АКТУАЛЬНЫЕ ПРОБЛЕМЫ ПРОМЫШЛЕННОЙ КИБЕРБЕЗОПАСНОСТИ

КЕВИН ПАРКЕР (KEVIN PARKER)

Взрывной рост числа атак с использованием криптовымогателей в прошлом году — удручающая новость для инженеров на производстве. Криптовымогатели, как подсказывает само название, представляют собой разновидность вредоносных программ, с помощью которых злоумышленники преграждают пользователю доступ к компьютерной системе до тех пор, пока не будут выполнены их требования. Их следующая вероятная цель — ПЛК.

Чтобы осуществить атаку с использованием криптовымогателя, навыки программирования как таковые не нужны, поскольку инструментарий для таких атак можно легко заполучить в темных закоулках Интернета либо бесплатно, либо за небольшую мзду. Согласно недавно выпущенному компанией SonicWall ежегодному отчету об угрозах (Annual Threat), в 2017 г. имел место экспоненциальный рост числа угроз криптовымогательства — с почти 4 миллионов попыток осуществления атак в 2015 г. до 638 миллионов попыток в 2016 г., что составляет годовой прирост более чем в 167 раз (рис. 1). «Взрывной рост применения криптовымогателей в 2016 г. не похож ни на что из того, что нам довелось наблюдать за последние годы», — говорится в отчете.

Вам нужны доказательства реальности угрозы? По данным брифинга компании Booz Allen Hamilton по угрозам кибербезопасности, в течение 2015 и 2016 гг. произошло не менее 15 крупных инцидентов в промышленности (и это притом, что о многих вторжениях не сообщается). Вот некоторые примеры:

- В апреле 2016 г. злоумышленники с помощью фишинга внедрили криптовымогатель в корпоративную сеть компании Board of Water & Light (BWL) — коммунального предприятия энерго- и водоснабжения в штате Мичиган (США). Администраторы отключили корпоративную сеть, чтобы изолировать криптовымогатель и не дать ему распространиться в производственно-техническую среду.
- В декабре 2015 г. группа лиц получила удаленный доступ к SCADA-системам трех украинских энергораспределительных компаний, обзаведясь перед этим действующими сетевыми реквизитами с помощью адресного фишинга. Исполнители атаки использовали полученный доступ для систематического размыкания автоматических выключателей, тем самым оставив без электричества 225 000 потребителей.
- В июне 2015 г. на форуме в теневом Интернете (Dark Web), где продаются краденые данные, было

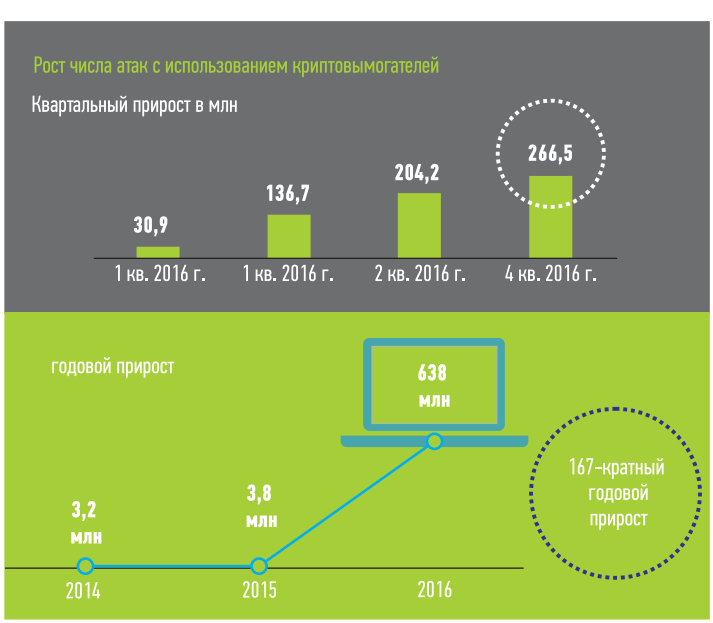


РИС. 1. ▶ Недавний колоссальный рост числа атак с использованием криптовымогателей стал следствием развития криптовалют, подобных биткоину (Bitcoin), которые облегчают незаконную наживу. (Публикуется с разрешения SonicWall)

размещено объявление о продаже реквизитов доступа к SCADA-системе. Запись содержала снимок экрана графического интерфейса пользователя, IP-адреса и пароли удаленного управления для SCADA-системы, управляющей гидрогенератором.

ПРАКТИЧЕСКОЕ ИССЛЕДОВАНИЕ ПРОБЛЕМЫ

Чтобы лучше изучить угрозу, ученые-исследователи из Технологического института Джорджии, занимающиеся вопросами кибербезопасности, недавно разработали криптовымогатель, способный перехватить контроль над имитационной моделью станции водоподготовки, как сообщает университетский новостной журнал Research Horizons. Получив доступ, исследователи передавали на ПЛК команды для запирания арматуры, избыточного хлорирования воды и отображения ложных показаний.

По словам ученых, продемонстрированная модельная атака ярко иллюстрирует уязвимости систем управления производством, используемых на предприятиях. Это исследование, которое считается первой демонстрацией компрометации реальных ПЛК с помощью криптовымогателей, было представлено в феврале этого года на конференции RSA в Сан-Франциско.

По данным SonicWall, атаки с использованием криптовымогателей обычно реализуются посредством фишинговых компаний и маскируются путем шифрования по протоколам SSL/TLS (рис. 2). Фишингом называется злонамеренная попытка собрать информацию или получить доступ к ней под видом заслуживающего доверия лица при взаимодействии по электронным каналам связи. TLS и SSL — это протоколы шифрования для защиты информации, передаваемой по каналам связи.

Как отмечает SonicWall, рост предложения криптовымогателей в форме услуги (упомянутого выше инструментария для атак) как никогда облегчает киберпреступникам доступ к криптовымогателям и их развертывание. Компании энергично пытаются защититься и найти ответ на дилеммы, возникающие в связи с новой киберугрозой.

К концу первого квартала 2016 г. компаниями было выплачено 209 миллионов долларов выкупа, а к середине года почти половина организаций сообщила, что стала объектом атак с использованием криптовымогателей за прошедшие 12 месяцев — такая информация приводится в отчете SonicWall.

Там же говорится, что в прошлом году атакам с использованием криптовымогателей подвергались компании всех размеров, хотя о многих из них не сообщалось публично. При этом зафиксированы случаи выплаты выкупа биткоинами в размере более чем $20 тыс. Затраты на полную ликвидацию последствий атаки, включая реагирование, стабилизацию и восстановление, вполне могут исчисляться миллионами долларов.

КРАТКАЯ ДЕМОНСТРАЦИЯ

Во многих системах управления предприятием не применяются стойкие протоколы защиты информации. Поэтому компрометация ответственных промышленных систем с требованием выкупа — это лишь вопрос времени. По словам исследователей из Технологического университета Джорджии, входящие в состав этих систем ПЛК являются следующей логичной целью для злоумышленников.

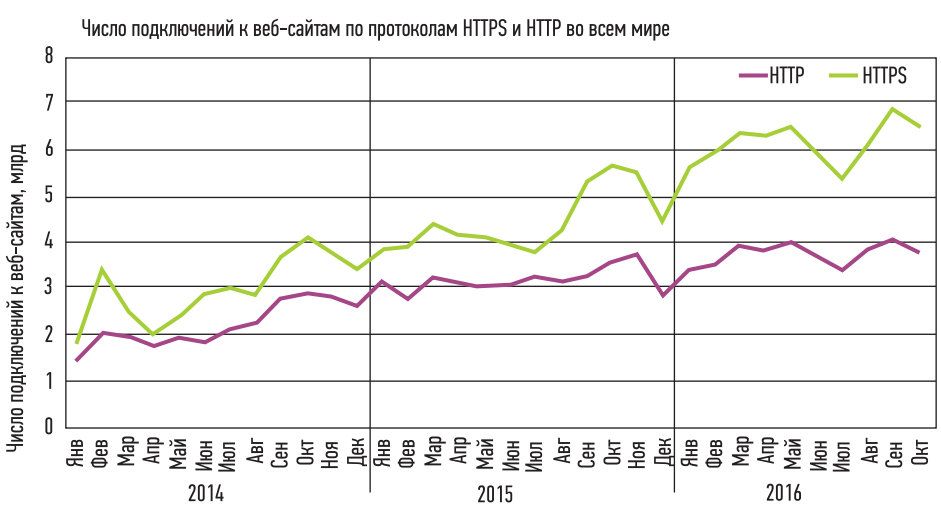
Чтобы это продемонстрировать, профессор Фонда Motorola и сопредседатель Института электротехники, электроники и вычислительной техники (School of Electrical and Computer Engineering) Рахим Бейя (Raheem Beyah) вместе с аспирантом того же института Дэвидом Формби (David Formby) нашел 1400 однотипных ПЛК, непосредственно доступных через Интернет.

Для начала исследователи задались перечнем из нескольких распространенных моделей ПЛК, используемых на промышленных объектах.

РИС. 2. ▼ Сегодня средства шифрования широко применяются для подключения к веб-сайтам — как легитимными пользователями с целью обеспечить кибербезопасность, так и злоумышленниками с целью ее нарушить. (Публикуется с разрешения SonicWall)

Шифрование по протоколу SSL/TLS

В 62 % подключений к веб-сайтам использовалось SSL/TLS-шифрование



Получив образцы трех различных устройств, они протестировали их на защищенность, включая парольную защиту и уязвимость к изменению настроек. После этого на базе данных устройств, а также насосов, труб и резервуаров была построена имитационная модель станции водоподготовки.

Большинство ПЛК располагается за бизнес-системами, которые до некоторой степени их защищают — но только пока не будет скомпрометирована корпоративная сеть. После того как злоумышленники проникнут в корпоративную ИТ-систему, уровень защищенности систем управления может оказаться недостаточным, предупреждают исследователи. Слишком многие предприятия устроены так, что любой пользователь сети уполномочен вносить изменения в системах управления. Слабость паролей и технических политик защиты информации может привести к тому, что злоумышленники получат контроль над насосами, арматурой и другими ключевыми компонентами системы управления предприятием.

Более того, сегодня подключенными к Интернету оказываются системы, которые для этого вовсе не предназначались, а пользователи по-прежнему пребывают в уверенности, что они не находятся в общедоступной сети и неуязвимы для атак. Исследователи отмечают, что в системах управления предприятиями зачастую есть неизвестные операторам подключения, служащие в том числе для обслуживания, диагностики и устранения неисправностей, обновления ПО.

ДЕЛЬНЫЕ СОВЕТЫ

Данные брифинга Booz Allen подтверждают, что основной метод атаки — это адресный фишинг. Как сказано в отчете, таким был «исходный вектор атаки в операции Clandestine Wolf — одной из крупнейших кампаний [2016 года] по проведению атак на системы управления предприятиями, а также в атаках на немецкий металлургический завод и украинские энергораспределительные компании — двух наиболее масштабных по последствиям атаках [из обнаруженных в 2015 году]».

На данный момент еще не поступало сообщений об атаках с использованием криптовымогателей на системы управления предприятиями, но уязвимость к ним — факт, широко известный уже на протяжении более чем десяти лет. Отличие нынешней ситуации в том, что цифровые валюты наподобие биткоина позволяют преступникам получать финансовую выгоду от атак. Исследователи из Технического университета Джорджии полагают, что по мере того как внедрение криптовымогателей в ИТ-системы коммерческих и других организаций затруднится, злоумышленники могут обратиться к системам управления предприятиями как более легким мишеням.

Помимо усиления парольной защиты и ограничения числа подключений, они рекомендуют операторам установить системы обнаружения вторжений, которые будут предупреждать о проникновении посторонних лиц в сети систем управления технологическими процессами.

Booz Allen подтверждает также рост числа таких вторжений, осуществленных через корпоративные сети, — этот вывод основывается на исследовании, проведенном Министерством внутренней безопасности США. Хотя доля вторжений через корпоративные сети оставалась низкой, составляя 12% от общего числа оглашенных инцидентов в 2015 г., число попыток такого вторжения за указанный период времени выросло на 33%. Общее число инцидентов, о которых сообщили операторы систем управления предприятиями, выросло в 2015 г. на 20%.

По словам Booz Allen, атаки на системы управления могут принести «осязаемый ущерб», что делает эти системы особо привлекательными мишенями. Вместо простого шифрования файлов, которое практикуется при атаках на коммерческие организации, атака на систему управления предприятием с использованием криптовымогателя может также сопровождаться нарушением работы системы или отказом в доступе к тому или иному активу.

Встраивание криптовымогателей в наборы эксплойтов способствует установлению прибыльной бизнес-модели, когда единожды созданный инструментарий позволяет атаковать множество компаний, отмечает Booz Allen. В результате образовалась уже целая армия злоумышленников, что вылилось в огромное число успешных попыток заражения вредоносными программами. По оценкам

СВОДКА ТЕНДЕНЦИЙ В ОБЛАСТИ ПРОМЫШЛЕННОЙ БЕЗОПАСНОСТИ ЗА 2016 ГОД

Вот некоторые заслуживающие внимания тенденции, которые упомянуты в недавно выпущенном компанией SonicWall ежегодном отчете об угрозах (Annual Threat) за 2017 год:

- **Некачественно спроектированные IoT-устройства компрометируются для использования в массовых распределенных атаках типа «отказ в обслуживании» (DDoS).**
- **Вредоносное программное обеспечение с SSL/TLS-шифрованием создает в сетях неконтролируемые закладки, которыми могут пользоваться киберпреступники. Одновременно зафиксирован рост трафика с SSL/TLS-шифрованием на 34%, отчасти связанный с более широким внедрением облачных приложений.**
- **Защита устройств на базе ОС Android была укреплена, но они остаются уязвимыми к оверлейным атакам. Есть, однако, и позитивные новости: к середине 2016 г. вышли из употребления некогда популярные наборы эксплойтов Angler, Nuclear и Neutrino. Более того, количество собранных уникальных образцов вредоносных программ уменьшилось с 63 млн в 2015 г. до 60 млн в 2016 г., т. е. на 6,25%. Впервые за несколько лет снизилось общее число попыток совершения атак — с 8,19 млрд в 2015 г. до 7,87 млрд в 2016 г.**

журнала Forbes, темпы заражения некоторыми вариантами таких программ в феврале 2016 г. составляли около 90 тыс. машин в день. В частности, организация Cryptothreat Alliance оценивает доход, полученный в период с января по октябрь 2015 г. всего от одного варианта вредоносной программы (Cryptowall 3.0), в $325 млн.

По словам Booz Allen, усугубляет проблему то, что системы управления предприятием зачастую относятся к старому типу систем, не предусматривающему восстановление из резервной копии. Вследствие этого могут возникнуть сложности с получением чистой версии системного программного обеспечения и настроек. Затруднен может быть и доступ к самой системе, а для ее восстановления может не хватать квалифицированного персонала.

«Частота и уровень серьезности заражений криптовымогателями в сетях систем управления предприятиями с высокой вероятностью будет расти», — заключает отчет.

ПОМОЩЬ ГОСУДАРСТВА

В апреле 2016 г. Национальным институтом стандартов и технологий Министерства торговли США был выпущен черновик документа под названием «Рамочные рекомендации NIST по кибербезопасности» (NIST Cybersecurity Framework), адресованного производственным отраслям. По словам института, предусмотренная этим документом анкета — простое методическое средство, которое позволяет производителю составить перечень организационно-технических мер, осуществляемых им для защиты ресурсов и эксплуатационных данных своей производственной системы. С ее помощью производитель может оценить возможность эксплуатации своей системы управления с приемлемым уровнем риска. Кроме того, в рамочных рекомендациях изложен стандартизированный подход к подготовке плана обеспечения кибербезопасности, согласно которому будет проверяться защищенность системы.

Анкета составляется на базе основных функциональных разделов «Рамочных рекомендаций NIST по кибербезопасности». В ней перечисляются основные функции и мероприятия, относящиеся к обеспечению кибербезопасности. Пять основных функциональных разделов — это определение, защита, обнаружение, реагирование и восстановление. В них сформулированы 98 различных задач по обеспечению безопасности, которые образуют отправную точку для разработки анкеты, специфичной для конкретного производителя или сектора, с определением низкого, среднего и высокого уровней риска. Помимо установления приоритета функций и категорий, предусмотренных «Рамочными рекомендациями NIST по кибербезопасности», анкета помогает определить подмножество актуальных практических методов обеспечения безопасности, которые могут быть внедрены для реализации стоящих перед предприятием целей.

ЗАКЛЮЧЕНИЕ

В феврале этого года компании IBM, Nokia, Palo Alto Networks, Symantec и Trustonic совместно учредили Альянс по кибербезопасности «Интернета вещей» (IoT Cybersecurity Alliance). Компании выражают намерение сотрудничать в деле поиска решений основных проблем безопасности «Интернета вещей», а также информирования общественности о наилучших способах укрепления защиты экосистемы IoT.

По результатам опроса, проведенного компанией AT&T в прошлом году, на 3,198% выросло число злоумышленников, ищущих уязвимости в IoT-устройствах для возможной их эксплуатации. Приблизительно 58% участников опроса выразило беспокойство относительно уровня защищенности своих устройств.

Мо Катибе (Mo Katibeh), старший вице-президент компании AT&T по передовым решениям, говорит: «Взрывной рост количества IoT-устройств будет только продолжаться — а значит, столь же непрерывными должны быть и меры по обеспечению кибербезопасности. Сегодня на предприятиях в сеть объединяются самые разнообразные устройства — от роботов в заводских цехах до кардиостимуляторов и холодильников. Чтобы помочь организациям защитить себя, необходимы инновации в масштабах всей экосистемы IoT, которые бы создали условия для устойчивого развития».

Участники Альянса указывают, что для обеспечения надлежащего уровня безопасности IoT важна защита на всех уровнях — от конечных точек и сетей до облака и приложений (рис. 3). Кроме того, они считают эффективным применение средств анализа угроз и проектирование продукции со встроенной постоянно действующей защитой. Входящие в Альянс компании планируют информировать потребителей, производителей и разработчиков о том, что необходимо для создания более безопасной экосистемы IoT.

Все это говорит о том, что опасности и угрозы, связанные с криптовымогателями и другими видами кибертерроризма, привлекли к себе внимание ведущих технологических компаний. Если они не будут противодействовать этим негативным явлениям, то поставят под угрозу своих клиентов, техническую инфраструктуру и мечты о будущем.

Каким бы эффективным ни было противодействие угрозам в отношении систем управления предприятиями, исключить все возможные риски не удастся никогда ввиду существования финансовых, технических и даже политических ограничений. Специалисты советуют решать вопрос постепенно и сосредоточиться на первоначальных шагах, которые при невысоких издержках позволят эффективно устранить наиболее значимые риски, и тем временем вырабатывать долгосрочную стратегию. ⬣

ЛИТЕРАТУРА

1. www.rh.gatech.edu/news/587359/simulated-ransomware-attack-shows-vulnerability-industrial-controls
2. www.sonicwall.com/whitepaper/2017-sonicwall-annual-threat-report8121810/
3. www.boozallen.com/insights/2016/06/industrial-cybersecurity-threat-briefing/
4. csrc.nist.gov/cyberframework/documents/Manufacturing-Profile-DRAFT.pdf

РИС. 3. ▼ В SCADA-системах и других системах управления предприятием встраивается облачная функциональность, что усложняет обеспечение кибербезопасности промышленного «Интернета вещей». (Публикуется с разрешения SonicWall)