов для обогащения ядерного топлива. Иран ответил кибератаками, которые уничтожили 30 тысяч компьютеров Saudi Aramco и нарушили работу американских банков. Этим летом, после введения санкций со стороны администрации Дональда Трампа, Иран сбил американский беспилотник. Жертв не было. Первоначально Трамп планировал в ответ нанести ракетный удар, но в последний момент передумал в пользу кибератаки, которая уничтожила ключевую базу данных, используемую иранскими военными для наведения на нефтяные танкеры. И снова - были затраты, но не жертвы. Затем Иран (сам или через своих ставленников) нанес удар по двум крупным саудовским нефтеперабатывающим заводам, используя более совершенные дроны и крылатые ракеты. Несмотря на то, что, судя по всему, жертв не было (или они были незначительны), эта атака привела к значительно более серьезному ущербу и рискам.

Проблема понимания уровней эскалации и контроля за ней не нова, пишет эксперт далее. В августе 1914 года крупные европейские державы были настроены на быструю и убедительную “третью балканскую войну”. Войска, о общему убеждению, должны были вернуться домой к Рождеству. После убийства австрийского эрцгерцога в июне, Австро-Венгрия намеревалась нанести решающий удар по Сербии, а Германия предоставила своему австрийскому союзнику свободу действий, вместо того, чтобы его сдерживать…

У кибертехнологий, безусловно, отсутствуют прямые поражающие факторы ядерного оружия, и это создает своеобразные проблемы, поскольку для киберугроз пока отсутствет "хрустальный шар". Во время "холодной войны" великие державы избегали прямых столкновений, но к нынешним киберконфликтам, замечает Най, эта сдержанность не относится - во многом из-за того, что до угрозы "кибер-Перл-Харбора" еще очень далеко. Большинство киберконфликтов проходят ниже порога, установленного правилами вооруженного конфликта. Их факторы скорее экономические и политические, нежели летальные. Поэтому невозможно представить, что кто-то станет угрожать ядерным ударом в ответ на взлом для кражи интеллектуальной собственности в пользу Китая или кибервмешательство в выборы со стороны России.

Согласно действующей американской доктрине, сдерживание не ограничивается киберответом (хотя он и возможен). США готовы отвечать на кибератаки на ее домены или промышленные сектора любым оружием по своему выбору пропорционально нанесенному ущербу. Ответ может варьироваться от раскрытия личных данных соучастников атаки до экономических санкций и применения кинетического оружия. В начале этого года новая доктрина “постоянного присутствия” была описана в терминах не только атаки для причинения ущерба, но и содействия и усиления сдерживания. Однако техническая сходность вторжения в сети для сбора разведданных и проведения сетевых наступательных операций часто стирает различие между эскалацией и деэскалацией. Вместо того, чтобы полагаться на "молчаливый паритет", как иногда именую такую ситуацию сторонники “постоянного присутствия”, для ограничения эскалации может потребоваться и прямая коммуникация.

В конце концов, мы не можем сказать, что мы накопили достаточный опыт для того, чтобы понять, что такое "допустимое противостояние" в киберпространстве, или что мы можем быть уверены, как будут толковаться действия, предпринимаемые в сетях других стран, пишет эксперт. Например, российское кибервмешательство в американские выборы не было "допустимым противостоянием". В таким новом пространстве стратегий, как киберпространство, прямая коммуникация (вместо "молчаливого паритета") может расширить нынешнее узкое понимание границ допустимого.

Най отмечает, что если переговоры по заключению договоров о контроле над кибероружием пока проблематичны, то инструменты дипломатии в этой сфере вполне применимы. В киберпространстве разница между оружием и не-оружием может сводиться к одной строке кода, а одна и та же программа может использоваться для законных или злонамеренных целей в зависимости от намерений пользователя. Но если это делает невозможным привычный для традиционных договоров контроль над вооружениями, все же остается возможность установить ограничения если не на кибероружие, то на определенные типы гражданских целей, и договориться о строгих правилах поведения, ограничивающих конфликт.

В любом случае, считает эксперт, поддерживать стратегическую стабильность в киберпространстве будет сложно. Поскольку в информационной отрасли технологические инновации внедряются быстрее, чем в ядерной сфере,

кибервойна характеризуется повышенной непредсказуемостью, которая порождает взаимное недоверие.

Най ожидает, что со временем более высокая компетентность судебных экспертиз при расследовании киберпреступлений может сделать наказания за кибератаки более неотвратимыми, а совершенствование систем защиты при помощи шифрования или машинного обучения может повысить эффективность кибероборонных систем. Более того: по мере того, как государства и организации начинают лучше понимать границы и угрозы кибератак и растущее значение интернета для их собственного экономического благополучия, расчеты "рентабельности" кибервойн могут измениться.

Однако на нынешнем этапе, подводит итог профессор Най, ключом к сдерживанию, управлению конфликтами и деэскалации в киберпространстве является именно признание того, что нам всем еще предстоит многому научиться и наладить процесс прямого общения между противниками.» ***(Джозеф Най. Скайнет все ближе? Удастся ли предотвратить мировую кибервойну // Информационное агентство ЛІГАБізнесІнформ (https://www.liga.net/politics/opinion/skaynet-vse-blije-udastsya-li-predotvratit-mirovuyu-kibervoynu).10.10.2019).***

***

«Польща належить до двадцятьох країн, яким найбільше загрожують кібератаки.

За майже щодругою кібератакою стоять групи, підтримувані урядами, для яких важливим є вилучення даних, важливих з геополітичної перспективи. Про це свідчить останні звіти фірм Thales і Verint, — інформує Rzeczpospolita.

Особливо активні в РП російські хакери, що є результатом російсько-української гібридної війни.

У Польщі головними цілями є енергетична і транспортна галузі, а також адміністрація і фінансовий сектор…

Найактивніша група у Польщі — це група Black Energy пов’язана з російською військовою розвідкою. Але геополітика стоїть не лише за атаками. За словами Thalesa, 26 відсотків атак — групи хакерів — ідеологів, 20 відсотків – «звичайні» інтернет-злочинці. 5 відсотків є кібертерористами.

Як зазначає Даріуш Ємєльняк, експерт з управління мереж з Академії Леона Козьмінського, більшість фірм не готова до протидії таким кібератакам, у тому числі й найпростіших із них.

«Натомість від найбільш просунутих з них повністю не захищені навіть ІТ-гіганти», — додає він. що Польща не належить до числа лідерів у галузі кібербезпеки.

«Це правда, що у нас одні з найкращих програмістів у світі, але щороку випускників кількох елітних університетів на ринку праці залишається дуже мало порівняно з іншими країнами», — наголошує експерт.» ***(Oksana Nagirna. Польща – на прицілі кіберзлочинців // inpoland.net. (https://inpoland.net.pl/novosti/polshha-na-pricili-kiberzlochinciv/). 10.10.2019).***

***

«Facebook заблокував мережу облікових записів Instagram, керованих із Росії, які були створені, аби впливати на американців напередодні президентських виборів у США у 2020 році…

"Мережа, пов'язана з Агентством інтернет-досліджень, використовувала 50 облікових записів Instagram і один обліковий запис в Facebook, і мала 246 тис. підписників. Приблизно 60% з них були мешканцями США", - повідомив глава політики кібербезпеки Facebook Натаніель Глейхер.

За його словами, створення цих акаунтів було направлено, в основному, на політичні дебати в США, а також гострі політичні проблеми, які викликають суспільні суперечки і протиріччя.

У заблокованих акаунтах розміщувався матеріал, який може сподобається прихильникам як республіканців, так і демократів.» ***(Facebook заблокував мережу російських акаунтів Instagram, які мали впливати на перебіг виборів у США у 2020 році // Espreso.tv (https://espreso.tv/news/2019/10/22/facebook_zablokuvav_merezhu_rosiyskykh_akauntiv_instagram_yaki_maly_vplyvaty_na_perebig_vyboriv_u_ssha_u_2020_roci). 22.10.2019).***

***

«Служба безопасности и информации Чехии (BIS) обезвредила хакерскую сеть, находившуюся под контролем Федеральной службы безопасности России…

По словам главы чешской спецслужбы, заданием хакеров было осуществление кибератак на Чехию и ее союзников. Сеть серверов для этой цели финансировал Кремль и российское посольство.

Коуделка утверждает, что обнаруженная в Чехии сеть серверов была частью большей структуры, которая должна проводить кибероперации также на территории других государств Европы.

…агентурная сеть действовала под прикрытием двух частных фирм в Праге, которые занимались продажей компьютерной техники и программного обеспечения.» ***(Максим Лесів. В Европе обезвредили агентурную сеть ФСБ // Публичные люди (https://pl.com.ua/v-evrope-obezvredyly-agenturnuyu-set-fsb/). 22.10.2019).***

***

«Размещенные в Эстонии британские войска жалуются на таинственные сообщения, которые появляются на их страничках в социальных сетях и приходят к ним на сотовые телефоны. Командование считает, что это составная часть кибервойны, которую ведет Москва, чтобы вывести из равновесия и запугать британских военных и их союзников.

В настоящее время в Эстонии размещена почти 1 000 военнослужащих из Британии, которые участвуют в крупной операции НАТО по сдерживанию российской агрессии в Восточной Европе. Когда в Эстонию в 2017 году впервые прибыли британские военнослужащие, многие из них получили подозрительные сообщения, которые появились в их аккаунтах в Фейсбуке и Твиттере, а к кому-то на смартфоны стали приходить текстовые послания. Один солдат, не пожелавший

сообщить свое имя, рассказал ""Телеграф"": "Некоторые из нас получают странные СМС, сообщения в Фейсбуке и так далее. Они всегда написаны на английском языке и иногда похожи на нечто вроде "Мы за вами наблюдаем". "Это вызывает небольшое беспокойство, потому что им явно известно, кто мы все такие. Но нас учили быть готовыми и игнорировать такие вещи. Я бы не сказал, что российский генеральный план сработал". Есть мнение, что сообщения в Фейсбуке и Твиттере — дело рук так называемых "ботов". Это анонимные и связанные с Россией аккаунты, регулярно распространяющие кремлевскую пропаганду. Руководство НАТО также опасается, что Москва при помощи портативных антенн взламывает солдатские смартфоны, извлекая из них полезные данные и контакты. Американские командиры ранее жаловались на то, что во время пребывания в Эстонии за ними осуществлялась электронная слежка через смартфоны, а голландские летчики рассказывали, что их женам и подругам регулярно досаждали звонками русские тролли. По словам женщин, им звонили мужчины и с русским акцентом задавали вопросы типа "Вы знаете, что там делает ваш партнер?" или "А может, ему лучше уехать оттуда?" Находящимся в Эстонии британским военнослужащим в настоящее время разрешено пользоваться личными смартфонами, однако в войсках принимаются "соответствующие меры предосторожности", чтобы защитить их от российского вмешательства, о чем рассказал источник из военного ведомства. На это пошли после того, как начальник генерального штаба выступил с предупреждением о том, что Британия "каждый день находится в состоянии войны" из-за постоянных кибератак со стороны России и других стран. Генерал сэр Ник Картер (Nick Carter) добавил, что в современных условиях "уже нет разницы" между войной и миром…» ***(The Telegraph: Россию обвиняют в отправке сообщений с угрозами британским военным в Эстонии // Новости Великобритании на русском языке (https://theuk.one/the-telegraph-rossiyu-obvinyayut-v-otpravke-soobshhenij-s-ugrozami-britanskim-voennym-v-estonii/). 17.10.2019).***

***

«Колишній директор Центрального розвідувального управління (ЦРУ) Джон Бреннан заявив, що російське втручання у вибори президента США 2016 року змінило думку виборців…

Як зазначається, виступаючи перед Національним пресклубом у Вашингтоні 30 жовтня, Бренан заявив, що "особисто впевнений, що ці російські зусилля змінили думку хоча б одного виборця".

Водночас він заявив, що ЦРУ "не оцінювало" російський вплив кампанії на голосування, тому Бренан не зміг назвати точну кількість американців, які піддалися цьому…

Бреннан обіймав посаду директора ЦРУ в адміністрації президента Барака Обами в період з 2013 по 2017 роки…» ***(Російські хакери та тролі вплинули на вибори у Штатах – ексдиректор ЦРУ // ТОВ «УКРАЇНСЬКА ПРЕС-ГРУПА» (https://day.kyiv.ua/uk/news/311019-rosiyski-hakery-ta-troli-vplynuly-na-vybory-u-shtatah-eksdyrektor-cru). 31.10.2019).***

***

«США провели секретную кибероперацию против Ирана в ответ на атаки на нефтяную компанию в Саудовской Аравии, имевшие место в прошлом месяце…

По словам источников, пожелавших остаться анонимными, операция проводилась в конце сентября с целью заблокировать Тегерану возможность распространять «пропаганду». Один из источников сообщил, что удар был нанесен по аппаратному обеспечению, но не стал вдаваться в подробности.

Данная операция является более компактной по сравнению с другими кибероперациями, проводимыми в нынешнем году правительством США в ответ на сбитый дрон в июне и атаку на нефтяной танкер в мае…» ***(США нанесли киберудар по Ирану за пожар на Saudi Aramco // SecurityLab.ru (https://www.securitylab.ru/news/501789.php). 16.10.2019).***

***

Кіберзахист критичної інфраструктури

«Соединенные Штаты окажут стратегическую и техническую поддержку Литве, Латвии и Эстонии в защите от кибератак на энергетическую инфраструктуру этих стран. Об этом говорится в совместной декларации, которую 6 октября подписали министр энергетики США Рик Перри и министры стран Балтии…

В декларации подчеркивается, что сейчас очень важно "повышать кибербезопасность стратегической энергетической инфраструктуры Балтии". "Мы видим очень важную роль, которую США могли бы сыграть в оказании Балтийским государствам стратегической и технической поддержки", - говорится в декларации.

Литва надеется на участие американских предприятий в модернизации компьютерных систем управления энергосетями SCADA, улучшении защиты от вторжения, также планируется обмен специалистами информацией…

Источники кибератак в документе не названы, но литовская разведка в этом году предупредила, что "энергетический сектор страны является одной из мишеней кибергруппировок России". В обнародованном отчете разведслужбы Литвы утверждают, что фиксируют повторяющиеся попытки России предпринять разведку на предмет систем энергетического сектора Литвы…» ***(США помогут защитить энергосистему стран Балтии от кибератак России// РБК-Украина (https://www.rbc.ua/rus/news/ssha-pomogut-zashchitit-energosistemu-stran-1570437927.html). 07.10.2019).***

***

«Представители сферы коммунальных услуг опасаются кибератак на критическую инфраструктуру в следующем году. Данный результат получен по итогам опроса, проведенного исследователями из института Ponemone (США) совместно с компанией Siemens. Опрос был проведен среди более 1700 человек, работающих в сфере коммунальных услуг в Северной Америке, Латинской Америке, Европе, на Ближнем Востоке и в Азиатско-Тихоокеанском регионе. Респонденты включали техников, менеджеров, директоров, руководителей и руководителей старшего звена.

По словам большинства респондентов, киберугрозы представляют намного больший риск для операционных технологий (ОТ), чем для информационных. Почти две трети опрошенных считают сложные кибератаки главной проблемой. 56% респондентов сообщили по крайней мере об одной успешной атаке, связанной с потерей конфиденциальной информации или сбоем в среде операционных технологий в прошлом году, тогда как 4% более 10 раз столкнулись с подобными инцидентами.

Больше половины опрошенных опасаются кибератак на критически важную инфраструктуру в следующем году, однако некоторые уверены, что 30% атак на системы ОТ вовсе не обнаруживаются.

С точки зрения подготовки, 42% респондентов оценили свою киберготовность как высокую. В среднем организациям потребовалось 72 дня для реагирования на атаки с применением вредоносного ПО — 88 дней для малых предприятий и 62 дня для крупных.

Основными трудностями с точки зрения управления безопасностью ОТ респонденты считают рост числа сложных атак (61% опрошенных), нехватка квалифицированных работников (56%), изолированные и фрагментированные системы (55%), быстрое обнаружение взломов и эксплойтов (52%)…» ***(Компании в сфере коммунальных услуг опасаются кибератак на критическую инфраструктуру // SecurityLab.ru (https://www.securitylab.ru/news/501694.php). 10.10.2019).***

***

«Два дня назад SecurityLab писал о сообщениях в Twitter о возможной кибератаке на атомную электростанцию Куданкулам (самую мощную АЭС в Индии). Спустя несколько часов после появления публикаций представители АЭС опровергли все подозрения и уведомили, что реакторы станции полностью функционируют. Однако теперь родительская компания Куданкулам Индийская корпорация по атомной энергии (NPCIL) в официальном заявлении подтвердила факт заражения.

По словам бывшего аналитика Национальной технической исследовательской организации Индии Пухраджа Сингха, системы станции оказались заражены одной из версий вредоноса, известного под названием DTrack. Образец, недавно загруженный на VirusTotal, включал вшитые учетные данные для внутренней сети Куданкулам, указывая на то, что вредоносная программа была специально скомпилирована для распространения и работы в сети электростанции.

Согласно заявлению NPCIL, Dtrack заразил только административную сеть и не достиг критической внутренней сети, которая используется для управления

ядерными реакторами электростанции. Корпорация получила уведомление о заражении от индийской команды реагирования на компьютерные инциденты (CERT) еще 4 сентября (именно тогда вредоносное ПО было впервые обнаружено) и приступила к расследованию инцидента.

DTrack представляет собой «шпионский инструмент», использовавшийся специализирующейся на кибершпионаже группировкой Lazarus (она же Hidden Cobra) для атак на индийские финансовые институты и исследовательские центры. Вредонос включает в себя функции кейлоггера, способен получать доступ к истории браузера, собирать IP-адреса хоста, информацию о доступных сетях и активных соединениях, список всех запущенных процессов и список всех файлов на всех доступных дисковых томах.» ***(Индийская корпорация по атомной энергетике подтвердила факт кибератаки на АЭС Куданкулам // SecurityLab.ru (https://www.securitylab.ru/news/502215.php). 31.10.2019).***

***

«Крупные технологические и ИБ-компании объединили силы в рамках новой инициативы «Альянс операционных технологий и кибербезопасности» (Operational Technology Cyber Security Alliance, OTCSA). Альянс призван помочь промышленным предприятиям и организациям критической инфраструктуры в обеспечении безопасности операционных технологий (OT) путем предоставления им руководств и ресурсов.

В список учредителей OTCSA входят: производители промышленного оборудования ABB и Wärtsilä, производители АСУ ТП Mocana и SCADAFence, компания Microsoft, а также ИБ-компании Check Point Software, BlackBerry Cylance, Forescout, Fortinet, NCC Group, Qualys и Splunk. Принять участие в проекте могут все желающие производители IT- и OT-решений, а также организации, управляющие критической инфраструктурой и OT-системами.

OTCSA определил для себя пять важных целей: помощь организациям в усилении кибербезопасности взаимодействий между IT и OT, создание руководств для операторов OT по обеспечению безопасности их инфраструктуры, создание руководств для производителей OT по разработке безопасных продуктов, поддержка разработки и реализации более безопасной критической инфраструктуры, помощь в продвижении более безопасной критической инфраструктуры.

Созданные OTCSA руководства будут охватывать полный жизненный цикл OT-систем, включая каждый аспект, связанный с людьми, процессами и технологиями. По словам учредителей альянса, OTCSA является первой в мире примышленной группой, чья цель – обеспечить операторов OT четкими рекомендациями по архитектуре, реализации и процессам.» ***(IT- и ИБ-компании создали альянс по защите OT-систем // SecurityLab.ru (https://www.securitylab.ru/news/502000.php). 24.10.2019).***

***

«Устаревшие и неподдерживаемые операционные системы все еще присутствуют в сетях промышленных предприятий, подвергая их серьезному риску.

В частности, 62% промышленных сетей используют устройства, работающие на устаревших версиях ОС Windows, таких как Windows XP и Windows 2000. С учетом Windows 7, поддержка которой заканчивается в январе 2020 года, данный показатель составит 71%. Такая информация приводится в отчете 2020 Global IoT/ICS Risk Report компании CyberX, основанном на данных, собранных из более чем 1800 сетей по всему миру в период с октября 2018 года по октябрь 2019 года.

Использование устаревших версий Windows подвергает компании серьезному риску, поскольку злоумышленники могут взломать системы с помощью уязвимостей, информация и PoC-коды для которых часто размещены в общем доступе. Даже если Microsoft выпустит исправления для опасных уязвимостей, как это было в случае с Bluekeep , не все предприятия смогут применить исправление в промышленных системах.

Исследователи выявили подозрительную активность в 22% отслеживаемых сетях. Подозрительные действия включают сканирование, некорректные HTTP-заголовки, известные вредоносные программы и чрезмерное количество соединений между устройствами. Более половины сетей использовали устройства, к которым можно было получить удаленный доступ через RDP, SSH-подключение или VNC. В 27% случаев устройства были доступны из интернета.

В 64% случаев в сетях предприятий использовались незашифрованные пароли, упрощая злоумышленникам их перехват. Усложняет ситуацию тот факт, что в средах IoT и промышленных автоматизации пароли редко, а иногда и вовсе не меняются. По словам специалистов, в 66% случаев было отключено автоматическое обновление ПО для обеспечения безопасности.

По словам исследователей, предприятия в нефтегазовом и энергетическом секторе являются более защищенными по сравнению с предприятиями в других сферах, поскольку представляют собой регулируемые отрасли, которые «обычно гораздо более закрыты». ***(Больше половины промышленных предприятий все еще используют устаревшие ОС // SecurityLab.ru (https://www.securitylab.ru/news/501969.php). 22.10.2019).***

***

Захист персональних даних

«Управление по защите персональных данных Турции оштрафовало Facebook на 1,6 млн турецких лир ($282 тыс.) за несоблюдение закона о хранении данных порядка 300 тысяч пользователей…

Штраф для американской корпорации состоит из двух частей: 1,15 млн турецких лир ($202 тыс.) управление постановило взыскать с Facebook после того, как компания не предприняла установленных законом технических и административных мер по предотвращению утечки. Еще 450 тысяч лир ($79 тыс.) турецкие власти рассчитывают взыскать с Facebook из-за того, что компания не уведомила власти о произошедшей утечке.

…турецкое управление ранее уже штрафовало Facebook на 1,65 млн лир ($289,8 тыс.) за утечку данных пользователей.» ***(Турция оштрафовала Facebook на $282 тысяч за утечку данных пользователей // Rambler News Service (RNS) (https://rns.online/internet/Turtsiya-oshtrafovala-Facebook-na-282-tisyach-za-utechku-dannih-polzovatelei-2019-10-03/). 03.10.2019).***

***

«На черный рынок попали данные 60 млн владельцев кредитных карт Сбербанка. Утечку называют самой крупной в российском банковском секторе…

Данные продают на одном из форумов, заблокированных Роскомнадзором. Покупателям предлагают проверить подлинность базы на пробном фрагменте, содержащем данные 200 клиентов Уральского территориального Сбербанка.

Помимо персональных данных, в базе отображается также подробная информация об операциях по кредитной карте.

Если заявление продавца правдиво и база действительно содержит информацию о 60 млн клиентов, утечка могла затронуть данные о всех кредитных картах Сбербанка…

Финансовая организация подтвердила о наличии проблемы, правда, в пресс-релизе идёт речь пока только о 200 клиентах. Однако сами продавцы уверяют, что в их распоряжении находится информация по 60 млн кредитных карт, как действующих, так и закрытых (в настоящее время у банка насчитывается порядка 18 млн активных карт).

В банке заверили, что угрозы снятия клиентских средств с карт нет — среди похищенной информации нет кодов CVV. Кроме того, каждая транзакция без предъявленной карты в Сбербанке подтверждается СМС-паролем.

Судя по всему, утечка могла произойти в конце августа текущего года. Указанные в базе данных слова way4 и w4 вероятно относятся к используемой Сбербанком процессинговой платформе Way4…» ***(Личные данные россиян продолжают утекать в Сеть — теперь из Сбера и Налоговой // РосКомСвобода (https://roskomsvoboda.org/50330/). 03.10.2019).***

***

«Американская компания Facebook согласилась выплатить штраф в £500 тысяч ($663 тыс.) после скандала, связанного с утечкой данных пользователей через компанию Cambridge Analytica, при этом отказавшись признать свою вину, говорится на сайте Управления комиссара по информации Великобритании (ICO).

«В настоящее время достигнуто соглашение между сторонами. В рамках этого соглашения Facebook и ICO согласились отозвать свои соответствующие претензии. Facebook согласился выплатить штраф в размере 500 000 фунтов стерлингов, но не признал ответственности», — отмечается в сообщении.

В 2017 году управление начало официальное расследование неправомерного использования личных данных в политических кампаниях. В рамках этого расследования 24 октября 2018 года ICO опубликовало уведомление о денежном штрафе в отношении Facebook, однако впоследствии решение было оспорено Facebook в суде…» ***(Facebook согласилась выплатить штраф по делу Cambridge***

Analytica // Rambler News Service (RNS) (https://rns.online/internet/Facebook-soglasilas-viplatit-shtraf-po-delu-Cambridge-Analytica-2019-10-30/). 30.10.2019).

***

«Один из крупнейших регистраторов доменов Network Solutions сообщил о компрометации систем, произошедшей в конце августа 2019 года, в результате которой сторонним лицам удалось проникнуть в некоторые компьютерные системы компании без авторизации и потенциально получить доступ к персональной информации некоторых клиентов, включая имена, адреса, номера телефонов и адреса электронной почты.

Network Solutions является дочерней компанией Web.com с 2011 года. Помимо регистрации доменных имен, Network Solutions предоставляет такие услуги, как web-хостинг, дизайн сайтов и online-маркетинг, включая оптимизацию поисковых систем и управление оплатой за клик.

«16 октября 2019 года Network Solutions зафиксировала несанкционированный доступ третьего лица к ограниченному количеству компьютерных систем в конце августа 2019 года, в результате которого, возможно, неизвестный также получил доступ к информации аккаунта. В ходе атаки данные кредитных карт не были скомпрометированы», — сообщается на официальном сайте Network Solutions.

В настоящее время компания проинформировала правоохранительные органы об инциденте и проводит расследование. По словам Network Solutions, данные кредитных карт не были скомпрометированы в ходе атаки, поскольку номера кредитных карт хранятся в зашифрованном виде.

Компания настоятельно рекомендует пользователям сбросить пароли для учетных записей при следующем входе в систему в качестве дополнительной меры предосторожности.» ***(Регистратор доменов Network Solutions сообщил об утечке данных // SecurityLab.ru (https://www.securitylab.ru/news/502209.php). 31.10.2019).***

***

«Во вторник, 29 октября, принадлежащая Facebook компания WhatsApp подала в суд на израильского производителя инструментов для взлома NSO Group. Как сообщается в исковом заявлении, NSO Group помог правительственным спецслужбам взломать телефоны порядка 1,4 тыс. пользователей по всему миру, в том числе дипломатов, оппозиционеров, журналистов и высокопоставленных должностных лиц.

WhatsApp обвинила NSO Group в пособничестве взломам, осуществленным в интересах правительств в 20 странах, в том числе в Мексике, ОАЭ и Бахрейне. Согласно иску, жертвами взломов стало более сотни членов гражданского общества.

Если верить WhatsApp, злоумышленники использовали ее систему видеозвонков для доставки шпионского ПО на мобильные устройства определенных пользователей. Речь идет об уязвимости CVE-2019-3568, обнаруженной и исправленной WhatsApp в мае нынешнего года. Данная уязвимость использовалась для установки разработанной NSO Group шпионской программы Pegasus. Атакующие звонили жертве в WhatsApp, и на ее устройство

загружался вредонос, независимо от того, ответила она на звонок или нет…» ***(WhatsApp подала в суд на производителя шпионского ПО NSO Group // SecurityLab.ru (https://www.securitylab.ru/news/502193.php). 30.10.2019).***

***

«Итальянская банковская и финансовая организация UniCredit сообщила об утечке персональных данных около 3 млн клиентов. Вся информация, включая имена, номера телефонов, адреса электронной почты, хранилась в одном файле, созданном в 2015 году.

Несмотря на то, что UniCredit обслуживает клиентов по всему миру, утечка затронула только итальянских пользователей. По словам компании, финансовая информация и учетные данные клиентов не были скомпрометированы.

Компания начала внутреннее расследование данного инцидента и сообщила в правоохранительные органы…» ***(Банк UniCredit сообщил об утечке персональных данных 3 млн клиентов // SecurityLab.ru (https://www.securitylab.ru/news/502098.php). 28.10.2019).***

***

«28 жовтня, сінгапурська компанія з кібербезпеки, яка спеціалізується на запобіганні кіберзлочинів, виявила на популярному дарквебі- сервісі величезну базу даних, що містить інформацію про 1,3 мільйона кредитних та дебетових карт.

Про це повідомляє видання group-ib. Зазначається, що база даних під назвою "INDIA-MIX-NEW-01" продається в одному з найвідоміших підпільних магазинів Joker's Stash. Вона була завантажена в даркнет 28 жовтня. Вартість бази оцінюється в понад 130 мільйонів доларів.

За словами експертів, це одна з наймасштабніших і дорогих баз даних, виставлених на чорному ринку за всю історію інтернету.

Зазначена база містить в основному карти клієнтів індійських банків - 98%. На продаж виставлені кредитки найрізноманітніших класів, включаючи корпоративні та платинові. Кожну з них продають за 100 доларів. Таким чином, загальна вартість бази становить 130 мільйонів доларів.

Хакери за ці 100 доларів пропонують копії магнітних смуг кредитних і дебетових карт. За допомогою цієї інформації можна створювати підроблені варіанти існуючих карт для їхнього подальшого переведення в готівку…» ***(Перевірте, чи ваші гроші на місці: в мережі продаються дані понад мільйон банківських карт // Znaj.ua (https://techno.znaj.ua/274238-perevirte-chi-vashi-groshi-na-misci-v-merezhi-prodayutsya-dani-ponad-milyon-bankivskih-kart). 30.10.2019).***

***

«Почтовая система российского посольства в Латвии подверглась кибератаке…

Как сообщается на странице посольства в Facebook, в связи с атакой «от имени российского диппредставительства» началась рассылка спама.

Дипмиссия просит обращать внимание на адрес отправителя и напоминает, что письма посольства могут быть получены только с адресов rusembas@ml.lv и rusembas@mid.ru.» ***(Антон Антонов. Хакеры атаковали посольство России в Латвии // Деловая газета «Взгляд» (https://vz.ru/news/2019/10/12/1002618.html). 12.10.2019).***

***

«В первой половине 2019 года специалисты из «Лаборатории Касперского» с помощью ханипотов (ресурс, представляющий собой приманку для злоумышленников) зафиксировали 105 млн атак на IoT-устройства, исходящих с 276 тыс. уникальных IP-адресов. Данный показатель в семь раз больше, чем в первой половине 2018 года, когда было обнаружено около 12 млн атак с 69 тыс. IP-адресов. Пользуясь слабой защитой IoT-продуктов, киберпреступники прикладывают больше усилий для создания и монетизации IoT-ботнетов.

Количество кибератак на IoT-устройства стремительно увеличивается, поскольку все частных пользователей и организаций приобретают «умные» устройства, такие как маршрутизаторы или камеры видеорегистрации, но при этом не все заботятся об их защите. Киберпреступники, в свою очередь, видят все больше финансовых возможностей в использовании таких устройств. Они используют сети зараженных «умных» устройств для проведения DDoS-атак или в качестве прокси-сервера для других типов вредоносных действий.

Согласно собранным данным, атаки на IoT-устройства не отличаются сложностью, однако достаточно скрытны, чтобы пользователи не заметили их. Семейство вредоносных программ Mirai применялось в 39% от всех атак, в рамках которых использовались эксплойты, позволяющие ботнетам компрометировать устройства, эксплуатируя старые уязвимости, и контролировать их. На втором месте оказалось семейство вредоносов Nyadrop (38,57%) с применением техники бруфорса. Nyadrop также часто служил в качестве загрузчика Mirai. Третьим наиболее распространенным ботнетом стал Gafgyt (2,12% от всех атак).

Исследователи также определили страны, которые чаще других оказывались источниками заражения в первой половине 2019 года. 30% от всех атак происходили в Китае, в Бразилии — 19%, за ней следует Египет с показателем в 12%. В первой половине 2018 года ситуация была иной — Бразилия лидировала с показателем в 28%, Китай занимал второе место (14%), Япония третье (11%).

IoT является плодотворной областью для злоумышленников, которые используют даже самые примитивные методы, такие как угадывание комбинаций паролей и логинов для авторизации в системе. Пользователи очень часто пользуются распространенными комбинациями, как, например, «support/support»,

за которыми следуют «admin/admin», «default/default». ***(В 1 половине 2019 года зафиксировано более 100 млн атак на IoT-устройства // SecurityLab.ru (https://www.securitylab.ru/news/501793.php). 16.10.2019).***

***

«Крупнейший во Франции частный медиахолдинг Groupe M6 стал жертвой вымогательского ПО. По словам представителей Groupe M6, сотрудникам по киберзопасности удалось сдержать распространение вредоноса, предотвратив простои на всех десяти телеканалах, а также радиостанциях и киностудиях.

Несмотря на оперативность сотрудников компания не смогла полностью избежать инцидента, поскольку телефонные линии и почтовые серверы до сих пор не работают, сообщает французская газета L'Express.

Однако не только французская компания пострадала от недавних атак киберпреступников. Компания Pitney Bowes, занимающаяся глобальной доставкой и почтовыми услугами, сообщила об атаке с использованием вымогательского ПО, которое зашифровало некоторые из ее систем. Атака привела к частичному отказу систем, повлияв на доступ клиентов к некоторым услугам.

Атаки киберпреступников затронули некоторые сервисы почтовой системы Pitney Bowes и заблокировали доступ к службе «Ваша учетная запись». Также клиенты в настоящее время не могут выполнять пересылку по почте или совершать транзакции на почтовом аппарате, недоступен сервис SendPro Online в Великобритании и Канаде, «Ваша учетная запись» и интернет-магазин Pitney Bowes Supplies, что в свою очередь затрагивает подписку клиентов AutoInk и приложение поставок.» ***(Французский медиахолдинг Groupe M6 стал жертвой вымогательского ПО // SecurityLab.ru (https://www.securitylab.ru/news/501779.php). 15.10.2019).***

***

«Атаки на банкоматы в европейских странах с использованием вредоносных программ и джекпоттинга (jackpotting) оказались неэффективными в первой половине 2019 года. Киберпреступникам удалось заработать менее 1000 евро за одно успешное ограбление.

Согласно отчету Европейской ассоциации безопасных транзакций (European Association for Secure Transactions, EAST), в указанный период банки сообщили в общей сложности о 35 атаках на банкоматы по всей Европе. В 3 атаках применялось вредоносное ПО, в остальных случаях — джекпоттинг. По словам специалистов, потери банков снизились на 100% (с 0,25 млн евро до 0,00 млн евро), и только в одном случае был зафиксирован небольшой ущерб (менее 1000 евро).

Но, как и в случае с вредоносным ПО для банкоматов, джекппоттинг применяется все реже. Основная причина заключается в том, что подобные атаки навсегда уничтожают банкоматы, требуют дорогих инструментов и большого количества времени для выполнения. В связи с этим преступники прибегли к методам, которые можно использовать бесчисленное количество раз, например, скимминг или мошенничество с отменой транзакций.

В течение многих лет оба типа атак были очень успешными в Европе, нанося ущерб в пределах от 250 до 350 млн евро в год. Но, согласно последнему отчету EAST, в первой половине 2019 года использование скиминговых устройств достигло рекордно низкого уровня и уступило место менее известному методу мошенничества с отменой транзакций.

Мошенничество с отменой транзакции, или TRF-атаки (transaction reversal fraud), предполагает использование ошибок в обычном режиме работы банкомата. В рамках TRF-атаки мошенники вводят действительную карту в банкомат, правильный PIN-код и запрашивают снятие наличных. Однако, когда банкомат извлекает платежную карту, преступник оставляет ее в слоте банкомата.

Злоумышленники намеренно оставляют карту в банкомате до тех пор, пока он не сочтет, что карта застряла и необходимо отменить предыдущую банковскую транзакцию, фактически повторно добавив деньги на счет мошенника. На данном этапе преступник использует инструмент (например, отвертку) для принудительного открытия заслонки банкомата и получения денежных средств, которые были предварительно подготовлены к выдаче для отмененной транзакции.

Подобные атаки стали преобладающей формой мошенничества с банкоматами в Европе. На их долю приходится 5649 случаев в первой половине 2019 года (против 2292 в прошлом году) и 45% от всех случаев мошенничества с банкоматами.

По прогнозам EAST, в обозримом будущем данная тенденция сохранится — количество вредоносных программ, джекпоттинга и скиммеров будет снижаться, а TRF-атак, наоборот, возрастет…» ***(Кибератаки на банкоматы почти перестали приносить выгоду преступникам // SecurityLab.ru (https://www.securitylab.ru/news/501696.php). 10.10.2019).***

***

«Неизвестные киберпреступники организовали атаку на компании в сфере нефтяной промышленности США. В рамках вредоносной кампании для кражи данных использовался троян для удаленного доступа (RAT) Adwind (другие названия jRAT, AlienSpy, JSocket и Sockrat), который ранее применялся против компаний электроэнергетического сектора.

По словам исследователей из Netskope, атаки осуществляются с домена, принадлежащего австралийскому интернет-провайдеру Westnet. Остается неясным, является ли участники группировки клиентами Westnet или они скомпрометировали учетные записи клиентов и используют их для распространения Adwind.

Adwind RAT предлагается на ряде торговых площадок в даркнете по модели вредоносное ПО-как-услуга (malware-as-a-service) и за последние два года неоднократно использовался в различных кампаниях. Вредонос способен шифровать и фильтровать данные, захватывать изображения web-камеры, проверять жесткие диски на наличие определенных файлов на основе расширений в конфигурации вредоносного ПО, внедрять вредоносный код в легитимные процессы для избежания обнаружения и мониторить состояние системы. ПО изменяет параметры реестра для обеспечения персистентности и может отключать

межсетевые экраны, антивирусные решения и другие службы безопасности на зараженных устройствах.

По словам исследователей, в новом варианте Adwind преступники реализовали сложные методы обфускации. Анализ вредоносного ПО показал, что оно использует несколько встроенных JAR-архивов (Java Archive) перед распаковкой окончательной полезной нагрузки. Уровень обфускации был настолько эффективным, что только 5 из 56 антивирусных решений на VirusTotal смогли обнаружить вредоносное ПО.

Согласно проведенному анализу, злоумышленники в первую очередь интересуются документами, файлами и другими локально сохраненными данными. Они также заинтересованы в поиске такой информации, как FTP-пароли и SSH-ключи, которые могут дать больший доступ к сети.» ***(Преступники атаковали нефтяные компании США с помощью трояна Adwind // SecurityLab.ru (https://www.securitylab.ru/news/501535.php). 02.10.2019).***

***

«На системы китайской корпорации Huawei в день совершается около миллиона кибератак. Такую статистику привёл глава безопасности техногиганта Джон Саффолк. Саффолк предполагает, что целью атак была кража IP. Руководство Huawei обвиняет США в организованной кампании, направленной против корпораций КНР. Помимо атак на внешние и внутренние системы Huawei, США запугивают сотрудников техногиганта. Об этом также заявило руководство китайской компании. Саффолк отметил, что большинство атак удаётся заблокировать, однако тем, что были направлены на более старые системы, удалось пробить защиту. Основной посыл этих кибератак остаётся загадкой, однако известно, что в ходе них преступники похитили конфиденциальную информацию, отправив вредоносную программу по электронной почте. Глава безопасности Huawei подчёркивает: несмотря на все обвинения китайской корпорации со стороны США, никаких бэкдоров и скрытых вредоносов в оборудовании обнаружено не было.» ***(Олег Иванов. Huawei отражает около миллиона кибератак ежедневно // ООО «АМ-МЕДИА» (https://www.anti-malware.ru/news/2019-10-14-1447/31040). 14.10.2019).***

***

«Эксперты Европола представили результаты исследования актуальных киберугроз. По словам аналитиков, наибольшую опасность сегодня представляет активность шифровальщиков и зловредов, которые охотятся за разнообразными пользовательскими данными.

Вымогатели и шифровальщики

По оценкам исследователей, в настоящий момент в европейском киберпространстве действуют около 25 семейств шифровальщиков, включая давно известные Locky, Rapid, ACCDFISA. В этом списке по-прежнему остаются зловреды, которые уже были фактически побеждены — Dharma, CrySiS, GandCrab.

Чаще всего зловреды попадают в инфраструктуру через мошеннические письма и уязвимые RDP-подключения. Эксперты подсчитали, что целевой фишинг

применяют в своих атаках 65% кибергруппировок. Около половины (48%) вредоносных вложений в электронных письмах приходится на офисные файлы.

Исследователи отмечают, что вымогатели переходят от массированных кампаний к таргетированным атакам. Злоумышленники стремятся повысить свою прибыль за счет тщательно проработанной тактики. Сумма выкупа, которую преступники требуют у пострадавших компаний, может превышать миллион евро.

Помимо коммерческих предприятий, жертвами шифровальщиков все чаще становятся государственные организации и целые города. Исследователи упомянули инциденты в США, когда кибератаки парализовали муниципальные службы в Атланте, Балтиморе, Флориде и Техасе. Аналитики Европола ожидают, что в скором будущем преступники могут направить усилия и на европейские страны.

Помимо вымогательства, операторы шифровальщиков занимаются и простым саботажем. По оценкам исследователей, за первые полгода количество таких разрушительных атак выросло вдвое, причем половина инцидентов пришлась на промышленный сектор. Если раньше вайперы использовали только спонсируемые государствами группировки, то теперь такие функции попадаются в инструментах рядовых киберпреступников.

Охота за информацией

Пользовательские данные, будь то реквизиты пластиковых карт, логины и пароли к онлайн-банкам или копии удостоверений личности, получают все большую ценность в глазах киберпреступников. Исследователи отмечают, что преступники находят применение любой информации. Деньги с ворованных карт идут на покупку дорогой электроники. Краденые паспортные данные используют работорговцы и террористы, чтобы бронировать авиабилеты и гостиницы. Кадровая информация, корпоративные логины и пароли помогают планировать фишинговые атаки и BEC-схемы.

По данным Европола, в первой половине 2019 года на черном рынке можно было купить 23 млн ворованных карт. Поскольку наученные опытом интернет-магазины стали защищаться от взлома, преступники смещают активность на другие секторы, где пользователи вводят платежные данные. Это в первую очередь сайты отелей, почтовых служб и аренды автомобилей.

Под угрозой оказываются не только сами сайты организаций, но и сторонние ресурсы. Немалая доля крупных утечек происходит через незащищенные облачные контейнеры Amazon, несмотря на последовательные усилия провайдера по упрощению настроек безопасности.

Атаки на цепочки поставок

Один из ключевых трендов 2019 года — это взлом IT-провайдеров и поставщиков ПО для получения доступа к их клиентам. По некоторым данным, в 2018-м количество таких инцидентов выросло почти вдвое (78%).

Причиной тому становится все большая популярность облачных сервисов и относительно небольших компаний, которые предлагают IT-продукты более крупным организациям. Аналитики привели в пример недавнюю атаку Magecart на разработчиков расширений для сайтов, когда преступники взломали сервер с дистрибутивами ПО.

Эксперты Европола указывают, что ключевую роль в нейтрализации таких угроз играет скорость реакции на вторжение. Они призывают к укреплению взаимодействия ИБ-индустрии и органов кибербезопасности в целях повышения общей устойчивости к киберугрозам.

DDoS-атаки

Вывод корпоративных систем из строя — это второй по популярности способ давления после атак шифровальщиков. Аналитики отмечают, что особую опасность такие инциденты представляют для финансовых организаций, которые несут не только материальные, но и репутационные потери.

Мощность DDoS-атак постоянно растет. В начале 2019 года эксперты зафиксировали очередной рекорд, когда поток мусорных запросов превысил отметку в 500 млн пакетов в секунду. Уже в апреле специалисты столкнулись с более массированной атакой, которая достигла показателей в 580 млн пакетов.

Как отмечают исследователи, правоохранительные органы добиваются определенных успехов в борьбе с этими угрозами. В 2018 году в результате совместной операции Европола, Национального управления Великобритании по борьбе с преступностью и еще более десяти служб удалось заблокировать webstresser.org — одну из крупнейших в мире площадок по продаже DDoS-услуг. По данным Европола, последствия этой операции ощущаются до сих пор, а правоохранители продолжают розыск, используя полученные улики.

Угрозы, уходящие в прошлое

На протяжении последних двух лет эксперты отмечают падение популярности банковских троянов — сегодня ущерб от их активности находится на рекордно низком уровне. В то же время такие зловреды, как Emotet и Trickbot, чья архитектура позволяет встраивать дополнительные модули, по-прежнему создают проблемы для корпоративных инфраструктур.

Немалую угрозу для здоровья сетей представляют и другие вредоносные семейства, включая давно известные Dridex, Retefe и относительно новый BackSwap.

С окончанием криптовалютной лихорадки заметно упала активность криптоджекеров. Одним из главных факторов эксперты называют закрытие сервиса Coinhive, который обеспечивал значительную долю скрытой добычи токенов. Впрочем, и здесь специалисты призывают не списывать угрозу со счетов. Появление бесфайловых криптомайнеров и новых червей-дропперов говорит о том, что преступники ищут новые способы добывать деньги на чужих мощностях

Как отметила глава Европола Катрин де Болль (Catherine De Bolle), многие новые угрозы связаны с уже известными технологиями, которые остаются уязвимыми, несмотря на существование защитных патчей.

«Правоохранительным органам не следует чрезмерно фокусироваться на грядущих технологических изменениях в мире киберпреступности, — сказано в пресс-релизе Европола. — В борьбе с киберпреступлениями нужен комплексный подход, включающий профилактику атак, просвещение и повышение устойчивости перед киберугрозами». ***(Maxim Zaitsev. Европол назвал основные киберугрозы 2019 года // Threatpost (https://threatpost.ru/europol-highlights-main-cyber-threats-2019/34473/). 11.10.2019).***

***

«Немецкий программист Тобиас Фрёмель (Tobias Frömel) получил доступ к серверам операторов вымогателя Muhstik и опубликовал ключи, необходимые для расшифровки данных. Это произошло после того, как специалист заплатил злоумышленникам более 600 евро за возможность декодирования своей информации.

Первые сообщения о ранее неизвестном шифровальщике появились в Сети 30 сентября этого года. Пострадавшие сообщали, что злоумышленники подбирают пароли к сетевым хранилищам на базе NAS-устройств QNAP и кодируют находящиеся там файлы. В документе README_FOR_DECRYPT.txt, размещенном на взломанном диске, жертве предлагают несколько ссылок на ресурсы с дальнейшими инструкциями. За расшифровку информации киберпреступники требуют 0,09 биткойна (примерно 670 евро)…

В своем сообщении на Pastebin Фрёмель написал, что авторы вымогателя развернули свои веб-оболочки на уже скомпрометированных серверах, поэтому ему не пришлось взламывать чужие компьютеры. Этичный хакер пояснил, что сумел получить доступ к PHP-скрипту для генерации ключей и использовал его для вывода идентификаторов каждой жертвы.

Опубликованный документ содержит почти 3 000 секретных кодов Muhstik, сформированных программистом на основании полученных данных. Пострадавшие пользователи подтвердили работоспособность выложенных ключей. Специалист выразил сожаление, что уже заплатил злоумышленникам, и сообщил, что будет рад вознаграждению за свою работу.

Чуть позже в Интернете появился декриптор для Muhstik, созданный Фрёмелем, а также еще одна утилита для расшифровки, разработанная сторонней командой ИБ-экспертов. Связь вымогателей с операторами ботнета Muhstik, замеченного в ряде кибератак, пока не доказана…» ***(Maxim Zaitsev. В Сети появились ключи для файлов, пораженных Muhstik // Threatpost (https://threatpost.ru/muhstik-ransomware-decryption-keys-published-online/34413/). 08.10.2019).***

***

«В России появился новый вид мошенничества. Злоумышленники выводят деньги клиентов банков, подключаясь к смартфону с помощью программы удаленного доступа. Об этом сообщил глава специализирующейся на кибербезопасности компании Group-IB Илья Сачков, передают РИА Новости.

Как рассказал эксперт, мошенники пытаются заставить клиентов банков установить на устройство программу удаленного доступа, которая позже позволяет им похищать средства жертвы. По словам Сачкова, в среднем крупный банк всего за месяц может лишиться от 6 млн до 10 млн рублей.

Как он отметил, за полгода система безопасности Secure Bank ежемесячно обнаруживала свыше 1 тыс. попыток похитить средства пользователей с помощью программы удаленного доступа к мобильному устройству.» ***(Появился новый способ кражи денег через смартфон // Вести-UA (https://vesti-***

ua.net/novosti/obschestvo/123484-poyavilsya-novyy-sposob-krazhi-deneg-cherez-smartfon.html). 24.10.2019).

***

«Некоторые поставщики интернет-услуг и провайдеры просто не могут не становится мишенями для различных злоумышленников – как, например, в свое время стала компания NordVPN, которая предоставляет не только услуги интернет-соединения, но также услуги VPN-сетей. Сегодня руководство компании решило выпустить специальный отчет, в котором призналась своим клиентам и широкой общественности в том, что стала жертвой взлома неизвестными злоумышленниками в марте прошлого 2018 года, таким образом удиви всех столь "своевременной" новостью. Однако сама компания решила сообщить об этом пользователям не с целью продемонстрировать свой скрытный характер.

А лишь потому, что сам взлом был успешно нейтрализован и специально нанятая команда по кибербезопасности не обнаружила никаких следов кражи каких бы то ни было пользовательских данных. Иными словами, взлом, произошедший в марте прошлого года, не представляет собой ничего опасного для самих пользователей сервиса NordVPN, однако команда предупредила, что некоторая часть пользовательских данных общего доступа все-таки могла стать достоянием хакеров – в частности, специалисты указывают на тот факт, что некоторая часть интернет-страниц стала доступной для стороннего просмотра, но все остальные данные остались при пользователях и системе шифрования от компании.

Таким образом, компания NordVPN столкнулась с очередной сессией удаленного взлома, благополучно его пережив и даже не подвергнув опасности основную пользовательскую аудиторию – хотя, конечно, узнавать о таком происшествии спустя почти два года является не самым радужным и позитивным вариантом новости, который можно было ожидать.

Тем не менее, компания NordVPN сообщает об этом также с привязкой к тому, что уже сумела преодолеть некоторые ранние баги и неувязки, связанные именно с работой своего сервиса – а потому можно лишь догадываться о том, какие работы в скрытом порядке проводились. Можно предположить, что с учетом всех ранних зарегистрированных случаев взлома сетей и серверов NordVPN, компания в самом деле решила серьезно взяться за улучшение составляющих своей защиты.» ***(Роман Розенталь. NordVPN сообщила о «новом» взломе своего сервиса // Faina Idea (https://fainaidea.com/interesnoe/neobychnoe/nordvpn-soobshhila-o-novom-vzlome-svoego-servisa-179418.html). 22.10.2019).***

***

«Международный разработчик антивирусного программного обеспечения – словацкая компания ESET обнаружила новые кибератаки, позволяющие воровать виртуальную валюту в сетевых играх. Об этом сообщается на сайте ESET. «Компания ESET — лидер в области информационной безопасности — сообщает об обнаружении нового бэкдора, нацеленного на Microsoft SQL (MSSQL), который распространяла известная группа киберпреступников Winnti. Стоит отметить, что злоумышленники активны по

меньшей мере с 2012 года и известны атаками на цепь поставки игровой индустрии», - говорится в сообщении.

Согласно сообщению, угроза под названием skip-2.0, обнаруженная специалистами ESET, может незаметно подключаться к любой учетной записи MSSQL с помощью специального пароля, при этом автоматически скрывать соединения от журналов. Простыми словами, жертвы не подозревают о том, что их компьютеры уже взломаны хакерами. Кроме этого, у киберпреступников есть возможность скрыто копировать, изменять или удалять содержимое базы данных. Таким образом, злоумышленники смогут осуществлять мошеннические операции с валютами в играх с целью получения финансовой выгоды.

Как сообщают специалисты ESET, вредоносное программное обеспечение skip-2.0 считается первым известным бэкдором, нацеленным на MSSQL Server. Целями злоумышленников стали 11 и 12 версии MSSQL Server (выпущенные в 2012 и 2014 годах соответственно), которые являются самыми распространенными среди пользователей…» ***(Международная IT-компания ESET обнаружила новые кибератаки, позволяющие воровать виртуальную валюту в сетевых играх // УНИАН (https://www.unian.net/science/10726740-mezhdunarodnaya-it-kompaniya-eset-obnaruzhila-novye-kiberataki-pozvolyayushchie-vorovat-virtualnuyu-valyutu-v-setevyh-igrah.html). 21.10.2019).***

***

«Специалисты компании BlackBerry Cylance выявили серию кибератак, при которых вредоносный код был скрыт в аудиофайлах с расширением .WAV. Это код позволял злоумышленникам добывать криптовалюту за счёт мощностей компьютера жертвы.

Это так называемые скрытые майнеры. На этот раз распространялись майнеры криптовалюты Monero. Впрочем, как и в большинстве случаев. По словам экспертов, каждый файл WAV был дополнен загрузчиком, который декодировал и запускал вредоносный контент. Для пользователя аудиофайлы либо звучали как музыка, либо просто воспроизводили белый шум…» ***(Хакеры распространяли скрытые добытчики криптовалюты в аудиофайлах // SmartPhone.ua (http://www.smartphone.ua/news/hakery_rasprostranyali_skrytye_dobytchiki_kriptovalyuty_v_audiofaylah_62577.html). 22.10.2019).***

***

«Ссылаясь на представителя компании Huawei Technologies, источник утверждает, что китайский производитель ежедневно выдерживает около 1 миллиона кибератак. Они исходят как изнутри страны, так и из-за ее пределов. В заголовке источник уточняет, что атаке подвергается оборудование 5G, но в тексте об этом речи нет, зато становится понятно, что большинство атак удается отразить, так что пострадали лишь немногое «компьютеры старого типа»…» ***(Huawei каждодневно подвергается миллиону кибератак // Украина сегодня (http://ukr-today.com/high-tech/412941-huawei-ezhednevno-podvergaetsja-millionu-kiberatak.html). 14.10.2019).***

***

«Европол обнародовал свой отчет касательно оценки угроз организованной преступности в Интернете (IOCTA) за 2019 год. Согласно данным, мошенники чаще всего используют вирусы-вымогатели.

В отчете говорится о том, что борьба с киберпреступностью подразумевает не только противодействие нынешним угрозам, а также прогнозирование будущих проблем. Появление новых угроз связано не только с развитием технологий, но и с использованием известных уязвимостей.

Вирусы-вымогатели являются самым распространенным способом для похищения криптовалют. Преступники требуют большой выкуп в цифровой валюте за расшифровку файлов пострадавших. Кроме того, злоумышленники часто пытаются получить доступ к финансовым данным, а именно кредитным картам, криптовалютным кошелькам и онлайн-банкингу.

Криптовалютные биржи все еще интересны мошенникам: согласно данным, в 2018 году с криптобирж и других платформ было украдено около $1 млрд в криптовалютах. Европол намерен наладить сотрудничество с криптовалютными фирмами для борьбы с преступностью.» ***(Европол назвал самый популярный инструмент для кибератак // PAYSPACE MAGAZINE (https://psm7.com/security/evropol-nazval-samyj-populyarnyj-instrument-dlya-kiberatak.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+Payspacemagazine+%28Payspacemagazine%29). 15.10.2019).***

***

«Неизвестные киберпреступники осуществили на данный момент самую крупную в истории Грузии атаку, в ходе которой осуществили дефейс 15 тыс. web-сайтов, которые были в последствии отключены. По данным местных СМИ, вредоносная кампания затронула сайт действующего президента Грузии, а также интернет-ресурсы различных правительственных учреждений, банков, судов, местных газет и телевизионных станций.

По признанию местного хостинг-провайдера Pro-Service, злоумышленник(и) взломал его сеть и скомпрометировал web-сайты клиентов. По крайней мере две телевизионные станции («ТВ Имеди» и «ТВ Маэстро») вышли из эфира после атак, телеканал Pirveli также пострадал, но остался в эфире, а некоторые газетные издания работали в автономном режиме. Атака произошла рано утром 28 октября, и к 20:00 того же дня провайдер восстановил работу более половины пострадавших сайтов.

Пока неизвестно, кто стоял за данной массовой атакой, и какие цели преследовали злоумышленники. МВД Грузии возбудило уголовное дело в связи со взломом официального сайта президента…» ***(Крупнейшая кибератака в истории Грузии затронула правительственные сайты // SecurityLab.ru (https://www.securitylab.ru/news/502113.php). 29.10.2019).***

***

«Специалисты компании Lookout обнаружили вредоносную кампанию против гуманитарных организаций ООН. В числе атакуемых оказались детский фонд UNICEF, Всемирная продовольственная программа, Программа

развития ООН и пр. Специалисты уведомили их об угрозе и предупредили, что атаки все еще продолжаются.

Злоумышленники создали фишинговые сайты, скопировав дизайн с оригинальных сайтов ООН, с целью заманивать сотрудников организаций на поддельные страницы авторизации и похищать их учетные данные. Как отмечают исследователи, злоумышленников интересуют не отдельные сотрудники, а вся организация в целом. Завладев учетными данными одних сотрудников, киберпреступники изучают их электронные ящики в поисках других сотрудников и пытаются скомпрометировать их учетные записи.

По данным исследователей, связанная с атаками инфраструктура используется с марта 2019 года. Фишинговый контент распространялся с доменов session-services[.]com и service-ssl-check[.]com, разрешенные в IP-адреса 111.90.142.105 и 111.90.142.91. Связанный блок IP-адресов и номер автономной системы (Autonomous System Number, ASN) имеют низкую репутацию и в прошлом уже использовались для хостинга вредоносного ПО.

Специалисты Lookout выявили несколько заслуживающих внимания методов, используемых в данной кампании, в том числе способность обнаруживать мобильные устройства и напрямую регистрировать нажатия клавиш, когда жертва вводит данные в поле пароля.

В частности, логика Javascript-кода на фишинговых страницах определяет, загружается ли страница на мобильное устройство. Если да, то используется контент для мобильных устройств. Поскольку мобильные версии браузеров обрезают URL-адреса, жертвам труднее обнаружить обман.

Исследователи также обнаружили кейлоггер, встроенный в поле пароля на фишинговых страницах авторизации. То есть, даже если жертва ввела учетные данные, но не нажала на кнопку ввода, они все равно будут перехвачены кейлоггером.» ***(Гуманитарные организации ООН находятся под кибератаками // SecurityLab.ru (https://www.securitylab.ru/news/502057.php). 25.10.2019).***

***

«Некоторые из недавних инцидентов кибербезопасности, связанных с автоматизированными системами управления (АСУ), привели к травмам и даже гибели людей, показал опрос, проведенный Международной ассоциацией систем управления кибербезопасностью (Control Systems Cyber Security Association International, CS2AI)…

Организация проводит ежегодный анализ состояния кибербезопасности АСУ с помощью опроса, который призван помочь ответить на ключевые вопросы о том, как защитить наиболее важные системы.

В недавнем опросе приняли участие около 300 сотрудников компаний, отвечающих за кибербезопасность промышленных систем и систем автоматизации. По словам экспертов, многие промышленные организации все еще не принимают всерьез кибербезопасность, часто утверждая, что они не были или вряд ли будут атакованы злоумышленниками.

По признанию примерно 1% респондентов, за последние 12 месяцев они сталкивались с инцидентами, приведшими к травмам или гибели людей. По словам

примерно четверти респондентов, произошедшие инциденты приводили к сбоям в производственных процессах.

В качестве главных векторов атак 34% опрошенных назвали зараженные вредоносным ПО диски, почти столько же сотрудников указали фишинговые атаки через электронную почту, 16% — предварительно зараженное аппаратное или программное обеспечение, 12% обвинили сторонние web-сайты, а 10% — зараженные или скомпрометированные мобильные устройства. Нарушения физической безопасности и компрометация Wi-Fi-сетей также были упомянуты некоторыми респондентами.

Некоторые организации признались в наличии промышленных систем управления, доступных напрямую из интернета, в том числе ПЛК, человеко-машинных интерфейсов, серверов и рабочих станций.

Главным приоритетом многих организаций является оценка рисков и управление ими, за ними следуют безопасность периметра сети и непрерывность бизнеса. Безопасность в облаке не особо популярна и является приоритетом только для нескольких промышленных организаций.

На вопрос о препятствиях в устранении или смягчении уязвимостей в АСУ наиболее распространенным ответом был недостаточный опыт, нехватка персонала, эксплуатационные требования (например, недостатки не могут быть устранены из-за обязательного времени безотказной работы), недостаточные финансовые ресурсы и слабая поддержка со стороны руководства.

Полный отчет по опросу CS2AI пообещала опубликовать в следующем месяце…» ***(Некоторые инциденты при работе с АСУ привели к травмам и гибели людей // SecurityLab.ru (https://www.securitylab.ru/news/502056.php). 25.10.2019).***

***

«В рамках проекта Pwnagotchi представили систему для взлома беспроводных сетей, которая оформлена в виде электронного питомца.

Это напоминает популярную игрушку «Тамагочи», а технически устройство построено на базе одноплатного компьютера Raspberry Pi Zero W (поддерживаются и другие модели). При этом программную часть можно использовать в любом Linux-окружении и на любом PC, где есть Wi-Fi-модуль с поддержкой режима мониторинга.

Для поддержания хорошего настроения питомца его необходимо кормить сетевыми пакетами, отправляемыми участниками беспроводных сетей на этапе согласования нового соединения (handshake). Устройство находит доступные беспроводные сети и пытается перехватывать handshake-последовательности. Так как handshake отправляется только при подключении клиента к сети, устройство использует различные приёмы для обрыва текущих подключений и принуждения пользователей выполнить операции переподключения к сети. В ходе перехвата накапливается база пакетов, включающих хэши, которые можно использовать для подбора ключей WPA.

По аналогии с тамагочи поддерживается определение находящихся поблизости других устройств, а также опционально возможно участие в построении общей карты охвата. Для соединения устройств Pwnagotchi по WiFi

используется протокол Dot11 . Находящиеся поблизости устройства обмениваются полученными данными о беспроводных сетях и организуют совместную работу, разделяя между собой каналы для проведения атаки.» ***(Выпущен тамагочи для взлома Wi-Fi сетей // SecurityLab.ru (https://www.securitylab.ru/news/501971.php). 22.10.2019).***

***

«Один из крупнейших в мире производителей инструментов для автоматизации немецкая компания Pilz уже больше недели не может восстановить работу после атаки вымогательского ПО.

Как сообщается на сайте Pilz, 13 октября нынешнего года компания подверглась кибератаке, затронувшей ее серверы и рабочие станции по всему миру. В качестве меры предосторожности все компьютеры были отключены от корпоративной сети, а доступ к ней был заблокирован. Инцидент затронул представительства Pilz в 76 странах, в результате чего их компьютеры были отключены от главной сети компании и они лишились возможности делать заказы и проверять статус клиентов.

На восстановление доступа к почтовому сервису у Pilz ушло три дня и еще столько же потребовалось для его восстановления в международных представительствах. Доступ к системе заказов и доставки был восстановлен только 21 октября. Кибератака не затронула производственные линии, однако отсутствие возможности принимать заказы существенно замедлила производство.

Как сообщил журналисту Каталину Кимпану (Catalin Cimpanu) старший аналитик компании FoxIT Маартен ван Дантциг (Maarten van Dantzig), немецкий производитель автоматики стал очередной жертвой вымогательского ПО BitPaymer. Напомним , 13 октября об атаке вымогателя также сообщил французский медиахолдинг Groupe M6, а днем позже – американская курьерская компания Pitney Bowes…» ***(Один из крупнейших производителей автоматики неделю не может восстановиться после кибератаки // SecurityLab.ru (https://www.securitylab.ru/news/501926.php). 22.10.2019).***

***

«Оператор одного из сервисов, работающего по модели «доступ-как-услуга» (access-as-a-service), начал сотрудничать с несколькими операторами вымогательского ПО, включая REvil (также известная как Sodinokibi), предлагая им доступ к сетям крупных компаний.

Преступники, занимающиеся взломом корпоративных сетей, предлагают свои навыки в даркнете и защищенных мессенджерах. Злоумышленники взламывают сети компании, а затем сдают в аренду или продают доступ операторам программ-шифровальщиков. Подобное взаимовыгодное сотрудничество позволяет распространять вымогательское ПО даже в защищенных сетях.

Исследователи из компании Advanced Intelligence (AdvIntel) обнаружили связь между двумя типами киберпреступных операций. Доступ к корпоративной сети может быть использован для нескольких вредоносных кампаний, включая BEC–атаки (business email compromise – компрометация деловой почты) и спам.

Киберпреступник под псевдонимом -TMT- начал сотрудничать с операторами REvil с августа 2019 года. Сотрудничать к REvil получилось благодаря Lalartu — известному пользователю даркнета, который практически поручился за разработчиков REvil. Lalartu и -TMT- обнаружили выгоду от партнерства с операторами вымогательского ПО и предложили им свои услуги.

В течение июня, июля и августа 2019 года -TMT- предлагал доступ к скомпрометированным корпоративным сетям, не называя имен жертв. Цены варьировались от $3 тыс. до $5 тыс. за доступ к сотням хостов и серверов компаний из разных стран, работающих в различных отраслях промышленности. Цены зависели от типа предлагаемого доступа, например, наиболее дешевые варианты предоставляли доступ к удаленному рабочему столу, который легче обнаружить.

В ходе одной из атак -TMT- получил полный доступ к административным панелям, хостам серверов и корпоративным VPN-сетям одной из жертв. Доступ был оценен в $20 тыс. По словам исследователей, киберпреступник «похитил учетные данные администратора, мог безопасно перемещаться по сети и повышать права доступа по мере необходимости».

Известно также, что тактики, методы и процедуры, применяемые -TMT-, включают использование Metasploit и платформы Cobalt Strike.» ***(Группировка REvil нашла партнеров для взлома корпоративных сетей // SecurityLab.ru (https://www.securitylab.ru/news/501890.php). 21.10.2019).***

***

Діяльність хакерів та хакерські угруповування

«У США одразу три лікарні штату Алабама закрилися через хакерські атаки на свої системи…

Лікарні, на які були здійснені атаки, є користувачами системи DCH Health. Після 1 жовтня вони перестали приймати пацієнтів, за винятком найекстренніших випадків. Причиною цієї зупинки в обслуговуванні стала атака вірусу, що блокує доступ до бази даних лікарень.

…мова йде про вірус Ryuk. За даними компанії CrowdStrike, що спеціалізується на кібербезпеці, цей вірус був розроблений хакерською групою Wizard Spider з Росії у 2018 році…» ***(Російські хакери заблокували роботу лікарень в США // 1NEWS (https://1news.com.ua/svit/rosijski-hakery-zablokuvaly-robotu-likaren-v-ssha.html_. 07.10.2019).***

***

«…Американська компанія Microsoft заявила про виявлення імовірно пов'язаної з іранським урядом хакерської групи, яка має на меті втручання в президентську кампанію в США. Серед інших цілей, як указує Microsoft, також є американські високопосадовці, засоби інформації та відомі іранці-емігранти…

Атаки групи, яку в Microsoft називають Phosphorous, спостерігалися впродовж 30 днів у період від серпня до вересня.

За даними віцепрезидента Microsoft з безпеки Тома Барта, хакерам удалося зламати чотири акаунти з 241 облікового запису, в роботу яких зловмисники намагалися втрутитися.

Уточнюється, що жоден з цих акаунтів не належав колишнім або чинним американським чиновникам і не був пов'язаний з виборчою кампанією…» ***(Microsoft зафіксувала атаки хакерів з Ірану // Українські медійні системи (https://glavcom.ua/world/observe/microsoft-zafiksuvala-ataki-hakeriv-z-iranu-630333.html). 05.10.2019).***

***

«Экспертный центр безопасности компании Positive Technologies представил анализ деятельности группы TA505. За последние полгода она резко усилила свою активность, атаковав по меньшей мере 26 компаний, нарастила ресурсы и стала использовать более сложные техники для сокрытия своего присутствия. (Специалисты выявили вредоносную активность группы в 64 странах. Подтвержденные данные о конкретных целях есть в 26 случаях). Среди целей – крупнейшие финансовые, производственные и транспортные компании, государственные структуры. Группировка атакует организации из Великобритании, Канады, США, Южной Кореи и десятков других стран.

Для проникновения в сети компаний-жертв группа использует фишинговые письма. С каждой новой волной атак злоумышленники привносят качественные изменения в свой инструментарий. С июня новые загрузчики вредоносной программы FlawedAmmyy существенно отличаются от предыдущих версий. Исследователи Positive Technologies изучили алгоритм распаковки этого вредоносного ПО: это поможет лучше атрибутировать активность группы и обнаруживать другие образцы ее инструментов, в том числе с новым набором функций. Так, ключевой части распаковщика предшествует изобилие бесполезных инструкций – к такой технике часто прибегают вирусописатели, чтобы сбить с толку эмуляторы антивирусных продуктов.

TA505 – одна из немногих групп, которые могут похвастаться активной деятельностью на протяжении долгого времени. С 2014 г. в их арсенале числятся банковский троян Dridex, ботнет Neutrino, а также целая серия шифровальщиков – Locky, Jaff, GlobeImposter и др. С весны 2018 г. группа использует remote access tool – FlawedAmmyy, а с конца прошлого года применяет новый бэкдор ServHelper.

«Обычно группа атакует тех, у кого можно украсть деньги. Однако в последние полгода она стала проявлять интерес к интеллектуальной собственности, которую можно монетизировать, – отсюда новые отрасли в списке мишеней. По совокупности признаков (частоте атак, географическому охвату, разнообразию целей, сложности инструментария) группу TA505 можно назвать наиболее опасной в последние полгода», – отмечает Алексей Новиков, директор экспертного центра безопасности компании Positive Technologies.

В 2019 г., кроме финансовых и государственных учреждений, мишенями TA505 стали исследовательские институты, энергетическая промышленность, компании из авиационной сферы, здравоохранения и других отраслей.» ***(Киберггруппа TA505 совершенствует инструментарий и активизирует деятельность // Компьютерное Обозрение***

(https://ko.com.ua/kibergruppa_ta505_sovershenstvuet_instrumentarij_i_aktiviziruet_deyatelnost_130385). 04.10.2019).

***

«Фирма кибербезопасности Imperva 10 октября представила подробный отчёт об инциденте, о котором она впервые сообщила два месяца назад, в августе. Согласно результатам её расследования, этот прорыв защиты стал возможен из-за того, что хакер похитил API-ключ Amazon Web Services (AWS) с внутреннего сервера, к которому по случайности был оставлен открытый доступ через Интернет.

Imperva не предоставила хронологии событий, поэтому в точности неизвестно, как долго взломщик имел доступ к серверам компании. Однако, она сообщила, что где-то в октябре 2018 г. хакер начал загружать копию снимка базы данных, которую Imperva выгрузила в тестовых целях на свой эккаунт AWS RDS.

По словам гендиректора Imperva Криса Хилена (Chris Hylen), о взломе стало известно спустя несколько месяцев, 20 августа 2019 года, когда третье лицо связалось с компанией, предоставив копию украденных данных, и запросило вознаграждение за обнаружение проблемы с защитой. Руководство Imperva не уточняет, был ли это законопослушный эксперт кибербезопасности или хакер, сам взломавший защиту этой компании.

В августовском сообщении блога, Imperva не говорила и о том сколько пользователей оказались затронуты этим происшествием. В этот раз Хилен смог предоставить приблизительные оценки. Он заявил, что после оповещения пострадавших, клиенты сменили 13 тысяч паролей, заново получили более 13500 сертификатов SSL и повторно сгенерировали свыше 1400 API-ключей Imperva.

В зону риска в результате инцидента попали только клиенты, зарегистрировавшиеся в Imperva до 15 сентября 2017 года — именно этим числом датируется образ базы данных, который компания выгрузила на тестовый эккаунт AWS RDS.

Imperva утверждает, что повторение этого прорыва более невозможно, поскольку компания в рамках независимого апгрейда безопасности по умолчанию переместила все свои внутренние вычислительные инстансы под защиту VPN.» ***(Причиной кражи данных Imperva стал случайно оставленный открытым внутренний сервер // Компьютерное Обозрение (https://ko.com.ua/prichinoj_krazhi_dannyh_imperva_stal_sluchajno_ostavlennyj_otkrytym_vnutrennij_server_130464). 11.10.2019).***

***

«Эксперты компании Positive Technologies проанализировали тактики и техники десяти APT-группировок, атаковавших финансовые компании за последние два года, и выяснили, что каждая из них прибегает к фишингу, а в поисках банковских систем в сети преступники используют легитимные утилиты для администрирования и скомпрометированные учетные данные.

Исследователи рассказали о техниках, которые используют APT-группировки, чтобы проникнуть в инфраструктуру финансовых компаний, и как

они действуют внутри, а также выяснили, на каких этапах можно выявить атаку и предотвратить кражу денег.

Самым распространенным и эффективным способом проникновения во внутреннюю сеть любой компании эксперты назвали фишинг. «По нашим данным, 75% банков уязвимы к фишинговым атакам, – говорит старший аналитик компании Positive Technologies Екатерина Килюшева. – Этот метод настолько зарекомендовал себя среди киберпреступников, что к нему прибегала каждая исследованная нами APT-группировка, замеченная в атаках на кредитно-финансовую сферу».

По статистике, в течение нескольких дней, а иногда и недель злоумышленники изучают сеть, готовясь к краже. Преступники активно перемещаются между узлами сети в поисках банковских систем, используя легитимные утилиты для администрирования (техники service execution и Windows admin shares) и скомпрометированные учетные записи. По мнению специалистов, именно на этом этапе злоумышленники оставляют множество следов, и можно заметить подозрительные действия в системе. Постоянный мониторинг событий ИБ, а также глубокий анализ сетевого трафика в реальном времени и в ретроспективе могут распознать APT-атаку до того, как преступники получат доступ к банковским системам.

Согласно данным опроса, в некоторых финансовых организациях используются лишь базовые средства защиты, которых недостаточно для своевременного выявления сложных целенаправленных атак и полноценного анализа произошедших событий. Лишь 22% респондентов, представляющих финансовую отрасль, считают, что их компания в состоянии отразить атаки APT-группировок. При этом 63% респондентов на практике сталкивались с последствиями кибератак, и 34% признали, что организация понесла прямые финансовые потери.» ***(APT-группировки активно используют фишинг для атак на кредитно-финансовые организации // Компьютерное Обозрение (https://ko.com.ua/apt-gruppirovki_aktivno_ispolzuyut_fishing_dlya_atak_na_kreditno-finansovye_organizacii_130468). 11.10.2019).***

***

«Киберпреступная группировка FIN7 вооружилась новыми инструментами BOOSTWRITE и RDFSNIFFER. Исследователи из команды Mandiant компании FireEye обнаружили несколько образцов нового вредоносного дроппера, названного BOOSTWRITE, способного загружать бэкдор Carbanak и троян для удаленного доступа (RAT) RDFSNIFFER.

Полезная нагрузка RDFSNIFFER была разработана для внедрения в работу клиента Aloha Command Center производителя банкоматов и платежных терминалов NCR Corporation. Aloha Command Center представляет набор инструментов удаленного администрирования, предназначенный для управления и исправления проблем на системах обработки платежных карт, на которых запущен Command Center. Вредоносная программа загружается в тот же процесс, что и Command Center, нарушая порядок загрузки DLL-библиотеки легитимной утилиты Aloha.

Недавно обнаруженный RAT попадает на скомпрометированные системы после того, как загрузчик BOOSTWRITE расшифровывает встроенную полезную нагрузку, используя при запуске ключи шифрования от операторов. BOOSTWRITE использует технику перехвата поиска DLL (DLL Search Order Hijacking) для загрузки собственных вредоносных DLL-библиотек в память зараженной системы, а затем загружает вектор инициализации и ключ, необходимый для дешифрования встроенных полезных нагрузок.

Один из образцов BOOSTWRITE был подписан цифровым сертификатом, выданным компанией MANGO ENTERPRISE LIMITED.

«Используя доверие, предоставляемое цифровыми сертификатами, FIN7 увеличивает свои шансы обойти различные меры безопасности и успешно скомпрометировать системы жертв», — отмечают исследователи.

Вредонос RDFSNIFFER позволяет преступникам «перехватывать установки Aloha Command Center и взаимодействовать с целевыми системами посредством существующих легитимных процессов двухфакторной авторизации». RDFSNIFFER загружается в процесс RDFClient каждый раз, когда на скомпрометированных компьютерах запускается легитимное программное обеспечение. Вредонос может отслеживать или изменять соединения, созданные с помощью RDFClient, предоставляя операторам возможность осуществлять MitM-атаки (Man-In-The-Middle), а также содержит бэкдор, позволяющий злоумышленнику загружать, скачивать, выполнять и удалять произвольные файлы.

Несмотря на то, что один из лидеров FIN7 признал себя виновным в мошенничестве, киберпреступная группировка все еще активна и продолжает пополнять свой арсенал новым предоносным ПО.» ***(Преступники из FIN7 загружают вредонос RDFSNIFFER в ПО производителя банкоматов // SecurityLab.ru (https://www.securitylab.ru/news/501749.php). 14.10.2019).***

***

«Команда исследователей безопасности из компаний Malwarebytes и HYAS обнаружила связь между киберпреступными группировками Magecart Group 4 и Cobalt. Согласно результатам анализа, Group 4 проводит скимминг не только на стороне клиента, но, вероятно, продолжает делать то же самое на сервере.

Magecart — термин, объединяющий больше десятка киберпреступных группировок, специализирующихся на внедрении скриптов для хищения данных банковских карт в платежных формах на сайтах. Они ответственны за атаки на такие компании, как Amerisleep , MyPillow , Ticketmaster , British Airways , OXO и Newegg .

Group 4 является одной из наиболее «продвинутых» группировок. Ее участники используют сложные методы для маскировки в трафике, например, с помощью регистрации доменных имен, связанных с аналитическими компаниями или рекламодателями. Группа имеет опыт работы с банковскими вредоносными программами, так же как и группировка Cobalt.

Исследователи отслеживали различные группы Magecart, искали элементы их инфраструктуры, а также связи между доменами и IP-адресами. На основе индикаторов компрометации, зарегистрированных доменов, использованных

тактик, методов и процедур исследователи пришли к выводу, что Cobalt, возможно, перешла на web-скимминг.

Домены, с которых загружались скимеры, были зарегистрированы на почтовый адрес в сервисе ProtonMail, который исследователи из RiskIQ ранее связали с Magecart. Проанализировав данные, специалисты связали данный адрес с другими регистрационными письмами и обнаружили общий характер, в частности, при создании почтовых ящиков использовался шаблон [имя], [инициалы], [фамилия], который Cobalt недавно использовала для учетных записей в ProtonMail.

При анализе инфраструктуры Group 4, исследователи обнаружили PHP-скрипт, который был ошибочно принят за JavaScript-код. Подобный тип исходного кода можно увидеть лишь при наличии доступа к серверу, скрипт взаимодействует исключительно с серверной частью.

«Он невидим для любого сканера, потому что все происходит на самом взломанном сервере. Скимеры Magecart обычно обнаруживались на стороне браузера, однако на стороне сервера их гораздо сложнее обнаружить», — отмечает исследователь Джером Сегура (Jerom Segura).

Дальнейшее исследование показало, что независимо от используемого сервиса электронной почты, в 10 отдельных учетных записях повторно использовались только два разных IP-адреса, даже спустя несколько недель и месяцев между регистрациями.

Одним из таких почтовых ящиков является petersmelanie@protonmail, который использовался для регистрации 23 доменов, включая my1xbet [.]top. Данный домен использовался в фишинговой кампании для эксплуатации уязвимости CVE-2017-0199 в Microsoft Office. Та же почтовая учетная запись использовалась для регистрации домена oracle-business[.]com и атак на Oracle, которые связали с группировкой Cobalt.» ***(Исследователи выявили связь между группировками Magecart Group 4 и Cobalt // SecurityLab.ru (https://www.securitylab.ru/news/501602.php). 07.10.2019).***

***

«Предположительно спонсируемая Ираном киберпреступная группировка APT35, (также известная как Phosphorus, Charming Kitten и Ajax Security Team) атаковала 241 почтовый ящик, связанный с предвыборной кампанией в США, текущими и бывшими американскими чиновниками, а также освещающими мировую политику журналистами, сообщила Microsoft, не уточняя, кто именно попал под прицел группировки.

Киберпреступники предприняли более 2700 попыток идентифицировать определенных владельцев учетных записей электронной почты, а затем атаковали 241 из них. Атаки осуществлялись в период с августа по сентябрь нынешнего года. Преступники взломали четыре учетные записи, которые не были связаны с президентской кампанией в США или действующими и бывшими должностными лицами правительства страны.

Phosphorus использовала собранную о своих жертвах информацию, в том числе телефонные номера, для сброса пароля или доступа к связанным с целевым аккаунтом учетных записей с целью дальнейшего взлома. Атаки не были

технически сложными, однако преступники использовали огромный объем личной информации как для идентификации владельцев учетных записей, так и для компрометации. По всей видимости, Phosphorus обладает высоким уровнем мотивации и готова инвестировать значительное время и ресурсы в исследования и другие способы сбора информации.» ***(Microsoft сообщила о попытке иранских киберпреступников вмешаться в ход предвыборной кампании в США // SecurityLab.ru (https://www.securitylab.ru/news/501585.php). 07.10.2019).***

***

«Специалистам компании «Лаборатория Касперского» удалось выявить киберпреступную группировку, предположительно связанную со Службой государственной безопасности Узбекистана, благодаря ошибкам, допущенным участниками подразделения, получившего название SandCat, при обеспечении собственной операционной безопасности. В частности, исследователи обнаружили ряд эксплоитов, используемых группировкой, а также вредоносное ПО, находящееся в процессе разработки, пишет издание Motherboard Vice.

Одна из сомнительных практик включала использование «названия военного подразделения, связанного с СГБ» для регистрации домена, задействованного в атаках. Кроме того, участники SandCat установили на компьютер, где разрабатывался новый вредонос, антивирус производства ЛК, что позволило экспертам обнаружить вредоносный код на стадии его создания. Еще одну ошибку группировка допустила, встроив скриншот с одного из компьютеров в тестовый файл, тем самым раскрыв крупную платформу для атак, которая находилась в разработке. Благодаря всем этим недочетам специалистам удалось выявить четыре эксплоита для уязвимостей нулевого дня, приобретенных SandCat у сторонних брокеров, а также отследить активность не только данной группировки, но и других хакерских групп в Саудовской Аравии и Объединенных Арабских Эмиратах, использующих те же эксплоиты.

В ходе проведенного исследования специалисты выявили, что IP-адреса машин, используемых для тестирования вредоносного ПО, связаны с доменом itt.uz, зарегистрированным на военную часть 02616 из Ташкента. Более того, с тех же компьютеров SandCat загружала образцы вредоносов на Virus Total.

Впервые эксперты ЛК выявили следы активности SandCat еще в 2018 году, однако в то время у них не было оснований предполагать связь группировки с СГБ. В своих операциях SandCat применяла вредонос под названием Chainshot, который также использовался группировками из Саудовской Аравии и ОАЭ. Однако в атаках SandCat была задействована другая инфраструктура, на основании чего эксперты пришли к выводу, что речь идет о разных преступниках.

По мнению экспертов, SandCat приобретала эксплоиты для атак у двух израильских компаний - NSO Group и Candiru. Обе фирмы прекратили поставлять SandCat эксплоиты в 2018 году, в результате группировка занялась разработкой собственного вредоносного ПО…» ***(Хакерское подразделение СГБ Узбекистана оказалось раскрыто из-за собственных ошибок // SecurityLab.ru (https://www.securitylab.ru/news/501570.php). 04.10.2019).***

***

«Исследователи из фирмы Context Information Security выявили новую киберпреступную группировку, получившую название Avivore, которая за последние несколько месяцев, предположительно, осуществила несколько крупных кибератак на компанию Airbus. Злоумышленники пытались атаковать Airbus через сети французской консалтинговой компании Expleo, британского производителя двигателей Rolls Royce и двух неназванных поставщиков Airbus.

Киберпреступники нацелены на крупные многонациональные и небольшие инженерные и консультационные фирмы в цепочках поставок. В рамках атак Island hopping (атаки на цепочки поставок) для проникновения в компьютерные сети злоумышленники используют связь между жертвой и ее партнерами, например, виртуальные частные сети (VPN).

«Предыдущие сообщения о недавних инцидентах, касающихся авиакосмической и оборонной промышленности, связывали их с APT10 и Министерством государственной безопасности провинции Цзянсу [Китай — прим. ред.]. Хотя характер деятельности преступников усложняет атрибуцию, анализ кампании указывает на новую группу, которую мы назвали Avivore», — сообщил главный аналитик фирмы Оливер Фэй (Oliver Fay).

По словам исследователей, группировка использует троян для удаленного доступа (RAT) PlugX, который часто применялся APT10. Тем не менее, тактики, техники и процедуры группировки, а также инфраструктура и другие инструменты существенно отличаются от китайских киберпреступников. Данный факт позволил специалистам сделать вывод, что Avivore является ранее неизвестной группировкой, спонсируемой правительством.

Преступники являются «весьма способными», так как умело используют технику под названием living-off-the-land (использование локальных приложений во вредоносных целях) и маскируют свою деятельность в повседневной деловой активности сотрудников целевых компаний. Они также соблюдают операционную безопасность и удаляют все следы во избежание обнаружения.» ***(Недавние атаки на Airbus могут быть делом рук ранее неизвестной группировки Avivore // SecurityLab.ru (https://www.securitylab.ru/news/501568.php). 04.10.2019).***

***

«Хакер под ником Gnosticplayers рассказал о взломе нескольких приложений крупнейшего американского разработчика онлайн-игр Zynga Inc. По его словам, он получил доступ к данным 218 млн игроков. Утечка затронула всех пользователей Android и iOS, которые установили игру-головоломку Words With Friends и зарегистрировались в ней до 3 сентября этого года.

Взломщик поделился с изданием The Hacker News данными нескольких аккаунтов. Судя по этим образцам, к нему попали имена пользователей, адреса электронной почты, хэшированные пароли с солью, токены сброса паролей (если их сбрасывали), номера телефонов и Facebook ID (если были указаны при регистрации), а также идентификаторы аккаунта Zynga.

Gnosticplayers добавил, что ему также удалось похитить данные пользователей Draw Something и игры OMGPOP, которая уже не поддерживается производителем. По его словам, среди информации, к которой он получил доступ, были 7 млн паролей пользователей в незашифрованном виде.

12 сентября представители Zynga опубликовали официальное заявление об утечке данных из Words With Friends и Draw Something, но не раскрыли количество пострадавших пользователей. Они сообщили, что уже начали расследование и привлекли к нему сторонних специалистов и правоохранительные органы. Также разработчики предприняли шаги для защиты учетных записей пользователей, но призвали самих игроков проявить бдительность…

Джавад Малик (Javvad Malik) из компании KnowBe4 отметил оперативную реакцию разработчика на инцидент, но заявил, что «в наши дни ни одна компания не должна хранить пароли в открытом доступе»…» ***(Julia Glazova. Хакер заявил о краже данных 218 миллионов пользователей // Threatpost (https://threatpost.ru/hacker-told-about-zynga-games-data-breach/34341/). 03.10.2019).***

***

«…Група російських хакерів під назвою Turla проникла до системи іранських кіберзлочинців OilRig, щоб шпигувати за країнами Близького Сходу.

Про це повідомив Національний центр кібербезпеки Великої Британії (NCSC).

Зазначається, що у дослідженні NCSC та Національного центру кібербезпеки США вказано, що російські хакери під виглядом іранських кіберзлочинців OilRig атакували держустанови 35 країн.

«Ми ніколи не бачили, щоб це робилося з такою майстерністю. Насправді дуже складно замаскуватися. Виявлено більш ніж 35 нападів на країни світу, причому більшість держав із Близького Сходу. Принаймні, 20 атак були успішно скомпрометовані. Мета полягала в тому, щоб вкрасти секретні документи», - розповів директор з операцій NCSC Пол Чічестер.

Поки не встановлено, чи знала група іранських хакерів OilRig про те, що Turla зламала їх мережі і скористалася даними для злому держустанов країн Близького Сходу…» ***(Російські хакери під виглядом іранських кіберзлочинців атакували держустанови 35 країн // Українські медійні системи (https://glavcom.ua/world/hitech/rosiyski-hakeri-pid-viglyadom-iranskih-kiberzlochinciv-atakuvali-derzhustanovi-35-krajin-634124.html). 21.10.2019).***

***

«Компания ESET сообщила о том, что ее специалисты обнаружили атаки группы хакеров Dukes (APT29 или Cozy Bear) на правительственные учреждения в Европе. Новая операция киберпреступников, которая получила название «Ghost», началась еще в 2013 году и продолжается до этого времени. В частности, хакеры Dukes осуществили вмешательство в информационные системы министерств иностранных дел минимум в трех странах Европы и посольства государства-члена ЕС в Вашингтоне.

Стоит отметить, что эта группа оказались в центре внимания после подозрения в причастности Dukes к кибератакам на Национальный комитет Демократической партии перед выборами в США в 2016 году. После фишинговой

кампании, направленной на правительство Норвегии, в январе 2017 года, киберпреступники, казалось бы, прекратили свою шпионскую деятельность.

Однако во время нового исследования специалисты ESET обнаружили три новых семейства вредоносных программ, связанных с Dukes — PolyglotDuke, RegDuke и FatDuke. «Одно из первых публичных указаний на эту кампанию можно найти на Reddit в июле 2014 года, — рассказывает Матье Фау, исследователь ESET. — Мы можем с высокой уверенностью подтвердить, что одна и та же группа стоит за операцией «Ghost» и атакой на Национальный комитет Демократической партии».

Причастность группы к этим атакам базируется на нескольких похожих элементах тактики этой и предыдущих кампаний группы. В частности, группа использовала Twitter и Reddit для распространения URL-адресов командного сервера и применяла стеганографии в картинках, чтобы скрыть вредоносные компоненты или команды. Кроме этого, два из трех атакованных министерств были предварительно скомпрометированы. По крайней мере, на одной машине был инсталлятор от группы Dukes, который был установлен еще несколько месяцев назад. Еще одним доказательством причастности группы является большое сходство кода между выявленными ранее образцами и операцией «Ghost»…» ***(Группа хакеров Dukes атакует правительственные учреждения // Компьютерное Обозрение (https://ko.com.ua/gruppa_hakerov_dukes_atakuet_pravitelstvennye_uchrezhdeniya_130543). 18.10.2019).***

***

«Специалисты экспертного центра безопасности Positive Technologies (PT Expert Security Center) выявили APT-группировку , получившую название Calypso. Группировка действует с 2016 года и нацелена на государственные учреждения. На данный момент она действует на территории шести стран.

По данным экспертов, от действий группировки уже пострадали организации из Индии (34% жертв), Бразилии, Казахстана (по 18%), России, Таиланда (по 12%) и Турции (6%). Злоумышленники взламывали сетевой периметр и размещали на нем специальную программу, через которую получали доступ к внутренним сетям скомпрометированных организаций. Как показало расследование, злоумышленники продвигаются внутри сети либо с помощью эксплуатации уязвимости удаленного исполнения кода MS17-010 , либо с помощью украденных учетных данных.

«Успеху атак этой группировки во многом способствует тот факт, что большинство утилит, применяемых ею для продвижения внутри сети, широко используются специалистами по всему миру для сетевого администрирования, — рассказал ведущий специалист группы исследования киберугроз Денис Кувшинов. — Группировка использовала общедоступные утилиты и эксплойты, например SysInternals [1], Mimikatz [2]; EternalBlue , EternalRomance[3]. При помощи распространенных эксплойтов преступники заражают компьютеры в локальной сети организации и похищают конфиденциальные данные».

По словам специалистов Positive Technologies, организация может предотвратить такие атаки при помощи специализированных систем глубокого

анализа трафика , которые позволят вычислить подозрительную активность на начальной стадии проникновения злоумышленников в локальную сеть и не дадут им закрепиться в инфраструктуре компании. Кроме того, обнаружить атаки и противодействовать им помогут мониторинг событий ИБ , защита периметра и веб-приложений.

Согласно полученным данным, выявленная APT-группировка предположительно имеет азиатские корни и относится к числу китайскоговорящих. В одной из атак группировка использовала вредоносную программу PlugX, которую традиционно используют многие APT-группы китайского происхождения, а также троян Byeby, который применялся во вредоносной кампании SongXY в 2017 году. Кроме того, во время отдельных атак злоумышленники по ошибке раскрывали свои реальные IP-адреса, принадлежащие китайским провайдерам…» ***(Расследование Positive Technologies: новая APT-группировка атакует госучреждения в разных странах мира // SecurityLab.ru (https://www.securitylab.ru/news/502220.php). 31.10.2019).***

***

«Перед летней Олимпиадой-2020 в Токио APT-группа Fancy Bear (она же APT28) снова взялась атаковать антидопинговые агентства и спортивные организации по всему миру.

Как сообщают специалисты Microsoft, вредоносная кампания началась 16 сентября и была нацелена как минимум на 16 национальных и международных спортивных и антидопинговых организаций на трех континентах. Хотя некоторые атаки и увенчались успехом, большинство оказались провальными.

В ходе новой кампании Fancy Bear использует свои стандартные техники. К таковым в частности относятся: целенаправленный фишинг, так называемое «распыление» паролей или password spraying (попытка взлома учетной записи, когда к одному распространенному паролю привязывается множество имен пользователей), эксплуатация уязвимостей в подключенном к интернету оборудовании, а также использование вредоносного ПО с открытым исходным кодом наряду с кастомными программами.

Microsoft уведомила об атаках всех затронутых клиентов и сотрудничает с теми, кто желает защитить скомпрометированные учетные записи и системы. Названия атакованных организаций компания не раскрывает…» ***(APT-группа Fancy Bear начала подготовку к Олимпиаде в Токио // SecurityLab.ru (https://www.securitylab.ru/news/502107.php). 29.10.2019).***

***

«В течение последней недели некая киберпреступная группировка осуществляет DDoS-атаки на компании финансового сектора и требует выкуп. При этом злоумышленники выдают себя за печально известную APT-группу Fancy Bear, обвиняемую во взломе Демократической партии США в 2016 году. Компании Link11 и Radware, предоставляющие защиту от DDoS-атак, подтвердили изданию ZDNet факт вымогательства.

По словам исследователя Radware Дэниела Смита (Daniel Smith), группировка осуществляет «масштабные мультивекторные демонстрационные

DDoS-атаки, отправляя жертвам письмо с требованием выкупа». По мнению исследователей, эти демо-атаки являются своего рода предупреждением и призваны убедить жертву заплатить выкуп.

Сумма, требуемая вымогателями, составляет 2 биткойна (около $15 тыс.). Если жертва не уплатит выкуп в течение недели, киберпреступники угрожают превратить демо-атаки в реальные. На момент обнаружения вымогательства никаких последующих полномасштабных атак зафиксировано не было, сообщил Смит.

Для демо-атак киберпреступники используют совокупность протоколов DNS, NTP, CLDAP, ARMS и WS-Discovery. Примечательно, что злоумышленники атакуют не публичные сайты компаний, а конечные серверы, на которых защита от DDoS-атак как правило отсутствует.» ***(У APT-группы Fancy Bear появились подражатели // SecurityLab.ru (https://www.securitylab.ru/news/502063.php). 25.10.2019).***

***

«Исследователи безопасности из компании Malwarebytes обнаружили связь между группировкой Magecart Group 5, фишинговыми кампаниями с использорванием банковского трояна Dridex и группировкой Carbanak.

Банковский троян Dridex был впервые обнаружен в 2014 году, пик его активности пришелся на 2014-2015 годы, а в 2016-2017 годах исследователи зафиксировали спад количества операций, осуществляемых с помощью данного вредоноса. Он до сих пор продолжает распространяться через вредоносные спам-кампании с использованием поддельных счетов.

Исследователи проанализировали домены Magecart, зарегистрированные через известный китайский «пуленепробиваемый» регистратор BIZCN/CNOBIN. Преступники зарегистрировали несколько доменов для своих вредоносных кампаний, используя сервисы, обеспечивающие конфиденциальность, однако не обеспечили защиту всех своих записей. Таким образом специалистам удалось выявить несколько вредоносных доменов, зарегистрированных на адрес guotang323@yahoo.com, ранее засветившимся как в атаках Magecart, так и во вредоносных кампаниях с использованием Dridex.

Еще одним интересным моментом в данных регистратора informaer.info является номер телефона, который упоминается специалистом Брайаном Кребсом (Brian Krebs) в материале о связи между российской охранной фирмой и группой Carbanak…» ***(Обнаружена возможная связь между Magecart Group 5 и группировкой Carbanak // SecurityLab.ru (https://www.securitylab.ru/news/501987.php). 23.10.2019).***

***

«Инструменты для нацеленной на криптовалютных инвесторов масштабной фишинговой атаки MasterMana Botnet обошлись всего в $160. Об этом говорится в исследовании компании по кибербезопасности Prevailion.

MasterMana Botnet массово рассылает электронные письма от имени существующих фирм с инфицированным файлом. Как только жертва открывает его, запускается цепочка действий, усложняющих обнаружение вируса. В итоге на компьютер устанавливается бесфайловый бэкдор для получения удаленного доступа.

Вредоносный код хакеры внедряют в файлы Microsoft Office, включая Word, Excel, PowerPoint и Publisher. Для опустошения кошельков они используют ПО Azorult, которое крадет личные данные и пароли.

По данным Prevailion, кампания MasterMana Botnet началась в декабре 2018 года. По состоянию на 24 сентября она оставалась активной. За текущий год ботнет взаимодействовал примерно с 72 000 устройств.

Стоимость аренды на год виртуального выделенного сервера (VPS) оценивается в $60, а троян Azorult в начале года продавался на российских хакерских форумах за $100…» ***(Масштабная фишинговая атака обошлась хакерам всего в $160 // LetKnow News (https://letknow.news/news/masshtabnaya-fishingovaya-ataka-oboshlas-hakeram-vsego-v-160-30777.html). 04.10.2019).***

***

«Злоумышленники используют файлы .odt для того, чтобы прятать различные троянцы от антивирусов, а также задействуют аналог макросов, унаследованный от StarOffice, чтобы заражать целевые системы различными вредоносами…

Неизвестная APT-группировка начала использовать документы LibreOffice для доставки вредоносного ПО. Причем речь идет не о каких-то экзотических вредоносах, а о вполне общеизвестных программах, с которыми обычно легко расправляются антивирусы. Однако документы формата .odt, как ни странно, обеспечивают рассылаемым троянцам эффективное прикрытие.

Файл формата .odt (или, шире, .odf — OpenDocument Format) представляет собой ZIP-архив: он включает в себя файловую иерархию, содержащую XML-файл самого документа, файлы включений (например, картинок или активных элементов), вспомогательные файлы с метаинформацией, картинку-миниатюру страницы документа и т. д.

Некоторые антивирусные решения рассматривают odf/odt-файлы как стандартные архивы и не проверяют их содержимое. Тем самым у злоумышленников появляется возможность «провозить контрабандой» вредоносы на целевую систему.

К тому же, как отмечают в Cisco Talos, информация о том, какие организации перешли на LibreOffice, публикуется в общем доступе, и злоумышленники легко могут использовать это в своих целях…

Одна из выявленных исследователями из Cisco Talos киберкриминальных кампаний, как выяснилось, использовала файлы .odt для атак на пользователей Microsoft Office (который вполне способен открывать файлы этого формата, наряду с «родными»). В документы формата .odt внедрялись активные OLE-объекты, которые запускали исполняемые файлы HTA, а те, в свою очередь, скачивали либо RevengeRAT, либо njRAT, два популярных у киберзлоумышленников троянца для удаленного управления зараженной системой.

В другом случае с помощью ODT-файла в систему устанавливался крадущий данные троянец AZORult. Процесс установки включал OLE-объект, который выгружал запускаемый файл, якобы относившийся к музыкальному сервису Spotify.

Была также отмечена серия атак на пользователей OpenOffice и LibreOffice, в ходе которой, по выражению экспертов Talos, использовался «эквивалент макросов в Microsoft Office, использовавшийся в открытой платформе StarOffice Basic.

StarOffice — старый офисный пакет, последняя версия которого вышла в 2008 г. Однако именно его исходники — и, соответственно, код, отвечающий за аналог макросов, — легли в основу OpenOffice.org, предшественника Apache OpenOffice.

Исследователи обнаружили, что злоумышленники встраивают в файлы OpenOffice макросы, которые используются для скачивания и запуска файла plink443.exe, устанавливающего SSH-соединения. Смысл этого, правда, остается неясным, поскольку для скачивания других вредоносов оно не использовалось.

Что касается других вредоносных программ, то это преимущественно эксплойты из набора Metasploit. По мнению экспертов Talos, хакеры пытаются обеспечить себе возможность перемещаться по всей локальной сети атакованной организации…». ***(Найден способ удаленно взламывать ПК с помощью LibreOffice // Goodnews.ua (http://goodnews.ua/technologies/najden-sposob-udalenno-vzlamyvat-pk-s-pomoshhyu-libreoffice/). 06.10.2019).***

***

«Команда исследователей из Cisco Talos обнаружила сайт checkrain[.]com, который маскируется под официальный сайт checkra1n для загрузки джейлбрейка. Однако вместо этого, вредоносный сайт checkrain побуждает посетителей загружать приложение, которое нажимает на опасную рекламу и устанавливает видеоигры для iOS.

На фальшивой странице checkrain загружается игровой автомат под названием «POP! Slots», который побуждает пользователю использовать приложение в течение семи дней, чтобы гарантировать работу джейлбрейка. Таким образом пользователь на протяжении всего игрового процесса совершает ненужные взаимодействия, предоставляя дополнительный доход преступникам. В то же время, похоже, происходит установка настоящего checkra1n…

Джейлбрейк – процесс, который проводится на устройствах на базе iOS и позволяет открыть программному обеспечению полный доступ к файловой системе мобильного устройства. Он позволяет расширить возможности гаджета, например, устанавливать стороннее ПО, которое не предусмотрено в App Store.» ***(Мошенники***

с помощью джейлбрейка для iOS заражают жертв вредоносным ПО // SecurityLab.ru (https://www.securitylab.ru/news/501795.php). 16.10.2019).

***

«Киберпреступная группировка Turla (также известна как Venomous Bear или Waterbug) распространяет новое вредоносное ПО, получивший название Reductor, для перехвата зашифрованного TLS-трафика и заражения целевой сети. По словам исследователей из «Лаборатории Касперского», между Reductor и ранее обнаруженным трояном COMPfun есть сходство, указывающее на общего создателя. Как считают эксперты, троян COMPfun, предположительно разработанный Turla, используется в качестве загрузчика.

Злоумышленники применяют два разных метода для распространения Reductor. В первом варианте они используют установщики зараженного программного обеспечения с встроенными 32- и 64-разрядными версиями Reductor. Данные установщики могут быть представлены такими популярными программами, как Internet Download Manager, WinRAR, пиратские сайты и пр.

Во втором сценарии цели уже заражены трояном COMpfun, который использует атрибут COM CLSID для достижения персистентности на системе. Получив доступ к адресной строке браузера, троян может выполнить команду на загрузку дополнительных модулей с C&C-сервера, в том числе дроппер/расшифровщик Reductor.

Вредонос добавляет цифровые сертификаты из своего раздела на целевой хост и предоставляет операторам возможность добавлять дополнительные сертификаты удаленно через именованный канал (named pipe). Авторы вредоноса разрывают TLS-рукопожатие без перехвата интернет-трафика. Вместо этого они анализируют исходный код браузеров Mozilla Firefox и бинарный код Google Chrome для исправления соответствующих функций генерации псевдослучайных чисел (ГПСЧ) в памяти процесса. Браузеры используют ГПСЧ для генерации «случайной клиентской» последовательности для сетевого пакета в самом начале TLS-рукопожатия. Reductor добавляет зашифрованные уникальные аппаратные и программные идентификаторы для жертв в поле «случайный клиент». Для исправления функций системы ГПСЧ разработчики использовали небольшой встроенный дизассемблер длины команд от Intel.

«Вредоносное ПО не выполняет MitM-атаку. Однако изначально мы полагали, что установленные сертификаты могут способствовать атакам MitM на TLS-трафик, и поле «случайный клиент» с уникальным идентификатором в рукопожатии будет идентифицировать интересующий трафик. Дальнейший анализ подтвердил наши догадки», — сообщают исследователи.

Согласно данным телеметрии, злоумышленники уже имели некоторый контроль над сетевым каналом жертвы, благодаря которому они заменяли вредоносный установщик легитимным.

«Все сообщения C&C-сервера обрабатываются в отдельном потоке. Редуктор отправляет HTTP POST-запросы с уникальным идентификатором оборудования цели, зашифрованный с помощью AES 128, скриптам /query.php на C&C-сервере, указанным в его конфигурации», — поясняют исследователи.

Вредоносная программа получает команды с C&C-сервера для выполнения различных операций, которые включают скачивание и загрузку файлов, поиск имени хоста, обновление установленного цифрового сертификата, создание нового процесса, удаление пути к файлу, проверку подключения к интернету и пр…» ***(Группировка Turla использует новое вредоносное ПО для перехвата TLS-трафика // SecurityLab.ru (https://www.securitylab.ru/news/501571.php). 04.10.2019).***

***

«Исследователи из Чешского технического университета, Национального университета Куйо (Аргентина) и компании Avast обнаружили один из крупнейших банковских ботнетов, получивший название Geost. Жертвами вредоносной кампании стали по меньшей мере 800 тыс. владельцев Android-устройств в РФ, в частности злоумышленники получили доступ к их банковским счетам, на которых в общей сложности хранилось несколько миллионов евро.

По словам исследователей, ботнет мог остаться незамеченным, если бы не ошибки в операционной безопасности (OpSec) киберпреступников, включая использование незашифрованных журналов чата, обнаруженных в ходе расследования, и незащищенной прокси-сети, которая не смогла обеспечить анонимность.

«Редкая цепь ошибок в OpSec привела к обнаружению нового банковского Android-ботнета. Необычное открытие было сделано, когда преступники решили довериться прокси-сети, созданной вредоносным ПО HtBot. HtBot предлагает в аренду прокси-сервис, предоставляющий пользователям псевдоанонимное общение в Интернете. Анализ сетевого взаимодействия HtBot привел к обнаружению и раскрытию крупной вредоносной операции», — пояснили исследователи.

HtBot работает, превращая жертв в частные незаконные интернет-прокси. Зараженные жертвы передают сообщения от пользователей HtBot в Интернет. Трафик постоянно перенаправляется новым жертвам, что затрудняет отслеживание.

Киберпреступники также не смогли зашифровать свои сообщения, позволив исследователям наблюдать за их действиями. Информация включала технические подробности обращения к серверам, ввод новых устройств в ботнет, методы уклонения от антивирусных решений и подробности об отношениях между злоумышленниками. Специалисты выяснили, что операторы более низкого ранга отвечают за ввод устройств в ботнет, а высокого — определяют, сколько денег находится под их контролем.

Ботнет Geost состоит Android-устройств, инфицированных через вредоносные и фальшивые программы, включая поддельные банковские приложения и социальные сети. После заражения телефоны подключаются к ботнету и управляются удаленно. Как пояснили исследователи, злоумышленники могут получать доступ и отправлять SMS-сообщения, осуществлять общение с банками и перенаправлять трафик телефона на разные сайты. Ботнет мог напрямую подключаться к пяти крупнейшим банкам России для работы и разворачивать более 200 Android APK для фальсификации десятков приложений.

Команда исследователей связалась с затронутыми российскими банками и вместе с ними принимает меры по обезвреживанию вредоносной кампании.» ***(Банковский ботнет Geost инфицировал как минимум 800 тыс. Android-устройств в РФ // SecurityLab.ru (https://www.securitylab.ru/news/501544.php). 03.10.2019).***

***

«Исследователи Confiant опубликовали новые сведения об обнаруженной ранее кампании по распространению вредоносной программы-дроппера OSX/Shlayer. Как выяснили специалисты, с ее помощью злоумышленники заражают пользователей macOS трояном Tarmac и используют продвинутые методы, чтобы скрыть свою активность.

Впервые о Shlayer стало известно в феврале 2018 года, когда эксперты обнаружили вредоносный код внутри magnet-ссылок на торрент-трекерах. Кликнувшие по ним пользователи macOS получали троян-дроппер Shlayer, замаскированный под обновление Adobe Flash Player и загружающий рекламное ПО.

В январе этого года Shlayer был обнаружен в ходе масштабной malvertising-кампании — он загружался на машины жертв после отработки JavaScript-кода, внедренного в рекламные баннеры. На тот момент было установлено, что Shlayer по-прежнему устанавливает на машины жертв adware-программы. По оценкам аналитиков, число жертв вредоносной кампании на тот момент приблизилось к миллиону, а рекламодатели ежедневно теряли от преступной активности более миллиона долларов.

Дальнейшее исследование показало, что преступники также используют распространяемый таким образом дроппер для доставки другой полезной нагрузки — неизвестного ранее зловреда OSX/Tarmac.

Собранные экспертами улики говорят о профессионализме организаторов Shlayer-кампаний. Ложное обновление Adobe Flash Player подписано действительным сертификатом Apple, что должно усыпить бдительность жертвы. В свою очередь, полезная нагрузка скачивается через команду curl в «Терминале», и файл разворачивается на машине, минуя встроенный карантин, а также проверки защитных систем Gatekeeper и XProtect. Более того, Shlayer таким образом получает возможность распаковать целевой вредоносный пакет с привилегиями администратора…

Эксперты получили устаревшие образцы Tarmac — управляющая инфраструктура, от которой зловред ожидает команд, уже отключена. Тем не менее аналитики изучили внутреннее устройство трояна и получили представление о его возможностях.

Создатели новой вредоносной программы максимально запутали код и вычистили из него большую часть информации, которую можно использовать в расследовании. Ключевые данные, включая наименования методов и классов, команды и сообщения об ошибках, оказались сжаты и зашифрованы. Собственный алгоритм на базе ассиметричной и симметричной криптографии защищает от взлома весь обмен данными с управляющим сервером.

Чтобы снизить шанс обнаружения, преступники старались использовать встроенные в macOS криптобиблиотеки и фреймворки. С этой же целью они не наделили Tarmac способностью закрепляться на зараженном компьютере.

Тем не менее аналитики выяснили, что зловред умеет загружать, распаковывать и запускать сторонние приложения. Что это за полезная нагрузка, пока неизвестно: поскольку управляющие серверы Tarmac сейчас недоступны, имеющиеся у экспертов образцы лишь отправляют на нерабочий адрес данные пораженной машины и уходят в режим ожидания.

Текущие атаки направлены против пользователей в Италии, США и Японии. По мнению экспертов, охота на итальянских пользователей, несвойственная киберпреступникам, может говорить о том, что злоумышленники нашли там уязвимую точку, которая открывает доступ к нужной цели.

Поскольку использованный преступниками метод позволяет обходить защиту macOS, аналитики рекомендуют пользователям этой системы проявлять особую осторожность при скачивании файлов из Интернета.» ***(Egor Nashilov. Пользователям macOS угрожает новый троян Tarmac // Threatpost (https://threatpost.ru/tarmac-malware-for-macos/34508/). 15.10.2019).***

***

«Специалисты компании Adaptive Mobile опубликовали список стран, чьи мобильные пользователи уязвимы для атаки Simjacker, эксплуатирующей недостатки вшитых в SIM-карты программ. По мнению экспертов, большинство операторов, использующих ненадежные чипы, работает в Центральной и Южной Америке, а также в Африке.

Атака Simjacker эксплуатирует уязвимости в программе S@T Browser, которая предназначена для обработки служебных запросов. Злоумышленник мог отправить на устаревшую SIM-карту специальное сообщение и получить в ответ идентификатор телефона, планшета или умных часов, а также данные об их местоположении. Такая атака не требует действий от владельца мобильного устройства и осуществляется при помощи недорогого GSM-модема…

Специалисты опубликовали перечень из 29 стран, чьи операторы связи используют ненадежную технологию. Среди них присутствуют как небольшие государства с относительно слабо развитой инфраструктурой связи, так и лидеры регионов.

В списке уязвимых государств оказались Бразилия, Мексика, Аргентина и Италия. Среди европейских стран эксперты также обратили внимание на Кипр и Болгарию. В России и на постсоветском пространстве проблемные SIM-карты не применяются.

Наибольшее беспокойство экспертов вызывают реальные атаки с применением Simjacker. ИБ-специалисты выявили три страны, где замечены подобные инциденты, — это Мексика, Перу и Колумбия. За месяц аналитики зафиксировали более 25 тыс. запросов в адрес 1500 абонентов. Как заявили эксперты, большая часть жертв – 45% — подвергались атаке единожды, но некоторые пользователи получили тысячи вредоносных посланий.

Исследователи не сообщают, кто стоит за кампанией Simjacker, однако утверждают, что в ней задействовано более 70 устройств для отправки SMS.

Большая их часть использовалась довольно редко, в то время как более 40% сообщений передано с трех GSM-модемов.

В конце сентября стало известно, что получить конфиденциальные данные о мобильном устройстве можно не только через запрос к S@T Browser. Аналогичная уязвимость присутствует в служебном браузере WIB (Wireless Internet Browser), также вшитом в некоторые SIM-карты. По мнению специалистов Adaptive Mobile, масштаб этой проблемы несравним с Simjacker — вредоносная технология, получившая название WIBattack, угрожает лишь абонентам восьми операторов сотовой связи из семи стран.» ***(Egor Nashilov. Операторы связи в 29 странах уязвимы для атак Simjacker // Threatpost (https://threatpost.ru/simjacker-threatens-29-countries/34498/). 15.10.2019).***

***

«Специалисты в сфере информационной безопасности обнаружили необычную вредоносную программу, нацеленную на русскоязычных пользователей. Приложение было названо Attor, оно имеет модульную структуру и предназначено для похищения информации. Эксперты предполагают, что зловред ориентирован на сотрудников дипломатических миссий и правительственных учреждений.

Как выяснили аналитики, командный сервер Attor размещен в защищенном пространстве сети TOR. Центральный компонент зловреда — диспетчер — отвечает за загрузку и установку плагинов, определяющих функциональность каждого конкретного экземпляра программы.

Они хранятся на диске в закодированном и сжатом виде и расшифровываются непосредственно в памяти целевой машины при помощи открытого ключа RSA, встроенного в диспетчер. Такой механизм затрудняет анализ — по словам исследователей, им понадобилось около года, чтобы восстановить восемь модулей шпиона.

Специалисты обнаружили следующие плагины Attor:

модуль записи звука;

компонент для загрузки файлов;

кейлоггер и программа перехвата буфера обмена;

утилита для создания скриншотов;

монитор устройств;

прокси-сервер;

установщик полезной нагрузки;

TOR-клиент.

Наибольший интерес экспертов вызвал модуль мониторинга, который создавал цифровой отпечаток подключенных к компьютеру модемов, мобильных телефонов и жестких дисков. Программа отправляла устройствам AT-команды и копировала номера IMEI, идентификаторы IMSI и другие метаданные. Несмотря на то что AT-инструкции поддерживаются современными смартфонами, вредоносный модуль игнорировал подключения через USB и начинал работу, только получив сигнал через COM-порт.

По мнению специалистов, такое поведение программы обусловлено тем, что преступники охотились за данными небольшой группы жертв, которые намеренно

пользуются для связи устаревшими моделями телефонов. Как заявили ИБ-аналитики, Attor активен с 2013 года, однако обнаружить его удалось лишь около года назад…» ***(Dmitry Nazarov. Модульный зловред Attor следит за русскоязычными жертвами // Threatpost (https://threatpost.ru/modular-malware-attor-spying-on-russian-speakers/34476/). 12.10.2019).***

***

«…NME со ссылкой на данные компании McAfee, специализирующаяся на кибербезопасности объявляют, что при поиске информации о Билли или Мэйси, очень большой шанс поймать какую вредоносную программу или вирус.

На третьей позиции оказался ведущий вечерней программы Джеймс Корден. Следом идет певица Ники Минаж.

"Люди хотят быть в курсе последних новостей поп-культуры и знаменитостей в любое время и с любого устройства. И поэтому часто они ставят скорость получения информации выше безопасности, нажимая на подозрительные ссылки, которые обещают контент с их любимыми звездами. Им нужно подумать, прежде чем кликнуть на ссылку", - отметил представитель компании McAfee Радж Самани.» ***(Билли Айлиш и Мэйси Уильямс стали самыми опасными звездами // Multikino (http://www.multikino.com/ru/news/?id=24142). 24.10.2019).***

***

«Google регулярно вносит в свой магазин Play Store различные улучшения, касающиеся системы безопасности для того, чтобы вирусы и другое нежелательное ПО не попадало на смартфоны пользователей. Но порой кажется, что все эти попытки тщетны, потому как не так давно на просторах виртуального магазина приложений было найдено еще 15 программ с вирусами. Естественно, если какие-то из них вдруг установлены на вашем смартфоне, то срочно удаляйте их от греха подальше…

…Недавно фирма, занимающаяся вопросами кибербезопасности, под названием SophosLabs обнаружила, как уже было сказано выше, 15 вредоносных приложений прямо в Google Play Store. Приложения генерируют большое количество объявлений, а затем скрывают свои значки, чтобы вам было сложнее найти и удалить их.

Выглядит все примерно так: когда приложение впервые запускается, оно отображает сообщение, в котором говорится: «Это приложение несовместимо с вашим устройством и будет удалено!». Затем пользователь нажимает «Ок», после чего программа скрывает свой собственный значок, чтобы он не отображался на главном экране. Но физического удаления не происходит. В программе просто осуществляется подмена текста на экране. Вместо запроса разрешения пользователь видит сообщения о несовместимости.

SophosLabs также обнаружили, что 9 из 15 приложений использовали и другую тактику. После того, как приложение устанавливалось, оно появлялось в настройках. В целом — это нормальная практика. Таким образом можно откалибровать разрешения доступа в любое удобное время. Только вот когда пользователь заходил в эти настройки, он вместе с ними запускал и программу. Она

начинала работать в фоновом режиме, а когда пользователь выходил из настроек — программа «стирала» себя оттуда, продолжая работать…

После того, как вы загрузитесь в безопасном режиме все «невидимые» программы станут видимыми.

Долго задержите палец на опасной программе и во всплывающем меню виберите пункт «Удалить». При этом также теперь вы сможете найти их и через поиск, если вдруг забыли, где располагалась программа изначально.

После очистки перезагружайте смартфон…» ***(В Google Play появились приложения с вирусами // Український телекомунікаційний портал (https://portaltele.com.ua/news/internet/v-google-play-poyavilis-prilozheniya-s-virusami.html). 17.10.2019).***

***

«Популярное в украинских пользователей «не совсем легальное» приложение Router Scan, которое находит в сети роутеры/маршрутизаторы, и извлекает из них имя WIFI сети и ключ (парольную фразу) точки доступа, уже несколько лет имеет встроенную систему удаленного доступа и все результаты сканирования сетей отправляет на сервер разработчика.

Об этом на своей странице в Facebook написал эксперт по кибербезопасности, ведущий разработчик компании ИТ-Лаборатория Александр Галущенко…

Также разработчики программы «интересуются» данными терминалов на ПК пользователя, сетевым окружением, уровнем сигналов от соседних точек Wi-Fi и другими данными пользователей приложения.

По словам эксперта, в программе обнаружено уже 9 «закладок» и с каждой новой версией Router Scan их количество только растет:

– Хочу обратить Ваше внимание на ситуацию с модной в кругах школьников и молодых коллег программой «Router Scan». Да, действительно, она хороша для аудита и других спорных действий, но есть большое «но». Уже года два как в нее встроена система удаленного доступа, и при запуске она открывает путь к вашим данным. Кроме этого, независимо от того, ставите вы галочки, или нет в меню, все результаты сканирования она отправляет на сервер разработчика. Это особенно неприятно, когда вы находитесь внутри закрытой локалки, в которой циркулируют критические данные, – пишет Александр Галущенко. – На сегодня мы нашли 9 закладок в самой программе. С каждым новым релизом их становится все больше (или мы становимся умнее). Плюс разработчик очень интересуется ключами RDP и данными терминалов на вашей машине. И буфером обмена. И нажатием клавиш. И сетевым окружением. И уровнем сигналов от соседних точек Wi-Fi.

Отметим, что, по данным специалистов, собственно использование Router Scan может являться преступлением, предусмотренным статьей 361 Уголовного кодекса Украины – «Незаконное вмешательство в работу автоматизированных электронно-вычислительных машин, их систем или компьютерных сетей». ***(Владимир Кондрашов. Программу Router Scan уличили в краже данных пользователей // Internetua (http://internetua.com/programmu-router-scan-ulicsili-v-kraje-dannyh-polzovatelei). 27.10.2019).***

***

«За последние несколько месяцев тысячи пользователей Android-устройств стали жертвами нового вредоносного ПО, получившего название Xhelper. Программа прячется на зараженных устройствах и способна переустанавливать себя даже после удаления или сброса настроек до заводских на устройстве.

По словам специалистов из компании Symantec, за последние полгода вредоносное ПО уже успело заразить более 45 тыс. Android-устройств и продолжает распространяться, инфицируя в среднем 2,4 тыс. устройств в месяц.

Xhelper является компонентом приложения и не предоставляет обычный пользовательский интерфейс. Он не отображается на панели запуска приложений. Вредонос запускается при помощи внешних событий, инициированных пользователем, например, подключении/отключении от источника питания, перезагрузки телефона или установки приложений. После запуска вредоносная программа регистрируется в качестве основной службы, тем самым снижая риск отключения при нехватке памяти. Заразив устройство жертвы, Xhelper расшифровывает в память вредоносную полезную нагрузку. Данный модуль подключается к C&C-серверу злоумышленника и ожидает команды. После успешного подключения к C&C-серверу на скомпрометированное устройство могут быть загружены дополнительные вредоносные модули, например, дропперы, кликеры и руткиты.

Впервые исследователи обнаружили Xhelper в марте 2019 года. На тот момент функционал вредоносного ПО был относительно простым, и его основной функцией было посещение рекламных страниц с целью монетизации. Однако за прошедшее время вирусописатели расширили функционал Xhelper, добавив возможности ухода от обнаружения. Судя по всему, вредоносное ПО все еще находится в стадии разработки, считают специалисты.

Исследователям не удалось определить каналы распространения вредоноса. Поскольку в Google Play Store вредонос обнаружить не удалось, специалисты полагают, что Xhelper может загружаться из неизвестных источников либо с помощью вредоносного системного приложения, предустановленного на некоторых смартфонах. Судя по числу заражений, злоумышленников интересуют определенные марки смартфонов (названия торговых марок не указываются). Наибольшее число инфицированных устройств наблюдалось в Индии, США и России.» ***(«Неудаляемый» вредонос Xhelper заразил более 45 тыс. Android-устройств // SecurityLab.ru (https://www.securitylab.ru/news/502207.php). 30.10.2019).***

***

«Новое вредоносное ПО под названием Racoon, созданное для хищения информации быстро завоевывает популярность у киберпреступников. По словам команды исследователей из Cybereason Nocturnus, всего за несколько месяцев вредонос заразил сотни тысяч устройств по всему миру, похищая данные кредитных карт жертв, учетные данные электронной почты и пр.

Вредоносное ПО не является сложным или инновационным, однако распространение по модели «вредоносное-ПО-как- услуга» (MaaS) предоставляет

киберпреступникам быстрый и простой способ заработать деньги. Raccoon уже входит в десятку самых упоминаемых вредоносных программ в даркнете.

«Основываясь на логах, выставленных на продажу в подпольном сообществе, Raccoon за несколько месяцев заразил более 100 тыс. конечных точек по всему миру. С ним легко разберется любой преступник, независимо от уровня технических навыков. Более того, команда Raccoon постоянно работает над ее улучшением и предоставлением отзывчивой поддержки. Это дает людям быстрый и простой способ заработать деньги, не вкладывая много средств и не имея глубоких технических знаний», — сообщили исследователи из Cybereason.

Исследователи впервые обнаружили Raccoon в апреле 2019 года. Вредоносное ПО, написанное на языке C++, использует несколько потенциальных методов доставки, включая наборы эксплоитов (в том числе Fallout и RIG), а также фишинговые атаки и вредоносное ПО, распространяемое в составе легитимных программных пакетов с «сомнительных» web-сайтов.

После установки Raccoon проверяет системы на наличие информации о кредитных картах, криптовалютных кошельках, паролях, электронных письмах, cookie-файлах и данных из популярных браузеров (включая сохраненную информацию о кредитной карте, URL-адреса, имена пользователей и пароли), а затем отправляет их оператору.

Предположительно, вредонос разработан русскоговорящими злоумышленниками. Изначально он продавался исключительно на русскоязычных форумах, но теперь предлагается и на англоязычных.» ***(Вредоносная программа Raccoon заразила более 100 тыс. устройств // SecurityLab.ru (https://www.securitylab.ru/news/502080.php). 25.10.2019).***

***

«Инструмент для тестирования на проникновения Metasploit даже спустя 15 используется для обхода современных механизмов защиты. Как сообщают исследователи из компании FireEye, киберпреступники все еще используют инструмент вместе с высокоэффективной техникой под названием Shikata Ga Nai (в переводе с японского «ничего не может быть сделано», — прим. ред.) для обхода современных механизмов защиты конечных точек.

Metasploit Framework — наиболее известный инструмент для создания, тестирования и использования эксплоитов. Позволяет производить эксплуатацию и постэксплуатацию уязвимостей, доставку «полезной нагрузки» (payloads) на атакуемую цель. Изначально инструмент разрабатывался как способ облегчить работу тестировщиков эксплоитов, однако злоумышленники взяли на вооружение Metasploit и начали использовать инструмент для атак на компьютерные системы.

Техника Shikata Ga Nai (SGN) использовалась в рамках недавних атак ряда киберпреступных группировок, в частности APT20, UNC902, TA505 и APT41 (группировка, предположительно взломавшая производителя утилиты TeamViewer).

«Несмотря на то, что Metasploit существует более 15 лет, все еще существуют ключевые техники, которые остаются незамеченными и позволяют злоумышленникам избежать обнаружения. Одной из основных техник Metasploit является схема кодирования полезной нагрузки Shikata Ga Nai. Современные

системы обнаружения значительно улучшились за последние несколько лет и часто могут устаревшие вредоносные техники. Тем не менее, во многих случаях, если преступник уверен в своих действиях, он может немного изменить существующий код и обойти системы обнаружения», — пишут исследователи.

Изменения кода с помощью метода Metasploit SGN по-прежнему очень опасны. Данный эффект обеспечивает уникальный «полиморфный аддитивный энкодер XOR» кодера SGN. Каждое создание закодированного shell-кода будет отличаться от предыдущего. SGN делает полезную нагрузку безопасной на вид, кодируя вредоносное ПО с помощью «динамической замены команд, динамического упорядочения блоков, случайного обмена регистрами, рандомизации порядка команд, вставки ненужного кода, использования случайного ключа и рандомизации расстояния между командами».

XOR представляет собой алгоритм шифрования, который работает на основе ряда известных принципов. Шифрование и дешифрование могут быть выполнены путем применения и повторного использования функции XOR.

По словам исследователей, SGN удалось обойти защиту конечных точек, которая слишком сильно полагается на методы статического и динамического обнаружения. Расшифровка полезной нагрузки в памяти для определения вредоносного кода слишком нагружает систему, делая такой подход непрактичным. Методы обнаружения с помощью поведенческих индикаторов и «песочниц» также могут быть неточными, отмечают в FireEye.» ***(Инструмент Metasploit представляет угрозу даже спустя 15 лет // SecurityLab.ru (https://www.securitylab.ru/news/502045.php). 24.10.2019).***

***

«Для получения доступа к сайтам, работающим на базе системы управления контентом WordPress, злоумышленники используют вредоносные плагины с функциями бэкдора, которые прячут на самом видном месте.

Как сообщают специалисты компании Sucuri, функционал некоторых таких плагинов, в частности initiatorseo и updrat123, скопирован с чрезвычайно популярного плагина UpdraftPlus, предназначенного для резервного копирования и восстановления данных. Создать подделку очень легко, достаточно лишь воспользоваться готовыми автоматизированными инструментами или внедрить в исходный код легитимного плагина вредоносную нагрузку, например, web-оболочку.

Администраторам скомпрометированного сайта вредоносные плагины на панели инструментов не видны. «Для тех, кто не использует браузеры с особыми строками User-Agent, плагин по умолчанию не отображается на панели инструментов. Эти строки варьируются в зависимости от плагина», - сообщили исследователи.

Обнаружить вредоносный плагин можно с помощью специального GET-запроса с заданными параметрами, такими как initiationactivity или testingkey. Главная задача подобных плагинов – выполнение роли бэкдора на скомпрометированном сайте и предоставление атакующему доступа к серверу, даже если первоначальный вектор атаки был закрыт.

С помощью бэкдора злоумышленники загружают на серверы взломанных сайтов вредоносные файлы путем отправки POST-запросов. В этих запросах содержатся параметры с URL-адресами мест загрузки, директориями для записи файлов и именами загружаемых файлов.

По словам специалистов Sucuri, злоумышленники загружают web-оболочки (вредоносные скрипты, предоставляющие удаленный доступ к серверу) в произвольные места на серверах взломанных сайтов. В частности, скрипты с произвольными именами загружаются в корневые папки и позволяют киберпреступникам осуществлять брутфорс-атаки на другие сайты.

Исследователи также обнаружили новое поколение вредоносных плагинов, обладающих функциями не только бэкдоров, но и майнеров криптовалюты.» ***(Киберпреступники прячут вредоносные WordPress-плагины на самых видных местах // SecurityLab.ru (https://www.securitylab.ru/news/501876.php). 20.10.2019).***

***

Операції правоохоронних органів та судові справи проти кіберзлочинців

«В Аргентине сотрудники правоохранительных органов временно задержали известного исследователя безопасности и устроили обыск в его квартире. Хавьер Смальдоне (Javier Smaldone) подозревается во взломе правительственных компьютерных систем и похищении конфиденциальных документов, но у самого исследователя есть другая теория на этот счет.

Смальдоне является хорошо известным в Аргентине активистом в области кибербезопасности. Он активно выступает против использования электронных машин для голосования и регулярно делает в своем блоге публикации с критикой решения правительства все-таки прибегнуть к ним. В 2016 году Смальдоне даже выступал в Сенате Аргентины, агитируя против использования на выборах уязвимого оборудования.

Как сообщил исследователь новостному изданию Perfil, его жилье и дома еще двух специалистов по безопасности были обысканы на прошлой неделе после того, как они сообщили об уязвимостях в электронных машинах для голосования от аргентинской компании Smartmatic. В настоящее время правительство страны проводит тестирование данного оборудования с целью использовать его на будущих выборах.

Однако, как сообщает другое новостное издание Clarin, Смальдоне является одним из целого ряда подозреваемых в похищении и публикации 5 ГБ персональных данных служащих Федеральной полиции Аргентины. По данным издания, 8 октября нынешнего года правоохранители провели обыски во множестве домах в разных городах страны в поисках хакера, известного под псевдоним La Gorra Leaks 2.0.

12 августа La Gorra Leaks 2.0 опубликовал в даркнете, Telegram и Twitter 200 тыс. PDF-файлов с персональной информацией сотрудников Федеральной полиции.

В файлах содержались имена, фамилии, домашние адреса, номера телефонов, идентификационные номера и банковские данные полицейских.

Судя по опубликованным Смальдоне судебным документам, он является подозреваемым в утечке, поскольку первым сообщил о ней в Twitter. Помимо него, у следствия есть еще один задержанный подозреваемый.» ***(ИБ-эксперт задержан за «хакерство» из-за твита об утечке правительственных данных // SecurityLab.ru (https://www.securitylab.ru/news/501787.php). 16.10.2019).***

***

«Нидерландская полиция обезвредила так называемый «пуленепробиваемый» хостинг-сервис, который обеспечивал работу десятков IoT-ботнетов, использовавшихся для проведения сотен тысяч DDoS-атак по всему миру.

Сотрудники полиции конфисковали серверы, а также арестовали двух подозреваемых в офисах хостинг-провайдера KV Solutions BV, предположительно являющихся основателями сети из пяти взаимосвязанных компаний — KV Solutions BV, Lifehosting BV, Bos IT Holding BV, Kreikamp IT Holding BV и KBIT Holding BV. В течение двух лет компания KV предоставляла хостинговую инфраструктуру киберпреступникам, которая использовалась для проведения фишинговых и криптомайнинговых кампаний, а также в качестве хранилища вредоносных программ. Также компания завоевала «славу» среди ИБ-экспертов как удобная площадка для размещения DDoS-ботнетов. Киберпреступники арендовали серверы KV для размещения своих бот-сканеров, вредоносных программ и C&C-серверов в безопасной среде.

Только в нынешнего году на KV были размещены десятки DDoS-ботнетов, созданных на основе IoT-вредоносов, которые предназначались для заражения умных устройств, работающих на базе Linux, маршрутизаторов от ASUS, GPON, Fritz! Box, MikroTik, Netgear, Huawei, IoT-устройств от AVTECH, web-серверов JAWS и кабельных модемов от ZTE.

В то время как подавляющее большинство размещенных в инфраструктуре KV DDoS-ботнетов были созданы на базе Mirai, сервис также предоставлял услуги хостинга ботнетам на основе других вредоносных IoT-семейств, в частности, Fbot, Gafgyt, Hakai, Handymanny, Moobot, Tsunami и Yowai. Операторами большинства ботнетов являлись так называемые скрипт-кидди — аматоры, использующие чужие разработки для хакерских атак.

По словам соучредителя фирмы Bad Packets Троя Марша (Troy Mursch), компания KV также служила хостинг-провайдером для некоторых ботнетов, используемых в рамках модели «DDoS на заказ» (DDoS-for-hire). Среди жертв DDoS-атак были такие компании, как Ubisoft, Wish.com и основные поставщики облачных и web-хостингов (AWS, Microsoft Azure, OVH, AT&T, Comcast, Cox, Charter и China Unicom).» ***(Нидерландская полиция обезвредила площадку, предоставляющую услуги хостинга десяткам IoT-ботнетов // SecurityLab.ru (https://www.securitylab.ru/news/501551.php). 03.10.2019).***

***

«Правоохранительные органы Нидерландов захватили серверы bulletproof-хостинга KV Solutions и арестовали двух предполагаемых основателей по подозрению в преступной деятельности.

Как утверждают следователи, компания предоставляла клиентам площадки для управления ботнетами, координирования DDoS-кампаний и размещения криминальных веб-ресурсов. Специалисты не исключают, что после изучения данных, хранившихся на компьютерах провайдера, последуют другие задержания.

Как выяснили эксперты, только в этом году с IP-адресов, принадлежавших KV Solutions, было произведено более 400 тыс. кибератак, которые затронули такие компании, как Ubisoft, AT&T и China Unicom. По сведениям правоохранительных органов, криминальный провайдер принадлежал двум голландцам, которые для прикрытия зарегистрировали пять аффилированных между собой фирм…

На серверах bulletproof-хостинга располагались центры управления десятками ботнетов, в состав которых входят роутеры и другие зараженные IoT-устройства. Большая часть вредоносных сетей была основана на коде Mirai, однако провайдер размещал C&C-платформы практически всех штаммов, замеченных ИБ-специалистами в последнее время:

Hakai
Tsunami
Gafgyt
Yowai
Fbot
Handymann и Moobot

Следователи отмечают, что помимо ботнетов KV Solutions предоставляла услуги хостинга множеству криминальных ресурсов — на ее серверах хранились фишинговые страницы, платформы управления майнерами, сканеры уязвимостей и коды вредоносных программ. Часть инфраструктуры хостера использовали сервисы, предоставляющие DDoS-услуги на заказ.

После ареста подозреваемых на странице провайдера в Facebook появилось сообщение о временных технических проблемах. Специалисты считают, что это было закодированное послание, призывающее клиентов уничтожить хранящиеся на арендованных серверах данные. В настоящий момент все домены и веб-ресурсы, принадлежащие KV Solutions, недоступны, а телефонные звонки в офис компании остаются без ответа.

Другой bulletproof-хостинг на днях разгромили в Германии. Полиция захватила старый бункер НАТО, где располагались более 200 серверов с криминальными ресурсами. Хостинг Cyberbunker 2.0 размещал сайты с детской порнографией, даркнет-форумы и сайты наркоторговцев.» ***(Egor Nashilov. Голландские полицейские разгромили криминальный хостинг // Threatpost (https://threatpost.ru/kv-solutions-rest-in-pepperoni/34366/). 04.10.2019).***

***

«32-річного іноземця підозрюють у викраденні 6 мільйонів доларів із рахунків американських фінансових установ. Затримання відбулося в одному зі столичних готелів, де він тимчасово проживав.

У рамках міжнародної правової допомоги працівники Департаменту кіберполіції, Департаменту карного розшуку Нацполіції та столичного управління карного розшуку, за процесуального керівництва Генеральної прокуратури України, затримали у Києві іноземця, який розшукувався за вчинення кіберзлочинів.

Розслідування щодо злочинної діяльності іноземця почалося ще у 2010 році співробітниками Федерального бюро розслідувань та Служби розслідування фінансових злочинів (FNTT) США. У 2019 році в Україну надійшов запит про надання міжнародно-правової допомоги щодо розшуку та затримання хакера.

Наразі чоловіка підозрюють у незаконному втручанні в роботу комп'ютерних систем, викраденні та відмиванні грошей в особливо великих розмірах і в шахрайстві.

Поліцейські затримали зловмисника в одному із найдорожчих столичних готелів, де той тимчасово проживав. Вирішується питання щодо видачі затриманого США.» ***(Кіберполіція затримала хакера, який переховувався в Україні від правоохоронних органів США // Офіційний сайт Національної поліції (https://www.npu.gov.ua/news/kiberzlochini/kiberpolicziya-zatrimala-xakera-yakij-perexovuvavsya-v-ukrajini-vid-pravooxoronnix-organiv-ssha/). 25.10.2019).***

***

«Два киберпреступника признали свою вину в масштабной утечке данных клиентов и водителей Uber, которую компания продолжительное время скрывала, и использовании похищенных данных с целью вымогательства.

26-летний Брэндон Чарльз Гловер (Brandon Charles Glover) и 23-летний Василе Мереакре (Vasile Mereacre) на этой неделе признали себя виновными в предъявленных им обвинениях в суде города Сан-Хосе (штат Калифорния, США). С октября 2016-го по январь 2017 года злоумышленники похищали хранящуюся в Amazon Web Services конфиденциальную корпоративную информацию, а затем требовали у компаний выкуп за ее удаление. Uber решила заплатить вымогателям требуемую сумму, но сообщила о краже данных только спустя год.

Uber стала жертвой киберпреступников в октябре 2016 года. Злоумышленники похитили персональные данные порядка 57 млн клиентов и водителей сервиса по всему миру. Компания пошла на сделку с вымогателями и через программу выплат вознаграждений за обнаруженные уязвимости перевела им $100 тыс.

По данным следствия, Гловер и Мереакре также пытались требовать выкуп у сервиса Lynda.com, являющегося частью LinkedIn, однако LinkedIn отказалась платить и попыталась вычислить преступников

…злоумышленникам грозит пять лет лишения свободы и штраф в размере $250 тыс.» ***(Виновные в утечке данных клиентов Uber киберпреступники признались в содеянном // SecurityLab.ru (https://www.securitylab.ru/news/502227.php). 31.10.2019).***

***

«45-летнему Анкуру Агарвалу (Ankur Agarwal) из Монтвилля (США) предъявлены обвинения в установке аппаратных кейлоггеров на компьютерные системы двух компаний для несанкционированного доступа к их сетям и кражи конфиденциальных данных.

В феврале 2017 года преступник проник в помещение одной из двух технологических компаний и установил на компьютеры кейлоггеры для сбора логинов и паролей сотрудников. Он также подключил свой ноутбук и жесткий диск к компьютерной сети компании. Собрав данные для входа в систему, Агарвал смог получить удаленный доступ к сети компании и осуществить атаку на сотрудников, работающих над новыми технологиями. Деятельность Агарвала оставалась незамеченной до апреля 2018 года, когда команда безопасности компании обнаружила цифровое вторжение и начала расследование. Это не остановило преступника, он продолжал использовать свой доступ для наблюдения за ходом внутреннего расследования.

Согласно судебному заключению, преступник использовал тот же метод против другой американской компании, в сети которой в июне 2016 года установил аппаратный кейлоггер для сбора учетных данных сотрудников. Ему также удалось получить пропуск в офисы, благодаря чему он смог восстановливать неавторизованные электронные устройства, установленные в системах компании.

Злоумышленник получил доступ к логинам и паролям, а также тысячам личным документам, принадлежащих 10 сотрудникам обеих компаний. В одной из двух пострадавших компаний преступник также получил доступ к файлам кадровой службы, содержащим информацию о более чем 50 старших менеджеров.

Во вторник, 22 октября, Анкур Агарвал признал свою вину. Теперь ему грозит до 12 лет тюремного заключения, а также штраф в размере $250 тыс.» ***(Преступнику грозит 12 лет тюрьмы за внедрение кейлоггеров в системы техкомпаний // SecurityLab.ru (https://www.securitylab.ru/news/502046.php). 24.10.2019).***

***

Технічні аспекти кібербезпеки

«…через несколько месяцев компания Microsoft прекратит поддержку Windows 7, последнее обновление для данной ОС будет выпущено 14 января 2020 года. По словам исследователей из компании Webroot, количество кибератак на Windows 7 увеличилось более чем на 71% по сравнению с 2018 годом. В целом, компьютеры, использующие операционную систему Windows 7, в два раза чаще подвержены заражению, чем компьютеры на базе Windows 10.

Пользователи домашних ПК на базе Windows 7 больше всего подвержены риску атак, поскольку 64% заражений нацелены на данные устройства.

«Существует множество факторов, способствующих таким показателям, не в последнюю очередь из-за того, что большинство корпоративных устройств защищены межсетевыми экранами для бизнеса, в то время как домашние

устройства пользователей могут быть менее защищены. Во-вторых, обычный человек с большей вероятностью будет проявлять осторожность при просмотре web-страниц на рабочем устройстве, которым владеет работодатель», — поясняют исследователи.

В случаях атак на устройства на базе Windows 7 большинство вредоносных программ скрывают свои файлы в местах, где их труднее найти. Например, 41% образцов вредоносных программ скрываются во временной папке, 24% перемещают свои файлы в appdata, а около 11% обитают в системной папке кэша.

На базе Windows 7 по-прежнему работает примерно 30% от всех компьютеров в мире.» ***(Число кибератак на Windows 7 увеличилось более чем на 71% // SecurityLab.ru (https://www.securitylab.ru/news/501785.php). 15.10.2019).***

***

«Исследователь безопасности Монта Элкинс (Monta Elkins) из фирмы FoxGuard продемонстрировал на примере прототипа, как можно собрать рабочий шпионский чип с помощью оборудования стоимостью всего $200. Исследователь решил показать, насколько легко и дешево можно внедрить крошечный шпионский чип в цепочку поставок оборудования компании, сообщает издание Wired.

Имея в распоряжении только инструмент для пайки горячим воздухом за $150, микроскопом за $40 и несколько микросхемам за $2, Элкинс смог перенастроить межсетевой экран от Cisco таким образом, что большинство IT-специалистов, вероятно, не заметят вмешательство. Элкинс использовал чип ATtiny85 размером около 5 мм с платы Digispark Arduino за 2$. После записи своего кода на чип исследователь снял его с платы Digispark и припаял к материнской плате межсетевого экрана ASA 5505 от Cisco. Он выбрал незаметное место, которое не требовало дополнительной проводки и дало чипу доступ к последовательному порту брандмауэра.

Элкинс запрограммировал крошечный чип на атаку, как только межсетевой экран загрузится в дата-центр жертвы. Он выполняет роль администратора, который обращается к настройкам межсетевого экрана, подключая компьютер напрямую к последовательному порту. Затем чип запускает функцию восстановления пароля, создает новую учетную запись администратора и получает доступ к настройкам межсетевого экрана. По словам Элкинса, в данном эксперименте межсетевой экран ASA 5505 от Cisco был самым дешевым вариантом, однако то же самое можно сделать с любым межсетевым экраном от Cisco с функцией восстановление пароля.

Данная атака может изменить настройки межсетевого экрана и предоставить злоумышленнику удаленный доступ к устройству, логам всех видимых соединений и отключить функции безопасности.» ***(Установка шпионского чипа обходится злоумышленникам всего в $200 // SecurityLab.ru (https://www.securitylab.ru/news/501724.php). 12.10.2019).***

***

«Антивирусное программное обеспечение Symantec Endpoint Protection (SEP) 14 вызывает сбой в работе браузера Google Chrome 78, выпущенного во

вторник, 22 октября. Согласно жалобам на Reddit , форумах поддержки Google и комментариям в официальном блоге Google Chrome, SEP 14 аварийно завершает работу браузера Chrome 78 с сообщением об ошибке.

По словам пострадавших, в последние два дня невозможно использовать Chrome 78, так как браузер отказывается загружать любые web-страницы. Подавляющее большинство жалоб поступает из корпоративных сред, где установки SEP более распространены.

Компания Symantec признала в сообщении на официальном сайте наличие проблемы. По словам Symantec, данные проблемы затрагивают только пользователей SEP 14, установленного на компьютерах с ОС Windows 10 RS1, Windows Server 2012 и Windows Server 2016. Проблема исправлена в SEP версии 14.2.

Проблема также затрагивает Microsoft Edge (на базе движка Chromium), но поскольку данная версия официально не выпущена, проблема не коснулась значительного количества пользователей.

По словам Symantec, проблема связана с функцией проверки целостности кода Microsoft, которую Google использует для защиты Chrome. В качестве временного решения Symantec рекомендует пользователям внести браузер в список исключений антивируса или отключить защиту целостности кода в настройках Chrome. Тем не менее, поскольку предложенные меры подвергают браузер риску различных атак, пользователям стоит временно отказаться от использования Chrome, пока проблема не будет решена.» ***(Антивирус Symantec вызывает сбой в работе Chrome 78 // SecurityLab.ru (https://www.securitylab.ru/news/502069.php). 25.10.2019).***

***

«Специалисты в области кибербезопасности Хоай Вьет Нгуен (Hoai Viet Nguyen), Луиджи Ло Лаконо (Luigi Lo Iacono) и Ханс Федеррат (Hannes Federrath) представили новую атаку cache poisoning (отравление кэша) на системы кэширования. Атака Cache Poisoned Denial of Service (CPDoS) позволяет заставить атакуемый сайт вместо легитимного контента отображать для большинства пользователей страницу с ошибкой.

Проблема затрагивает системы кэширования наподобие Varnish, а также популярные сети доставки контента (CDN), в частности Amazon CloudFront, Cloudflare, Fastly, Akamai и CDN77. Исследователи осуществили три атаки на различные комбинации систем кэширования и реализации HTTP, и самым уязвимым к CPDoS оказался сервис Amazon CloudFront CDN.

Суть атаки заключается в том, чтобы заставить промежуточные серверы CDN кэшировать возвращенные исходным сервером web-ресурсы или страницы с ответами об ошибках. CPDoS позволяет злоумышленнику сделать сайт или ресурс недоступным путем отправки одного лишь HTTP-запроса с особым заголовком.

Как пояснили исследователи, атакующий может сгенерировать для кэшируемого ресурса HTTP-запрос с неправильными полями, которые игнорируются системой кэширования, но вызывают ошибку во время обработки исходным сервером.

Исследователи сообщили о проблеме всем затронутым ею производителям в феврале нынешнего года. Команда Amazon Web Services (AWS) подтвердила наличие уязвимостей в CloudFront и исправила их путем блокировки кэширования страниц с ошибками 400 Bad Request по умолчанию. Компания Microsoft также подтвердила наличие и исправила уязвимость (CVE-2019-0941) в рамках июньского «вторника исправлений».

Разработчики Play Framework исправили проблему, ограничив влияние заголовка X-HTTP-Method-Override в версиях Play Framework 1.5.3 и 1.4.6. Остальные затронутые проблемой вендоры, в том числе Flask, также были уведомлены исследователями, однако не предоставили никакого ответа.» ***(Новый способ отравления кэша позволяет атаковать защищенные CDN сайты // SecurityLab.ru (https://www.securitylab.ru/news/501991.php). 23.10.2019).***

***

Виявлені вразливості технічних засобів та програмного забезпечення

«Служба кібербезпеки Google Project Zero повідомила, що знайшла технічну проблему в популярній операційній системі (ОС) Android. Через неї хто завгодно зможе контролювати чуже пристрій і порушувати його роботу.

Системна помилка позначилася на Pixel, Samsung, Xiaomi, Oppo і Moto, які оновлені до ОС 8.

Так, виявлена проблема поширилася на лінійку смартфонів, які підтримують Android не нижче 8 версії: Pixal, Samsung, Xiaomi, Oppo, і Moto. Вона дає можливість підготовленій людині отримати можливість контролювати чужий пристрій і порушувати його роботу.

Відома позиція Google з приводу використання цієї діри в системі: фахівці переконані, що її використовувала приватна компанія з Ізраїлю під назвою NSO Group. Її основний рід діяльності – створення засобів кіберрозвідки.

Цікаво, що раніше згадана вразливість системи Android вже була виявлена розробниками, а також була усунена на гаджетах старих моделей. Схоже, що рішення не поширилося на оновлені пристрої.» ***(Google знайшов серйозну проблему в пристроях на Android // Молодий буковинець (https://molbuk.ua/news/183316-google-znayshov-seryoznu-problemu-v-prystroyakh-na-android.html). 06. 10.2019).***

***

«В месенджері WhatsApp для операційної системи Android виявлена уразливість, яка дозволяє отримати доступ до смартфону за допомогою файлів GIF-анімації…

Як з'ясував спеціаліст з кібербезпеки під псевдонімом Awakened, потенційну жертву можна атакувати за допомогою шкідливого GIF-файлу. Після запуску

файлу, хакери отримують доступ до мультимедіа користувача, причому не тільки в самому месенджері, але в смартфоні.

Якщо номер зловмисника є в записній книжці жертви, зображення завантажиться автоматично, без необхідності підтвердження користувача. Схоже, компанія не могла передбачати винахідливість хакерів.

Втім, розробники вже закрили цю уразливість, так що настійно радимо оновити додаток до актуальної версії…» ***(У WhatsApp знайшли спосіб читати чуже листування: як уникнути злому // Znaj.ua (https://techno.znaj.ua/267253-u-whatsapp-znayshli-sposib-chitati-chuzhe-listuvannya-yak-uniknuti-zlomu). 04.10.2019).***

***

«Исследователи из компании SafeBreach, специализирующейся на симуляции взломов и атак, обнаружили опасную уязвимость (CVE-2019-6333) в службе HP Touchpoint Analytics. По оценкам специалистов, данная проблема затрагивает десятки миллионов компьютеров, на которых установлена данная служба.

HP Touchpoint Analytics поставляется со многими ноутбуками и персональными компьютерами на базе Windows производства Hewlett-Packard. Служба предназначена для анонимного сбора диагностической информации о производительности оборудования и для этого использует инструмент с открытым исходным кодом под названием Open Hardware Monitor.

При запуске службы HP Touchpoint Analytics служба пытается загрузить три отсутствующих DLL-библиотеки. Злоумышленник с правами администратора в целевой системе может создавать вредоносные DLL-библиотеки с именами отсутствующих файлов и размещать там, где они будут выполняться при запуске службы HP. Преступник таким образом может повысить привилегии до уровня SYSTEM и обойти механизмы безопасности (такие как «белый список» приложений и проверка цифровой подписи).

Специалисты также выяснили, что библиотеку Open Hardware Monitor можно использовать для чтения и записи в физическую память. Данная уязвимость представляет большую ценность для злоумышленников, поскольку службы Open Hardware Monitor и HP Touchpoint Analytics установлены на десятках миллионов компьютеров. Следует отметить, библиотека Open Hardware Monitor больше не поддерживается разработчиками. Последняя версия программы была выпущена в ноябре 2016 года, а последние изменения в коде, размещенном на GitHub, датируются январем 2018 года.

Исследователи предупредили компанию HP о данной проблеме в начале июля нынешнего года, и уязвимость была исправлена в версии Touchpoint Analytics 4.1.4.2827…» ***(Уязвимость в службе HP Touchpoint Analytics затрагивает миллионы ПК // SecurityLab.ru (https://www.securitylab.ru/news/501722.php). 11.10.2019).***

***

«Как сообщают специалисты компании Morphisec, операторы вымогательского ПО BitPaymer активно используют уязвимость нулевого дня

в сервисе iTunes для Windows для запуска вредоносного кода и обхода обнаружения.

Проблема затрагивает встроенный в iTunes для Windows механизм обновления Bonjour. С ее помощью злоумышленник может воспользоваться неквотируемым путем (unquoted path) и благодаря этому не только обойти обнаружение антивирусным решением, но и получить персистентность на системе.

В большинстве случаев, когда пользователи деинсталлируют iTunes, компонент Bonjour все равно остается. Поскольку в корпоративной среде насчитывается великое множество компьютеров со все еще запущенным механизмом Bonjour, неудивительно, что операторы вымогательского ПО BitPaymer избрали его в качестве вектора атаки.

Решения безопасности обычно осуществляют мониторинг поведения приложений, в котором главную роль играет цепь процесса выполнения. Bonjour является подписанным и хорошо известным процессом, поэтому решения безопасности не отмечают его, во избежание ненужного вмешательства. Злоумышленники могут воспользоваться этим для выполнения нового дочернего вредоносного процесса и остаться незамеченными. Более того, вредоносная нагрузка лишена расширения .exe, и решения безопасности вряд ли будут ее сканировать.

Apple исправила уязвимость на прошлой неделе, после того как стало известно о ее эксплуатации операторами BitPaymer. Проблема исправлена в версии iTunes для Windows 12.10.1…» ***(Операторы вымогателя BitPaymer взялись за уязвимость нулевого дня в iTunes // SecurityLab.ru (https://www.securitylab.ru/news/501702.php). 11.10.2019).***

***

«Исследователь Тхана Нгуен Нгуен из FortiGuard Labs опубликовал подробности о критической уязвимости CVE-2019-16920 в прошивке некоторых маршрутизаторов от D-Link. Проблема была обнаружена в сентябре 2019 года, однако поставщик не будет выпускать патч.

Проблема связана с неаутентифицированным внедрением команд и затрагивает прошивку маршрутизаторов DIR-655, DIR-866L, DIR-652 и DHP-1565. Уязвимость может быть проэксплуатирована злоумышленником путем ввода произвольных символов в интерфейсе шлюза PingTest, что позволит удаленно выполнить код и полностью скомпрометировать систему. Критическая уязвимость получила 9,8 балла из 10 по версии CVSS v3.1 и 10,0 балла по версии CVSS v2.0…» ***(D-Link не намерена исправлять критическую уязвимость в своих маршрутизаторах // SecurityLab.ru (https://www.securitylab.ru/news/501603.php). 07.10.2019).***

***

«Исследователь безопасности под псевдонимом Awakened обнаружил в популярном мессенджере WhatsApp уязвимость, позволяющую злоумышленникам получать доступ к файлам и сообщениям жертвы с помощью вредоносного GIF-изображения.

Проблема представляет собой уязвимость двойного высвобождения памяти (double-free) – аномалии повреждения памяти, способной вызвать аварийное завершение работы приложение или, еще хуже, предоставить злоумышленнику «лазейку» к содержимому устройства. Все что нужно для осуществления атаки – создать вредоносный GIF-файл, отправить его жертве и дождаться, пока она его откроет в галерее WhatsApp.

Как пояснил исследователь, уязвимость затрагивает реализацию галереи, а именно механизм создания превью для изображений, видео и «гифок».

Представленный исследователем эксплоит работает преимущественно на устройствах под управлением версий Android 8.1 и 9.0 и не работает на Android 8.0 и более ранних. По словам Awakened, на более старых устройствах уязвимость также можно проэксплуатировать, но только для аварийного завершения работы приложения.

Awakened уведомил Facebook о проблеме, и компания выпустила исправление. Во избежание атак с эксплуатацией данной уязвимости пользователям WhatsApp настоятельно рекомендуется обновить свои приложения до версии 2.19.244 или более поздней.» ***(Уязвимость в WhatsApp позволяет получить доступ к устройству с помощью «гифки» // SecurityLab.ru (https://www.securitylab.ru/news/501543.php). 03.10.2019).***

***

«Специалисты компании Akamai Technologies выяснили, что злоумышленники все еще пользуются уязвимостью Drupalgeddon2, пропатченной полтора года назад. Исследователи обнаружили следы атак в журналах сканеров безопасности, а также провели анализ полезной нагрузки, найденной на одном из скомпрометированных сайтов.

По мнению экспертов, текущая кампания относительно скромная: она нацелена на отдельные сайты с большим трафиком и не имеет отраслевой направленности.

В руки ИБ-специалистов попали два объекта, найденных на бразильском веб-ресурсе. Обфусцированный вредоносный код размещен в GIF-файле, а незашифрованный Perl-сценарий для коммуникаций с C&C-сервером — в текстовом документе.

Сценарий новых атак через Drupalgeddon2

Перед запуском скриптов злоумышленники ищут и удаляют предыдущие варианты полезной нагрузки, а также изменяют ключевые настройки сайта. Файл index.inc.gif содержит PHP-код, зашифрованный при помощи алгоритмов base64, rot13 и архиватора gzip. Вредоносный сценарий пытается выполнить следующие команды:

запуск собственной веб-оболочки;

распаковка и удаленный запуск скриптов;

поиск учетных данных на диске и отправка их злоумышленникам;

замена файла конфигурации .htaccess;

вывод системной информации и конфигурации SQL-базы;

переименование файлов на целевой машине.

Вторая часть полезной нагрузки находится в текстовом файле — это набор команд для подключения к IRC-чату, через который идет связь скомпрометированного ресурса с центром управления. Скрипт позволяет собирать информацию об уязвимой системе, использовать ее для DDoS-атак и перехватывать управление сайтом. По мнению специалистов, злоумышленники использовали готовый код, доступный в даркнете, изменив часть сценария для своих целей.

Разработчики Drupal исправили уязвимость Drupalgeddon2 в марте 2018 года. Баг позволяет неавторизованному злоумышленнику удаленно выполнить код на сайте, работающем под управлением CMS версий с 3.3 по 8.5. Проблема зарегистрирована как CVE-2018-7600 и получила критический уровень угрозы по шкале CVSS.» ***(Egor Nashilov. Киберпреступники вновь атакуют сайты на Drupal // Threatpost (https://threatpost.ru/drupalgeddon2-is-still-being-used-oct-2019/34405/). 08.10.2019).***

***

«Исследователи из двух немецких университетов смогли прочитать зашифрованные PDF-документы. Эксперты предложили два способа атаки под общим названием PDFex: оба позволяют взламывать файлы через 27 программ, включая Adobe Acrobat, Foxit Reader, средства просмотра PDF в Chrome и Firefox.

Столь широкий набор ПО объясняется тем, что уязвимость содержится в механизмах, встроенных в сам стандарт PDF. Его создатели предусмотрели в коде функцию нативного шифрования, благодаря которой документы можно открывать в любых программах, не переживая за совместимость криптографических алгоритмов. Как выяснили эксперты, эта опция оставляет незашифрованными некоторые данные PDF-файла, позволяя с их помощью получить все содержимое целевого документа.

Атака PDFex методом прямого извлечения

Первый сценарий использует упомянутые незашифрованные участки данных — созданный на их основе PDF-документ при открытии отправит злоумышленнику всю информацию.

Для этого взломщики могут добавить в незащищенные данные активный элемент: PDF-форму, интернет-ссылку или JavaScript-сценарий. Эти компоненты автоматически запустятся, когда пользователь расшифрует и откроет документ.

При использовании PDF-формы это все, что требуется от жертвы. Вариант с вредоносной ссылкой менее надежен для злоумышленника, поскольку требует запуска внешнего браузера, а это может вызвать у жертвы подозрения. Последний тип атаки и вовсе можно заблокировать собственными средствами PDF-программы, многие из которых запрещают фоновое выполнение JavaScript.

Атака PDFex через блоки шифротекста

Вторая вариация PDFex, напротив, направлена на зашифрованную часть файла. Для взлома документа специалисты используют участки кода, которые обрабатывают сцепленные блоки шифротекста и по результатам этих операций редактируют открытые данные. Эксперты использовали эти методы, чтобы внедрить в защищенное содержимое команду на отправку информации.

Как и в первом варианте атаки, это можно сделать тремя способами: с помощью PDF-форм, вредоносных ссылок и манипуляций сжатыми данными

документа. В последнем случае файл сам отправляет расшифрованное содержимое на удаленный сервер при открытии…

Все предложенные сценарии предполагают, что взломщик получил доступ к редактированию PDF-документов — будь то напрямую или через перехват трафика жертвы. Исследователи призывают не преуменьшать возможные риски для пользователя, указывая, что, по идее, средства шифрования должны защищать именно от таких атак.

Специалисты доказали работоспособность своих методов на 27 распространенных программах для просмотра PDF…» ***(Egor Nashilov. Ученые научились взламывать зашифрованные PDF-файлы // Threatpost (https://threatpost.ru/pdfex-poc-attack/34313/). 01.10.2019).***

***

Нещодавно стало відомо про цікаву розробку, яку випустили у Ватикані. Це розумна вервиця, яку можна синхронізувати зі смартфоном. Однак, французькі хакери дуже швидко зламали цей девайс…

Експерт з кібербезпеки з Франції Батист Роберт виявив у цьому девайсі критичну уразливість.

Як пояснив експерт, ця уразливість дає змогу зловмисникам отримати доступ до електронної пошти користувачів…

Аби зламати одну таку вервицю хакери витрачали всього 15 хвилин. Уразливість пов’язана з обробкою облікових даних при вході в додаток. Так, коли користувач реєструється у додатку, то використовує для цього електронну пошту. На неї має прийти підтвердження, натомість надходить ПІН-код. А після цього “пін” потрапляє в мережу…

Експерт вже повідомив про уразливість експертам з Ватикану. Там запевнили, що її вже виправили.» ***(Хакери доволі швидко зламали ватиканську розумну вервицю // ОКІА "Новини Полтавщини" (https://np.pl.ua/2019/10/khakery-dovoli-shvydko-zlamaly-vatykans-ku-rozumnu-vervytsiu/). 22.10.2019).***

***

«Международный разработчик антивирусного программного обеспечения – словацкая компания ESET предупреждает об обнаруженных уязвимостях в устройствах интернета вещей, которые могут быть использованы киберпреступниками для заражения системы и похищения данных жертв. Об этом сообщается на сайте компании. «В большинстве случаев устройства интернета вещей имеют уязвимости, которые киберпреступники могут использовать для заражения системы и похищения данных жертвы. В частности, в прошлом году было выявлено масштабную операцию для скрытой добычи криптовалют с использованием домашних роутеров», – говорится в сообщении.

По данным IT-специалистов ESET, целью злоумышленников могут стать «умные» счетчики, которые используются для точного контроля потребленной электроэнергии, газа и воды. В случае заражения устройств киберпреступники могут получить доступ к системам приборов и управлять ими. Кроме того, по данным ESET, под прицелом хакеров могут оказаться технологии «умного» города,

которые предполагают широкое использование информационно-телекоммуникационных технологий для управления электроснабжением, коммунальными услугами и транспортной инфраструктурой и позволяют экономить расходы, сокращать вредоносное воздействие на окружающую среду и т.д.

«В большинстве случаев при реализации подобных проектов заботятся только о доступности и использовании новейших технологий, забывая о вопросах безопасности. Однако, с ростом взаимосвязи между всеми важными системами города, реализация мер по кибербезопасности должна стать приоритетной задачей, от успеха которой зависит бесперебойное функционирование всех процессов города и соответственно уровень качества жизни его жителей», – добавили IT-специалисты. В компании напомнили, что в Украине уже было зафиксировано несколько кибератак на государственном уровне, в результате которых пострадали целые отрасли экономики. «В частности, стоит упомянуть атаку хакеров на украинские энергетические компании в 2015 году, которая вызвала отключение электроэнергии на несколько часов. Кроме этого, еще одним известным примером стало распространение целенаправленного вредоносного кода для подрыва важных промышленных процессов в 2017 году», – приводится информация на сайте компании. Также, согласно сообщению, IT-специалисты обнаружили по меньшей мере два случая распространения вредоносных программ для скрытого майнинга криптовалют на зараженных системах управления электростанциями. Кроме финансовых затрат и создания проблем электроснабжения, процесс майнинга криптовалют потребляет значительное количество энергии, что приносит вред окружающей среде…» ***(Эксперты по кибербезопасности предупреждают об обнаруженных уязвимостях в устройствах интернета вещей // УНИАН (https://www.unian.net/science/10729521-eksperty-po-kiberbezopasnosti-preduprezhdayut-ob-obnaruzhennyh-uyazvimostyah-v-ustroystvah-interneta-veshchey.html). 24.10.2019).***

***

«Европейские власти выпустили патч для двух уязвимостей в системе авторизации eIDAS (electronic IDentification, Authentication and trust Services), эксплуатация которых позволяет злоумышленнику выдать себя за любого гражданина или предприятие ЕС во время официальных транзакций.

eIDAS представляет собой сложную, криптографически защищенную, электронную систему для управления цифровыми транзакциями и подписями между государствами-членами ЕС, гражданами и предприятиями. Созданная в 2014 году eIDAS позволяет проверять по официальным базам данных транзакции в любой стране, независимо от государства, откуда происходила транзакция.

eIDAS-Node является официальным пакетом программного обеспечения, используемым правительственными организациями на своих серверах для поддержки eIDAS-транзакций в частных базах данных. Поэтому любые уязвимости в программном обеспечении eIDAS-Node могут позволить злоумышленникам вмешиваться в официальные цифровые транзакции ЕС, такие как налоговые платежи, банковские переводы, отгрузки товаров и пр.

Две уязвимости обнаружили исследователи из компании SEC Consult. Их эксплуатация позволяет злоумышленнику выдать себя за любого гражданина или предприятия ЕС. По словам специалистов, текущие версии пакета eIDAS-Node не проверяют сертификаты, используемые в операциях eIDAS, позволяя преступникам подделывать сертификаты любого другого гражданина или предприятия eIDAS.

Для осуществления атаки преступнику нужно инициировать злонамеренное соединение с сервером eIDAS-Node любого государства-члена и предоставить поддельные сертификаты во время начального процесса аутентификации.

Обновление программного пакета eIDAS-Node (v2.3.1), исправляющее данные уязвимости, доступно для загрузки на официальном сайте.» ***(Исправлены уязвимости в системе аутентификации eIDAS ЕС // SecurityLab.ru (https://www.securitylab.ru/news/502192.php). 30.10.2019).***

***

«Японский турагент H.I.S. Group проигнорировал предупреждения об уязвимости в его роботах Tapia, которые обслуживают пользователей в сети отелей Henn na Maihama, и теперь приносит извинения. В Сети размещен PoC-код уязвимости, эксплуатация которой позволяет злоумышленникам удаленно следить за посетителями через камеры, сообщает Tokyo Reporter.

В сети отелей Henn na Maihama клиентов обслуживают роботы. Персонал на стойке регистрации представлен в виде динозавров, а в номере гостей обслуживают специальные роботы Tapia. Устройство умеет распознавать голоса и действия, определять настроение пользователя по его интонации, запоминать имена и дни рождения, воспроизводить музыку, следить за безопасностью в помещении, а также осуществлять звонки и делать заказы в интернете.

Ранее в нынешнем году исследователь под псевдонимом lrvick предупредил H.I.S. Group об уязвимости в роботах Tapia, эксплуатация которой позволяла получить удаленный доступ к камерам и микрофонам робота. Компания проигнорировала предупреждение, и исследователь разместил в общем доступе PoC-код для уязвимости.

Отель входит в сеть из 10 гостиниц, которые используют разнообразных роботов вместо «живого» персонала. Пока что речь идет только о роботах Tapia в одном отеле, но в настоящее время неясно, используются ли в отелях другие устройства.

H.I.S. Group принесла извинения за причиненное беспокойство и выпустила обновление для роботов, исправив данную уязвимость.» ***(Взлом роботов в сети японских отелей позволил следить за клиентами // SecurityLab.ru (https://www.securitylab.ru/news/501983.php). 23.10.2019).***

***

«В антивирусной программе Avira 2019 обнаружена опасная уязвимость (CVE-2019-17449), эксплуатация которой позволяет обойти защиту на целевой системе, обеспечить персистентность и повысить привилегии путем загрузки произвольной неподписанной DLL-библиотеки. Для эксплуатации уязвимости злоумышленник должен иметь права администратора.

Эксперты из компании SafeBreach протестировали службу Avira ServiceHost (служба Avira Launcher). Avira ServiceHost — подписанный процесс, который запускается с правами NT AUTHORITY/SYSTEM и первым устанавливается после запуска установщика. По словам экспертов, при запуске Avira.ServiceHost.exe пытается загрузить недостающую библиотеку Windtrust.dll из своего каталога. Уязвимость затрагивает версии Avira Launcher ниже 1.2.137 и версии Avira Software Updater ниже 2.0.6.21094.

Как правило, антивирусные решения ограничивают любые модификации (например, добавление, запись или изменение файлов) в папках с помощью мини-фильтра, применяющего политику «только для чтения» к любому пользователю, включая Администратора. В рамках эксперимента исследователи скомпилировали произвольную DLL-библиотеку, записывающую в текстовый файл название процесса, который его загрузил, имя пользователя, который его выполнил, и название DLL-библиотеки.

«Нам удалось загрузить произвольную DLL-библиотеку и выполнить код внутри Avira.ServiceHost.exe, который был подписан «Avira Operations GmbH & Co. KG» и выполнен как NT AUTHORITY/SYSTEM», — отмечают эксперты.

Подобные действия исследователям удалось провести и с другими службами Avira (System Speedup, Software Updater и Optimizer Host).

Эксперты обнаружили три типа атак, возможных при эксплуатации данной уязвимости: обход защиты антивирусного ПО; загрузка и выполнение вредоносной полезной нагрузки в контексте подписанного процесса Avira; обеспечение персистентности на системе.

Исследователи уведомили компанию об уязвимости в июле нынешнего года. В сентябре Avira выпустила исправленную версию Launcher (1.2.137).» ***(Уязвимость в антивирусе Avira позволяет повысить права на системе // SecurityLab.ru (https://www.securitylab.ru/news/501934.php). 22.10.2019).***

***

«Уязвимость в Trend Micro Anti-Threat Toolkit позволяет запускать вредоносное ПО на компьютерах под управлением Windows. Как пояснил исследователь безопасности Джон Пейдж (John Page), также известный под псевдонимом hyp3rlinx, злоумышленник может обмануть Trend Micro Anti-Threat Toolkit и заставить во время сканирования выполнить любой код, в том числе вредоносный, если имя файла будет cmd.exe или regedit.exe.

«Trend Micro Anti-Threat Toolkit (ATTK) загрузит и выполнит произвольные файлы .EXE, если автор вредоносного ПО использует уязвимое соглашение об именах 'cmd.exe' или 'regedit.exe'», - сообщил исследователь. Проще говоря, если с помощью загрузки, электронной почты или еще каким-то способом злоумышленник сохранит файл с именем cmd.exe или regedit.exe на компьютере жертвы с включенным ATTK, он сможет запустить на системе вредоносное ПО.

«Вредоносная программа может быть размещена в непосредственной близости от ATTK, когда конечный пользователь запускает сканирование», - пояснил Пейдж.

Так как ATTK подписан проверенным издателем и поэтому считается доверенным, вредонос легко обходит предупреждения об угрозах.

По словам Пейджа, Trend Micro стало известно об уязвимости (CVE-2019-9491) 9 сентября нынешнего года, а 25-го компания подтвердила ее наличие. Был ли выпущен патч, пока неизвестно.» ***(Антивирус Trend Micro можно использовать для запуска вирусов // SecurityLab.ru (https://www.securitylab.ru/news/501933.php). 22.10.2019).***

***

«Компания Microsoft запустила программу вознаграждения за обнаружение уязвимостей в ElectionGuard — программном обеспечении для выборов с открытым исходным кодом. Новая программа позволит исследователям выявлять проблемы в ПО и поможет повысить безопасность выборов.

ElectionGuard представляет собой SDK с открытым исходным кодом, призванном обеспечить безопасность процесса голосования. В ПО используется гомоморфное шифрование, гарантирующее, что результаты голосования остаются зашифрованными. ElectionGuard также позволяет проверять и точно подсчитывать бюллетени сторонним организациям без нарушения секретности или безопасности.

Размер вознаграждения будет зависеть от опасности проблемы и может достигать $15 тыс. Исследователям необходимо предоставить отчеты с четким POC-кодом, демонстрирующим, как обнаруженная уязвимость может затронуть безопасность пользователей.

ElectionGuard был официально запущен в мае, а в прошлом стал доступен для других компаний, позволив поставщикам технологий интегрировать программное обеспечение в свои системы голосования…» ***(Microsoft запустила программу вознаграждения за найденные уязвимости в ElectionGuard // SecurityLab.ru (https://www.securitylab.ru/news/501924.php). 22.10.2019).***

***

Технічні та програмні рішення для протидії кібернетичним загрозам

«Корпорація Google запускає нову функцію. Вона має назву Password Checkup і буде попереджати користувачів про те, що їхні паролі легко зламати.

Як сказано у блозі компанії, функцію запустили 2 жовтня. Password Checkup пропонуватиме користувачеві змінити пароль, який система вважатиме ненадійним.

Також користувачів попереджатимуть про те, що вони використовують однаковий пароль для декількох акаунтів адже це теж небезпечно.

До речі, перевірити надійність паролів можна на сайті passwords.google.com або в спеціальному додатку для Android. У Google також зазначили, що планують за замовчуванням вбудувати перевірку паролів у браузер Chrome…» ***(Google попереджатиме користувачів, якщо пароль легко зламати // Телеканал новин***

«24»(https://24tv.ua/techno/google_poperedzhatime_koristuvachiv_yakshho_parol_legko_zlamati_n1213820). 03.10.2019).

***

«Искусственный интеллект и системы, основанные на этой технологии, находят все большее применение в реальной жизни. Однако зачастую сфера их действия ограничивается анализом больших объемов данных или сложных вычислений. Но почему бы не применить ИИ в его, можно сказать, "естественной среде обитания"? В цифровом мире? Возможно, примерно так и подумали специалисты из Массачусетского технологического института (MIT) и Калифорнийского университета в Сан-Диего (UCSD) при создании ИИ, который будет охотиться на хакеров.

Угон IP-адресов становится все более популярной формой кибератак. Это делается по целому ряду причин: от рассылки спама и вредоносных программ до кражи криптовалюты и данных банковских карт. По некоторыми оценкам только в 2017 году подобные инциденты затронули более 10 процентов всех доменов в мире. Пострадали даже крупные игроки вроде Amazon и Google. Что уж говорить о более мелких компаниях.

Защитные меры по предотвращению перехватов IP-адресов обычно предпринимаются уже тогда, когда атака совершена. Но что, если эти события можно было бы предсказать и впоследствии отследить злоумышленников? Руководствуясь этим тезисом, команда специалистов проанализировала способы, которыми пользовались "серийные взломщики" и натренировала свою нейросеть вычислять подозрительную активность. В итоге она смогла идентифицировать примерно 800 подозрительных сетей и обнаружила, что некоторые из них систематически захватывали IP-адреса в течение многих лет.

"Для передачи данных между различными шлюзами используется динамический протокол маршрутизации (BGP). Однако у него есть два главных недостатка: отсутствует аутентификация и базовая верификация источника. Это делает его доступным для хакерских атак. Предоставив ИИ-алгоритму данные о совершенных в прошлом атаках, мы обучили модель искусственного интеллекта идентифицировать ключевые характеристики работы хакеров. Такие, как, например, множественные блокировки IP-адресов", — говорит ведущий автор работы Сесилия Тестарт …

Чтобы лучше определить тактику атак, группа ученых сначала извлекла данные по работе сетевых операторов за последние несколько лет. Исходя из этого, они смогли вывести корреляцию между взломом адресов и всплесками интернет-активности хакеров. После этого оставалось лишь "скормить" эти данные системе машинного обучения и "натаскать" ИИ.

Работа команды ученых — это первый шаг в создании автоматической системы предотвращения киберпреступлений. В будущем алгоритм будет лишь совершенствоваться. Полный отчет о проделанной работе и демонстрацию функционирующего ИИ по поиску хакеров ученые планирую представить уже в этом октябре на Международной IT-конференции в Амстердаме. Чуть позже они также обещают выложить на портал GitHub список обнаруженных ими подозрительных сетей.» ***(Да начнется битва: Искусственный интеллект***

"натравили" на хакеров // Телеграф (https://telegraf.com.ua/tehnologii/5188891-da-nachnetsya-bitva-iskusstvennyiy-intellekt-natravili-na-hakerov.html). 11.10.2019).

***

«Лаборатория Касперского» и Angara Technologies Group запускают в России новые управляемые системы защиты от сложных целевых кибератак (APT) на корпоративные сети – Angara Cyber Resilience Services EDR и antiAPT… EDR отслеживает все процессы, происходящие на компьютере, и, если возникает угроза, сообщает пользователю об инциденте и блокирует подозрительные файлы; antiAPT анализирует трафик между всеми устройствами, подключенными к сети через прокси-сервер, и проверяет почтовые ящики пользователей на наличие угроз, рассказывает гендиректор Angara Professional Assistance Оксана Васильева. Сами по себе решения EDR и antiAPT уже давно существуют на рынке, признает она, – новизна конкретной программы в том, что она предполагает удаленный доступ аналитиков Angara к системе киберзащиты клиента, прежде ему пришлось бы самому настраивать решение. Программа ориентирована на малый и средний бизнес, все чаще подвергающийся хакерским атакам в последние годы.

По словам директора департамента корпоративного бизнеса «Лаборатории Касперского» Вениамина Левцова, в схеме взаимодействия «Лаборатории Касперского» и Angara с заказчиком первая поставляет программные решения, которые выявляют вредоносную активность и упрощают реагирование на нее. Вторая – обеспечивает заказчика командой аналитиков, которые занимаются непрерывным мониторингом и расследуют каждый конкретный инцидент, говорит гендиректор Angara Technologies Group Сергей Шерстобитов. Системы защиты автоматические, но софт без экспертов будет для заказчика малоэффективен, говорит Васильева.

В плане маркетинга тема antiAPT перегрета в мировом масштабе, считает директор по развитию бизнеса компании Positive Technologies в России Максим Филиппов, но поймать таргетированную атаку исключительно в автоматическом режиме практически невозможно. Поэтому поставщики защиты от APT в том или ином виде добавляют в решения человеческую экспертизу: кто-то – команду экспертов, кто-то – телеметрию и облака, кто-то – новомодные техники (например, машинного обучения, различных видов анализа поведения и т. п.), рассказывает Филиппов. На сегодняшнем этапе это правильно и логично, считает он: без экспертных знаний, без человека эффективность средств защиты подобного класса – под большим вопросом.

Ядро antiAPT-решения от «Лаборатории Касперского» (Kaspersky Anti Targeted Attack) – эвристический анализатор, системно исследующий поведение подозрительных объектов в специально отведенной для этого виртуальной машине, объясняет Левцов: объект разбивается на подпроцессы, из которых состоит, и каждый запускается, после чего система анализирует его поведение и внешние коммуникации. Второй компонент решения, KEDR, позволяет в автоматизированном режиме искать сложные целевые атаки, продолжает Левцов. Эта система сканирует объекты сетевого пространства и, если какой-то из них вызывает подозрения, реагирует по одному из предопределенных правил: либо

изолирует станцию от сети, либо блокирует конкретный файл и направляет его в карантин…

По данным Positive Technologies, доля целенаправленных атак в последнее время превышает долю массовых: во II квартале 2019 г. – 59%, или на 12 процентных пунктов выше, чем в I квартале. В ходе расследований киберинцидентов экспертный центр безопасности Positive Technologies все чаще встречает атаки на крупные организации через компании-партнеры, рассказывает Филиппов: выбирая целью крупную компанию и понимая, что атака на нее в лоб потребует бОльших усилий, злоумышленники взламывают менее защищенного и менее крупного партнера этой организации и используют его как плацдарм для дальнейшей целенаправленной атаки.» ***(Петр Харатьян. Предложена новая система защиты бизнеса от кибератак // АО Бизнес Ньюс Медиа (https://www.vedomosti.ru/technology/articles/2019/10/09/813272-novaya-sistema-zaschiti). 09.10.2019).***

***

«Компания Mozilla выпустила патч, блокирующий возможности для осуществления атак внедрения кода в браузере Firefox.

«Эффективным способом борьбы с атаками внедрения кода является уменьшение поверхности атаки путем удаления потенциально опасных элементов из кодовой базы и усиления кода на различных уровнях. Для того чтобы сделать Firefox устойчивым к атакам внедрения кода, мы удалили встроенные скрипты и функции наподобие eval()», - сообщила команда безопасности Mozilla.

Mozilla переписала встроенный обработчик событий и перенесла встроенный JavaScript-код в заархивированные файлы для всех страниц about:pages браузера (ознакомиться со списком из 45 about:pages можно здесь), уязвимых к атакам внедрения кода через встроенные скрипты.

Страницы about:pages предоставляют пользователям простой интерфейс для проверки информации, связанной с внутренней работой Firefox (например, страница about: config предоставляет API для проверки и обновления настроек и параметров). Поскольку, как и все другие страницы браузера, about:pages используют HTML и JavaScript, злоумышленники могут внедрить вредоносные скрипты в контексте безопасности браузера и выполнять произвольные действия от лица пользователей Firefox.

Сделав невозможным внедрение встроенных скриптов на страницах about:pages в Firefox, Mozilla создала барьер против атак внедрения кода, которые могут привести к выполнению произвольного кода.» ***(Mozilla устранила вектор для атак внедрения кода в Firefox // SecurityLab.ru (https://www.securitylab.ru/news/501784.php). 15.10.2019).***

***

«Специалисты Национального института стандартов и технологий США (US National Institute for Standards and Technology, NIST) работают над технологией защиты от перехвата BGP, базирующейся на искусственном интеллекте.

Border Gateway Protocol (BGP) является ключевым протоколом интернета, к сожалению, открытым для злоупотребления. Злоумышленники могут с легкостью заставить сети передавать трафик туда, куда им нужно с целью слежения за пользователями, фишинга и пр. Хотя во многих случаях переадресация трафика происходит случайно из-за технических ошибок, за последние несколько лет злоумышленники не раз злоупотребляли BGP в крупномасштабных атаках.

Утечка маршрутов BGP происходит, когда оператор сети ошибочно объявляет блок IP-адресов другой сети. Проблема заключается в том, что определить, произошел инцидент случайно или кто-то вызвал утечку намеренно, невозможно. Даже если все указывает на злонамеренность, трафик может идти по неверному маршруту в течение нескольких часов, пока ситуация не будет исправлена.

Решением проблемы может стать новый алгоритм, разрабатываемый NIST. С помощью инфраструктуры открытых ключей для IP-адресов (RPKI) алгоритм позволяет облачным операторам и операторам сети, управляющим блоками IP-адресов, контролировать, какие сети могут объявлять непосредственный доступ к их блокам.

Специалисты NIST также работают над технологией проверки подлинности BGP, позволяющей маршрутизаторам с помощью RPKI фильтровать неавторизованные объявления маршрутов BGP.

Выявление проблем будет осуществляться с помощью искусственного интеллекта. Специалисты используют модель машинного обучения для автоматической идентификации автономных систем (так в таблицах маршрутов BGP обозначаются интернет-провайдеры), демонстрирующих характеристики, присущие перехвату BGP.

Модель обнаружения перехвата основывается на теории, что вызванное злоумышленником вредоносное поведение BGP согласовано со временем. С помощью анализа действий с течением времени исследователи стремились создать систему оценки, которая могла бы определять репутацию оператора.» ***(Новая технология на базе ИИ защитит от перехвата BGP // SecurityLab.ru (https://www.securitylab.ru/news/501684.php). 10.10.2019).***

***

«Компания Facebook добавила в Instagram новую функцию безопасности для защиты от фишинговых атак. Отныне, получив уведомление от Instagram, пользователи смогут проверять, действительно ли его прислала компания, или это приманка фишеров.

Для того чтобы проверить подлинность сообщения, нужно зайти в настройки приложения и в разделе «Безопасность» открыть «Письма от Instagram», где хранятся все полученные от Instagram уведомления за последние 14 дней. Рассылка обновления только началась и займет некоторое время.

Новое меню разделяет сообщения от Instagram на две категории – «уведомления безопасности» и «другое». Письма в данном разделе являются безопасными, и пользователи могут смело кликать на содержащиеся в них ссылки. Если письмо, якобы полученное от Instagram, в данном разделе отсутствует, значит, оно поддельное, и злоумышленники пытаются обмануть потенциальную жертву.

Новая функция безопасности является более чем желанной, поскольку число фишинговых атак постоянно растет, а сами фишеры становятся все более изобретательными и даже научились обходить двухфакторную аутентификацию.» ***(В Instagram появилась новая функция для защиты от фишинга // SecurityLab.ru (https://www.securitylab.ru/news/501629.php). 08.10.2019).***

***

«Американский производитель оборонных технологий Raytheon представил новое решение безопасности Cyber Anomaly Detection System (CADS), призванное защитить самолеты от «кибераномалий». Как сообщается на сайте Defense One, CADS представляет собой систему оповещения, предупреждающую пилотов в случае взлома компьютерных систем самолета.

По словам руководителя проекта Аманды Бьюкенен (Amanda Buchanan), ее команда работает над системой, которая давала бы пилотам полную картину происходящего с самолетом в режиме реального времени. Электроника многих самолетов намного проще по сравнению с электроникой наземных систем. Хотя в некоторых для передачи данных используются последовательные шины, ниша решений безопасности для пилотов на рынке все еще свободна, считают в Raytheon.

Во время демонстрационного тестирования инженеры Raytheon запустили симуляцию полета вертолета и с помощью планшета через беспроводное соединение внедрили вредоносный код, отключивший двигатель вертолета. Перед отключением двигателя система вывела предупреждение о «кибераномалии».

CADS предназначена для самолетов, где используются шины STD-1553 и ARINC-429. Шина STD-1553 является своего рода «трубопроводом» для внутренних коммуникаций в авиационных системах, в том числе в системе автопилотирования, GPS-навигации, выключения топливного клапана и пр. Шины MIL-STD-1553 в частности используются в вертолетах Вооруженных сил США Boeing CH-47 и AH-64, истребителях F-16 производства Lockheed Martin и F-15 производства Boeing». ***(Новая система оповещения предупредит пилотов в случае взлома самолета // SecurityLab.ru (https://www.securitylab.ru/news/501627.php). 08.10.2019).***

***

«Разработчики Mozilla укрепили защиту Firefox от атак внедрением кода, запретив использование встроенных скриптов (inline scripts) и функций eval() на служебных страницах браузера. Нововведения не позволят злоумышленникам выполнить вредоносную команду, изменить настройки браузера и похитить важные данные.

Обе опции, которые устранили специалисты, позволяют исполнять код в контексте приложения с его уровнем привилегий. Как отметил технический руководитель Mozilla по безопасности контента Кристоф Кершбаумер (Christoph Kerschbaumer), новые меры направлены на сокращение площади возможной атаки — теперь у злоумышленников будет меньше возможностей для злоупотребления возможностями браузера.

В Firefox встроено 45 служебных страниц about:, многие из которых открывают доступ к важным техническим данным. Например, about:config позволяет пользователю менять ключевые настройки браузера, на about:memory он может отслеживать потребление памяти, about:networking отображает информацию о сети.

Все эти страницы написаны на HTML и JavaScript. Поэтому взломщик может попытаться внедрить в них собственный код, который затем будет выполнен с теми же правами, с которыми работает Firefox. Исключение встроенных скриптов и eval-функций блокирует такую угрозу.

Теперь весь JavaScript-код будет исполняться, только если он был загружен через внутренний протокол браузера. Для этого разработчики Mozilla переписали все обработчики событий и перенесли встроенные JavaScript-сценарии в упакованные файлы для всех служебных страниц. Кроме того, была исключена возможность выполнения eval и подобных ей функций в контексте любого процесса, запущенного с системными привилегиями.

Специалисты также предусмотрели некоторые исключения из новых правил. Как пояснил Кершбаумер, некоторые пользователи используют вызов внешней eval-функции для кастомной настройки Firefox при запуске браузера. Это заменяет им компонент userChrome.js, который был заблокирован какое-то время назад из соображений безопасности. Эксперт Mozilla отметил, что в этом случае новый блокировщик будет разрешать выполнение eval().

Изменения не коснутся отображения интернет-сайтов в Firefox. В то же время разработчики намерены следить за тем, как потенциально опасные функции используются в сторонних расширениях и встраиваемых модулях. Если злоумышленники найдут новый способ применения этих команд, браузер будет отправлять уведомления команде безопасности Mozilla.» ***(Maxim Zaitsev. Firefox получил дополнительную защиту от инъекций кода // Threatpost (https://threatpost.ru/mozilla-hardens-firefox-against-code-injection-attacks/34523/). 16.09.2019).***

***

«Оператор сети Tor начал блокировать доступ к серверам с устаревшим программным обеспечением. В настоящее время в анонимной сети функционируют порядка 750 таких ретрансляторов; 62 из них используются как выходные узлы. По оценкам Tor Project, на долю попавших в черный список серверов приходилось чуть более 12% трафика в onion-зоне.

«Присутствие в сети релеев с истекшим сроком поддержки чревато рядом негативных последствий, — пишут участники проекта в блоге. — Релеи с устаревшей версией ПО ставят под угрозу стабильность и безопасность сети: они осложняют развертывание важных исправлений, а в некоторых случаях — и нововведений».

По данным Tor Project, на настоящий момент в состав анонимной сети входят более 6 тыс. активных узлов, использующих 85 различных вариантов ПО Tor. Самый давний релиз, 0.2.4.x, был введен в оборот в декабре 2013 года и уже не поддерживается. Из остальных на обновления могут претендовать лишь пять веток:

0.2.9.x (до 1 января 2020 года по программе долгосрочной поддержки — LTS);

0.3.5.x (LTS до 1 февраля 2022 года);

0.4.0.x (до 2 февраля 2020 года);

0.4.1.x (до 20 мая 2020 года, с надеждой на продление срока поддержки);

тестовая 0.4.2.x (выпуск стабильной версии запланирован на 15 декабря этого года).

В начале прошлого месяца членам сообщества Tor были разосланы письма с уведомлением о предстоящей чистке. Блокировка доступа к узлам с устаревшим ПО осуществляется по цифровым отпечаткам и пока через серверы каталогов (directory authority — выделенный сервер со списком всех ретрансляторов, в onion-сети таких справочников девять). С выпуском очередной стабильной версии Tor (должна выйти в ноябре) участники проекта надеются поставить блокировку на поток: они уже готовят опцию, которая будет по умолчанию пресекать попытки установить потенциально опасное соединение.

В стоплист также будут включены ненадежные мостовые узлы анонимной сети, которые пока не блокируются. Операторам Tor-релеев настоятельно рекомендуется обновить используемое ПО — в идеале до последней стабильной версии (в настоящий момент это 0.4.1.6).

Комментируя новую меру безопасности onion-сети для издания ZDNet, эксперт TorWorld, известный в Сети как Lunar, отметил: «По моему мнению, операторы этих релеев попросту халатно относятся к своим обязанностям — у хостеров такое случается сплошь и рядом. Большинство не волнует, что их серверы работают под ОС с истекшим сроком поддержки и используют устаревшее программное обеспечение. Они не примут никаких мер, пока что-нибудь не разладится или не откажет». ***(Maxim Zaitsev. Tor Project повысил безопасность анонимной сети // Threatpost (https://threatpost.ru/tor-project-starts-removing-end-of-life-relays-from-its-network/34456/). 10.10.2019).***

***

«…Киберполиция внедрила для предприятий новую систему оповещения ENS (Emergency Notification System). С ее помощью компании смогут получать информацию о совершенных против них кибератаках, сообщил руководитель департамента Сергей Демедюк.

В рамках форума «Кибербезопасность. Защити свой бизнес» Демедюк рассказал, что если компании сами не будут сообщать о кибератаке в госструктуры, те, длительное время могут ничего не знать о совершенной атаке и не смогут предпринять необходимые меры.

Мы выступаем с инициативой создания механизма, который позволит частным компаниям сообщать нам деперсонифицированные данные об обстоятельствах кибератак, без официального заявления о совершенном преступлении. Это позволит нам (правоохранительным органам - ред.) своевременно реагировать на угрозу и даже предупреждать ее…

Как отмечает пресс-служба ведомства, внедренная киберполицией система ENS способна информировать всех подключенных к ней субъектов о совершенных кибератаках. В частности, оповещение проинформирует о факте атаки, ее

признаках и факторах компрометации.» ***(Представлена система быстрого информирования бизнеса о кибератаках // PaySpace Magazine (https://psm7.com/security/predstavlena-sistema-bystrogo-informirovaniya-biznesa-o-kiberatakax.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+Payspacemagazine+%28Payspacemagazine%29). 17.10.2019).***

***

«Firefox единственный из браузеров получил максимальные баллы в аудите, который недавно проводил Федеральный офис информационной безопасности Германии (Bundesamt für Sicherheit in der Informationstechnik — BSI). Всего германскими экспертами тестировались четыре веб-браузера: Mozilla Firefox 68 (ESR), Google Chrome 76, Microsoft Internet Explorer 11 и Microsoft Edge 44. За бортом остались все прочие браузерные программы, в том числе Safari, Brave, Opera или Vivaldi.

В ходе испытаний проверялось соответствие этих программ требованиям, изложенным в руководстве по «современным безопасным браузерам», которое BSI опубликовал в сентябре 2019 года. BSI применяет этот документ, чтобы рекомендовать государственным и частными организациям браузеры, безопасные в использовании.

Первая редакция руководства по безопасным браузерам вышла в Германии в 2017 году. Этим лето она была пересмотрена с учётом новейших технологий обеспечения безопасности, таких как HSTS, SRI, CSP 2.0, обработка телеметрии и улучшенные механизмы работы с сертификатами.

Согласно информации BSI, только Firefox смог продемонстрировать соответствие необходимому минимуму обновлённых требований к «безопасному», браузеру. В их число входят: поддержка TLS, HTTP Strict Transport Security (HSTS) (RFC 6797), Same Origin Policy (SOP). Content Security Policy (CSP) 2.0, Sub-resource integrity (SRI). Браузер должен иметь защиту памяти уровня ОС, изолировать (лучше всего в виде отдельных процессов) открытые веб-страницы, проверять загруженные сертификаты по списку аннулированных сертификаций (CRL) или по протоколу онлайнового статуса сертификатов (OCSP), поддерживать автоматические обновления, шифровать записи в менеджере паролей и удалять их при необходимости, также как файлы куки, историю автозавершений и посещений страниц, и многое другое.

Не прошедшие аудит браузеры имели следующие упущения:

отсутствовала поддержка мастер-пароля (Chrome, IE, Edge);

не было встроенного механизма обновлений (IE);

не предусмотрено блокирование сбора телеметрии (Chrome, IE, Edge);

нет поддержки SOP (IE), CSP (IE), SRI (IE);

не предусмотрено профилей браузера, различных конфигураций (IE, Edge);

отсутствует организационная прозрачность (Chrome, IE, Edge).»

(В аудите браузеров Офиса кибербезопасности Германии лидировал Firefox // Компьютерное Обозрение (https://ko.com.ua/v_audite_brauzerov_ofisa_kiberbezopasnosti_germanii_lidiroval_firefox_130551). 18.10.2019).

***

«На первом глобальном саммите Acronis, проходящем в Майами, компания представаила решения, предназначенные для обеспечения современных требований к кибербезопасности.

…Число устройств и обмен данными между разными устройствами, местоположениями и облачными сервисами растет и создает все большую сложность для инфраструктуры работы с данными. Такая децентрализованная система становится уязвима для кибератак. Acronis опирается на опыт защиты своих клиентов — 500 000 компаний и 5,5 миллионов физических пользователей — с помощью технологии Acronis Active Protection. В 2018 году она предотвратила более 400 000 атак программ-вымогателей и уберегла клиентов от сотен миллионов долларов ущерба.

«Сегодняшняя зависимость от данных создает новые вызовы, с которыми компаниям никогда приходилось сталкиваться прежде. Существующие системы не были созданы для таких задач, — заявила Сергей Белоусов, основатель и генеральный директор Acronis. — Для их решения необходим новый подход к управлению и защите данных, который будет направлен на защиту, доступность, конфиденциальность, подлинность и безопасность данных. Acronis называет их "Пять векторов киберзащиты", или SAPAS, а наш набор решений для кибербезопасности специально разработан так, чтобы работать по всем направлениям».

Новые и обновленные решения доступны через глобальную партнерскую сеть Acronis в которой более 50 000 партнеров, и включают:

Acronis Cyber Protect – объединение семи ключевых функций кибербезопасности в единое простое решение. В него входит резервное копирование, аварийное восстановление, защита от вредоносных программ на основе ИИ, сертификация и проверка подлинности данных, оценка уязвимостей, управление исправлениями и удаленный мониторинг и управление.

Acronis Cyber Platform – возможность для разработчиков интегрировать собственные решения с Acronis Cyber Protection.

Acronis Cyber Infrastructure – реализация экономичной, простой в использовании и надежной гиперконвергентной инфраструктуры, оптимизированной для развертывания киберзащиты…». ***(Представлены решения семейства Acronis Cyber Protection // Компьютерное Обозрение (https://ko.com.ua/predstavleny_resheniya_semejstva_acronis_cyber_130532). 17.10.2019).***

***

«Компания Mozilla добавила в свой браузер Firefox новую функцию безопасности, позволяющую пользователям видеть, кто конкретно следит за их действиями в Сети. Функция будет представлять отчеты обо всех cookie-файлах и трекерах, обнаруженных и заблокированных за заданный период. Таким образом, пользователи смогут понять, почему им отображается та или иная реклама, и какие сайты следят за их активностью в интернете.

В отчете о заблокированных отслеживающих технологиях также будут указаны все попытки создания цифрового отпечатка с целью идентификации пользователя и попытки установки майнера криптовалюты. Кроме того, Firefox

теперь позволяет проверять хранящиеся в менеджере паролей Firefox Lockwise учетные данные на предмет утечки, поскольку браузер может сверять содержимое менеджера с имеющимися у него списками утекших данных.

Функция блокировки отслеживающих технологий Enhanced Tracking Protection (ETP) по умолчанию включена во всех версиях Firefox, начиная с Firefox 69, вышедшего в сентябре нынешнего года. Функция «Protection Report» («Отчет о защите»), отображающая информацию о заблокированных ETP скриптах, впервые появилась в ночной сборке Firefox 69….

Отчет ETP включает:

Данные по количеству заблокированных попыток отметить пользователя с помощью cookie-файлов, установки криптовалютных майнеров, снятия цифровых отпечатков и использования межсайтовых трекеров;

Данные о потенциально небезопасных и скомпрометированных паролях;

Сведения об учетных данных, безопасно хранящихся в Firefox Lockwise.»

(Firefox позволяет пользователям следить за отслеживающими технологиями // SecurityLab.ru (https://www.securitylab.ru/news/501975.php). 23.10.2019).

***

«Если у компании Apple есть полный контроль над своим аппаратным обеспечением, то Microsoft этим похвастаться не может. Однако теперь Microsoft получит контроль на том же уровне, что и Apple, и в этом ей помогут производители Windows-ПК. Целью компании является защита устройств от атак на прошивку, у которой привилегии выше, чем у ядра Windows.

Microsoft является производителем не только программного, но и аппаратного обеспечения. Усвоив на примере Xbox уроки взлома технических средств защиты авторских прав (DRM), компания намерена перенести полученный опыт на экосистему Windows в рамках новой инициативы Secured-core, сообщил партнерский директор по безопасности Windows Дэвид Уэстон (David Weston) изданию ZDNet.

Инициатива распространяется только на самые новые модели устройств под управлением Windows 10 с процессорами Intel, Qualcomm и AMD. Пользователи высококлассных устройств наподобие ноутбуков Surface Pro X и HP Dragonfly получат дополнительный уровень защиты, изолирующий ключи шифрования и идентификационные данные на Windows 10, которые могут быть скомпрометированы в результате атак на прошивку.

Новая функция безопасности прошивки System Guard станет частью Windows Defender. Данная функция предназначена для защиты Windows 10 от атак киберпреступной группировки APT28 (другое название Fancy Bear), в арсенале которой есть первый в мире рабочий руткит UEFI.» ***(Устройства под управлением Windows 10 получат защиту от атак на прошивку // SecurityLab.ru (https://www.securitylab.ru/news/501968.php). 22.10.2019).***

***

Актуальні питання забезпечення службово-бойової діяльності сил сектору безпеки і оборони : Матеріали регіонального круглого столу (м. Харків, 19 квітня 2019 року). – Харків, 2019. - Вип. 3. - 306 с.

Зі змісту:

- Голубничий Д.Ю., Ільїна І.В., Семеренко Ю.О., Радівілова А.С. Активний захист інформації при протидії кіберзагрозам в інформаційно-телекомунікаційній мережі;
- Голубничий Д.Ю., Соловйова О.І., Мартовицький В.О., Борщевський О.О. Захист електронної пошти з використанням інфраструктури відкритого ключа.

Шифр зберігання НБУВ: В357905/3

***

Бондаренко О. Аналіз загроз безпеці розвитку країн крізь призму кіберзлочинності / Бондаренко Олена // Науковий вісник Східноєвропейського національного університету імені Лесі Українки. Міжнародні відносини. - 2018. - № 5. - С. 54-65.

Проаналізовано статистичні дані двадцяти показників, які розкривають загрози безпеці країн. Установлено, що злочинність в інформаційній сфері чинить суттєві перешкоди для розвитку країн.

Шифр зберігання НБУВ: Ж69212

***

Довженоко О.Ю. Деякі питання призначення комп'ютерно-технічної експертизи під час розслідування кіберзлочинів / Довженоко О.Ю. // Науковий вісник Ужгородського національного університету. Серія : Право. - 2019. - Вип. 55(2). - С. 124-127.

Розглянуто деякі питання призначення комп'ютерно-технічної експертизи під час розслідування кіберзлочинів. Проаналізовано сучасний стан правового регулювання цього питання. Наведено рекомендації щодо постановки питань слідчим під час призначення комп'ютерно-технічної експертизи у справах про кіберзлочини.

Шифр зберігання НБУВ: Ж68850/пр.

***

Довженко О.Ю. До питання про тактику допитів у справах про кіберзлочинність /Довженоко О.Ю. // Науковий вісник Міжнародного гуманітарного університету. Серія : Юриспруденція. - 2019. - Вип. 37. - С. 143-145.

Розглянуто деякі питання призначення і проведення допитів під час розслідування кіберзлочинів. Проаналізовано сучасний стан правового регулювання даного питання. Наведено рекомендації щодо постановки питань слідчим у процесі призначення та проведення допиту у справах про кіберзлочини.

Шифр зберігання НБУВ: Ж74042/юр.

***

Забезпечення прав людини четвертого покоління у системі охорони здоров'я : матеріали Міжнар. наук.-практ. конф. (12 квіт. 2019 р., м. Ужгород). - Ужгород, 2019. - 200 с.

Зі змісту:

- Логвиненко О.Л. Окремі питання забезпечення права на охорону здоров'я у кіберпросторі.

Шифр зберігання НБУВ: ВА836471

***

Збірник тез доповідей ІІ Всеукраїнської науково-практичної конференції молодих учених, курсантів та студентів «Авіація, промисловість, суспільство» : (посвідчення № 72 від 22.02.209 р.) = Сборник тезисов докладов Всеукраинской научно-практической конференции молодых ученых, курсантов и студентов «Авиация, промышленность, общество» : (свидетельство № 72 от 22.02.2019 г.). - Кременчук, 2019. - 475 с.

Зі змісту:

- Борисенко О.М. Основні проблеми кібербезпеки транспортної галузі;
- Гиренко В.О. Інформаційна безпека в умовах сучасного розвитку інформаційних технологій. Кібербезпека;
- Гордыман Н.С., Соколов Д.М. Проблемы кибербезопасности и пути их решений.

Шифр зберігання НБУВ: ВА836459

***

Живило Є.О. Сутність основних завдань системи кібероборони України / Живило Євген Олександрович // Теорія та практика державного управління. - 2019. - Вип. 2. - С. 263-279.

Проаналізовано сутність сучасних напрямів створення та функціонування системи кібероборони держави. Визначено, що для сучасної України успішний перехід до реалізації заходів із підготовки та ведення кібероборони можливий лише за умови попереднього визначення напрямів і завдань функціонування системи кібероборони. Сформульовано висновки щодо ролі нинішнього політико-правового курсу функціонування системи кібероборони. Запропоновано подальші вимоги до набуття спроможностей сектору безпеки і оборони держави в системі кібероборони України на основі найкращих практик держав – членів ЄС та країн – членів НАТО.

Шифр зберігання НБУВ: Ж72481

***

Кримінальна відповідальність за несанкціоноване втручання в роботу ЕОМ : монографія / Ю. А. Бельський [та ін.]. - Київ : Юрінком Інтер, 2019. - 263 с.

Досліджено теоретичні і практичні питань кримінальної відповідальності за злочин, передбачений ст. 361 Кримінального кодексу України. Проаналізовано

історичний та зарубіжний досвід кримінальної відповідальності за несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. Визначено об'єктивні та суб'єктивні ознаки складу вказаного злочину, його кваліфікуючі ознаки, а також покарання за вчинення цього злочину. На підставі отриманих результатів наукового дослідження вироблено низку пропозицій щодо удосконалення кримінальної відповідальності за несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку.

Шифр зберігання НБУВ: ВА835495

***

Островий О. В. Формування державної політики забезпечення кібернетичної безпеки в Україні : автореф. дис. ... канд. наук з держ. упр. : 25.00.02 / Островий Олексій Володимирович ; Донец. держ. ун-т упр. - Маріуполь, 2019. - 20 с.

Поглиблено теоретичні засади та науково-методичні і практичні рекомендації щодо формування державної політики забезпечення кібернетичної безпеки. Узагальнено та систематизовано теоретичні основи формування державної політики забезпечення кібернетичної безпеки. Досліджено зарубіжний досвід державної політики забезпечення кібернетичної безпеки і виявлено можливості його адаптації до вітчизняних умов. Удосконалено методичні засади аналітичного забезпечення державного управління кібернетичною безпекою. Розвинуто методичні підходи до формування державної політики забезпечення кібернетичної безпеки. Аргументовано концепцію формування державної політики забезпечення національної кібернетичної безпеки. Запропоновано методичний підхід до обґрунтування напрямів управлінського впливу в сфері кібернетичної безпеки на основі методів моделювання Удосконалено механізм формування державної політики забезпечення кібернетичної безпеки.

Шифр зберігання НБУВ: РА441934

***

Релейний захист та кібербезпека енергетичних систем : [підручник]. - Харків, 2019. - 389 с.

Розглянуто теорію та практику стосовно традиційних і мікропроцесорних релейних захистів для основних елементів систем виробництва і розподілу електричної енергії, енергоблоків, ліній, шин та трансформаторів. Надано практичні приклади розрахунків захистів і аналізу роботи релейного захисту і автоматики, та кібербезпеки енергосистем.

Шифр зберігання НБУВ: ВА835534

***

Савенко О. С. Теорія та практика створення розподілених систем виявлення зловмисного програмного забезпечення в локальних комп'ютерних мережах : автореф. дис. ... д-ра техн. наук : 05.13.05 / Савенко Олег Станіславович ; Нац. ун-т "Львів. політехніка". - Львів, 2019. - 40 с.

Запропоновано удосконалену модель архітектури розподіленої системи виявлення зловмисного програмного забезпечення в локальних комп'ютерних мережах та модель архітектури її типових компонентів на основі структур Кріпке, а також метод взаємодії компонентів розподіленої багаторівневої системи виявлення зловмисного програмного забезпечення для підтримки її цілісності та визначення порядку передачі знань між її компонентами. Розроблено метод виявлення бот-мереж у локальних комп'ютерних мережах, суть якого полягає в здійсненні активного моніторингу системних подій та узгодженій взаємодії компонентів розподіленої системи при прийнятті рішення. Представлено метод виявлення файлового зловмисного програмного забезпечення в локальних комп'ютерних мережах, який полягає в поєднанні роботи програмних агентів, що здійснюють виявлення зловмисного програмного забезпечення в окремих комп'ютерних системах.

Шифр зберігання НБУВ: РА441907

***

Яцишин М. Ю. Міжнародно-правове співробітництво у сфері боротьби з кіберзлочинністю : автореф. дис. ... канд. юрид. наук : 12.00.11 / Яцишин Марта Юріївна ; Київ. нац. ун-т ім. Тараса Шевченка. - Київ, 2019. - 20 с.

Здійснено узагальнення основних засад універсальної концепції кіберзлочинності, а також визначення шляхів її розвитку. Розкрито сутність цього поняття, визначено його основні ознаки, узагальнено класифікацію. Охарактеризовано процес еволюції інституту міжнародно-правового співробітництва у сфері боротьби з кіберзлочинністю. Особливу увагу приділено окремим перспективним напрямам міжнародно-правового співробітництва держав щодо протидії кібернетичним злочинам. Досліджено міжнародноправове регулювання кібервоєн. Розглянуто шляхи удосконалення матеріальних та процесуальних норм інституту міжнародно-правового співробітництва у сфері боротьби з кіберзлочинністю. Здійснено аналіз правових та інституційних основ протидії кіберзлочинності в Україні. Визначено можливості міжнародно-правової кваліфікації кібератак, вчинених на території України під час агресії Російської Федерації.

Шифр зберігання НБУВ: РА440872

***