МВД России

М И Н И С Т Е Р С Т В О
ВНУТРЕННИХ ДЕЛ
ПО РЕСПУБЛИКЕ ТАТАРСТАН
(МВД по Республике Татарстан)

ул. Дзержинского, 19, г. Казань, 420111

Председателю Совета
Банковской ассоциации
Татарстана

Л.Р.Китайцевой

08.06.2016 года № 28/5170

на № _____
от_____

Уважаемая Людмила Романовна!

МВД по Республике Татарстан крайне заинтересовано в обеспечении информационной безопасности кредитных организации республики с целью недопущения совершения хакерских и иных преступлений, объектом которых могут стать банки Республики Татарстан.

С целью информирования руководства и специалистов по информационной безопасности кредитных организаций, направляем сведения о новых способах совершения киберпреступлений, выявленных уязвимостях, механизмах проведения хакерских атак и их последствиях для размещения на интернет-ресурсах либо в печатных изданиях.

Информация получена от специализированной организации по обеспечению информационной безопасности.

О результатах размещения просим сообщить на электронную почту it-mvd-rt@mail.ru.

Приложение на 7-ми листах

С уважением,
Руководитель аналитической специализированной группы
по раскрытию и расследованию преступлений в сфере высоких технологий
М.Ю.Машин

Вирус-вымогатель Jigsaw. При внедрении в ПЭВМ (способ не установлен) появляется сообщение о передаче 150 долларов за расшифрование сведений. При затягивании срока оплаты либо отказа платить, вирус уничтожает 1 файл каждые 60 минут, а если «перезагрузить» компьютер, то сразу 1 тысячу файлов. Пока имеется информация, что зловред осуществляет поиск 226 файлов разного типа и осуществляет их криптошифрование с расширением .KKK, .FUN,. .BTC, .GWS.

***

Специалисты BAE Systems обнаружили новую версию ботнета Qbot, задача которого - кража учетных данных и создание «черных ходов» на зараженных системах. В состав ботнета входит 54,5млн. инфицированных ПЭВМ в тысячах организаций. Qbot запрограммирован на автоматическое распространение и не обнаруживается многими антивирусными решениями. Попав в компьютер, Qbot пытается заразить другие ПЭВМ в сети, а если они защищены паролем, зловред осуществляет попытки доступа к диспетчеру паролей, а если и это не получается, применяет список с распространенными сочетаниями логин/пароль, находящемся в теле трояна, для реализации брутфорс-атаки.

Qbot ориентирован на заражение неограниченного числа компьютеров. Программа обновляется каждые шесть часов, что не позволяет модифицировать его структуру и эффективно ему противоборствовать.

Ранее в 2014 года сотрудники Proofpoint был установлен ботнет Qbot из из 500 тыс.инфицированных систем, что меньше в разы выявленному в настоящее время. Тогда троян перехватил около 800 тыс.транзакций online-банкинга.

***

Стандарты Банка России (ИББС-1.0-2014) исчерпывающе описывают систему менеджмента информационной безопасности организаций банковской системы.

При этом абсолютно верно в основу исходной концептуальной схемы положено противостояние собственника и злоумышленника, цель которых, с одной стороны защитить информационные активы, второго – осуществить над ними контроль.

В тоже время, большинством кредитных организаций не исполняются п.5.11 указанного Стандарта: привлечение специализированных организаций для составления моделей угроз и нарушителя, политики информационной безопасности, моделирование попыток угроз «извне» не привлекаются.

Дополнительно, как стало известно из отчетности Русского международного банка по МСФО за 2015 год, киберзлоумышленники похитили принадлежащие Банку 500 млн.рублей, находящиеся на кор.счете в Банке России.

В марте 2016 года с корсчета Металлинвестбанка виртуальными преступниками похищено 667 млн.рублей.

***

В виртуальном пространстве создан первый червь, ориентированный на распространение через программируемые логические контроллеры (ПЛК) фактически без инфицирования ПЭВМ или иных систем.

Механизм распространения, безусловно, традиционен в начале, то есть червю необходимо попасть на компьютер, но дальше начинают функционировать его новые свойства.

Пока создатели (Ralf Spenneberg и Maik Brüggeman) обозначают возможность распространения вируса между ПЛК Siemens S7 1200, но поясняют, что он может быть модифицирован под любые контроллеры.

Более того, инициатива немецких хакеров была подхвачена специалистом IOActive Александром Большевым, который выявил способ повышения скрытности червя, что было подтверждено в ходе дальнейших исследований специалистов Honeywell.

***

В Сети диагностирован вид трояна-вымогателя Bucbi, распространяемого посредством брутворс-атаки, вместе традиционного фишингового способа или эксплоита. Ориентир нового вируса-вымогателя – корпоративные сети с RDP-серверами на платформе Windows. Распространение происходит через создание удаленного рабочего стола к серверным оборудованиям.

Уже зафиксированы случаи использования трояна, злоумышленники «заразив» и зашифровав сведения одной организации (Прим.автора - наименование не раскрывается) за расшифровку потребовали более 2.000 долларов США (в эквиваленте 5 биткоинов).

Данный вид вредоносного ПО представляет повышенную опасность, поскольку шифруют всю корпоративную сеть.

***

Bozkurtlar (Прим. автора - группа хакеров) «выбросили» в Интернет в открытый доступ подробную финансовую информацию (около 10 Гб) «Инвест-Банка» («InvestBank», ОАЭ).

По мнению специалистов**,** опубликованию подверглись номера счетов, банковские выписки, транзакции, сведения о регистрации имущества, сканы личных документов (паспортов), особенности внутренних сетей кредитной организации, логины и пароли.

Представители InvestBank признали данный факт, указав что инцидент имел место в конце 2015 года. Предполагается, что Bozkurtlar имеет непосредственное отношение также и к краже информации Центробанка Катара.

Как стало известно проведенная злоумышленниками в марте 2016 года хакерская кампания с использованием уязвимостей «нулевого дня» (CVE-2016-0167) затронула торговые предприятия, организации гостиничного бизнеса и ресторатороов (всего более 100 объектов атак), осуществляющих свою деятельность на территории Северной Америки.

При совершении атак использовались фишинговые письма с вложениями документов Word с макросами, которые после активации загружали на ПЭВМ

вредонос PUNCHBUGGY.

По мнению специалистов FireEye, указанное программное обеспечение представляет из себя 32-битную и 64-битную библиотеку, способное получать посредством HTTPS-протокола информацию об осуществленном внедрении, после чего злоумышленники осуществляли доступ к «зараженным» системам.

При этом, в процессе проникновения использовался доселе неизвестный механизм (Прим.автора – обозначенный как PUNCHTRACK) получения информации о банковских картах из PoS-терминалов. Специфика зловреда заключалась в том, что при инсталяции на терминале, программа не сохранялась на диске. В настоящее время известно лишь об одном случае совершения атаки в паре (PUNCHBUGGY+ PUNCHTRACK).

***

Как стало известно на систему SWIFT (прим.автора - финансовая система, к которой подключены 11 тысяч банков по всему миру) вновь была атакована хакерами.

При этом интервал между атаками составил всего несколько месяцев.

Данный инцидент может быть рассмотрен, как преследующий цель скомпрометировать товарообладателя (SWIFT), так и являющийся частью широкой кампании в отношении кредитных организаций.

Ранее подобной атаке был подвергнут Центральный банк Бангладеша, тогда было похищено 81 млн.долларов США. В этот же раз целью виртуальных преступников стал коммерческий банк (наименование и сумма ущерба не разглашается), что подтвердила представитель SWIFT Natasha de Teran.

При совершении данного нападения хакеры также как и ранее использовали уязвимости обеспечения и, получив доступ к учетным данным авторизации, подделали при помощи трояна PDF-отчеты о перечислении денежных средств на подконтрольные счета. Именно использование трояна несколько отличает данный инцидент от произошедшего с Центробанком Бангладеша.

***

Последние месяцы в IT-сфере прошли под девизом хакеров – «всё в Сеть» и охарактеризовались глобальными «вбросами» информации в свободный доступ. Так, в апреле 2016 года в Сеть просочились сведения с электронных хранилищ Центробанка Катара, мы уже освещали о выкладывании в свободный доступ конфиденциальных сведений ИнвестБанка (ОАЭ), имеется информация об опубликовании в Twitter личных данных китайских миллионеров.

Учитывая массовость подобных инцидентов, предполагаем, что это только та часть, которая стала известна и опубликована, не исключается вероятность, что в настоящее время хакерами осуществляется «переписка» с собственниками информации об её выкупе и, в случае отказа, в Интернет вновь поступят очередные личные данные.

Стоит отметить, что к кражам учетных и иных конфиденциальных сведений имеются прямые предпосылки.

Так, в настоящее время, практически во всех компаниях имеются свои сайты, приложения, личные кабинеты, другими словами web-ориентированные

продукты с нередко «оставленными без внимания» поддоменами или «заброшенными» интернет-приложениями. Все это привлекает хакеров.

Что же делать?

Безусловно, самым эффективным способом снизить риск хакерской атаки является ограничение доступа к подобным ресурсам и «переработка» с закрытием внешних выходов для приложений, используемых исключительно для внутренних нужд предприятия.

Не менее эффективным является установка и правильная настройка межсетевых экранов, но надо быть подготовленным к тому, что «файрволлы» могут обеспечить защиту исключительно от несложных либо автоматизированных активных проникновений и «не закроет» полностью внутренние активы предприятия от хакеров – профессионалов.

Можно отметить, что на «вооружении» нашей компании имеется спектр мер, применение которых позволит минимизировать угрозы для Вашей компании.

***

В Сети вновь выявлена вредоносная программа, цель которой финансовые организации, на этот раз, осуществляющие свою деятельность на Ближнем Востоке.

Механизм распространения – рассылка злоумышленниками электронных писем с приложением вредоносного ПО.

При этом, уникальность атак характеризуется использованием специальных скриптов, что не так часто можно обнаружить в Сети, поскольку их написание требует дополнительных затрат от хакеров, а в ряден случаев особенности атакуемых систем.

Распространение «зараженных» писем осуществляется посредством электронных сообщений с присвоением грифа «служебности» документа, например, «отчета о состоянии сервера».

Также зафиксировано, что в одном из случаев, текст документа действительно содержал оригинал переписки между сотрудниками с указанием их контактной информации.

Что же касается собственно применяемого скрипта. Активация встроенного во вредоносное ПО макроса приводит в действие скрипт, загружающий на ПЭВМ утилиты Mimikatz и BAT-файл, ориентированных на сбор сведений о системе, включая данных об авторизации пользователя, имени хоста, учетных записей и т.д.

Интереснейшая особенность «зловреда» - использование DNS-запросов для эксфильтрации информации, что, в свою очередь, скрывает активность самой программы, поскольку блокирование DNS-протокола не происходит, а наоборот, его применение не вызывает подозрений.

Отметим, что пока «вредонос» диагностирован только на ПЭВМ с ОС Windows Vista.

***

Многим известно, что в ходе своего функционирования TeamViewer

(программа удаленного управления ПЭВМ) применяет различные функции, чем постоянно пользуются хакеры для получения неправомерного доступа к компьютерам жертвы. До настоящего времени, в принципе, было известно об основных способах применения данной программы в преступных целях, но… диагностирован ранее не известный троян BackDoor.TeamViewer.49, который использует данную утилиту в иных целях.

В теле трояна запрограммированы данные о C&C-серверах, с которых вредоносное ПО может «получать» инструкции злоумышленника, при этом передача сведений осуществляется в зашифрованном виде.

Для «инфицирования» компьютера данный «вредонос» использует другое ПО Trojan.MulDrop6.39120, маскирующегося под апгрейд Adobe Flash Player. Одновременно с установкой плеера осуществляется загрузка на компьютер трояна BackDoor.TeamViewer.49, а также инсталлируется необходимые для его работы конфигурационные файлы. Вычислить данный процесс весьма затруднительно, поскольку на мониторе отображается прогресс установки настоящего Flash Player.

После своего запуска «Бэкдор» скрывает соответствующий значок-уведомление из строки трея Windows и деактивирует процесс оповещения пользователя об ошибках. Троян размещается в автозагрузочных файлах, туда же инсталлирует необходимые для функционирования файлы «системы» и «скрытый» для папки, где хранятся «нужные» для него файлы и вредоносная библиотека.

Указанный механизм позволяет киберзлоумышленникам использовать «зараженный» компьютер жертвы в качестве прокси-сервера и обеспечивает анонимность действий в Сети.

***

Сотрудниками специального подразделения ФБР по борьбе с преступлениями в Интернете (Internet Crime Complaint Center, FBI, USA), приводя официальные отчетные данные за 2015 год, обозначили, что в минувшем году ущерб от незаконной деятельности отдельных хакеров и (-или) групп киберзлоумышленников превысил 1 млрд.долларов США.

Учет компьютерных инцидентов осуществлялся исходя из количества поступивших в Центр жалоб на действия виртуальных преступников с указанием последствий атаки и суммы ущерба.

Количество атак и специфика совершенных виртуальных преступлений не приводится.

***

За последний год экспертами ряда компаний в области IT-безопасности зафиксировано 30 случаев, когда «хакеры», осуществляя мониторинг систем безопасности предприятий, находят уязвимости, осуществляют проникновение, копируют различную конфиденциальную информацию.

В последующем, киберзлоумышленники связываются с руководством организации и предлагают «выкупить» сведения о наличии уязвимости и способах их устранения, подтверждая свои требования о «скачивании» сведений конкретными внутренними файлами компаний, демонстрированием переписки

сотрудников, служебными документами. Средняя цена «выкупа» 30 тыс.долларов США.

Данная незаконная тактика уже получила наименование, как bug poaching.

***

По мнению сотрудников Positive Technologies, с которым сложно не согласится, единственным средством защиты от вирусов многие пользователи считают установку антивирусного обеспечения.

В Интернете много сайтов с обсуждениями, какие из антивирусников выбрать, у кого какие достоинства и т.д., и при этом установка данного программного продукта относится к числу доверенных приложений.

Конечно, антивирусы – первая линия обороны, ориентированные на ограничение доступа на ПЭВМ различных вредоносных программ. Но….

понимая, что «вредонос» та же программа, только ориентированная на причинение ущерба при использовании уязвимостей и человеческого фактора, многие не задумываются, что антивирусники – тоже программный код, написанный программистами, а значит также склонны к наличию уязвимостей.

Особая опасность, что утилиты антивирусного ПО имеют приоритет к запуску на компьютерах, получают доступ к основным программным процессам ПЭВМ, а значит, злоумышленник, получив через уязвимость доступ к антивирусу, фактически получает доступ и к центру управления ПЭВМ и, в итоге, может скомпрометировать всю систему.

Несколько статистических примеров. Так, в 2002 году не было найдено ни одной уязвимости в антивирусном программном обеспечении, по крайней мере сведений и опубликований об этом не осуществлялось, через пять лет - уже 13, в 2010 году – 39, а в 2015 году найдены 53 уязвимости в наиболее популярных продуктах: Avast, Kaspersky Lab, ESET и других.

***

В *Сети распространена информация о появлении нового трояна с признаками различных вариантов реализации вредоносных функций: хищение денежных средств, сбор важных сведений о пользователях, шпионство.*

Название данного вредоносного программного продукта Trojan.Bolik.1.

Согласно принципа действия данного вируса допускается относить его к банковским троянам, поскольку использует в своей активности возможности диагностированных ранее таких «зловредов» как Zeus и Carberp.

Одновременно, по мнению специалистов компании Др.Веб рассматриваемый троян способен распространяться самостоятельно, т.е. без участия своего хозяина-пользователя.

В функционале вируса заложены возможности осуществления сканирования сетевых папок, накопителей, в том числе и USB, исследовать и инфицировать 32-битные и 64-битные файлы.

Основной способ попадания в систему через браузеры, к функционалу Trojan.Bolik.1 также необходимо отнести возможности делать «скриншоты» экрана и осуществлять запись использования пользователем клавиатуры, что

после анализа, может привести к побору логинов и паролей пользователей.

Информацию своему «хозяину» троян передает, используя обратные, реверсные соединения, передаваемые сведения подвергаются шифрованию.

***

Ранее уже рассказывали о вредоносном программном обеспечении, позволяющем злоумышленнику похищать сведения банковских карт, а в последствии и денежные средства, с использованием POS-терминалов.

В настоящее время вновь выявлено подобное вредоносное ПО.

Так, по информации Trend Micro диагностировано новый вредонос FastPOS. Если говорить об особенностях, то данному вирусу характерно отсутствие необходимости хранения сведений о банковских платежных картах, FastPOS передаёт все сведения в режиме он-лайн на сервер виртуальных злоумышленников.

Учитывая данную особенность, можно сделать вывод, что FastPOS ориентирован на похищение сведений из малых сетевых сред, с небольшой частотой использования POS-терминалов, что характерно для небольшого и среднего бизнеса с не самой высокой активностью осуществления платежей с использованием платежных пластиковых карт.

Тело трояна состоит из двух программ – скрапера, получающего идентификационную информацию о банковской карте, и кейлогера, осуществляющего контроль ввода ПИН-кода. Полученную информацию FastPOS немедленно отправляет злоумышленникам, при этом «особый интерес» для трояна представляют платежные карты, позволяющие осуществлять платежи без использования «секретного» (ПИН) кода.

Данное программное обеспечение доступно к приобретению на специализированных форумах хакеров.

По информации Trend Micro активность трояна FastPOS зафиксирована в европейских и азиатских странах, США, Японии.

Сведения предоставлены специалистами «МГА-Секьюрити» (г.Иннополис)