Ежемесячник по информационной безопасности для всех

OUCH!

В ЭТОМ ВЫПУСКЕ…

Уроки WannaCry

Обзор

Об авторе

Доктор Джоханнес Ульрих – декан факультета исследований Технологического Института SANS и основатель сайта DShield.org. Он отвечает за работу команды «Центр Циклона» Института SANS (**SANS Internet Storm Center**), который осуществляет наблюдение за актуальными угрозами кибербезопасности. Джоханнес преподает курсы «Безопасность веб приложений» (Web Application Security **DEV522**), «Обнаружение вторжений» (Intrusion Detection **SEC503**) и IPv6 (**SEC546**).

Недавно вы могли заметить огромное внимание средств массовой информации к новой кибератаке «WannaCry». «WannaCry» заразил более 200 тысяч компьютеров, заблокировав многим организациям, включая госпиталя в Соединенном Королевстве, доступ к их данным. Эта атака привлекла столь много внимания по ряду причин. Во-первых, она быстро распространяется от компьютера к компьютеру, атакуя известные уязвимости компьютеров, использующих операционную систему Windows. Во-вторых, эта атака была осуществлена зловредной «программой-вымогателем»; это значит, что как только она заразила ваш компьютер, она шифрует все ваши файлы, блокируя вам доступ к вашим данным. Вы можете восстановить ваши данные из резервной копии или заплатив преступникам 300 долларов США за расшифровку ваших файлов. В-третьих, и это самое главное: эта атака никогда не должна была случиться. Уязвимость компьютеров на базе Windows, которую атаковал «WannaCry», была хорошо известна компании Microsoft, которая выпустила обновление для устранения этой уязвимости несколько месяцев назад. Но многие организации не установили это обновление или продолжали использовать устаревшие операционные системы типа Windows XP, к которым обновления не выпускаются. Мы приводим три простых шага, которые помогут вам противостоять атакам, подобным «WannaCry».

Обновления

Первое, и самое важное: удостоверьтесь, что ваши компьютеры, мобильные устройства, приложения и всё, что подключено к интернету, своевременно обновляется. Кибер преступники постоянно ищут новые уязвимости в программах, используемых вашими устройствами. Когда они находят уязвимости, они используют специальные программы для взлома ваших устройств. В то же время, производители программ для ваших устройств интенсивно работают над обновлениями, позволяющими устранить эти уязвимости. Устанавливая эти обновления на свои компьютеры и мобильные устройства, вы делаете ваши устройства значительно более защищенными от атак. Обновления, способные предотвратить и остановить WannaCry были выпущены двумя месяцами ранее компанией Microsoft; это делает успешное распространение WannaCry трудно объяснимым. Если бы организации своевременно обновляли свои компьютеры, эта атака не произошла бы. Для обеспечения своевременных обновлений своих

Уроки WannaCry

устройств, сконфигурируйте функции автоматического обмена, если это возможно. Эта рекомендация применима не только к вашим компьютерам и мобильным устройствам, но и почти к любой технике, подключенной к сети: к телевизорам с выходом в интернет, домашним роутерам, игровым консолям и, в скором будущем, даже вашему автомобилю. Если ваши операционные системы или устройства настолько стары, что к ним уже не выпускаются обновления безопасности (например, Windows XP), замените их новыми, имеющими поддержку производителя.

Успешно защититься от атак подобных WannaCry вам помогут три простых шага: Обновляйте ваши компьютеры, остерегайтесь фишинговых атак и делайте резервные копии своих систем.

Резервное копирование

В некоторых случаях, кибератаки, использующие программы-вымогатели, могут заразить даже системы с обновлениями. Вторая возможность защитить себя – сделать резервную копию своих данных. Резервная копия – это копия вашей информации, которая хранится не на вашем компьютере или мобильном устройстве, а где-то в другом месте. Когда вы утратите ценные данные, вы можете восстановить свои данные из резервных копий. К сожалению, многие люди не делают регулярных резервных копий, хотя делать их просто и недорого. Существуют две возможности делать резервные копии ваших данных: на физическом носителе или в облачном хранилище данных. Каждый подход имеет свои достоинства и недостатки. Вы можете использовать оба варианта одновременно, если вы не уверены, какой метод лучше. Физические носители – это устройства, которые вы можете контролировать, такие, как внешние USB диски или диски, подключенные к вашей домашней или корпоративной сети.

Преимущество использования своих собственных носителей – возможность резервного копирования и восстановления больших объемов информации с высокой скоростью. Недостаток этого подхода – возможность одновременного поражения ваших компьютеров и ваших резервных копий зловредными программами, такими, как программы-вымогатели. Если вы используете физические носители для резервного копирования, вы должны хранить их в безопасном месте, удаленном от ваших компьютеров. Промаркируйте свои резервные копии.
Облачные хранилища данных – это интернет сервисы, которые делают резервные копии ваших данных и хранят ваши данные в интернете. Обычно для этого вам нужно установить программу на своем компьютере. Преимущество облачных решений – их простота. Кроме того, если ваши компьютеры будут заражены программой-вымогателем, инфекция обычно не может поразить ваши резервные копии, хранящиеся в облачном хранилище

Уроки WannaCry

данных. Недостаток: резервное копирование и восстановление больших объемов данных занимает длительное время. Изучите безопасность и приватность облачных решений. Предоставляет ли поставщик услуг надёжные меры защиты, такие как шифрование ваших данных и сильную аутентификацию?

Фишинг

Кибер преступники постоянно обновляют и совершенствуют методы атак. Они часто используют метод «Фишинг» для атаки и заражения своих жертв. Фишинг заключается в рассылке кибер преступниками сообщений электронной почты, которые пытаются заставить вас открыть зараженное вложение или посетить зараженный веб сайт. Если вы выполните любое из этих действий, ваш компьютер может заразиться. Хотя WannaCry не использовал этот метод атаки, он часто используется многими другими типами атак, включая большинство программ-вымогателей.

Кибер преступники, создавшие WannaCry, несомненно обновят методы атак в ближайшие месяцы и будут использовать фишинг для заражения ещё большего количества компьютеров. Основной способ защиты себя от таких атак, использующих электронную почту – использование здравого смысла. Если сообщение выглядит странным, подозрительным или слишком хорошим, чтобы быть правдой, это скорее всего атака.

Узнайте Больше

Подпишитесь на OUCH! – ежемесячный журнал по информационной безопасности, получите доступ к архивам OUCH! и узнайте больше о решениях SANS в вопросах информационной безопасности на нашем сайте securingthehuman.sans.org/ouch/archives.

Ресурсы

Что такое вредоносные программы:	https://securingthehuman.sans.org/ouch/2016#march2016
Программы-вымогатели:	https://securingthehuman.sans.org/ouch/2016#august2016
Резервное копирование и восстановление данных:	https://securingthehuman.sans.org/ouch/2015#august2015
Фишинг:	https://securingthehuman.sans.org/ouch/2015#december2015
Безопасность при использовании «облака»:	https://securingthehuman.sans.org/ouch/2016#november2016

OUCH! выпускается Институтом SANS в рамках программы «Securing The Human». Распространение журнала регулируется Creative Commons BY-NC-ND 4.0 license. Вы можете использовать и распространять журнал при условии, что ничего не будете менять. Для перевода или получения более подробной информации, пожалуйста, обращайтесь: ouch@securingthehuman.org

Редакция: Билл Уайман, Уолт Скривенс, Фил Хоффман, Кэти Клик, Шерил Конли
Русский перевод: Александр Котков, Ирина Коткова

