KASPERSKY lab

Kaspersky Security Bulletin 2018

ВАЖНЫЕ СОБЫТИЯ ГОДА

Дэвид Эмм, Виктор Чебышев

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

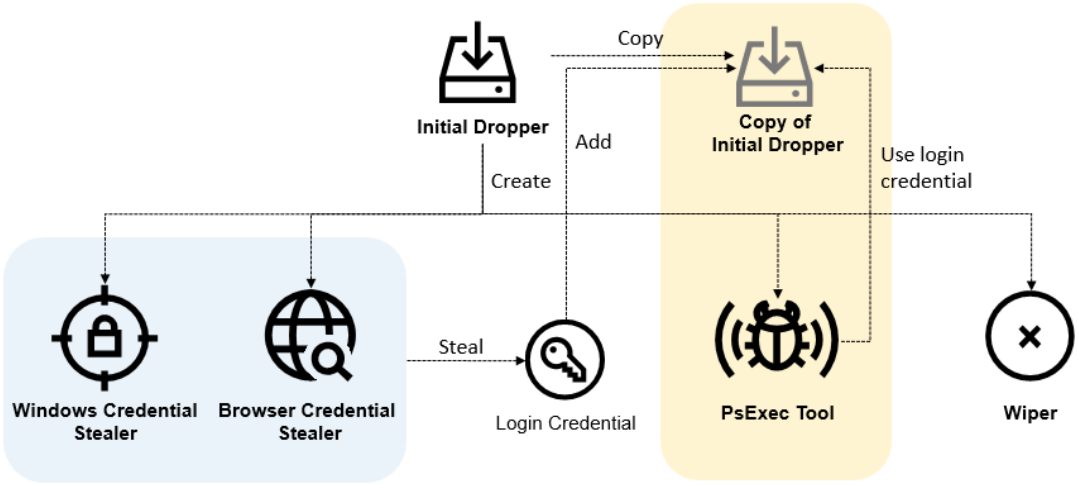
Интернет прочно вошел в нашу жизнь: онлайн-банкинг, онлайн-шоппинг, общение в Сети стали обычным делом для множества людей. Для коммерческих организаций интернет стал источником жизненной силы. Зависимость государств, бизнеса и потребителей от интернет-технологий предоставляет киберпреступникам широкие возможности для проведения атак, с какими бы то ни было целями – кража денег или данных, нарушение работы, нанесение ущерба, в том числе репутационного, или просто «для лулзов». В результате мы имеем ландшафт угроз, в котором высокотехнологичные целевые атаки соседствуют со спонтанной ситуативной киберпреступностью. Нередко и в том, и в другом случае применяются технологии манипулирования человеческой психологией как способ скомпрометировать целые системы или отдельные компьютеры. Все чаще среди атакуемых устройств оказываются те, которые мы не считаем компьютерами – от детских игрушек до камер наблюдения. Представляем вам наш ежегодный обзор крупных инцидентов и ключевых тенденций 2018 года.

ЦЕЛЕВЫЕ АТАКИ

Одним из наиболее интересных докладов наших исследователей на конференции Kaspersky Security Analyst Summit в этом году стал отчет о Slingshot — крайне изощренной шпионской кампании, действующей с 2012 года на Ближнем Востоке и в Африке. Мы обнаружили эту угрозу, которая по своей сложности может посоперничать с Regin и ProjectSauron, в процессе расследования инцидента. Slingshot использует необычный (и насколько мы знаем, уникальный) вектор атаки: своих жертв преступники атаковали через скомпрометированные роутеры MikroTik. Точный способ компрометации устройств не до конца понятен, но киберпреступники нашли способ добавить свой вредоносный DLL. Библиотека подгружала целый букет вредоносных файлов, которые затем хранились на роутере. Когда системный администратор входит в систему для настройки маршрутизатора, программное обеспечение управления маршрутизатором загружает и запускает вредоносный модуль на его компьютере. Slingshot загружает на компьютер жертвы несколько модулей, в том числе два огромных и мощных — Cahnadr, работающий в режиме ядра, и GollumApp, работающий в режиме пользователя. Эти два модуля реализуют большинство процедур для закрепления в системе, управления файловой системой, фильтрации данных и взаимодействия с C&C-сервером. Образцы, которые мы изучали, имели маркировку «версия 6.x», т.е. можно предположить, что угроза существует уже достаточно долго. Время, навыки и стоимость, затраченные на создание Slingshot, говорят о том, что стоящая за ним группировка скорее всего является высокоорганизованной и профессиональной, и, вероятно, спонсируется государством.

Вскоре после церемонии открытия Зимней олимпиады в Пхенчхане мы стали получать сообщения об атаках на инфраструктуру Игр. Тогда Olympic Destroyer парализовал работу IT-систем: были отключены экраны, не было сети Wi-Fi, не работал официальный веб-сайт Олимпиады, из-за чего болельщики не могли распечатать билеты. Атака также затронула другие организации в регионе, например, на нескольких горнолыжных курортах Южной Кореи была нарушена работа горнолыжных подъемников. Olympic Destroyer – это сетевой червь, целью которого является уничтожение файлов, найденных в сетевых папках доступных текущему пользователю. Сразу после атаки международные исследовательские группы и медиа-компании стали называть в качестве ее автора Россию, Китай и Северную Корею, основываясь на ряде функций зловреда, которые ранее использовали в своей деятельности кибершпионские группировки, якобы расположенные в этих странах или работавшие на правительства этих стран. Наши исследователи тоже попытались выяснить, какая группировка стоит за этой атакой. На одном из этапов

исследования мы увидели признаки, указывавшие на группировку Lazarus. Мы обнаружили оставленный злоумышленниками уникальный след, который полностью соответствовал ранее известному вредоносному компоненту Lazarus. Однако отсутствие очевидных мотивов и выявленные нами во время исследования на зараженном объекте в Южной Корее несовпадения с почерком и методами Lazarus, заставили нас вернуться к рассмотрению данного артефакта. После тщательного изучения оказалось, что набор функций не соответствует коду: стало ясно, что мы имеем дело с подделкой, которая точно имитировала почерк Lazarus. Из этого мы сделали вывод, что «почерк» был очень сложным «ложным флагом», намеренно добавленным во вредоносную программу, чтобы создать у аналитиков впечатление, будто они нашли неоспоримое доказательство участия группировки Lazarus, и помешать точной атрибуции угрозы.

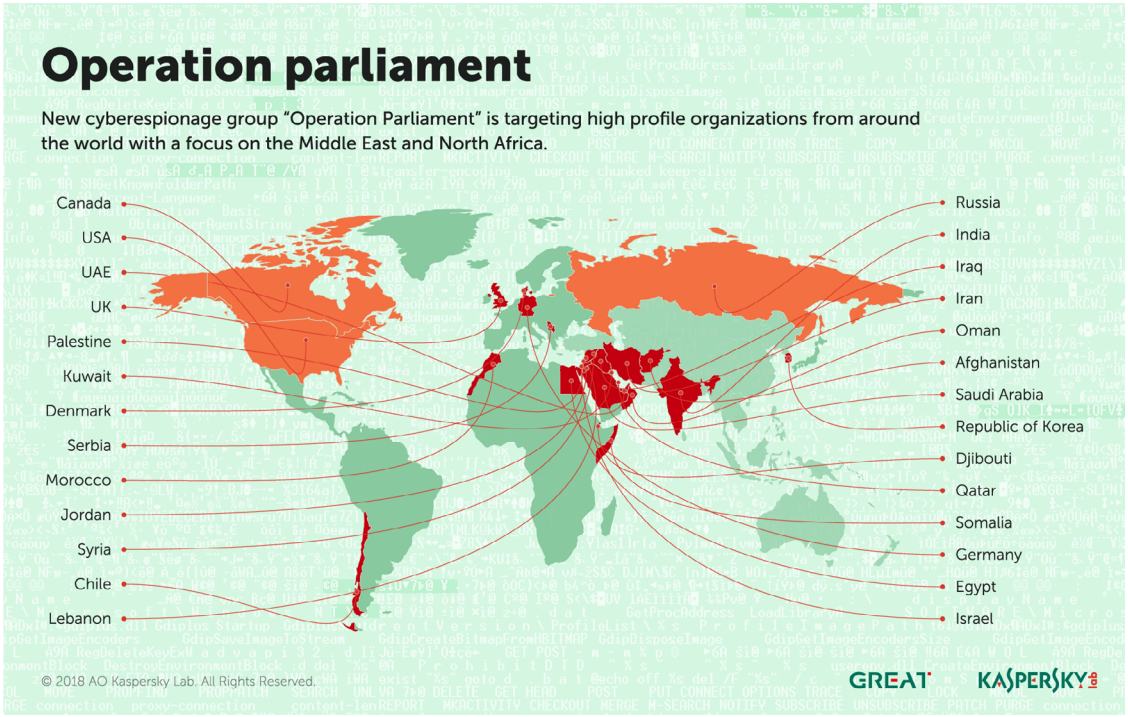


Связь компонентов OlympicDestroyer

Мы продолжили отслеживать деятельность данной APT-группировки и в июне заметили, что она начала новую кампанию с новой географией жертв и с использованием новых тем. По данным нашей телеметрии и судя по характеристикам проанализированных нами спирфишинговых документов, атаки Olympic Destroyer теперь нацелены на финансовые и биотехнологические организации, расположенные в Европе, а именно в России, Нидерландах, Германии, Швейцарии и Украине. Ранее описанные атаки Olympic Destroyer были направлены на уничтожение и вывод из строя инфраструктуры Зимних Олимпийских Игр, обслуживающих организаций, партнеров Олимпиады и мест проведения мероприятий. Им предшествовал этап

разведки. Возможно, новые действия злоумышленников опять являются разведкой, за которой последует волна деструктивных атак с новыми мотивами. Целью новых атак стала разнообразная группа как финансовых, так и нефинансовых организаций; это может указывать на то, что зловред используется несколькими группировками с различными интересами. Другой причиной может быть аутсорсинг, что не редкость при проведении кибератак в интересах конкретных государств. Наконец, возможно также, что финансовый мотив служит лишь прикрытием для кибератак; в прошлой кампании данная кибергруппировка уже показала свое мастерство в проведении операций под ложным флагом.

В апреле мы рассказывали о том, как «работает» Operation Parliament – кампания по кибершпионажу, целями которой являются крупнейшие законодательные, исполнительные и судебные организации по всему миру, причем основное внимание уделяется Ближнему Востоку и Северной Африке, особенно Палестине. В списке мишеней атак, начавшихся в первые месяцы 2017 года, парламенты, сенаты, высшие государственные чиновники и должностные лица, ученые-политологи, военные и разведывательные структуры, министерства, средства массовой информации, исследовательские центры, избирательные комиссии, олимпийские организации, крупные торговые компании и прочие. Выбор жертв отличается от предыдущих кампаний на Ближнем Востоке, организованных группами Gaza Cybergang и Desert Falcons, и указывает на то, что атаки предварял тщательный сбор информации (физической и цифровой). Чтобы защитить свои командные серверы от обнаружения, киберпреступники особенно внимательно проверяли устройства-жертвы, прежде чем приступить к заражению. Похоже на то, что с начала 2018 года количество атак уменьшилось, вероятно, после того, как нападавшие достигли своих целей.



Мы продолжили наблюдать за деятельностью Energetic Bear/Crouching Yeti – широко известной APT-группы, действующей по крайней мере с 2010 года. Как правило, участники группы атакуют различные компании с явным фокусом на энергетику и промышленность. Атакованные организации разбросаны по всему миру с заметным преобладанием Европы и США. В 2016 – 2017 годах значительно выросло количество атак на компании в Турции. Основная тактика группы включает рассылку фишинговых писем с вредоносными документами, заражение серверов с различными целями, в т.ч. для размещения на них различных инструментов и логов, а также для проведения атак watering hole. О недавней активности этой группировки, направленной против целей в США, говорится в опубликованном US-CERT документе, а также в бюллетене Национального центра кибербезопасности Великобритании (National Cyber Security Centre). В апреле Kaspersky Lab ICS CERT опубликовала отчет, в котором представлены сведения об обнаруженных серверах, зараженных и используемых группировкой, а также приведены результаты анализа нескольких веб-серверов, скомпрометированных группой Energetic Bear в течение 2016 – в начале 2017 года. Полностью отчет можно прочитать здесь, а ниже приведены краткие результаты анализа скомпрометированных серверов и действий на них атакующих:

1. За исключением редких случаев, участники группы довольствуются публично доступным инструментарием. Это делает задачу атрибуции атак без дополнительных «маркеров» группы весьма сложной.
2. Потенциально любой уязвимый сервер в интернете представляет для атакующих интерес в качестве «плацдарма» для развития дальнейших атак на целевые объекты.
3. В большинстве наблюдаемых нами случаев группа выполняла задачи по поиску уязвимостей, закреплению на различных узлах, краже аутентификационных данных.
4. Разнообразие жертв может говорить о разнообразии интересов атакующих.
5. С некоторой долей уверенности можно предположить, что группа работает в интересах или по заданиям от внешних по отношению к ней заказчиков, выполняя первоначальный сбор данных, кражу данных аутентификации и закрепление на подходящих ресурсах для обеспечения возможности дальнейшего развития атаки.

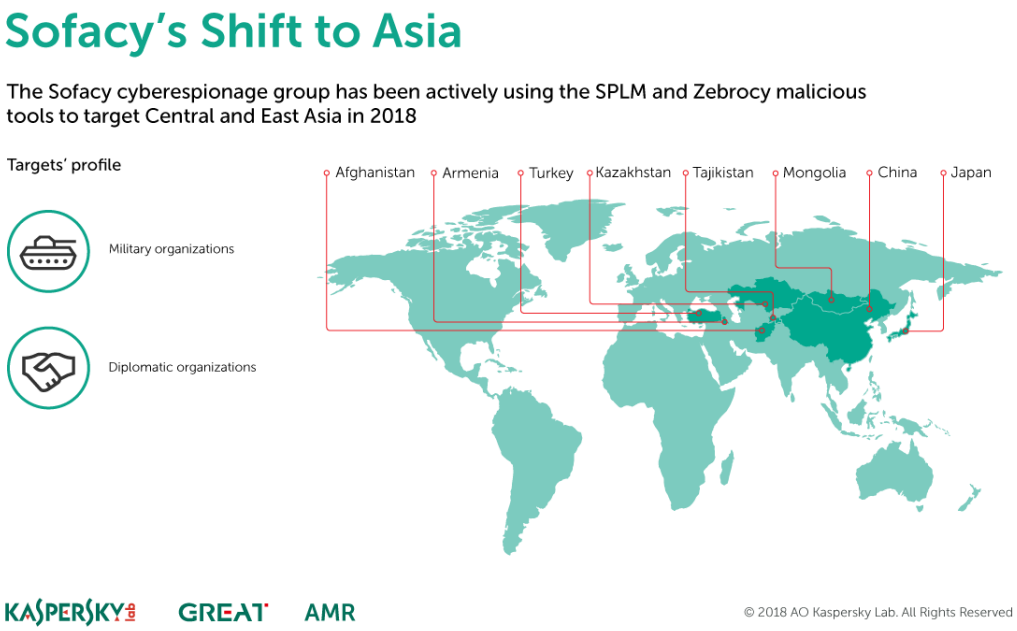
В мае аналитики Cisco Talos опубликовали результаты своего исследования VPNFilter – вредоносного ПО, используемому для заражения маршрутизаторов различных производителей в 54 странах мира, но в первую очередь на Украине. Вы можете прочить их отчеты здесь и здесь. Первоначально они считали, что вредоносная программа заразила порядка 500 000 маршрутизаторов Linksys, MikroTik, Netgear и TP-Link компаний малого бизнеса, а также сетевые накопители QNAP. Однако позже выяснилось, что список производителей зараженных маршрутизаторов намного длиннее — всего 75, включая ASUS, D-Link, Huawei, Ubiquiti, UPVEL и ZTE. Вредоносная программа способна вывести зараженное устройство из строя, выполнять shell-команды для совершения дальнейших манипуляций, создать конфигурацию TOR для анонимного доступа к устройству, сконфигурировать порт и URL-адрес прокси-сервера на маршрутизаторе для манипулирования сеансами браузера. Дальнейшие исследования показали, что вредоносное ПО может распространяться по сети через подключенные устройства, тем самым расширяя область атаки. Специалисты Центра глобальных исследований и анализа угроз «Лаборатории Касперского» (GReAT) проанализировали механизм обработки данных, используемый VPNFilter. Еще один интересный вопрос — кто стоит за этим вредоносным ПО. Cisco Talos считает, что ответственность за него несет киберпреступная группа с государственной поддержкой. В своем письменном заявлении о развертывании sinkhole-маршрутизатора на домене командного сервера ФБР называет предположительным виновником «преступления» группу

Sofacy (она же APT28, Pawn Storm, Sednit, STRONTIUM и Tsar Team). Есть небольшое совпадение кода с вредоносным ПО BlackEnergy, использованным в предыдущих атаках на Украине (в заявлении ФБР указывает, что оно рассматривает BlackEnergy (также известна как Sandworm) как подгруппу Sofacy).

Sofacy — очень активная и плодовитая кибершпионская группа, за которой «Лаборатория Касперского» наблюдает на протяжении нескольких лет. В феврале мы опубликовали отчет о деятельности Sofacy, в котором говорится, что с начала 2017 года интерес группировки постепенно смещался от целей, связанных с НАТО, в сторону целей на Ближнем Востоке, в Центральной Азии и за ее пределами. Для кражи информации — учетных данных, конфиденциальных сообщений, документов и пр. — Sofacy использует целевой фишинг и атаки типа watering hole, а для развертывания своего вредоносного ПО — уязвимости нулевого дня. Для целей разного профиля Sofacy использует разные инструменты. В начале 2017 года для атак на военные и дипломатические организации (в основном в странах НАТО и Украине) группировка запустила кампанию группы «Dealer's Choice». Позже в этом году группа использовала и другие инструменты из своего арсенала - Zebrocy и SPLM — для охвата более широкого круга организаций, включая научно-технические центры и пресс-службы, и все в большей степени ориентируясь на Центральную и Восточную Азию. Опытные кибергруппировки, такие как Sofacy, постоянно разрабатывают новые инструменты для использования в атаках. Группа поддерживает высокий уровень скрытности своих действий и уделяет много внимания тому, чтобы ее вредоносное ПО было трудно обнаружить. В случае с такими группами как Sofacy при обнаружении любых признаков их активности в сети необходимо срочно проверить все факты аутентификации и странные случаи администраторского доступа к системе, тщательно проверять и помещать в «песочницу» входящие вложения, а также поддерживать двухфакторную аутентификацию для таких сервисов, как электронная почта и доступ к VPN. Использование отчетов об APT-угрозах, инструментов для поиска и выявления угроз, таких как правила YARA, и новейших решений для защиты от целенаправленных атак, таких как KATA (Kaspersky Anti Targeted Attack Platform), поможет выявить цели этих атак и предоставит мощные способы обнаружения вредоносных действий.

Наши исследования показывают, что Sofacy – не единственная действующая в Азии кибергруппировка, и это иногда приводит к тому, что в поле зрения разных групп оказывается одна цель. Мы наблюдали случаи, когда вредоносное ПО Zebrocy от Sofacy конкурировало за доступ к компьютерам жертвы с русскоязычными

кластерами Mosquito Turla, а его бэкдор SPLM — с традиционными атаками Turla и китайскоязычной Danti. В числе целей, представляющих общий интерес, были правительственная администрация, технологические, научные и военные организации из Центральной Азии. Наверное, самое интригующее «совпадение интересов» произошло между Sofacy и англоговорящей кибергруппировкой, стоящей за The Lamberts. Связь была обнаружена после того, как исследователи обнаружили присутствие Sofacy на сервере, который ранее был идентифицирован сервисами информирования об угрозах, как зараженный вредоносным ПО Grey Lambert. Сервер принадлежит китайскому конгломерату, который разрабатывает и производит аэрокосмические и противовоздушные технологии. Однако в этом случае исходный вектор доставки SPLM остается неизвестным. Это порождает ряд гипотетических возможностей, например, то, что Sofacy может использовать новый и пока еще не обнаруженный эксплойт или новую разновидность своего бэкдора, или что Sofacy каким-то образом удалось использовать каналы связи Gray Lambert для загрузки своих вредоносных программ. Это может быть даже «ложный флаг», установленный во время предыдущей атаки Lambert. Мы считаем наиболее вероятным ответом то, что для загрузки и исполнения кода SPLM был использован неизвестный новый сценарий PowerShell или легитимное, но уязвимое веб-приложение.



В июне мы сообщали активной целевой атаке, направленной на национальный центр обработки данных (ЦОД) одной из стран Центральной Азии. Особенной эту атаку делает выбор в качестве мишени именно национального дата-центра: ее операторы получили доступ сразу к целому ряду правительственных ресурсов. Мы считаем, что помимо прочего этот доступ затем использовался для внедрения вредоносного JavaScript на официальные государственные веб-сайты и проведения второго этапа атаки (watering hole). Можно с высокой долей уверенности сказать, что за кампанией против национального дата-центра стоит китаеязычная группа LuckyMouse (также известная как EmissaryPanda и APT27). На это указывают применяемые ею инструменты и тактика, а также то, что раньше LuckyMouse уже использовала для своих командных серверов домен update.iaacstudio[.]com. а госучреждения, в т.ч. стран Центральной Азии, уже становились ее мишенью. Первоначальный вектор заражения, использованный в атаке на ЦОД, остается неясным. Даже в тех случаях, когда мы заметили, что LuckyMouse использует вредоносные документы, эксплуатирующие CVE-2017-118822 (уязвимость в Microsoft Office Equation Editor, широко используемая китаеязычными группами с декабря 2017 г.), нам не удалось доказать, что эти документы были связаны с конкретной атакой. Возможно, злоумышленники заразили сотрудников ЦОД при помощи watering hole.

О еще одной вредоносной кампании, организованной кибергруппировкой LuckyMouse мы писали в сентябре. Начиная с марта 2018 г. мы обнаружили несколько случаев заражения, во время которых в память системного процесса lsass.exe был внедрен ранее неизвестный троянец. Импланты были внедрены посредством 32- и 64-битных версий драйвера NDISProxy. Интересно, что этот драйвер подписан цифровым сертификатом, принадлежащим китайской компании LeagSoft, расположенной в Шэньчжэне и занимающейся разработкой ПО для обеспечения информационной безопасности. Мы сообщили компании о случившемся через китайскую группу реагирования на инциденты CN-CERT. Эта кампания была нацелена на государственные учреждения стран Средней Азии. Мы полагаем, что атака была связана со встречей на высоком уровне, проходившей в регионе. По нашему мнению, за этой новой вредоносной кампанией стоит китаеязычная группа LuckyMouse. В частности, для китаеязычных хакеров типичен выбор инструмента туннелирования Earthworm. Кроме того, одна из используемых злоумышленниками команд («-s rssocks -d 103.75.190[.]28 -e 443») создает туннель к уже известному командному серверу LuckyMouse. Выбор мишеней в данной кампании также соотносится с интересами, которые ранее демонстрировала

эта группа. Мы не наблюдали никаких признаков целевого фишинга и watering hole активности. Полагаем, что для распространения зловреда злоумышленники использовали уже зараженные сети.

Lazarus – это давно сложившаяся кибергруппировка, которая занимается кибершпионажем и киберсаботажем как минимум с 2009 г. В последние годы группа проводит кампании против финансовых организаций по всему миру. В августе мы сообщали, что группа успешно взломала сети нескольких банков, внедрилась в несколько глобальных бирж криптовалют и финансово-технических компаний. Помогая одному из клиентов справиться с киберинцидентом, мы узнали, что атака осуществлялась через приложение для торговли криптовалютами, которое было заражено троянцем; компании порекомендовали его по электронной почте. Ничего не подозревающий сотрудник загрузил стороннее приложение с легитимного на вид веб-сайта, и таким образом заразил компьютер зловредом Fallchill – это старый инструмент, который Lazarus недавно опять стала использовать. Судя по всему, Lazarus нашла способ создать легитимный на вид сайт и внедрить вредоносный компонент в «легитимно выглядящий» механизм обновления ПО – в данном конкретном случае была создана целая поддельная цепочка поставок вместо заражения существующей. В любом случае, успешная компрометация цепочки поставок означает, что группа Lazarus будет продолжать использовать этот метод атаки. Злоумышленники не остановились на достигнутом и разработали зловред для не-Windows платформ. Они опубликовали версию зловреда macOS и сообщили на сайте о скором выходе версии для Linux. Пожалуй, это первый случай на нашей памяти, чтобы эта APT-группировка использовала вредоносную программу для macOS. Судя по всему, злоумышленники были вынуждены пойти на разработку вредоносных инструментов для macOS в погоне за продвинутыми пользователями, разработчиками ПО из цепочки поставок и другими важными мишенями. Расширение списка операционных систем, интересующих группировку Lazarus, должно насторожить пользователей не-Windows платформ. Наш отчет об операции AppleJeus доступен здесь.

Группировка Turla (которую также называют Venomous Bear, Waterbug или Uroboros) известна своим суперсложным по тем временам руткитом Snake, мишенями которого были структуры, входящие в НАТО. Однако интересы этой группы гораздо шире. В октябре, рассказывая о нынешней активности Turla, мы обращали внимание на интересное сочетание старого кода и нового кода, строили прогнозы о том, где они нанесут следующий удар. В 2018 году мы посвятили

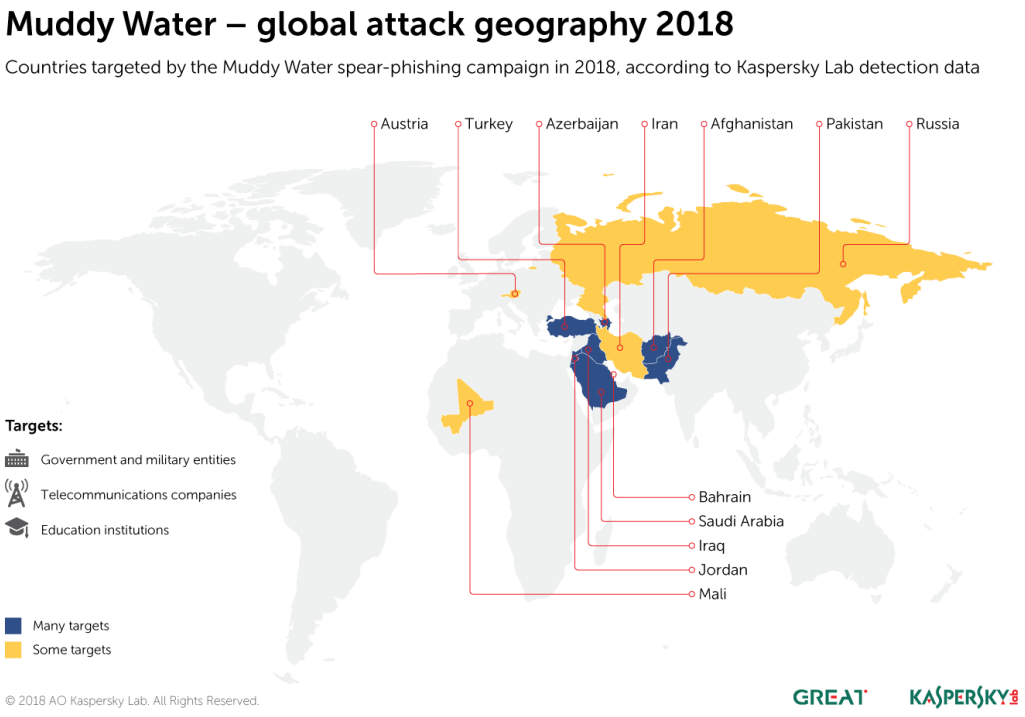
много времени изучению используемого группой бэкдора KopiLuwak JavaScript, новых вариантов фреймворка Carbon и методов доставки кода Meterpreter. Среди других интересных аспектов деятельности группировки были изменения в методах доставки бэкдора Mosquito, использование доработанного PowerShell PoshSec-Mod с открытым исходным кодом и применение стороннего кода инжектора. Нам удалось частично сопоставить эту активность с инфраструктурой и известными нам данными кампании WhiteBear, а также инфраструктурой и активностью Mosquito в 2017 и 2018 годах. Одним из любопытных наблюдений, сделанных в ходе нашего исследования, стало отсутствие пересечения в выборе целей с другими APT-группировками. Например, Turla не участвовала в эпохальном взломе DNC (в котором отметились Sofacy и CozyDuke), в это время она спокойно занималась другим проектами в разных странах мира. Это дает некоторое представление о нынешней мотивации и целях группы. Любопытно, что данные атакованных организаций не использованы для проведения атак и не попали в интернет; при этом Turla без лишнего шума продолжает свою деятельность. Проект Mosquito как и Carbon нацелены главным образом на дипломатические ведомства и структуры, работающие в сфере международных отношений. WhiteAtlas и WhiteBear, действующие по всему миру, также интересуются организациями, работающими в области внешней политики, но не только: в списках мишеней группы - научно-технические центры и организации, никак не связанные с политикой. Группа KopiLuwak в своей деятельности не ориентируется на дипломатические и внешнеполитические ведомства; в 2018 году ее внимание было сосредоточено на государственных организациях, занимающихся научными исследованиями и исследованиями в области энергетики, а также коммуникационных компаниях Афганистана. И скорее всего, этот очень избирательный подход, но включающий более широкий подбор жертв, продолжится в 2019 году.

В октябре мы сообщили последние новости о деятельности APT-группировки MuddyWater. Полученные нами ранее данные показывают, что эта относительно новая группа, появившаяся в 2017 году, нацелена главным образом на государственные структуры в Ираке и Саудовской Аравии. И тем не менее известно, что интересы киберпреступников, стоящих за MuddyWater, распространялись и на другие страны Ближнего Востока, Европы и США. Недавно мы обнаружили большое количество документов, содержащих целевой фишинг, которые, как представляется, предназначены для атак на правительственные и военные организации, телекоммуникационные и образовательные учреждения не только в Ираке и Саудовской Аравии, но и Иордании, Турции, Азербайджане и Пакистане.

Другие жертвы были обнаружены в Мали, Австрии, России, Иране и Бахрейне. Эти документы появлялись на протяжении всего 2018 года и с мая стали использоваться особенно активно. В документах, содержащих целевой фишинг, используются методы социальной инженерии с целью убедить жертв разрешить макросы. Для осуществления своих атак киберпреступники используют зараженные хосты. На более углубленных этапах нашего исследования мы смогли не только познакомиться с дополнительными файлами и инструментами, которые группа держит в своем арсенале, но и обнаружить сделанные ею ошибки OPSEC. Чтобы защитить себя от вредоносных атак, мы рекомендуем соблюдать следующие рекомендации:

- Обучать всех сотрудников идентифицировать вредоносное поведение, например, распознавать фишинговые ссылки.
- Обучать сотрудников службы информационной безопасности всем необходимым навыкам настройки, анализа и отслеживания вредоносного ПО.
- Использовать надежное решение для защиты крупных предприятий в сочетании с решениями для защиты от целевых атак, способных обнаруживать атаки с помощью анализа сетевых аномалий.
- Обеспечить сотрудникам службы безопасности доступ к данным о новейших угрозах. Это позволит им получить полезные инструменты для обнаружения и предотвращения целевых атак, такие как IoC (индикаторы заражения) и правила YARA.
- Внедрить процессы управления установкой обновлений на корпоративном уровне.

Критически важным предприятиям следует устанавливать повышенные уровни кибербезопасности, поскольку атаки на них неизбежны и вряд ли когда-либо прекратятся.



DustSquad – еще одна кибершпионская группировка, целями которой являются организации из стран Центральной Азии. Эксперты «Лаборатории Касперского» наблюдают за ее деятельностью уже два года и за это время предоставили своим клиентам в индивидуальном порядке отчеты о четырех проведенных DustSquad кампаниях с участием специального вредоносного ПО для Android и Windows. Недавно мы писали о вредоносной программе Octopus, которую группировка DustSquad использовала для шпионажа за дипломатическими организациями в регионе. Это название зловреду дала в 2017 году компания ESET – по имени скрипта 0ct0pus3.php, который группировка использовала на своих старых командных серверах. С помощью автоматизированной системы атрибуции «Лаборатории Касперского» (Kaspersky Attribution Engine), основанной на алгоритмах обнаружения совпадений в коде, мы обнаружили связь между Octopus и DustSquad. По данным нашей телеметрии, мы наблюдали за этой кампанией еще в 2014 году, когда киберпреступники атаковали организации в бывших советских республиках Центральной Азии (в основном русскоязычных) и в Афганистане.

В апреле мы обнаружили новый образец Octopus, который маскировался под мессенджер Telegram с русским интерфейсом. Мы не смогли найти легитимное программное обеспечение, за которое это вредоносное ПО себя выдает, и, честно говоря, не верится, что оно существует. Подпишитесь на наши отчеты об APT-угрозах, и вы получите доступ к материалам о нашим исследованиях и новейших открытиях, а также к широкому спектру технических данных.

В октябре мы опубликовали результаты нашего исследования импланта Dark Pulsar. В марте 2017 года группа хакеров, называющих себя «ShadowBrokers», опубликовала украденные данные, среди которые были два фреймворка: FuzzBunch and DanderSpritz. FuzzBunch содержит плагины разных типов, большинство из которых предназначены для изучения жертв, эксплуатации уязвимостей, удаленной работы с планировщиком задач и т.д. Второй фреймворк, DanderSpritz, используется для контроля уже скомпрометированных машин и сбора данных. Вместе они представляют собой мощную платформу для осуществления кибершпионажа. Фреймворк из утечки содержал только администраторский модуль для работы с DarkPulsar, но не сам бэкдор. Однако с помощью созданных нами на основе нескольких магических констант специальных сигнатур мы смогли найти сам имплант. Этот имплант позволяет киберпреступникам удаленно осуществлять управление зараженными устройствами. Нам удалось обнаружить 50 жертв (все они располагались в России, Иране и Египте), но, по-видимому, их значительно больше. Во-первых, интерфейс DanderSpritz может одновременно управлять большим количеством компьютеров-жертв. Плюс к этому, преступники, как правило, удаляют свои вредоносные программы сражу же после окончания кампании. Мы полагаем, что кампания прекратила свою активность после публикации группой хакеров, называющих себя ShadowBrokers, утечки «Lost in Translation» в апреле 2017 года. О предлагаемых нами стратегиях смягчения для сложных угроз, таких как Dark Pulsar читайте здесь.

МОБИЛЬНЫЕ APT КАМПАНИИ

В сегменте мобильных APT угроз случилось сразу три знаковых события: были раскрыты шпионские кампании Zoopark, BusyGasper и Skygofree.

Технически все участники троицы хорошо сконструированы и схожи по своему основному предназначению – шпионаж за выбранными жертвами. Их основной задачей является похищение всех доступных личных данных с мобильного устройства: перехват звонков, сообщений, геолокации и т.д. Есть даже функция прослушивания через микрофон – смартфон используется в качестве «жучка», который даже не нужно прятать от ничего не подозревающей жертвы. Особое внимание киберпреступники уделяли краже сообщений из популярных мессенджеров, которые сегодня во многом заменили стандартные средства коммуникации. В ряде случаев злоумышленники использовали эксплойты, повышающие локальные привилегии троянцев на устройстве и открывающие практически безграничный доступ к удаленному наблюдению, а зачастую и управлению устройством. Кроме того, в двух из трех описываемых зловредов была реализована функция кейлоггера – киберпреступники записывали каждую манипуляцию жертвы с клавиатурой устройства. Примечательно, что для такого перехвата нажатий им даже не были нужны повышенные привилегии.

География жертв представлена различными странами мира: если Skygofree был нацелен на жертв в Италии, то BusyGasper работал с отдельными российскими пользователями, а Zoopark орудовал в странах Среднего Востока.

Нужно отметить все более очевидную тенденцию – преступники, занимающиеся шпионажем, все чаще предпочитают мобильные платформы для атаки, так как в этом случае они получают куда больше персональных данных.

ЭКСПЛОЙТЫ

Эксплуатация уязвимостей в ПО и аппаратном обеспечении остается важным средством компрометации всех видов устройств.

В этом году были описаны две серьезных уязвимости, касающиеся процессоров Intel и получившие названия Meltdown и Spectre. Они предоставляют атакующему доступ к чтению памяти любого процесса и эксплуатируемого процесса соответственно. Уязвимости существуют как минимум с 2011 г. Meltdown (CVE-2017-5754) затрагивает центральные процессоры Intel и позволяет атакующему читать данные в памяти любого процесса в системе. Для эксплуатации требуется выполнение кода; его можно обеспечить различными способами, например, путем эксплуатации ошибки в ПО или через посещение вредоносного веб-сайта, который загружает JavaScript-код, осуществляющий атаку. Таким образом, при успешной эксплуатации уязвимости могут быть считаны все данные, находящиеся в памяти – пароли, ключи шифрования, PIN-коды и т.д. Производители оперативно опубликовали патчи для наиболее популярных ОС. Обновление от Microsoft, опубликованное 3 января, не оказалось совместимо со всеми антивирусными программами, и на некоторых системах потенциально могло привести к BSoD. Обновления можно было установить только в том случае, если защитное решение заранее выставило особый ключ в реестре, указывающий на то, что проблем с совместимостью нет.

В отличие от Meltdown, уязвимость Spectre (CVE-2017-5753 и CVE-2017-5715) может успешно эксплуатироваться и на других архитектурах (таких как AMD и ARM). Кроме того, Spectre может читать данные в памяти только эксплуатируемого процесса. При этом от эксплуатации Spectre не существует универсального решения – существуют лишь определенные защитные меры в некоторых браузерах. В недели, последовавшие за публикацией уязвимостей, стало ясно, что легкого решения проблемы не существует.

Большая часть выпущенных патчей привела к сокращению поверхности атаки, уменьшив риск эксплуатации уязвимостей известными способами, но при этом они не устраняют опасность полностью. Поскольку это фундаментальная проблема для уязвимых типов процессоров, ясно, что производителям в ближайшие годы придется бороться со вновь возникающими эксплойтами. Собственно, эксплойты не заставили себя долго ждать: в июле Intel выплатил $100000 в качестве премии за новые обнаруженные процессорные уязвимости, связанные с первым вариантом Spectre (CVE-2017-5753). Spectre 1.1 (CVE-2018-3693) может использоваться для выполнения спекулятивных операций, приводящих к переполнению

буфера. Spectre 1.2 позволяет атакующему перезаписывать данные, доступные только для чтения, и указатели в коде, вызывая нарушения изолированных сред на процессорах, которые не применяют защиту памяти при чтении и записи. Эти новые уязвимости были обнаружены Владимиром Кирианским, исследователем из Массачусетского технологического университета, и независимым исследователем Карлом Вальдспургером.

18 апреля кто-то загрузил на VirusTotal интересный эксплойт, который был задетектирован несколькими поставщиками защитных решений, включая «Лабораторию Касперского» – в нашем случае детектирование произошло благодаря общей эвристике, направленной на распознавание некоторых старых документов Microsoft Word. Оказалось, что это новая уязвимость нулевого дня в Internet Explorer (CVE-2018-8174), патч к которой Microsoft выпустил 8 мая 2018. После обработки образца в нашей песочнице мы заметили, что он успешно эксплуатирует полностью пропатченную версию Microsoft Word. Это заставило нас глубже проанализировать уязвимость. Цепочка заражения состоит из следующих этапов. Жертва получает вредоносный документ Microsoft Word. При его открытии загружается второй этап эксплойта – HTML-страница, содержащая VBScript-код. Это задействует уязвимость UAF (Use After Free) и запускает шелл-код. Хотя первичным вектором атаки является документ Word, сама уязвимость была в VBScript. Это первый на нашей памяти случай, когда URL Moniker используется для загрузки эксплойта Internet Explorer в Word; при этом мы полагаем, что в будущем эта техника будет широко использоваться злоумышленниками, поскольку она позволяет вынудить пользователей загрузить Internet Explorer вне зависимости от того, какой браузер выставлен в настройках по умолчанию. Вероятно, авторы эксплойт-пака начнут использовать эту технику как для проведения drive-by атак (через браузер), так и в спирфишинговых кампаниях. Чтобы защититься от этой техники, мы рекомендуем установить новейшие обновления безопасности и использовать защитный продукт с функцией поведенческого анализа.

В августе наша технология автоматической защиты от эксплойтов обнаружила новую кибератака, которая оказалась попыткой эксплуатации уязвимости нулевого дня в win32k.sys – файле драйвера Windows. Мы сообщили об уязвимости в Microsoft; 9 октября Microsoft раскрыли ее выпустили обновление безопасности. Уязвимость очень опасна – эксплуатируя ее, злоумышленники могут получить контроль над скомпрометированным компьютером. Уязвимость использовалась

при проведении точечных целевых атак на организации в странах Ближнего Востока – мы обнаружили менее десятка жертв. Мы связываем эти атаки с группировкой FruityArmor.

В конце октября мы сообщили в Microsoft еще об одной уязвимости. На этот раз это была уязвимость нулевого дня в win32k.sys, приводящая к эскалации привилегий; эксплуатируя ее, атакующий может получить права, необходимые, чтобы обеспечить устойчивое присутствие зловреда в зараженной системе. Эта уязвимость также эксплуатировалась в очень ограниченном числе атак против организаций на Ближнем Востоке. 13 ноября Microsoft выпустила обновление безопасности, закрывающее эту уязвимость (CVE-2018-8589). Эта угроза также была задетектирована благодаря нашим проактивным технологиям – продвинутого антивирусного движка и песочницы, созданной для платформы Kaspersky Anti Targeted Attack, также нашей технологии Automatic Exploit Prevention (AEP).

БРАУЗЕРНЫЕ РАСШИРЕНИЯ КАК ВРЕДОНОСНЫЙ ИНСТРУМЕНТ

Расширения для браузеров упрощают нам жизнь: прячут назойливую рекламу, переводят текст, помогают сделать выбор в онлайн-магазинах и т.п. Есть среди них и нежелательные – те, что подсовывают пользователю рекламу или собирают информацию о его действиях. Есть даже расширения, предназначенные для кражи денег. В этом году наше внимание привлекло вредоносное расширение, которое обращалось к подозрительному домену. Оно получило название *Desbloquear Conteúdo* («Разблокировать содержимое» в переводе с португальского), было нацелено на пользователей бразильских интернет-банков и собирало логины и пароли для получения доступа к банковским счетам жертв.

В сентябре хакеры опубликовали личные сообщения не менее чем из 81000 учетных записей Facebook. При этом они утверждали, что в их руки попало гораздо больше информации, а именно данные из 120 миллионов учетных записей Facebook. В Dark Web появилась реклама, где хакеры предлагают купить эти личные сообщения по цене 10 центов за учетную запись. Эта атака была расследована Русской службой BBC и компанией Digital Shadows, занимающейся исследованиями в области кибербезопасности. Он обнаружили, что большая часть из этих 81000 учетных записей принадлежала украинцам и россиянам, хотя среди них были также аккаунты жителей Великобритании, США и Бразилии. Представители Facebook высказали предположение, что сообщения были украдены при помощи вредоносного браузерного расширения.

Вредоносные расширения встречаются довольно редко, но требуют серьезного внимания из-за потенциального ущерба, к которому могут привести. Мы рекомендуем пользователям устанавливать только проверенные расширения, у которых большое число установок и отзывов в Chrome Web Store или на другом официальном сервисе. И даже в этом случае стоит учитывать, что вредоносные расширения все же могут быть опубликованы на таких официальных сервисах, поэтому мы также рекомендуем использовать защитный продукт класса Internet Security, который предупредит вас о подозрительном поведении браузерного расширения.

ЧЕМПИОНАТ МИРА ПО ОБМАНУ

Социальная инженерия остается важным инструментом в арсенале киберпреступников всех мастей. Мошенники всегда видят в крупных спортивных мероприятиях возможность заработать денег, и Чемпионат мира по футболу не стал исключением. Задолго до начала чемпионата в России киберпреступники стали активно эксплуатировать эту тему в рассылках и создавать под нее фишинговые страницы. Одним из видов такого мошенничества стали рассылки-уведомления о денежных выигрышах в лотереях, а также сообщения о розыгрыше билетов на матчи. Мошеннические веб-страницы зачастую очень похожи на настоящие: они качественно проработаны и даже имеют SSL-сертификаты для дополнительного правдоподобия. Мошенники также пытаются выманить данные у пользователей, имитируя официальные уведомления FIFA: жертве сообщают, что была обновлена система безопасности, и по этой причине (под угрозой блокировки аккаунта) требуется заново ввести все данные о себе. Ссылка из письма ведет в поддельный личный кабинет. Введенная там личная информация «утекает» напрямую к мошенникам.

Наш отчет о том, как киберпреступники эксплуатируют Чемпионат мира и пытаются заработать на нем денег, доступен здесь. Также мы опубликовали правила безопасности, которые помогут защититься от любого фишинга – не обязательно связанного с Чемпионатом мира.

В преддверии Чемпионата мира мы проанализировали почти 32 000 точек Wi-Fi доступа в 11 городах, где должны были пройти матчи. Оценив алгоритмы шифрования и проверки подлинности, мы подсчитали количество открытых сетей и сетей, защищенных по стандарту WPA2, а также их доли от общего числа точек доступа. Оказалось, что более 20% точек доступа используют ненадежные подключения – преступникам достаточно оказаться рядом с такой точкой доступа, чтобы перехватить трафик, а вместе с ним и пользовательские данные. Около трех четвертей всех точек используют шифрование по стандарту WPA/WPA2, который считается одним из самых безопасных. Уровень защиты зависит в основном от настроек WPA, установленных владельцем сети, в частности от сложности пароля, установленного собственником сети. Для подбора сложного ключа шифрования могут потребоваться годы. При этом даже сети, использующие надежные протоколы, такие как WPA2, нельзя автоматически считать полностью безопасными: они уязвимы, например, перед методом полного перебора, перебором по словарю и атаками с переустановкой ключа – все это популярные типы взлома, для которых в свободный доступ выложено множество инструкций и инструментов с открытым

исходным кодом. Попытку перехвата трафика из общедоступной точки Wi-Fi с шифрованием WPA также можно совершить, если поймать «рукопожатие» между точкой доступа и устройством в начале сеанса.

Здесь лежит наш отчет, а также рекомендации по безопасному использованию точек доступа Wi-Fi – рекомендации актуальны в любом месте, не только на Чемпионате мира.

ФИНАНСОВОЕ МОШЕННИЧЕСТВО В ПРОМЫШЛЕННОМ МАСШТАБЕ

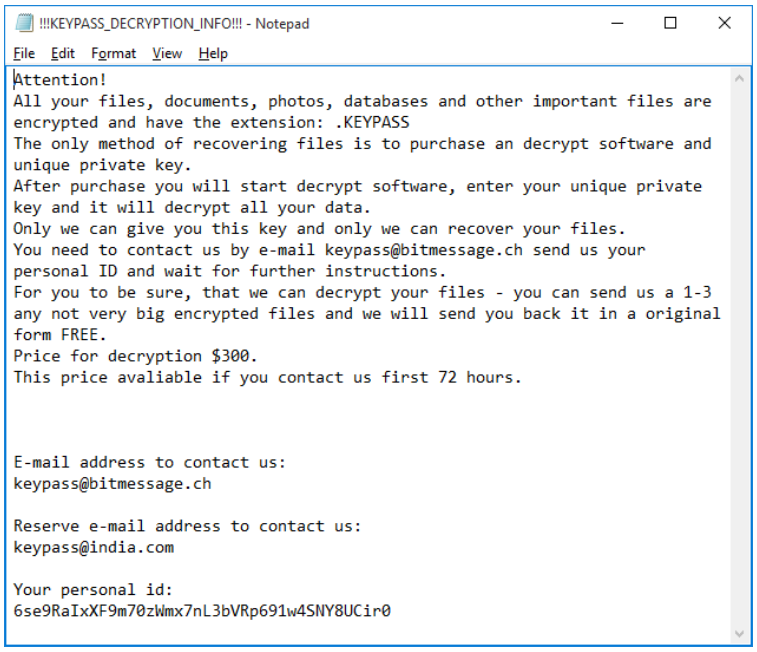
В августе Kaspersky Lab ICS CERT сообщил о фишинговой кампании, направленной на кражу денег у организаций, преимущественно связанных с промышленным производством. Злоумышленники использовали стандартные методы фишинга, обманом заставляли пользователей открывать зараженные почтовые вложения, маскируя фишинговые письма под коммерческие предложения и другие финансовые документы. Киберпреступники использовали легитимное ПО для удаленного администрирования – TeamViewer или Remote Manipulator System (RMS). С их помощью злоумышленники получали удаленный контроль над зараженными системами, находили и изучали документы о проводимых закупках, а также данные об используемом ПО для осуществления финансовых и бухгалтерских операций. Далее злоумышленники использовали всевозможные способы для совершения финансовых махинаций, в частности подменяли банковские реквизиты в транзакциях. 1 августа, на момент публикации отчета, мы зафиксировали заражении около 800 компьютеров не менее чем в 400 промышленных компаниях, относящихся к разным отраслям – промпроизводству, нефтегазовой отрасли, металлургии, инжинирингу, энергетике, строительству, добыче полезных ископаемых и логистике. Фишинговая кампания велась с октября 2017 г.

Наше исследование демонстрирует, что даже с помощью простых техник атаки и известного вредоносного ПО злоумышленники могут успешно атаковать промышленные компании, используя методы социальной инженерии и сокрытия вредоносного кода в системе, а также применяя легитимное ПО для удаленного администрирования, чтобы избежать детектирования антивирусными решениями.

Здесь можно подробнее прочитать о том, как злоумышленники используют инструменты удаленного администрирования для компрометации жертв, а здесь лежит обзор ситуации вокруг угроз, направленных на системы промышленной автоматизации, в первом полугодии 2018 г.

ВЫМОГАТЕЛИ ПО-ПРЕЖНЕМУ ПРЕДСТАВЛЯЮТ УГРОЗУ

Количество атак программ-вымогателей весь последний год снижалось, но несмотря на это данный вид вредоносного ПО по-прежнему угрожает пользователям, а новые семейства вымогателей продолжают появляться. В начале августа наш модуль защиты от программ-шифровальщиков начал детектировать троянец KeyPass. За два дня он был обнаружен более чем в 20 странах – основной удар пришелся на Бразилию и Вьетнам, также имелись жертвы в Европе, Африке и в Юго-Восточной Азии. KeyPass шифрует все файлы (вне зависимости от их расширения) на локальных дисках и в сетевых папках, доступных с зараженного компьютера. Некоторые он при этом игнорирует – список таких файлов «зашит» в сам зловред. После шифрования файлы приобретают расширение *.KEYPASS; в каждую директорию, содержащую зашифрованные данные, записывается файл «!!!KEYPASS_DECRYPTION_INFO!!!.txt» с требованием выкупа. В данном троянце реализована очень простая схема: используется симметричный алгоритм шифрования AES-256 в режиме CipherFeedback (CFB) с нулевым вектором инициализации и одним и тем же 32-байтовым ключом для всех файлов. Шифруется максимум 0x500000 байтов (~5 МБ) данных в начале каждого файла. Вскоре после запуска зловред устанавливает соединение с командным сервером и получает ключ шифрования и идентификатор для текущей жертвы. Эти данные пересылаются по простому протоколу HTTP в формате JSON. Если соединение с командным сервером невозможно (например, у зараженного компьютера нет подключения к интернету или сервер недоступен), зловред использует зашитый в него дефолтный ключ и идентификатор жертвы – в этом случае (при офлайн-шифровании) задача расшифровки файлов становится совсем простой.



Пожалуй, самая интересная черта троянца KeyPass – это возможность «ручного контроля». Троянец содержит форму, которая по умолчанию скрыта, но показывается после нажатия специальной клавиши на клавиатуре. Эта форма позволяет злоумышленникам кастомизировать процесс шифрования, изменяя такие параметры, как ключ шифрования, название и содержание требования выкупа, идентификатор жертвы, расширение зашифрованных файлов и список директорий, которые следует исключить из шифрования. Эта функция позволяет предположить, что злоумышленники планируют использовать этот троянец в атаках, проводимых вручную.

При этом проблемы возникают не только из-за новых шифровальщиков. Прошло уже полтора года после эпидемии WannaCry, а этот зловред продолжает оставаться в TOP 10 наиболее распространенных семейств троянцев-шифровальщиков – на данный момент по всему миру зафиксировано 74621 уникальная атака; в третьем квартале WannaCry стал причиной 28,72% от числа всех заражений шифровальщиками, и эта доля выросла за год на две трети. Это не может не вызывать беспокойства, тем более что патч для эксплойта EternalBlue, используемого WannaCry, был выпущен еще до начала эпидемии в мае 2017 г.

ASACUB И БАНКОВСКИЕ ТРОЯНЦЫ

Уходящий год показал самые впечатляющие цифры по числу атак с участием мобильных банковских троянцев. В начале года казалось, что данный вид угроз стабилизировался как по количеству обнаруженных уникальных образцов, так и по количеству атакованных пользователей. Однако уже во втором квартале ситуация радикально изменилась в худшую сторону: число обнаруженных мобильных банковских троянцев оказалось рекордным, равно как и число атакованных пользователей. Первопричина такого существенного скачка неизвестна, однако основными виновниками сложившейся ситуации оказались создатели троянцев Asacub и Hqwar. Интересной особенностью первого является его долгая история - по нашим данным стоящая за ним группировка орудует уже больше трёх лет. А сам Asacub эволюционировал из SMS-троянца, который с самого начала располагал техниками, противодействующими удалению и обеспечивающими перехват входящих звонков и SMS. Впоследствии его создатели усложнили логику зловреда и занялись его массовым распространением. Вектор при этом был выбран тот же, что и в самом начале – социальная инженерия через SMS. Другое дело, что источником действующих номеров, владельцы которых зачастую ждали сообщений от незнакомых абонентов, стали популярные доски объявлений. Далее срабатывала лавинная техника распространения, и уже устройства жертв троянца сами становились распространителями заразы – Asacub рассылал себя сам по всей телефонной книге жертвы.

УМНЫЙ – НЕ ЗНАЧИТ БЕЗОПАСНЫЙ

Сегодня мы окружены «умными» устройствами – повседневными бытовыми приборами, такими как телевизоры, интеллектуальные счетчики, термостаты, рядионяни и детские игрушки, но также еще и машинами, медицинскими устройствами, камерами видеонаблюдения и счетчиками на парковках. Появляются даже «умные» города. У этого многообразия, однако, есть оборотная сторона: чем больше устройств, тем шире поверхность атаки, и тем больше возможностей для тех, кто в каких-либо целях хочет воспользоваться слабыми местами в безопасности таких устройств. Обеспечить безопасность традиционного компьютера непросто; еще сложнее, когда дело касается интернета вещей – из-за недостаточной стандартизации разработчики не думают о безопасности или учитывают ее «по остаточному принципу». Это можно продемонстрировать на множестве примеров.

В феврале мы опубликовали исследование о том, насколько уязвимы к атакам «умные» концентраторы (smart hubs). Концентратор позволяет контролировать работу других умных устройств в доме, получать информацию с них и передавать им команды. Управление концентратором возможно с сенсорного экрана, через мобильное приложение или веб-интерфейс. Если в концентраторе есть уязвимость, то он потенциально создает единую точку отказа. Концентратор, который исследовали наши эксперты, не содержал значительных уязвимостей, но нашлись достаточно логических ошибок, чтобы позволить исследователям получить удаленный доступ.

Исследователи из Kaspersky Lab ICS CERT проверили популярную «умную» камеру на предмет защищенности от хакеров. Такие устройства уже прочно вошли в повседневную жизнь. Многие из них имеют возможность подключаться к «облаку», предоставляя таким образом возможность наблюдать за тем, что происходит в удалённой точке – следить за животными, безопасностью жилища и т.д. Исследованная камера имеет широкий функционал и может быть использована в качестве видео-няни или элемента общей системы безопасности жилища. Устройство имеет функцию ночного видения, датчик движения, может передавать видео и звук на смартфон или планшет, а также проигрывать звук через встроенный динамик. При этом, в ходе исследования в устройстве было выявлено 13 уязвимостей – почти столько же, сколько у нее функций – позволяющих удаленно сменить пароль администратора, выполнить на устройстве произвольный код, собрать ботнет из скомпрометированных камер или вывести камеру из строя.

Потенциальные проблемы не ограничены бытовыми устройствами. В начале года Идо Наор, эксперт из нашей группы GReAT, совместно с Амихаем Нейдерманом из компании Azimuth Security обнаружили уязвимость в средстве автоматизации для заправочной станции. Это устройство имеет прямое подключению к интернету и отвечает за управление всеми компонентами АЗС, в том числе топливораздаточной колонкой (ТРК) и платежными терминалами. Дальше – больше: оказалось, что в веб-интерфейс можно получить доступ, используя стандартный логин и пароль. Дальнейшее исследование показало, что злоумышленник может выключить все заправочные системы, вызвать утечку топлива, менять цены на бензин, украсть деньги в обход платежного терминала, украсть данные о номерных знаках машин и личные данные водителей, выполнить код на блоке контроллера и даже получить свободный доступ ко всей сети АЗС.

Технологии – двигатель прогресса в здравоохранении; они способны качественно улучшить медицинские услуги, снизить расходы на лечение и уход за больными. Также технологии могут дать пациентам и гражданам больше возможностей контроля над качеством услуг здравоохранения, создать карьерные возможности, поддерживать разработку новых лекарств и схем лечения. С другой стороны, новые технологии в здравоохранении и практика работы с мобильными устройствами генерируют больше данных, чем когда-либо до этого, и в то же время создают больше вероятности их утери и кражи. В последнее годы мы неоднократно обращали внимание на эти проблемы (см. наши публикации здесь, здесь и здесь). Мы продолжаем отслеживать деятельность киберпреступников, смотрим, как они проникают в сети медучреждений, находят данные на публично доступных медицинских ресурсах и извлекают. В сентябре мы рассмотрели состояние безопасности в учреждениях здравоохранения. В более 60% медицинских организаций на компьютерах обнаружились те или иные вредоносные программы. Увеличивается число кибератак и на фармацевтические организации. Крайне важно, чтобы медучреждения убрали все узлы, на которых происходит обработка личных медицинских данных, из публичного доступа, обновили ПО, удалили приложения, которые более не нужны, а также не подключали дорогостоящее медицинское оборудование к основной локальной сети. Подробные рекомендации доступны здесь.

В этом году мы также исследовали умные устройства для животных, а именно трекеры – устройства для отслеживания их местоположения. Такие гаджеты могут обладать доступом к сети, телефону хозяина, а также данными о местоположении животного. Нашей целью было оценить, насколько безопасные такие

устройства. Наши эксперты проанализировали несколько популярных моделей трекеров на предмет потенциальных уязвимостей. Четыре исследованных трекера используют технологию Bluetooth LE для связи со смартфоном владельца, и только один из них делает это корректно; остальные же могут принимать и исполнять команды от кого угодно. Более того, их можно вывести из строя или скрыть от владельца — для этого достаточно просто находиться рядом с трекером. Всего одно из протестированных Android-приложений проверяет сертификат своего сервера, не полагаясь на систему. Как итог — большинство подвержено атаке «человек посередине», т. е. злоумышленник может перехватить передаваемые данные, если «уговорит» жертву установить свой сертификат.

Недавно наши исследователи обратили внимание на носимые устройства для людей, а именно умные часы и фитнес-трекеры. Нас интересовал сценарий, в котором установленное на смартфоне шпионское приложение могло бы отсылать данные со встроенных датчиков движения (акселерометров и гироскопов) на удаленный сервер и из этих данных воссоздавать действия пользователя – ходьбу, сидение, набор текста на клавиатуре и т.д. Для начала мы взяли Android-смартфон, создали простое приложение для обработки и передачи данных, а затем стали анализировать, что же можно получить из этих данных. Оказалось, что возможно не только распознать, сидит ли человек или идет, но и различить, например, характер ходьбы – прогуливается человек или делает переход между поездами метро. Это возможно, потому что каждому виду движения соответствует свой паттерн данных с акселерометра – именно благодаря этому фитнес-трекеры отличают ходьбу от езды на велосипеде. Легко распознать, что человек набирает текст на клавиатуре; однако узнать, *что именно* человек набирает, сложно и потребует неоднократного ввода текста. Наши исследователи смогли достичь 96%-ной точности при определении момента ввода пароля с компьютерной клавиатуры и 87%-ной точности при определении ввода PIN-кода с клавиатуры банкомата. Однако, считать другую информацию, например, номер кредитной карты или ее CVC-код, гораздо сложнее из-за сложности прогнозирования момента ввода жертвой такой информации. На практике сложность получения такой информации означает, что злоумышленнику понадобится сильная мотивация, чтобы отслеживать конкретную жертву. Конечно, возникают ситуации, когда такая игра для злоумышленника стоит свеч.

В последние годы растет популярность сервисов краткосрочного проката автомобилей (каршеринга). Такие сервисы значительно повышают мобильность людей в крупных городах. Однако при этом возникает вопрос: насколько защищены личные данные пользователей подобных сервисов? В июле мы протестировали 13 приложений каршеринга на предмет безопасности. Результаты исследования нас не порадовали. Судя по всему, у разработчиков приложений отсутствует понимание текущих угроз для мобильных платформ как при проектировании приложений, так и при создании инфраструктуры. Для начала было бы неплохо добавить функцию оповещения пользователя о подозрительной активности — на данный момент только один сервис отправляет пользователю оповещение в случае, если в его аккаунт пытаются зайти с другого устройства. Большинство рассмотренных нами приложений плохо продуманы с точки зрения безопасности и нуждаются в доработке. Кроме того, многие программы не просто очень похожи друг на друга, но созданы на базе того же кода.

Количество умных устройств неуклонно растет. По некоторым прогнозам, к 2020 году их количество в несколько раз превысит население планеты. При этом производители все еще уделяют недостаточно внимания их безопасности: отсутствуют напоминания о необходимости смены стандартных паролей при первой настройке и уведомления о выходе новых версий прошивок, а сам процесс обновления зачастую слишком сложен для обычного пользователя. Все это делает IoT-устройства привлекательной мишенью для злоумышленников. Их проще заразить, чем персональные компьютеры, а в домашней инфраструктуре они играют важную роль: одни управляют интернет-трафиком, другие делают видеозаписи, а третьи управляют домашними устройствами –например, установкой климат-контроля. Растет не только количество, но и качество вредоносного ПО для умных устройств. В арсенале злоумышленников появляется все больше эксплойтов, а зараженные устройства используются для организации DDoS-атак, кражи персональных данных и майнинга криптовалют. В сентябре мы опубликовали отчет по IoT-угрозам, а с этого года мы начали включать данные по IoT-атакам в наши квартальные и годовые статистические отчеты.

Важно, чтобы производители устройств изменили свое отношение к кибербезопасности – необходимо, чтобы вопросы безопасности учитывались уже на этапе проектирования устройств. В некоторых странах органы власти уже взялись за вопросы обеспечения безопасности умных устройств на этапе проектирования и принимают руководящие документы на этот счет. В октябре

правительство Великобритании практическое руководство по обеспечению IoT-безопасности потребителей. Правительство Германии недавно опубликовало свои предложения по минимальным стандартам безопасности для широкополосных маршрутизаторов.

Прежде чем купить какое-либо умное устройство, подумайте о безопасности.

- Вам действительно нужно это устройство? Если да, проверьте доступные функции и отключите все, что вам не нужно, чтобы уменьшить возможную поверхность атаки.
- Почитайте в интернете информацию о любых обнаруженных уязвимостях.
- Проверьте, возможно ли обновление прошивки на устройстве.
- Всегда меняйте пароль по умолчанию на уникальный сложный пароль.
- Не сообщайте никому серийные номера, IP-адреса и другие конфиденциальные данные своего умного устройства.

ВЗЛОМЫ И УТЕЧКИ ДАННЫХ

Личные данные – это ценный товар. Это очевидно хотя бы по постоянному потоку новостей об утечках данных – см. новости про утечки из Under Armour, FIFA, Adidas, Ticketmaster, T-Mobile, Reddit, British Airways и Cathay Pacific.

Нашумевший случай с компанией Cambridge Analytica, использовавшей данные из Facebook – это напоминание о том, что личная информация имеет ценность не только для киберпреступников. Во многих случаях личные данные – это та цена, которую люди платят, чтобы получить продукт или сервис – «бесплатные» браузеры, «бесплатные» ящики электронной почты, «бесплатные» учетные записи в соцсетях и т.д. Во многих случаях, но не всегда. Нас все плотнее окружают «умные» устройства, которые способны собирать данные о самых мелких деталях нашей жизни. В этом году одна журналистка превратила свою квартиру в «умный» дом, чтобы оценить объем данных, собираемых производителями устройств. Такие устройства, как правила, приобретаются за деньги, поэтому собираемые ими данные едва ли можно рассматривать как плату за пользу, которую они приносят.

В результате взломов и утечек данных были оштрафованы соответствующие компании (например, британское Управление комиссара по информации оштрафовало Equifax и Facebook). При этом штрафы пока что наложены за утечки данных, которые произошли до вступления в силу в мае Общего регламента ЕС по защите персональных данных. Взыскания за любые серьезные утечки, которые произойдут в будущем, скорее всего будут гораздо выше.

Стопроцентной безопасности, конечно, не существует. Но, с другой стороны, любая организация, которая хранит данные личного характера, обязана обеспечивать их эффективную защиту. Если взлом или утечка приводит к краже личных данных, то компания должна вовремя предупредить своих клиентов, чтобы у них была возможность принять меры к ограничению потенциального ущерба.

Хотя мы, индивидуальные пользователи, ничего не можем сделать, чтобы предотвратить кражу своих личных данных в случае взлома на уровне провайдера, важно принять меры, чтобы обезопасить свои учетные записи и минимизировать возможный ущерб, в частности выбирая уникальные сложные пароли для каждого сайта и используя двухфакторную аутентификацию.