Мафия высоколобых умников с электронными отмычками

Совсем недавно голливудские фильмы про суперкрутых хакеров, шантажирующих полмира атомным пуском и требующих за спасение миллиарды долларов, казались только слегка напоминающей жизнь фантастикой. А что сегодня?

Пароли взламываются, личные данные становятся предметом охоты. Причём, купить готовы всё: начиная от наших паспортных данных и телефона, заканчивая медкартой. На любую информацию найдётся покупатель, который придумает, как её использовать. Спектр - широчайший, начиная от адресной рекламы, заканчивая шантажом и вымогательством.

Вот свеженькая новость из Австрии. Неизвестный шифровальщик "взломал" четырёхзвездочный отель. Пострадали система бронирования, кассовая система, но самое печальное заключалось в том, что шифровальщик вошёл в систему электронный замков и заблокировал почти все двери отеля. Электронные замки не реагировали на свои ключ-карты, а быстро выпустить новые оказалось просто невозможно. Новые гости заведения не могли подтвердить бронирование и поселиться в отеле.

Впрочем, с замками всё было не так уж и страшно - их нетрудно открыть изнутри и снаружи. Благодаря страховочным мерам, в номерах никого не заперли, но раскошелиться на 1600 долларов выкупа в биткоин-эквиваленте, руководству отеля всё-таки пришлось, потому что работать в таких условиях было невозможно.

"*Нас взломали, но никто не был заперт, ни внутри, ни снаружи*", — *рассказал изданию Bleeping Computer управляющий отелем Кристофер Брандштеттер (Christopher Brandstaetter), опровергая мрачные сообщения других СМИ. — Но в течение суток мы не могли сделать новые ключ-карты, так как компьютеры были зашифрованы. Так как запорные системы должны продолжать работать даже при полном отключении электроэнергии, гости отеля практически не заметили случившегося*".

Издание The Local пишет, что хотя руководство Romantik Seehotel Jägerwirt выплатило выкуп, злоумышленники попытались оставить бэкдор в системах отеля, очевидно, планируя совершить еще одну атаку. Однако наученные горьким опытом сотрудники отеля поработали над улучшением безопасности, и новая попытка хакеров не увенчалась успехом.

История почти невинная - никто не пострадал, выкуп оказался не таким уж и огромным. Но главное не ущерб и последствия, а прецедент. Тем более что нынешний январь отмечен целой серией подобных прецедентов. Но, обо всём по порядку.

В том, что хакеры только и думают, где бы и чего вскрыть, убеждают и данные,собранные лабораторией Касперского.

Как и все порядочные люди, в новогодние каникулы хакеры отдыхали, а в середине января с удвоенной активностью взялись за дело.

Пока в России отмечали Старый Новый год, хакеры взялись за Facebook. С целью завладеть чужими учетными данными со взломанных аккаунтов злоумышленники рассылают сообщения с темой "You are in this Video?" ("Вы на этом видео?") и вредоносной ссылкой, ведущей либо на поддельную форму авторизации, либо на сайт с вредоносным ПО.

Следом пришла очередь пользователей Chrome. С начала текущего года ИБ-эксперты зафиксировали новый виток операции EITest, проводимой злоумышленниками, по крайней мере, с 2014 года. В ходе кампании используется цепь скомпрометированных легитимных сайтов, распространяющих различные наборы эксплойтов.

Исследователь безопасности MalwareHunterTeam обнаружил новое семейство вредоносного ПО, позволяющего получить полный контроль над целевой системой при помощи команд по IRC-каналу. Предполагают, что GhostAdmin - вариант активного 3-4 года назад вредоносного ПО CrimeScene.

Новый Android-троян, способный внедряться в активный процесс Play Market и накручивать счетчик установок в каталоге Google Play, обнаружили эксперты "Доктор Веб". Android-троян внедряется в активный процесс P. Android.Skyfin.1.origin, загружает приложения и сохраняет их на карту памяти устройства без последующей установки. Такой вредонос трудно обнаружить, но сам он может и дальше накручивать счетчик установок, искусственно повышая популярность программ в каталоге.

Эксперты компании Malwarebytes сообщили о шпионском ПО для Mac. Бэкдор Quimitchin использует устаревший код и атакует медицинские исследовательские лаборатории. Основными функциями вредоноса является похищение снимков экрана и доступ к web-камерам на зараженных Mac. Apple назвала его Fruitfly и пообещала вскоре выпустить решение безопасности для борьбы с ним.

Если говорить об утечках информации, то в середине января некие умельцы атаковали хакерский форум Darkode и похитили базу данных его пользователей. По признанию одного из администраторов

ресурса, отчасти атака оказалась успешной из-за повторного применения пароля, уже использовавшегося им на другом взломанном сайте.

Об утечке данных пользователей своего форума также сообщил разработчик игры Clash of Clans, компания Supercell. Из-за уязвимости в движке vBulletin злоумышленникам удалось похитить электронные адреса и зашифрованные пароли порядка 1 млн пользователей.

Самым вызывающим событием второй декады января смело можно назвать взлом учётной записи в Twitter, принадлежащей The New York Times. Ссылаясь на утечку информации от Президента РФ Владимира Путина, хакеры опубликовали ложный твит о готовящемся ракетном ударе со стороны России.

Последняя неделя января была отмечена сразу несколькими крупными утечками данных. Хакер под псевдонимом DoubleFlag выставил на продажу в даркнете данные одного миллиарда пользователей китайских операторов связи и интернет-сервисов, и 127 миллионов клиентов американской телекоммуникационной компании United States Cellular Corporation (U.S. Cellular).

О том, что некто украл сведения об одном миллионе пользователей сообщил разработчик популярной мобильной игры Clash of Clans, финская компания Supercell. Для достижения своей цели хакеры проэксплуатировали уязвимость в движке vBulletin, используемом на форуме сообщества. В результате инцидента, произошедшего в сентябре прошлого года, были похищены данные (электронные адреса и зашифрованные пароли).

Некорректно сконфигурированная база данных стала причиной того, что в сеть утекла персональная информация 180 тысяч пользователей сайта для взрослых The Candid Board. База включает уникальные адреса электронной почты, логины, хэшированные пароли, даты рождения, IP-адреса и логи web-сайта. Всего вышеперечисленного достаточно, чтобы сотни тысяч вполне достопочтенных граждан ночей не спали, опасаясь, как бы их виртуальные развлечения не стали достоянием общественности.

Ещё один тренд сезона - учащение DDoS-атак, цель которых получение выкупа за прекращение. Как стало известно на прошлой неделе, некая киберпреступная группировка в середине текущего месяца атаковала банк Lloyds Banking Group. За прекращение атаки злоумышленники потребовали выкуп в размере 100 биткоинов.

Жертвами аналогичных атак стали брокерские компании Гонконга. Киберпреступники атаковали их сайты, вывели из строя сервисы и требовали выкуп за прекращение атак. В среду, 25 января, также началась DDoS-атака на официальный сайт Национальной гвардии РФ. Кто стоит за инцидентом, и какие цели преследовал - неизвестно.

Почти одновременно масштабная кибератака была произведена на компьютерную сеть вооруженных сил Швеции. Как полагают аналитики Радиокоммуникационной службы шведской обороны, атака могла быть осуществлена как для сбора секретных данных, так и для подключения компьютеров ВС к атакам на ресурсы других стран.

Интерес для взломщиков чужих данных представляет абсолютно всё, от наших с вами домашних компьютеров до информационных систем больниц или городской инфраструктуры. Подтверждают это многочисленные атаки на медицинские учреждения или систему городского транспорта Сан-Франциско.

Сравнительно недавно полиция небольшого техасского города Кокрелл Хилл выпустила официальный пресс релиз, в котором признала, что в декабре 2016 года управление стало жертвой атаки некоего шифровальщика OSIRIS. В результате взлома полицейские потеряли множество цифровых улик, собранных за последние годы: записей с видеорегистраторов, камер наблюдения, фотографий, документов. Некоторые утраченные файлы были датированы 2009 годом.

Заражение произошло из-за обычного спамерского письма: один из сотрудников открыл email, якобы пришедший с адреса, принадлежащего другому сотруднику департамента, хотя на деле адрес был подделан.

Большая часть данных была продублирована на дисках, но в архиве держали только достаточно старую информацию. А вот новые файлы, связанные с текущими расследованиями, были потеряны навсегда. Пресс-релиз, выпущенный по этому поводу, гласит, что "в настоящий момент неизвестно, какое количество цифровых копий документов утрачено, а также неизвестно, сколько видео и фотографий, которые могли бы быть полезны в расследованиях более новых дел, более недоступны". Известно, что атака на полицейское управление была обнаружена 12 декабря 2016 года. За восстановление данных злоумышленники требовали $4 000, но платить вымогателям полицейские не стали. Вместо этого, проконсультировавшись со специалистами из ФБР, правоохранители решили полностью очистить свои серверы и переустановить все с нуля.

Параллельно со взломом сетей, кражей данных или разрушением баз данных, хакеры уверенно входят в мир "Интернета вещей" (IoT). Там, безусловно, есть чем поживиться, да защита "умных устройств" пока нет так хороша, как хотелось бы. В результате кухонные приборы, системы видеонаблюдения, и прочие программируемые приборы превращаются в руках киберпреступников в настоящее оружие.

По мнению экспертов, преступники также найдут новые способы монетизировать взломанные IoT-устройства.

Старший исследователь безопасности компании ESET Стивен Кобб (Stephen Cobb) выделил три угрозы, ставшие особенно актуальными в 2016 году: вымогательское ПО, DDoS-атаки и вредоносные программы для устройств "Интернета вещей" (IoT).

По мнению эксперта, эти тенденции получат развитие и в текущем году. Более того, преступники начнут комбинировать их между собой. К примеру, злоумышленники могут использовать взломанные IoT-устройства для осуществления DDoS-атак на коммерческие сайты или блокировать работу IoT-устройств, требуя выкуп за ее восстановление. Такие комбинированные угрозы Кобб назвал "jackware". Если некоторые считают 2016 год "годом вымогателей", то 2017 станет "годом jackware", уверен эксперт.

"Jackware" – это вредоносная программа, предназначенная для заражения устройств, у которых хранение или обработка данных не самые главные функции. В качестве примера Кобб привел "подключенный" автомобиль. Системы машины хранят и обрабатывают большие объёмы данных, но нужна она для перевозки пассажиров и грузов.

Обычные вымогатели наподобие Locky и CryptoLocker шифруют документы на вашем компьютере и требуют выкуп за их восстановление. Jackware будет блокировать машину или другое устройство, до тех пор, пока вы не заплатите", - пояснил эксперт.

Jackware может перерасти в угрозу для всего "Интернета вещей". Кобб даже предложил термин для нее – Ransomware of Things или RoT. Не допустить такого развития событий можно, изменив некоторые сложившиеся тенденции, уверен эксперт. Во-первых, производители "умных" устройств должны больше внимания уделить безопасности своей продукции. Во-вторых, необходимо внести соответствующие изменения в законодательство.

А между тем, аппетиты хакеров растут не по дням, а по часам. По данным экспертов, в 2015 году максимальная мощность DDoS-атак достигала 500 Гб/с, но уже в 2016 году показатель увеличился до 800 Гб/с. В прошлом году мощность 558 зафиксированных исследователями Arbor Networks DDoS-атак превышала 100 Гб/с. Для сравнения, в 2015 году таких атак насчитывалось 223. Мощность 87 атак достигала 200 Гб/с, тогда как годом ранее эксперты зафиксировали лишь 16 подобных инцидентов. По подсчетам исследователей, ежегодно средняя мощность DDoS-атак увеличивается на 23%, а значит, к концу текущего года она достигнет 1,2 Тб/с.

Росту мощности DDoS-атак поспособствовали созданные из огромного числа незащищенных устройств "Интернета вещей" ботнеты наподобие Mirai и Bashlite. К примеру, IoT-ботнет LizardStresser позволял осуществлять DDoS-атаки мощностью до 400 Гб/с без использования каких-либо техник усиления и отражения. Правда, совсем от использования методов усиления киберпреступники все же не отказались. Согласно отчёту, в 2016 году наиболее популярным был метод DNS-отражения пакетов.

Помимо мощности, выросло и количество самих атак. 53 процента от 356 опрошенных исследователями провайдеров ежемесячно фиксировали свыше 51 DDoS-атаки. Годом ранее этот показатель составлял 44 процента. С более 10 атаками в месяц сталкивались 45% частных, правительственных и образовательных организаций. Свыше 50 атак в месяц фиксировали 21 процент дата-центров – существенный рост показателя по сравнению с 2015 годом (восемь процентов).

Судя по всему вышесказанному, скоро главные преступники уйдут в сеть. Я не верю, что главари преступного мира спокойно смотрят, как развиваются хакерские сети, как растут аппетиты высоколобых умников. И если однажды окажется, что именно в недра недремлющей мафии уходят нити и связи, то никто этому особенно не удивится. В чём же тогда главная беда происходящего? Да в отсутствии ограничений и моральных принципов. В игре, где цель оправдывает средства, все методы хороши, и прогноз мой весьма неутешителен.

Если связи между взломщиками проследить невозможно - это не значит, что их нет. Что делать? Придумывать хитрые пароли, ставить антивирусы, беречь личные данные и не выкладывать в сеть компрометирующие личные данные.