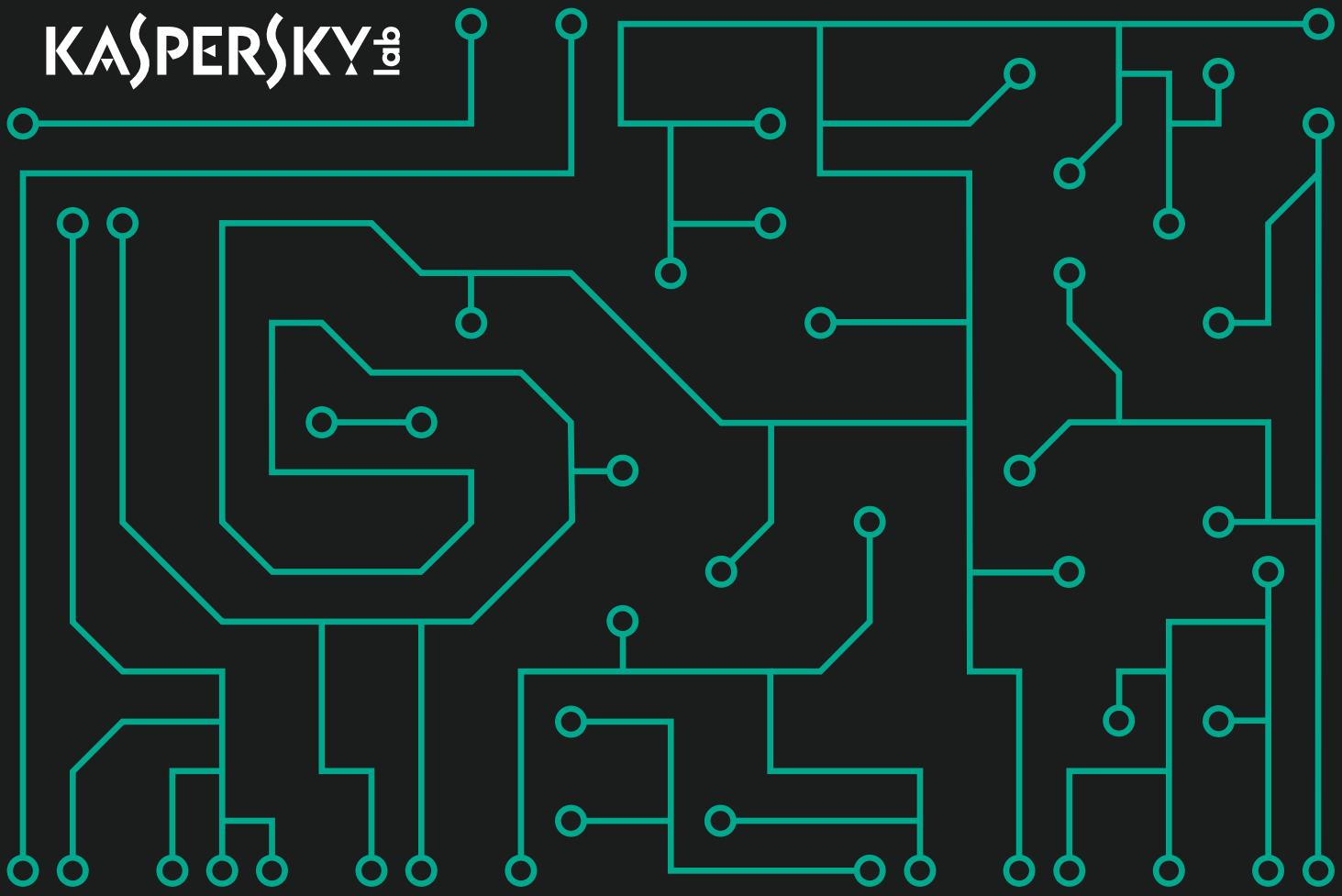
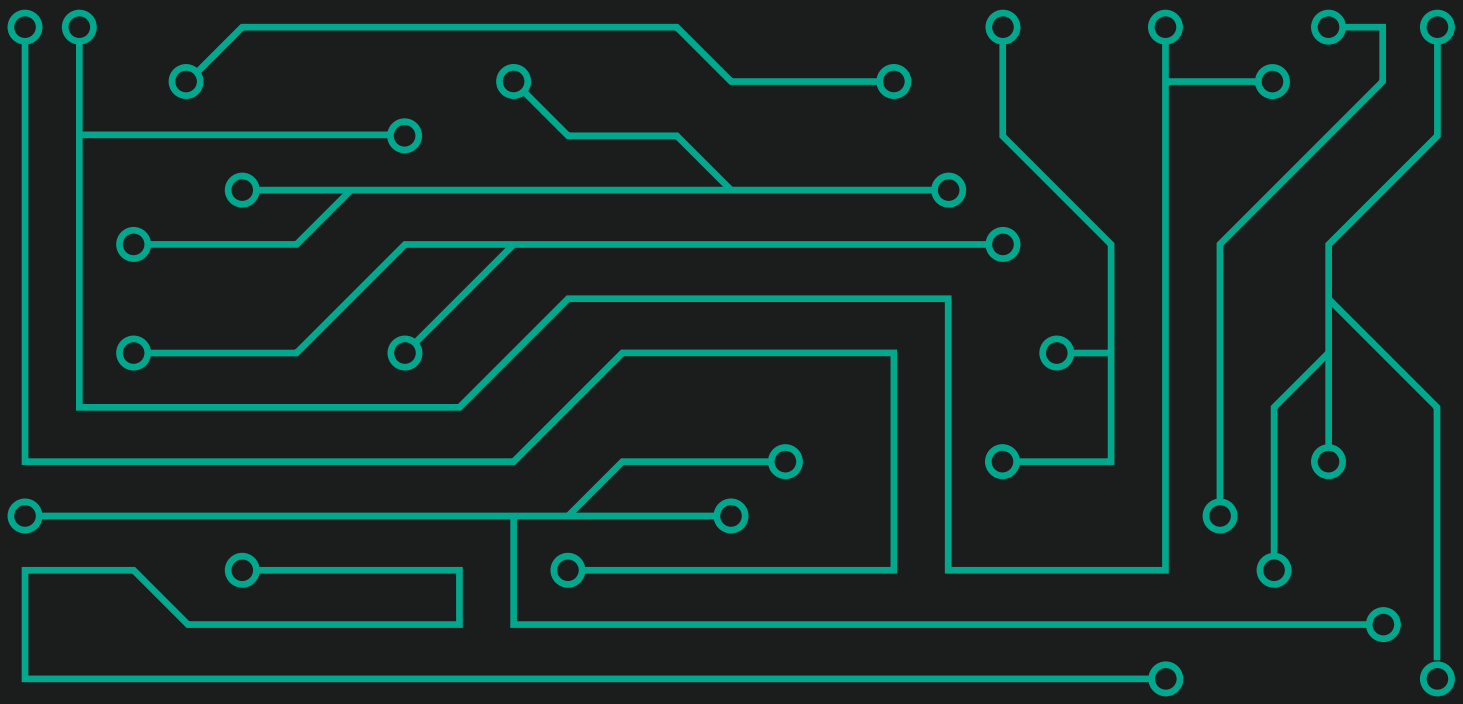
KASPERSKY lab



Kaspersky Security Bulletin:

УГРОЗЫ В 2019 ГОДУ

Висенте Диаз



СОДЕРЖАНИЕ

Нет ничего сложнее, чем делать прогнозы. Мы не гадаем на хрустальном шаре. Наш метод –делать обоснованные предположения исходя из событий недавнего прошлого и анализа тенденций, которые могут быть актуальными в ближайшие месяцы.

После консультаций с самыми грамотными специалистами мы исходили из того сценария, что наиболее значимые угрозы будут связаны с APT-атаками – именно они демонстрируют максимальную степень инновационности в сфере нарушений кибербезопасности. Вот наши основные прогнозы относительно того, что может произойти в ближайшие месяцы.

КОНЕЦ ЭРЫ КРУПНЫХ APT-КАМПАНИЙ

Как же так? Число раскрытых вредоносных кампаний растет день ото дня. Почему же наш первый прогноз противоречит этой очевидной тенденции?

Здесь мы исходим из того наблюдения, что индустрия кибербезопасности регулярно обнаруживает сложные высокотехнологичные кампании, за которыми стоит поддержка различных государств и которые готовились на протяжении нескольких лет. Логичной реакцией со стороны злоумышленников стало бы освоение новых, более сложных техник, которые будет гораздо труднее обнаружить и связать с конкретными кибергруппировками.

Достичь этого можно разными способами. Единственное необходимое условие – понимание методов, используемых отраслевыми экспертами при атрибуции атак и выявлении сходства между различными атаками и используемыми в них артефактами. Особого секрета эти сведения не представляют. При наличии достаточных ресурсов простым решением для атакующей стороны было бы действие сразу в нескольких направлениях, которые будет очень трудно привязать к одному агенту или кампании. Располагающие ресурсами злоумышленники могли бы запускать новые инновационные операции, не останавливая при этом старые. Конечно, существует вероятность раскрытия старых операций, но обнаружение новых становится куда более сложной задачей.

Вместо того, чтобы запускать более сложные вредоносные кампании, в некоторых случаях для конкретных кибергруппировок более эффективной тактикой может быть прямое воздействие на инфраструктуру и компании, где есть потенциальные жертвы (например, на интернет-провайдеров). Иногда этого можно достичь за счет регулирования, не прибегая к использованию вредоносного ПО.

Некоторые операции «отдаются на откуп» различным группировкам и компаниям, которые используют разные инструменты и техники, что чрезвычайно усложняет атрибуцию. Следует помнить, что в случае операций, за которыми стоит поддержка государств, такое «разделение труда» может повлиять на будущее кампаний. В этом сценарии технические возможности и инструменты являются собственностью частных компаний и продаются любым покупателям, которые зачастую не вдаются в технические детали и не задумываются над возможными последствиями применения.

Все это означает, что вероятность обнаружения новых высокотехнологичных вредоносных кампаний мала – располагающие ресурсами злоумышленники скорее предпочтут использовать новые подходы.

СЕТЕВОЕ ОБОРУДОВАНИЕ И ИНТЕРНЕТ ВЕЩЕЙ

Представляется логичным, что в какой-то момент любой вредоносный агент будет использовать возможности и инструменты, предназначенные для воздействия на сетевое оборудование. Кампании, подобные VPNFilter, служат ярким примером того, как злоумышленники развертывают вредоносное ПО, чтобы создать универсальный ботнет. В данном случае обнаружение атаки заняло некоторое время, даже несмотря на широкое распространение вредоносной программы. Это вызывает дополнительные опасения в отношении раскрытия более узконаправленных атак.

В отношении злоумышленников, располагающих ресурсами, эту идею можно развить еще дальше. Почему бы им не атаковать базовые элементы инфраструктуры вместо отдельно взятой организации? Насколько нам известно, этот уровень еще не достигнут, но имевшие место вредоносные кампании (такие как Regin) показывают, насколько привлекателен такой уровень контроля для любого киберпреступника.

Уязвимости в сетевом оборудовании позволяют атакующим использовать различные подходы. Они могут осуществить массовое заражение по типу ботнетов и в дальнейшем использовать такие сети в своих целях, либо проводить менее заметные атаки на отдельных жертв. В рамках второго подхода можно рассмотреть атаки без применения вредоносного ПО, в которых VPN-тоннель, открытый для зеркалирования или перенаправления трафика, может предоставить атакующим всю необходимую информацию.

Все эти элементы сетевой инфраструктуры могут быть также частью интернета вещей, где развитие ботнетов идет огромными темпами. В умелых руках такие ботнеты могут стать невероятно мощным и опасным инструментом – например, для вывода из строя критической инфраструктуры. Этот факт может использоваться злоумышленниками, располагающими соответствующими ресурсами – возможно, через подставную группировку или в рамках террористической атаки.

Еще один пример того, как могут применяться универсальные ботнеты, помимо проведения деструктивных атак, – скачкообразная перестройка частоты в узком диапазоне при ведении вредоносных коммуникаций, что позволяет избежать использования традиционных каналов эксфильтрации данных, чтобы обойти средства мониторинга.

Пусть это предупреждение звучит каждый год, повторим его вновь: не следует недооценивать IoT-ботнеты – они становятся все мощнее.

КИБЕРАТАКИ КАК ИНСТРУМЕНТ ВОЗМЕЗДИЯ

В области дипломатии и геополитики один из главных вопросов – как действовать в случае активной кибератаки. Ответ неочевиден и сильно зависит, кроме прочего, от уровня и масштаба конкретной атаки. При этом, после некоторых недавних атак, в частности на Национальный комитет Демократической партии США, отношение к ним стало более серьезным.

Расследования некоторых нашумевших атак, имевших место в последнее время – например, на Sony Entertainment Network и Национальный комитет Демократической партии США, – привели к появлению списков подозреваемых, против которых были выдвинуты обвинения. При этом обвиняемые в проведении кибератак предстали перед судом и стали известны широкой публике. Это может использоваться для формирования общественного мнения, которое в дальнейшем будет иметь более серьезные дипломатические последствия.

Примером, в частности, может служить Россия, которая оказалась в непростой ситуации в результате своего предполагаемого вмешательства в демократические процессы. Ее пример может заставить определенных лиц изменить свое отношение к возможности проведения подобных операций в будущем.

Однако самым большим достижением злоумышленников стало появление в обществе опасений, что подобное может произойти или уже произошло. Теперь можно эксплуатировать этот страх, неопределенность и сомнения более изощренными способами, что наблюдается в некоторых крупных кампаниях, включая Shadowbrokers. Мы ожидаем, что в ближайшем будущем таких вредоносных кампаний станет больше.

Что еще мы увидим в будущем? Имевшие место вредоносные кампании, по всей вероятности, служили лишь пробными вылазками, и в дальнейшем эта сфера будет эксплуатироваться множеством различных способов. Характерным примером может служить псевдо-вредоносный инцидент с Olympic Destroyer, конечная цель и последствия которого до сих пор неясны.

ПОЯВЛЕНИЕ НОВИЧКОВ

Слегка упрощая, всех APT-агентов можно разделить на две группы: традиционные продвинутые, располагающие крупными ресурсами APT-группировки (которым мы предсказываем вымирание), и энергичные новички, желающие присоединиться к большой игре.

Специфика момента состоит в том, что входной барьер никогда не был настолько низок – в открытом доступе находятся сотни весьма эффективных инструментов, утекших переработанных эксплойтов и программных пакетов всех видов и мастей. Кроме всего прочего, использование этих средств делает атрибуцию атак практически невозможной, а сами инструменты при необходимости легко кастомизируются.

В мире есть два региона – Юго-Восточная Азия и Ближний Восток, – где число таких групп активно растет. Они традиционно используют приемы социальной инженерии в отношении локальных жертв, эксплуатируют их слабую защиту и общий недостаток культуры кибербезопасности. По мере того, как потенциальные жертвы усиливают защитные меры, злоумышленники также наращивают свой вредоносный арсенал и повышают технологический уровень вредоносных инструментов, что позволяет им распространять свои операции на другие регионы. В рамках данного сценария с применением скриптовых инструментов встречаются молодые перспективные компании, предлагающие региональные сервисы, которые планомерно повышают качество своих операций несмотря на неудачи в области защиты критических данных (OPSEC).

Интересный аспект, заслуживающий рассмотрения под более техническим углом, – это второе дыхание, которое могут обрести в ближайшее время JavaScript-инструменты постэксплуатации, учитывая сложность ограничения их функциональности администратором (по сравнению с PowerShell), недостаточность системных журналов и возможность выполнения на более старых операционных системах.

ОТРИЦАТЕЛЬНЫЕ КОЛЬЦА

2018 год прошел под флагом критических аппаратных уязвимостей Meltdown, Specter, AMD и связанных с ними, включая еще не обнаруженные. В этой связи нам пришлось пересмотреть свои представления о самом опасном вредоносном ПО. И хотя пока что мы не наблюдали эксплуатацию уязвимостей ниже Кольца 0 в «дикой природе», сама возможность появления таких угроз, которые практически недоступны для современных защитных механизмов, по-настоящему пугает.

Например, в случае System Management Mode (режима системного управления) с 2015 г. был опубликован по меньшей мере один пилотный вариант (PoC). System Management Mode – это режим работы процессора, который предоставляет полный удаленный доступ к компьютеру, даже не допуская процессы Кольца 0 к его памяти. Возникает вопрос: может быть, мы до сих пор не обнаружили вредоносное ПО, эксплуатирующее эту уязвимость, только потому, что его очень сложно обнаружить? Это слишком привлекательная возможность, чтобы ее упускать, и мы уверены, что несколько групп пытались эксплуатировать подобные механизмы на протяжении последних нескольких лет – в некоторых случаях, возможно, успешно.

Аналогичная ситуация наблюдается с вредоносным ПО для виртуальных сред, гипервизоров и единого расширяемого интерфейса прошивки (UEFI). Для всех трех уже были выпущены пилотные версии, а HackingTeam даже продемонстрировали руткит для UEFI, доступный по крайней мере с 2014 г., но опять же, действующих в «дикой природе» образцов пока нет.

Обнаружим ли мы когда-нибудь этих редких представителей вредоносной фауны? Или таких эксплойтов пока просто не было? Последнее представляется маловероятным.

ВАШ ЛЮБИМЫЙ ВЕКТОР ЗАРАЖЕНИЯ

Настало время дать прогноз по целевому фишингу – сюрпризов в нем, наверное, будет меньше всего. Это самый успешный вектор заражения, и мы полагаем, что в ближайшем будущем он станет еще более важным. Секрет его успеха заключается в способности вызвать у жертвы любопытство, и недавние массовые утечки данных из различных социальных медиа платформ могут помочь злоумышленникам усовершенствовать этот подход.

Данные, полученные в результате атак на такие соцмедиа-гиганты, как Facebook, Instagram, LinkedIn и Twitter, сейчас широко доступны на рынке. В некоторых случаях по-прежнему неясно, за какой именно информацией охотились атакующие, но можно предположить, что их интересовали личные сообщения или даже учетные данные. Для киберпреступников, применяющих методы социальной инженерии, это золотая жила. Например, злоумышленник может использовать краденные учетные данные вашего друга, чтобы поделиться в социальной сети чем-то, что вы ранее обсуждали с ним в личной переписке, и таким образом значительно повысить свои шансы на проведение успешной атаки.

Такой подход можно совместить с традиционными разведметодами, когда злоумышленники дополнительно проверяют правильность выбора жертвы, чтобы свести к минимуму распространение вредоносного ПО и вероятность его обнаружения. В случае распространения через почтовые вложения стандартной практикой является проверка на взаимодействие с реальным человеком до запуска какой бы то ни было вредоносной активности, с целью обхода автоматических систем обнаружения.

Кроме того, имеется ряд инициатив по использованию машинного обучения для повышения эффективности фишинга. Пока непонятно, каковы будут результаты при реальном сценарии, но очевидно, что под действием всех перечисленных факторов целевой фишинг в ближайшие месяцы останется весьма эффективным вектором заражения, особенно через социальные медиа.

ДЕСТРУКТИВНЫЙ OLYMPIC DESTROYER

В прошлом году Olympic destroyer стал одним из самых известных случаев потенциально деструктивного вредоносного ПО, но многие киберпреступники регулярно включают такие инструменты в свои вредоносные кампании. Деструктивные атаки дают злоумышленникам ряд преимуществ и используются, в частности, для осуществления отвлекающих маневров, «подчистки» журналов и улик после завершения атаки, либо просто в виде неприятного сюрприза для жертвы.

Некоторые из этих деструктивных атак имеют геостратегические цели, связанные с текущими конфликтами, в частности на Украине, а также с политическими интересами, как в случае атак на нефтяные компании в Саудовской Аравии. В других случаях атаки могут быть результатом хактивизма, либо проводиться группами-посредниками, действующими по заказу более влиятельных агентов, которые предпочитают оставаться в тени.

В любом случае, у всех подобных атак есть общая черта – это слишком привлекательный инструмент, чтобы им пренебречь. Например, государства могут использовать кибератаки в качестве инструмента возмездия, занимающего промежуточное положение между дипломатическим ответом и военными действиями. Некоторые государства уже экспериментируют с этим оружием. Такие атаки чаще всего планируются заранее, их подготовка на раннем этапе включает сбор разведданных и вторжение. Трудно сказать, сколько потенциальных жертв сейчас находятся в ситуации, когда атака уже подготовлена и нужна лишь команда, чтобы ее начать. Также сложно предположить, какие еще инструменты для проведения деструктивных атак имеются в арсенале киберпреступников.

Особенно уязвимы для подобных атак промышленные системы управления (ICS) и критическая инфраструктура. Хотя индустрия кибербезопасности и госструктуры в последние несколько лет приложили немало усилий для улучшения ситуации, пока что она далека от идеальной. Мы полагаем, что атаки такого рода никогда не будут распространены повсеместно, но в будущем году ожидаем увидеть несколько таких атак, особенно в качестве акта политического возмездия.

ПРОДВИНУТАЯ ЦЕПОЧКА ПОСТАВОК

Этот вектор атак успешно эксплуатируется в течение последних двух лет, что не может не вызывать беспокойство – многие задумались о количестве и безопасности своих поставщиков. К сожалению, на атаки подобного рода нет простого ответа.

Хотя этот вектор идеален, чтобы взять на мушку целую отрасль (подобно тому, как это делается в watering-hole атаках) или даже целую страну (как в случае шифровальщика NotPetya), он значительно менее эффективен при проведении целевых атак, когда риск обнаружения выше. Мы также наблюдали случаи неизбирательных атак – например, инъекцию вредоносного кода в популярные библиотеки на публичных репозиториях. Такой подход может применяться для проведения атаки в тщательно выбранный момент времени, когда эти библиотеки используются в конкретном проекте, с последующим удалением из репозитория вредоносного кода.

Может ли этот вид атак использоваться более направленным способом? В случае программного обеспечения это сложно, поскольку оно оставляет следы повсюду, а вредоносный код, вероятно, попадет на компьютеры нескольких пользователей. Подход выглядит более реалистичным, если провайдер работает исключительно для конкретного клиента.

А как насчет аппаратных имплантов, представляют ли они реальную возможность? Недавняя полемика по этому поводу не позволяет дать однозначный ответ. С одной стороны, в данных Сноудена приводился яркий пример того, как аппаратное обеспечение может подвергаться манипуляциям на пути к клиенту. С другой стороны, похоже, что такие манипуляции под силу только самым мощным группам, и даже для них имеется ряд ограничений.

Однако в тех случаях, когда известно, для какого клиента предназначен конкретный заказ, злоумышленник может произвести манипуляции с аппаратным обеспечением в исходной точке, а не на пути к заказчику.

Сложно представить, как можно обойти все этапы технического контроля на производстве, и как подобное вмешательство может быть реализовано. Мы не исключаем такой вариант, но он, вероятно, предполагает содействие со стороны производителя.

В целом, атаки на цепочку поставок являются эффективным вектором заражения, и мы ожидаем, что в будущем они не потеряют свою актуальность. Что касается аппаратных имплантов, мы считаем это крайне маловероятным, а если подобное все же случится, мы скорее всего никогда об этом не узнаем...

МОБИЛЬНЫЕ УСТРОЙСТВА

Это традиционный раздел нашего ежегодного прогноза. Ничего принципиально нового не ожидается, но всегда интересно думать о двух скоростях этой медленной волны заражений. Понятно, что все киберпреступники включают мобильные компоненты в свои вредоносные кампании – заражать только компьютеры Windows не имеет смысла. Можно найти много примеров вредоносного ПО для Android, но также встречаются случаи атак на iOS.

Хотя успешное заражение iPhone требует эксплуатации сразу несколько уязвимостей нулевого дня, всегда стоит помнить, что у располагающих ресурсами злоумышленников есть возможность заплатить за такую технологию и использовать ее для проведения критических атак. Некоторые частные компании утверждают, что они могут взломать любой iPhone, к которому у них есть физический доступ. Другие, менее богатые группы могут применять весьма хитроумные методы обхода защиты на этих устройствах – например, используя фальшивые MDM-серверы и заставляя жертв с помощью методов социальной инженерии подключать к ним свои устройства, что позволяет злоумышленникам устанавливать на iPhone вредоносные приложения.

В начале года произошла утечка загрузочного кода iOS. Интересно, смогут ли киберпреступники использовать ее для своих целей и найти новые способы эксплуатации кода.

В любом случае, мы не предвидим никаких крупных эпидемий, связанных с мобильным вредоносным ПО, но ожидаем продолжения активности продвинутых злоумышленников по поиску новых способов получения доступа к устройствам потенциальных жертв.

ПРОЧЕЕ

Какие идеи могут прийти в голову киберпреступникам в более долгосрочной перспективе? На военной арене это замена относительно слабых и склонных к ошибкам людей чем-то более механическим. Или, учитывая выдворение из Нидерландов в апреле прошлого года предполагаемых агентов ГРУ после их попытки проникнуть в Wi-Fi сеть ОЗХО, – как насчет использования дронов вместо агентов-людей для проведения хакерских атак на близком расстоянии?

Или внедрения бэкдоров в проекты криптовалют, которых сотни, для сбора информации или получения финансовой выгоды?

А если говорить о применении цифровых ценностей для отмывания денег – как насчет использования внутриигровых покупок и дальнейшей продажи таких учетных записей?

Конечно, реальность всегда превосходит любые прогнозы – предвидеть все сценарии просто невозможно. Сложность цифровой среды уже нельзя полностью понять, что повышает вероятность специализированных атак в различных областях. Как можно использовать внутреннюю межбанковскую систему фондовой биржи в мошеннических целях? Я не знаю. Я даже не знаю, существует ли такая система. Это лишь один пример того, насколько сложно предугадать возможности злоумышленников, стоящих за такими кампаниями.

Наша задача – попытаться предвидеть грядущие атаки, понять те, что мы сейчас не понимаем, и предотвратить их в будущем.