WANNACRY:
УЖ СКОЛЬКО РАЗ ТВЕРДИЛИ МИРУ

POSITIVE TECHNOLOGIES

ВВЕДЕНИЕ

Последние дни по всему миру только и разговоров, что о массовой ransomware-атаке WannaCry. Среди пострадавших крупные международные компании, правительственные учреждения и, конечно, рядовые пользователи интернета. Охват заражения превысил планку в 200 тысяч машин и, судя по всему, продолжит расти. Атаки зарегистрированы в 150 странах мира, Россия также в числе пострадавших. Есть информация о попытках заражения в нескольких организациях — «Мегафоне», «ВымпелКоме», Сбербанке, «РЖД», Минздраве, МЧС и МВД. Атака оказалась столь масштабной, что Microsoft выпустила соответствующее обновление даже для ОС Windows XP, поддержка которой приостановлена с 2014 года.

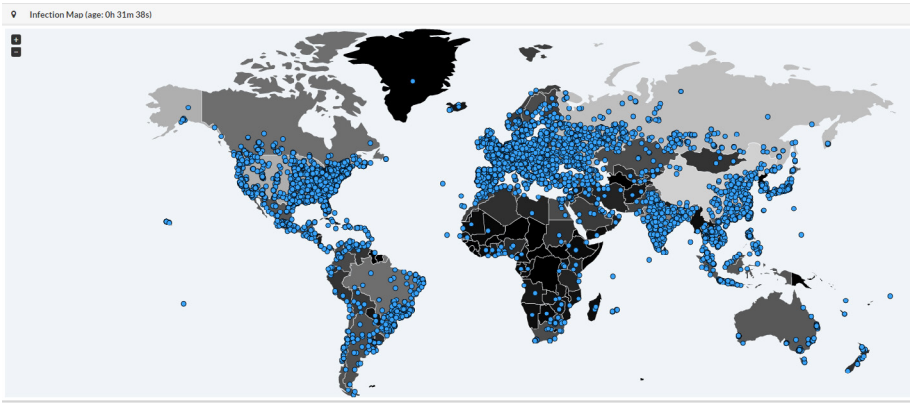

Рис. 1. Распространение WannaCry по данным на 17 мая 2017 г.

Для распространения WannaCry используется ETERNALBLUE-эксплойт для ОС Windows из утекшего в сеть набора группировки Shadow Brokers. Стоит отметить, что обновление, устраняющее данную уязвимость, было выпущено еще в марте, то есть за два месяца до этой атаки.

Злоумышленники (к слову, получившие на текущий момент порядка 90 тысяч долларов, судя по выплатам на биткойн-кошельки — 1, 2 и 3) уже успели выпустить несколько модификаций вредоноса. Вероятно, в определенной степени это связано с преждевременной регистрацией домена-выключателя специалистом по кибербезопасности. Такой шаг замедлил распространение вредоноса на несколько часов. Над решением проблемы расшифровки файлов без оплаты «услуг» распространителей блокера бьются многие специалисты. Ряд компаний уже представили разбор принципа действия WannaCry, распространяемого через SMB и далее заражающего рабочие станции в ЛВС. Но в данной статье мы хотели бы показать, почему изначально данная атака была обречена на успех.

ОБНОВЛЕНИЯ? НЕ, НЕ СЛЫШАЛИ

Про небезопасность использования SMBv1 известно уже достаточно давно. Патч для устранения уязвимости вышел два месяца назад. Про утечку эксплойт-пака группировки Shadow Brokers говорили буквально везде. О необходимости использования резервных копий не слышал только человек, никогда не пользовавшийся интернетом.

Казалось бы, в таких условиях никакой эпидемии и вовсе не должно быть, но увы.

Все говорит о неправильном подходе к vulnerability management, безответственном отношении администраторов, специалистов по безопасности и, в определенной степени, о неосведомленности пользователей в вопросах ИБ.

Результаты наших исследований подтверждают распространенную проблему использования уязвимых версий ПО в корпоративной инфраструктуре. При этом, как показала эпидемия WannaCry, защищенность системы не зависит от отрасли компании, что в целом подтверждается и нашей аналитикой. Атакам через уязвимости устаревшего ПО в равной степени подвержены системы промышленных компаний, ИТ, телекома, финансового сектора и государственные учреждения.

Вообще, сценарии атак на корпоративные информационные системы с эксплуатацией уязвимостей в устаревшем ПО крайне распространены. Это один из наиболее часто встречающихся недостатков безопасности.

Так, за 2016 год в рамках работ по тестированию на проникновение специалисты Positive Technologies выявили уязвимости, связанные с отсутствием обновлений, в 87% проектов.

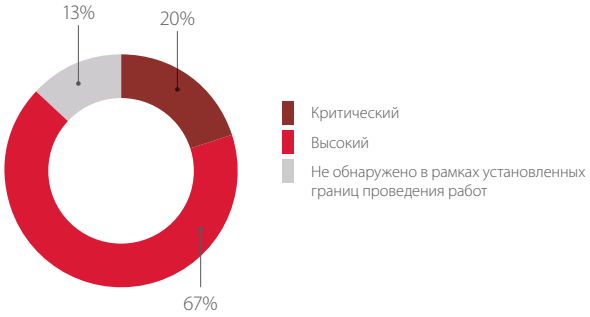

Рис. 2. Максимальный уровень опасности уязвимостей, связанных с отсутствием обновлений

При этом, как можно заметить, высока доля систем, где выявлялись уязвимости вплоть до высокой степени опасности по шкале CVSS (67%). Кстати, такой же уровень угрозы присвоен и уязвимости в SMB, использованной для проведения атаки с распространением вируса-шифровальщика WannaCry. В 20% случаев были выявлены критически опасные уязвимости, эксплуатация которых может значительно повлиять на систему вплоть до получения злоумышленником полного контроля над инфраструктурой или вывода ее компонентов из строя.

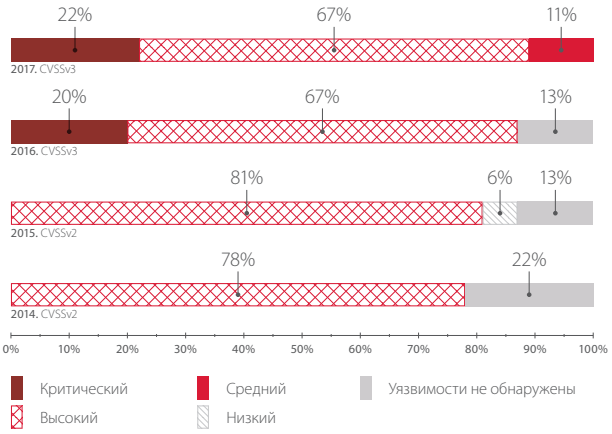

Рис. 3. Максимальный уровень опасности уязвимостей, связанных с отсутствием обновлений (доли систем)

Мы можем наблюдать рост опасности уязвимостей и доли систем, где присутствуют уязвимости высокого и критического уровня риска. Стоит отметить, что до 2016 года оценка велась с использованием системы оценки уязвимости CVSS версии 2, а категория критически опасных уязвимостей была введена только в CVSS версии 3. Соответственно, в прошлые годы аналогичные уязвимости также присутствовали, и их доля входит в категорию высоких. Если говорить о тех системах, где уязвимости выявлены не были, то это не означает их отсутствия: в рамках тестирования на проникновение не ставится цель выявить все возможные уязвимости.

Если посмотреть на статистику по выявленным уязвимостям устаревшего ПО, то ситуация за последние несколько лет в целом не меняется. Отсутствие актуальных обновлений — распространенная проблема, доля систем, где выявлены такие недостатки, по-прежнему достаточно высока.

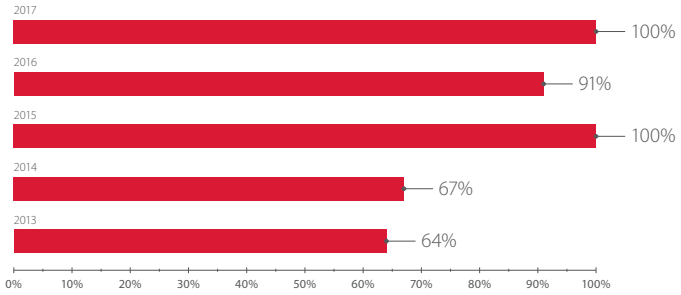

Рис. 4. Уязвимости устаревшего ПО, выявленные при тестах на проникновение (доля систем)

Можно отметить, что использование уязвимых версий ПО не просто остается актуальной проблемой, но и в целом доля систем с такими недостатками растет из года в год. Например, в 2015 году в рамках работ по тестированию на проникновение во всех без исключения проектах были обнаружены уязвимости, устраняемые путем обновления. Определенное снижение количества выявленного устаревшего ПО наблюдалось в ходе работ за прошедший 2016 год. Это связано с тем, что ряд компаний обратились к нашим экспертам повторно, предварительно устранив недостатки, а также свою роль сыграло то, что пентест проводится методом черного ящика, при котором не преследуется цель выявить все уязвимости. Некоторые системы могут содержать недостатки подобного рода, но для их выявления необходимо проводить регулярный аудит узлов внешней и внутренней сети, осуществлять плановое автоматизированное сканирование.

Пока еще рано говорить о результатах 2017 года, но на данный момент во всех проектах были выявлены уязвимости устаревшего ПО. Наши специалисты еще в апреле демонстрировали использование теперь уже известного на весь мир эксплойта ETERNALBLUE в ходе проведения тестирования на проникновение. К тому моменту патч был доступен уже более месяца, что лишний раз подтверждает проблему в организации процессов по управлению уязвимостями и обновлениями в корпоративных информационных системах.

Вообще достаточно упомянуть тот факт, что средний возраст наиболее старой уязвимости среди выявленных на каждом проекте составляет порядка 8 лет. При этом по-прежнему можно встретить уязвимости, информация о которых появилась 20 лет назад!

Если говорить именно про нашумевшие уязвимости в ОС Windows, устраняемые путем обновления, то они по-прежнему остаются актуальными. Наши эксперты, например, все еще встречают в корпоративном сегменте возможность эксплуатации критически опасной уязвимости MS08-067. Эксплуатация подобных уязвимостей не требует от атакующего особых знаний и навыков, зато позволяет получить доступ к атакуемой системе с максимальными привилегиями.

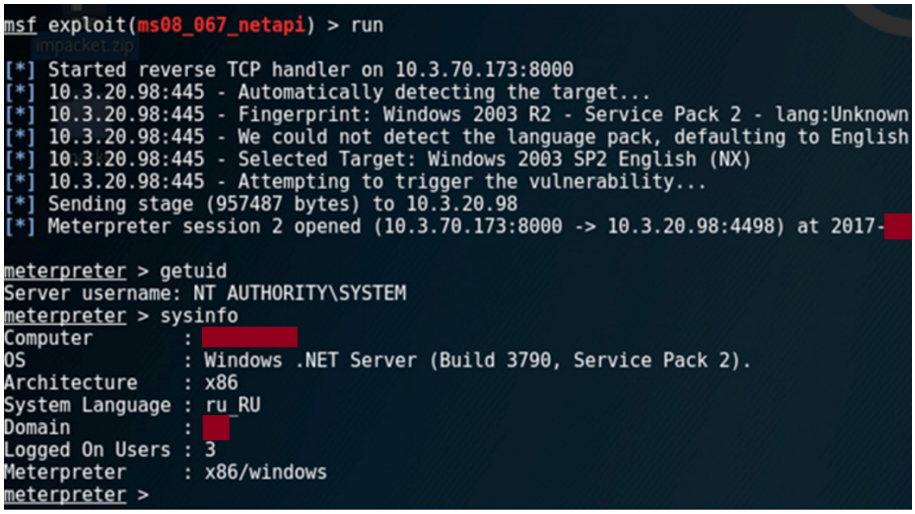

Рис. 5. Эксплуатация уязвимости 2008 года в корпоративной инфраструктуре

Одновременно забавный и грустный факт: страница для загрузки соответствующих обновлений в какой-то момент даже стала недоступна, что говорит о «своевременном» принятии мер по устранению.

К слову об обновлениях старых ОС. Обновление той же Windows XP не везде возможно оперативно. Это может быть связано с тем, что обновления не централизованы или обновление одной системы может повлиять на работу остальных. В определенной степени это, например, касается АСУ ТП, где системы могут не обновляться долгое время, поскольку обновления могут нарушить рабочие процессы. В промышленных организациях в первую очередь нужно принять во внимание возможные риски и начать с превентивных мер защиты.

Зачем держать открытыми 139 и 445 TCP-порты на периметре? Этот фактор позволил атаке достичь такого масштаба, который мы можем теперь наблюдать на карте распространения WannaCry. В рамках услуги мониторинга защищенности периметра корпоративной сети нашими специалистами в 14,6% компаний была обнаружена доступная из сети Интернет служба SMB. То есть каждая шестая компания оказалась под угрозой!

Если говорить о финансовом секторе, то 63 сервиса из 5626 выявленных — это SMB, открытая для доступа из внешней сети. При этом речь идет об организациях, которые входят в топ-50 или топ-100 крупнейших банков и страховых компаний России.

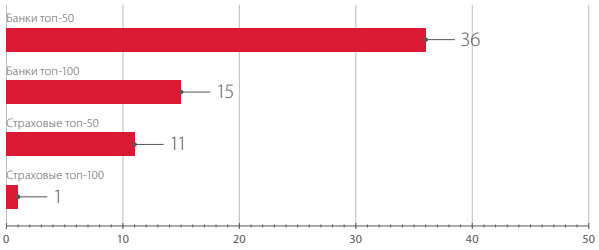

Рис. 6. Количество служб SMB, доступных из внешней сети (финансовый сектор)

При этом в инфраструктуре компании даже может быть всего лишь одна уязвимая к атаке машина. Но в случае заражения ransomware разносится уже по локальной сети, заражая инфраструктуру все глубже.

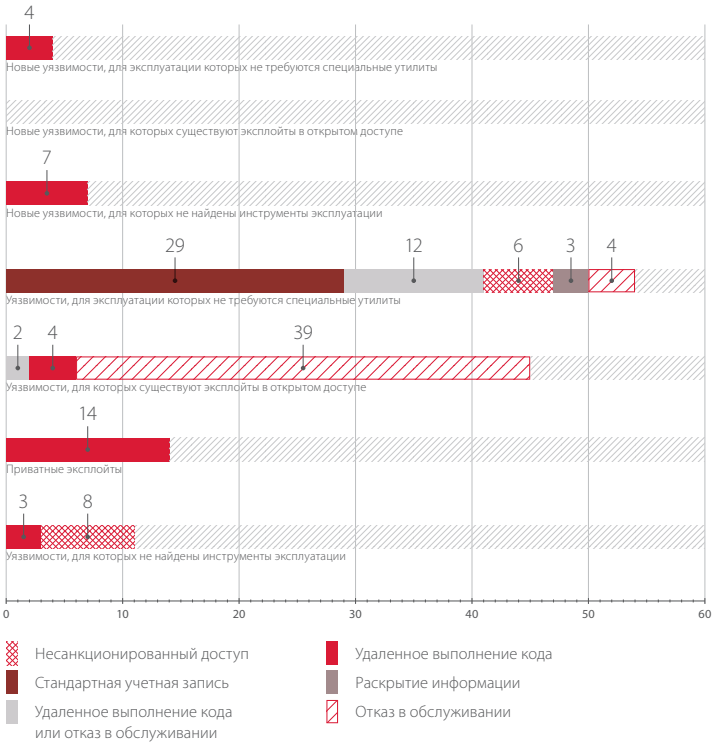

Рис. 7. Количество различных уязвимостей на внешнем периметре организаций

На каждую третью уязвимость высокого и критического уровней риска, выявляемую в ходе наших тестирований на проникновение, можно найти общедоступный эксплойт. Что же говорить про коммерческие эксплойты! Кстати в Metasploit Framework модуль поиска и эксплуатации этой нашумевшей уязвимости SMB уже присутствует.

Результаты нашего исследования, связанного с мониторингом внешнего периметра, показывают, что более чем для половины уязвимостей, выявленных в рамках таких работ, существуют общедоступные инструменты, а четверть позволяет удаленно выполнять код.

300 $

Проблема ransomware не нова: вирусы-шифровальщики существуют уже более 10 лет, да и масштабами данного криминального бизнеса сложно удивить. Так, еще в 2013 году авторы шифровальщика CryptoLocker смогли выручить порядка 41 928 биткойнов, что на тот момент составляло около 27 миллионов долларов. В отличие от WannaCry для доставки вируса на компьютеры использовалась обычная электронная почта с вложениями вроде VERY_IMPORTANT_LETTER.pdf.exe.

В случае же текущей эпидемии злоумышленники сработали достаточно оперативно. Использовались утечка свежего эксплойт-пака и халатность в вопросах обновления ПО. Механизм распространения — как у компьютерного червя. Это привело к сотням тысяч заражений за пару дней.

Для рядового пользователя сумма за возврат доступа к данным составляет 300 долларов. Если деньги не поступают в течение трех дней, то улов вирусописателей составит уже 600 долларов. Хотя, безусловно, большинство простых пользователей скорее будет готово пожертвовать переустановкой системы с последующей потерей данных, чем такими деньгами. Политика «не платить» в целом верна — об этом также регулярно упоминают специалисты по безопасности. Но проблема в том, что для некоторых, особенно крупных организаций утрата данных, а также простои в работе инфраструктуры могут привести к более значительному ущербу. Подобные эпидемии обречены на успех до тех пор, пока во всех организациях не будет грамотно построен процесс управления уязвимостями, в том числе превентивная установка обновлений, реализация резервного копирования, использование защитного ПО, проведение регулярного анализа защищенности. В качестве довода в пользу такого грамотного подхода можно заметить следующее: никто не гарантирует, что вы получите свои данные, даже если переведете деньги.

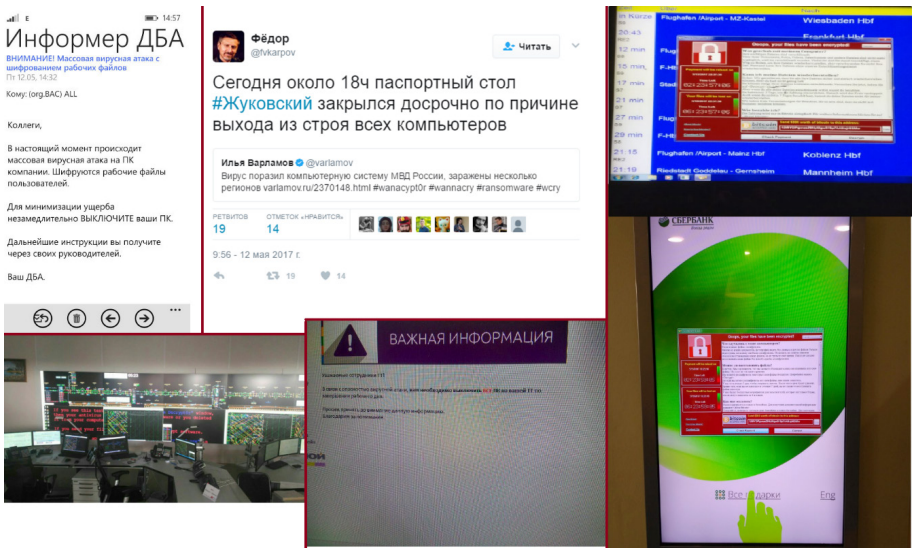

Рис. 8. Примеры публичных инцидентов заражения

Существует ошибочное мнение, что использование другой ОС (например, macOS) гарантированно защитит от подобных проблем, но это миф. Проблема кроется не в конкретной ОС, а в неправильном подходе к организации безопасности в корпоративных системах.

На текущий момент нет информации о дешифраторах, позволяющих восстановить файлы после атаки. Жертвы ransomware поставлены перед выбором — плати или забудь про свои файлы (как минимум до тех пор, пока не появятся средства расшифровки). Ransomware — определенно ключевой тренд развития киберпреступности в 2017 году.

Пользователи, регулярно устанавливающие обновления безопасности и использующие антивирусное ПО, могут в целом чувствовать себя в безопасности. Регулярное резервное копирование спасет критически важные данные от блокеров. Наши эксперты подготовили обширный перечень рекомендаций, позволяющих обнаружить WannaCry и противодействовать этому вирусу-шифровальщику. Неоспоримый факт, что в некоторых случаях обновиться сразу невозможно, например в критически важных системах, где необходимо предварительно протестировать стабильную работоспособность. В таких случаях рекомендуется проводить регулярное сканирование узлов на наличие уязвимостей, что позволит предпринять превентивные меры до установки обновлений. Это актуально и для любой другой уязвимости. Подобная эпидемия далеко не последняя, и если не изменить подход к обеспечению безопасности, то история повторится вновь.

К сожалению, полученные результаты позволяют утверждать, что большинство компаний не предпринимают достаточных мер по защите, а процессы по управлению уязвимостями неэффективны.

О компании

Positive Technologies — один из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений. Деятельность компании лицензирована Минобороны России, ФСБ России и ФСТЭК России, продукция сертифицирована ФСТЭК России и в системе добровольной сертификации «Газпромсерт». Организации во многих странах мира используют решения Positive Technologies для оценки уровня безопасности своих сетей и приложений, для выполнения требований регулирующих организаций и блокирования атак в режиме реального времени. Благодаря многолетним исследованиям специалисты Positive Technologies заслужили репутацию экспертов международного уровня в вопросах защиты SCADA- и ERP-систем, крупнейших банков и телеком-операторов.

POSITIVE TECHNOLOGIES

pt@ptsecurity.com ptsecurity.com facebook.com/PositiveTechnologies facebook.com/PHDays