Санкт-Петербургский Политехнический Университет Петра Великого

Кафедра компьютерных систем и программных технологий

Реферат

Курс: «Защита информации»

Тема: «Основные новые угрозы информационной безопасности 2017 года»

Выполнил студент:

Ерниязов Т.Е.
Группа: 43501/3

Проверил:

Новопашенный А.Г.

Санкт-Петербург
2018 г.

Содержание

1 Введение

В данном реферате обозреваются актуальные угрозы информационной безопасности 2017 года. Угроза информационной безопасности — совокупность условий и факторов, создающих опасность нарушения информационной безопасности. Под угрозой (в общем) понимается потенциально возможное событие, действие (воздействие), процесс или явление, которые могут привести к нанесению ущерба чьим-либо интересам.

Общее мнение спецалистов, скорее, пессимистично и сводится к неутешительному прогнозу. Суть его такова: в 2017 году кто угодно может оказаться мишенью для злоумышленников и любое устройство может стать инструментом атаки. Прогнозы омрачаются тем, что многие явления, например, интернет вещей или облачные платформы, – относительно новые, и компании еще не успели выработать оптимальную стратегию защиты.

2 Общие направления

2.1 Вредоносные программы

Отдел исследования угроз компании Fortinet среди главных источников опасности назвал вредоносные программы с зачатками искусственного интеллекта. В исследовании FortiGuard Labs эксперты объясняют, что вредоносное ПО станет быстрее адаптироваться к окружающей среде и учиться на основе собственного удачного опыта. Это значит – самостоятельно определять цель, выбирать метод атаки и выстраивать самозащиту от обнаружения.

Автономные самообучающиеся программы начнут атаковать различные типы устройств одновременно. Специалистам по безопасности потребуются новые интеллектуальные технологии, способные обнаруживать угрозу на всех платформах и самостоятельно применять скоординированные защитные меры.

2.2 Облачные решения

Облачным сервисам в 2017 году предстоит решать задачу множественности подключений. В FortiGuard Labs подсчитали, что количество устройств, обращающихся к облакам, достигнет 20 миллиардов. Стратегия злоумышленников будет состоять в том, чтобы использовать уязвимости в гаджетах пользователей для «заражения» и самого облака, и других устройств. Внимание злоумышленников к облачным решениям связано с тем, что все больше организаций планируют в 2017 году перевести часть инфраструктуры в облака.

2.3 Вымогательские программы

Автоматизированные атаки в 2017 году станут массовыми и нацелятся на наиболее платежеспособных жертв, включая и отдельных знаменитостей, и целых организаций. Блокировка системы дополнится сбором персональных данных и конфиденциальной информации, которую используют для шантажа. Структуры, которые не сумеют защитить пользовательские данные: поставщики решений и производители устройств – будут нести ответственность.

2.4 Привилегированные пользователи

В 2017 году целью злоумышленников станут данные привилегированных пользователей: руководителей компаний, поставщиков решений, системных администраторов. ИБ-специалистами придется обеспечивать защиту не только систем, но и самих пользователей с особыми правами доступа. В интервью изданию CIO глава компании Bomgar, создавшей ПО удаленного администрирования Мэтт Диркс объяснил, что привилегированных пользователей «поставят на учет», чтобы контролировать их действия и блокировать доступ к компонентам системы, которые для работы им не нужны.

2.5 Мобильные устройства

Инциденты, связанные с мобильными технологиями, эксперты Trend Micro включили в число наиболее реальных угроз 2017 года. Предприятия все чаще используют мобильные устройства, чтобы контролироваться системы управления на производстве и объектах инфраструктуры. В сочетании с критической массой уязвимостей, обнаруженных как в системах, так и в устройствах, степень угрозы возрастет многократно.

В России 3 из 5 инцидентов в компаниях в 2016 году так или иначе были связаны с мобильными устройствами. Тенденция только усилится на фоне роста численности мобильных сотрудников, которые готовы поступиться принципами информационной безопасности ради удобства.

2.6 Слияние корпоративного и личного

По данным Gemalto, 90 процента IT-специалистов в компаниях опасаются того, что сотрудники используют личные учетные данные для рабочих целей. Такая конвергенция подрывает основы информационной безопасности. Поэтому специалисты предсказывают внедрение в корпоративную среду средств аутентификации, которые применяются в потребительских сервисах, например, сканирование отпечатков пальцев и сетчатки глаза.

Компании изменят подход к аутентификации и управлению доступом, чтобы соответствовать ожиданиям сотрудников, которые хотят практичности, удобства и мобильности. Половина участников исследования Gemalto указала, что руководство увеличит расходы на реорганизацию управления доступом: 62 процента предполагают внедрить решения для строгой аутентификации в 2017 и 2018 году.

2.7 Интернет вещей

В отличие от вредоносных программ, устройства, подключенные к Сети, не успевают «учиться». Производители наводнили рынок «умными» – и крайне небезопасными – устройствами. Оборудование для корпоративного использования чаще всего подлежит обязательной сертификации, а вот единых требований к устройствам для частного применения все еще нет.

В 2017 году производителям придется самим заботиться о том, чтобы их продукция удовлетворяла требованиям информационной безопасности. И они будут вынуждены брать на себя ответственность, если устройства все же взломают. Иначе «умные вещи» просто перестанут пользоваться спросом.[1]

3 Примеры конкретных новых угроз

3.1 Spectre и Meltdown

Проблема касается не только процессоров Intel в ПК, выпущенных в последние 20 лет, но и других производителей и устройств, в том числе смартфонов. Главное, что известно: компании были в курсе уязвимости сравнительно давно и вели подготовку по её устранению, планируя выпустить подробный совместный отчёт 9 января. Из-за утечки информации они оказались вынуждены делать это раньше, поэтому новые подробности продолжают поступать. Что известно о проблеме на данный момент: Главный корень проблемы — так называемое спекулятивное исполнение команд. Упрощённо, это технология в современных микропроцессорах, которая позволяет «предугадывать», какие команды потребуется исполнить в будущем. Например, программа А выполняет сложную математическую операцию, в ходе которой будет использована сумма каких-то переменных. Программа В заранее (когда процессор менее нагружен) считает эту сумму, чтобы ускорить работу процесса в будущем, и в нужный момент подсовывает результат программе А. Если результат программы В не потребовался программе А, то ничего страшного, а если потребовался, то процессор ускорил свою работу. Всё это происходит во внутренней памяти процессора на нескольких слоях кэша (в зависимости от архитектуры чипа). Уязвимость спекулятивного исполнения заключается в том, что злоумышленники могут по-

лучить доступ к данным, которые находятся в этой общей памяти — а это даёт злоумышленникам доступ к приложениям, которые оперируют этими данными.

По большому счёту, уязвимость открывает два типа атак, говорят исследователи — им даны условные названия Meltdown («Крах») и Spectre («Призрак»). Meltdown позволяет нарушить барьер между приложениями и внутренней памятью операционной системы (название символизирует слом этого барьера), что открывает доступ к данным, хранимым в памяти ОС.[3] Spectre нарушает такой барьер между самими приложениями: условно, один сервис может залезть в память другого. Spectre более сложна в исполнении, но её и сложнее победить, поэтому исследователи считают, что атака будет как призрак ещё какое-то время преследовать пользователей и разработчиков. Более подробно атаки описаны на специальном сайте, созданном группой исследователей безопасности из Грацского технического университета (Австрия), Google Project Zero и других организаций. Из одной только сути атак Meltdown и Spectre можно сделать вывод об уровне опасности уязвимости: она затрагивает не только системные данные, но и данные внутри приложений, потому что все они обрабатываются на процессоре. А подвержены ей все крупнейшие производители. Хотя изначально появилась информация об уязвимости процессоров Intel, ей подвержены и другие производители — AMD и ARM, но, по предварительным данным, в меньшей мере. В случае с Intel, по грубым оценкам исследователей, проблема касается почти всех процессоров, выпущенных примерно с 1995 года — когда компания начала внедрять спекулятивное исполнение команд.[2]

3.2 Шифровальщик Bad Rabbit

Во вторник 24 октября произошли массовые атаки с использованием вымогателя Bad Rabbit («Плохой кролик»). Пострадали организации и отдельные пользователи — преимущественно в России, но были и сообщения о жертвах из Украины. Bad Rabbit относится к ранее неизвестному семейству программ-вымогателей. Зловред распространятся с помощью drive-by-атаки: жертва посещает легитимный веб-сайт, а на ее компьютер из инфраструктуры организатора атаки загружается дроппер. Преступники не использовали эксплойты, поэтому для заражения пользователь должен был вручную запустить файл, замаскированный под установщик Adobe Flash. Тем не менее, наш анализ подтверждает, что Bad Rabbit использовал эксплойт EternalRomance для распространения внутри корпоративных сетей. Этот же эксплойт использовался шифровальщиком ExPetr. Большинство жертв находятся в России. Схожие, но менее массовые атаки затронули другие страны — Украину, Турцию и Германию. Общее количество целей, согласно статистике KSN, доходит до 200. Исходный вектор атаки отследили в самом ее начале, утром 24 октября. Активная фаза продолжалась до полудня, хотя отдельные атаки фиксировались до 19.55 по Москве.

Сервер, с которого распространялся дроппер Bad rabbit, был отключен тем же вечером. По нашим наблюдениям, сейчас речь идет о целевой атаке на корпоративные сети, ее методы схожи с применявшимися во время атаки ExPetr. Более того, анализ кода Bad Rabbit продемонстрировал его заметное сходство с кодом ExPetr. Вымогатель Bad Rabbit шифрует файлы и жесткий диск жертвы. Для файлов используются следующие алгоритмы:

1. AES-128-CBC
2. RSA-2048

Это типичная схема, используемая зловредами-вымогателями. Интересно, что вымогатель перечисляет все запущенные процессы и сравнивает хэш от имени каждого процесса с имеющимся у него списком хэшей. При этом используемый алгоритм хэширования похож на тот, что использовался зловредом exPetr. Bad Rabbit не удаляет теневые копии файлов после их шифрования. Это означает, что если служба теневого копирования была включена до заражения и полное шифрование диска по какой-то причине не произошло, жертва может восстановить зашифрованные файлы, используя стандартные средства Windows или сторонние утилиты.[4]

3.3 Petya/Petrwrap/exPetr

27 июня, появились сообщения о прокатившейся по всему миру новой волне атак с использованием троянца-вымогателя (в прессе его называют Petya, Petrwrap, NotPetya и exPetr). В первую очередь нападению подверглись компании в Украине, России и Западной Европе. Решения «Лаборатории Касперского» успешно блокируют эту атаку с помощью компонента System Watcher. Эта технология позволяет отследить изменения в системе и произвести откат любых потенциально вредоносных действий. Чтобы завладеть учетными данными для распространения, программа-вымогатель использует специальные утилиты а-ля Mimikatz. Они извлекают учетные данные из процесса lsass.exe. После этого данные передаются утилитам PsExec или WMIC для распространения внутри сети.[5] Среди других наблюдаемых векторов заражения:

1. Модифицированный эксплойт EternalBlue, также использовавшийся WannaCry
2. EternalRomance — эксплойт с удаленным исполнением кода, использующий уязвимости в операционной системе Windows – версий от XP до 2008 – через TCPпорт 445 (Примечание: уязвимость закрыта с помощью MS17-010)
3. Атака на механизм обновления стороннего программного продукта украинского производства под названием MeDoc

Одна зараженная система в сети, обладающая административными полномочиями, способна заразить все остальные компьютеры через WMI или PSEXEC.

После заражения вредоносная программа выжидает 10-60 минут и затем перезагружает систему. Перезагрузка происходит с использованием системных средств с инструментами «at» или «schtasks» и «shutdown.exe». После перезагрузки троянец начинает шифровать главную файловую таблицу в разделах NTFS, перезаписывая с помощью кастомизированного загрузчика главную загрузочную запись (MBR) сообщением с требованием выкупа. Подробнее о требовании выкупа ниже.

Есть ли у жертв какая-то надежда на расшифровку своих файлов? К сожалению, вымогатель использует стандартную, надежную схему шифрования, поэтому расшифровка представляется маловероятной, если только не допущена какая-то мелкая ошибка в имплементации. Механизм шифрования имеет следующие особенности:

1. Для всех файлов генерируется единый ключ AES-128.
2. Этот AES-ключ зашифровывается с помощью открытого ключа RSA-2048, принадлежащего злоумышленникам.
3. Зашифрованные AES-ключи хранятся в файле README.
4. Ключи сгенерированы надежно.

За ключ, который расшифровывает данные, организовавшие эту атаку злоумышленники требуют у жертвы выкуп в биткойнах, эквивалентный 300 долларам. Сумма должна быть перечислена в общий Bitcoin-кошелек. В отличие от ситуации с Wannacry, эта техника вполне работоспособна, потому что злоумышленники просят жертв отправить номер своего кошелька по электронной почте на адрес wowsmith123456@posteo.net, подтвердив таким образом транзакции. Мы видели сообщения о том, что этот электронный адрес уже заблокирован, что на данный момент лишает жертв надежды на полную расшифровку их файлов.[6]

4 Список литературы

[1] Анализ главных угроз в безопасности в 2017 году от FortiGuard Labs [Электронный ресурс]. — URL: https://searchinform.ru/blog/2016/12/22/idealnyj-shtorm-glavnye-ugrozy-informatsionnoj-bezopasnosti-v-2017-godu/.

[2] Атаки Spectre и Meltdown [Электронный ресурс]. — URL: https://tjournal.ru/64-faq-po-chipokalipsisu-chto-izvestno-o-masshtabnoyuyazvimosti-processorov.

[3] Разбор угрозы атаки Meltdown [Электронный ресурс]. — URL: https://meltdow

[4] Исследование Лаборатории Касперского Bad Rabbit [Электронный ресурс]. — URL: https://securelist.ru/badrabbit/88421/.

[5] Исследование Лаборатории Касперского вируса Petya [Электронный ресурс]. — URL: https://securelist.ru/schroedingers-petya/31001/.

[6] Вирус Petya [Электронный ресурс]. — URL: https://securelist.ru/petya-ransomware-used-in-widespread-attacks-all-over-theworld/30662/.