УДК 004.031

АНАЛИЗ ВИРУСНОЙ ОПАСНОСТИ И СРЕДСТВА ПО ЕЕ НЕЙТРАЛИЗАЦИИ НА ПРИМЕРЕ «WANNACRY»

Волков Е.И.
Магистрант 2 курса
ЧОУ ВО Южный Университет (ИУБиП)
E-mail: njvcty 8olhwe@mail.ru
Осипенко И.А.
канд. физ.-матем.наук, доцент кафедры «Физика»
Донской государственный технический университет

Аннотация: Рассмотрены вопросы кибербезопасности в условиях противодействия вирусу – вымогателю WannaCry., проведен анализ внедрения и работы вируса, а также ошибки в его коде и рекомендации по противостоянию вирусной атаке подобных вредительских программ

Ключевые слова: WANNACRY, вирус, шифрование, эксплойт, бэкдор.

ANALYSIS OF VIRAL DANGER AND MEANS FOR ITS NEUTRALIZATION ON THE EXAMPLE OF “WannaCry”

Volkov E.I.
Khramov V.V.

Abstract: Cybersecurity issues were considered in the context of anti-extortionist WannaCry. The analysis of the introduction and operation of the virus, as well as errors in its code and recommendations for countering the virus attack of such malicious programs were carried out.

Keywords: wannacry, virus, encryption, exploit, becdor.

История вопроса

Летом 2016 года стало известно о некой хакерской группировке The Shadow Brokers [1,2]. Группа стала известна общественности за взлом информационных систем Агентства национальной безопасности США (АНБ), кражу информации, последующей продажей и опубликованием её в общий доступ. В частности, в 2017 году группой The Shadow Brokers была украдена у АНБ документация о найденных уязвимостях, которым подвержены компьютеры работающие на операционных системах семейства Windows, через протокол Server Message Block (SMB). Также были похищены экспорты для эксплуатации найденных уязвимостей (EternalBlue,

DoublePulsar). Позже группа опубликовала уязвимости нулевого дня (0day - уязвимость). Все опубликованные уязвимости – это экспорты, нацеленные на получение несанкционированного доступа к системам семейства Windows. Позже стало известно, что авторство будара Double Pulsar и экспорта EternalBlue принадлежит непосредственно АНБ, то есть они, не просто нашли уязвимости в системах семейства Windows, но и эксплуатировали их.

Анализ вируса – вымогателя WANNACRY

WannaCry (так же известен как WCry, Wanna Decryptor, WannaCrypt и WannaCrypt0r 2.0) – вредоносная программа, сетевой червь [3,4], вирус и программа – вымогатель денежных средств, поражающая компьютеры только под управлением операционных систем семейства Microsoft Windows (См. рис.1)

Рис. 1 -Скриншот вируса – вымогателя WannaCry

После попадания на компьютер программный код червя распространяется по сети, локальной или интернет, для заражения других компьютеров. После чего вирус шифрует почти все найденные файлы на компьютере и предлагает заплатить за них выкуп в крипто валюте за их расшифровку. Жертве на оплату дается 7 дней, если средства не поступят на указанный в главном окне шифровальщика bitcoin – кошелек, то возможность расшифровать файлы теряется навсегда.

Как работает WANNACRY

WannaCry попадает на компьютеры через протоколы обмена файлами (SMB) [5], установленных на компьютерах всех компаний и государственных учреждений, а также на большинстве компьютеров для домашнего использования. После проникновения вируса на компьютер жертвы он шифрует большинство файлов и присваивает им расширение .WNCRY. В то время как вредоносное программное средство (ПС) начало свою работу, его невозможно остановить. На рабочем столе меняется фон, который информирует жертву о том, что его компьютер заражен вирусом – шифровальщиком. Вскоре после этого появляется окно вируса с bitcoin – кошельком для оплаты и расшифровки файлов пользователя. Стоимость в bitcoin эквивалентна от 300 до 600 долларов США (в зависимости от версии вируса). Если не заплатить указанную сумму в течении семи дней, то файлы жертвы будут удалены или не будет возможности их расшифровать[6-8].

В целом WannaCry – это эксплойт (использующий уязвимости программ компьютера), с помощью которого происходит заражение и распространение, плюс шифровальщик, который скачивается на компьютер жертвы после того, как заражение уже произошло. В этом и состоит главное отличие WannaCry от большинства других вирусов – шифровальщиков. Для того что бы заразить компьютер «обычным» вирусом – шифровальщиком, надо совершить некую ошибку – перейти по подозрительной ссылке в интернете, открыть ссылку в письме от неизвестного пользователя, включить исполнение макросов в скаченном из интернета файле Microsoft Word и так далее. Но что бы заразиться вирусом WannaCry можно, вообще ничего не делать. То есть совсем, пользователь может даже отсутствовать за компьютером, важен лишь доступ в интернет[7-9].

Для этого создатели WannaCry использовали эксплойты, которые опубликовала хакерская группа The Shadow Brokers украденные у АНБ, известные под именами EternalBlue и DoublePulsar [9,10]. Эксплойт EternalBlue использует уязвимость в реализации протокола SMB, в частности 445 порт. Злоумышленник, сформировав и передав на удаленный узел

особым образом подготовленный пакет, способен получить доступ к системе и запустить на ней произвольный код [11] Компания – разработчик операционной системы Windows - Microsoft подтвердила, что уязвимости подвержены все версии ОС Windows, начиная с Windows XP и заканчивая Windows Server 2016. DoublePulsar – бэкдор, работающий в режиме ядра, который предоставляет хакерам высокий уровень контроля над компьютером. С помощью этих эксплойтов злоумышленники могли получать удаленный доступ к компьютеру жертвы без каких-либо действий со стороны последней. И запускать на компьютере вирус – шифровальщик.

После успешного взлома компьютера вирус WannaCry пытается распространиться на другие компьютеры, найденные в локальной сети уже зараженного. Он сканирует другие компьютеры на наличие уязвимостей EternalBlue, DoublePulsar и, если находит, атакует их шифруя файлы. То есть, попав на один компьютер, вирус WannaCry распространится на все компьютеры по локальной сети и зашифрует их. Именно поэтому серьезнее всего от WannaCry пострадали крупные компании, чем больше компьютеров в компании, тем серьезнее ущерб.

Ошибки в коде вируса – вымогателя WANNACRY

Код вируса WannaCry был полон ошибок и имел очень низкое качество (См. понятие «студенческий вирус» [12,13]. Настолько низкое, что некоторые жертвы смогли восстановить свои оригинальные файлы даже после их шифрования, не перебегая к различным программным комплексам.

Анализ вируса WannaCry, проведенный исследователями из специализирующейся на безопасности «Лаборатории Касперского», выявил, что большинство ошибок в коде вируса позволяют пользователям, подвергшимся заражению, восстановить свои файлы общедоступными программами инструментами или даже с помощью командной строки (CMD).

Из-за некоторых ошибок WannaCry в обработке файлов с атрибутом «Только для чтения», вирус просто делает зашифрованную копию этого файла, для показа его жертве. Для того что бы получать его назад нужно

заплатить выкуп. Однако, оригинальные файлы с атрибутом «Только для чтения», не только не шифруются, но даже не удаляются, а просто скрываются в системе. Такие фалы очень легко вернуть, нужно просто снять атрибут «Скрытый» [14].

Это не единственный пример плохого кодирования вируса WannaCry. Попав в систему вирус проверяет «важные» для него папки, то есть те, которые разработчики считают важными для пользователя, это «Рабочий стол», «Мои документы» и т.д. Так или иначе, вирус перебирает все файлы, но есть некоторые файлы и папки, которые WannaCry считает «не важными». Например, некоторые папки на диске «D», папки с точками в начале и т.д. Такие «не важные» для вируса фалы, помещаются во временную папку. А во временной папке лежат оригинальные файлы, и они не шифруются, а лишь удаляются. Исходя из этого, такие фалы легко восстановить любым ПС для восстановления данных. Однако восстановить файлы из «важных папок» будет нельзя.

Выводы: как защититься от вируса типа WANNACRY

На данный момент вирус WannaCry практически не опасен, если на вашем компьютере стоят обновления безопасности MS17-01, то вирус навредить вам из сети интернет не сможет. Однако это не значит, что он не навредит вам, если он каким - либо образом попадет на ваш компьютер и будет запущен, он все равно сможет зашифровать все ваши данные. К сожалению, на данный момент нет способов расшифровать уже зашифрованные файлы. То есть бороться с заражением можно одним способом – не допустить его.

Вот несколько советов [15], как избежать заражения вирусом WannaCry или хотя бы уменьшить нанесенный урон:

– установить все обновления безопасности Windows, особенно обновление MS17-01;

– откажитесь от использования ОС Microsoft Windows, которые уже не поддерживаются производителем.

– установить надежный антивирус, с межсетевым экраном и firewall;

– при подозрении на заражение отключите инфицированный ПК от корпоративной сети;

– при подозрении на заражение отключите компьютер, возможно специалисты смогут восстановить данные, которые вирус не успел зашифровать.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК:

1. Что такое кибербезопасность? // URL:https://www.cisco.com/c/ru_ru/products/security/what-is-cybersecurity.html (Дата обращения 14.02.2019)
2. Эпидемия шифровальщика WannaCry: что произошло и как защитится // URL:https://www.kaspersky.ru/blog/wannacry-ransomware/16147/ (Дата обращения 5.03.2019)
3. Храмов В.В., Садовов В.В., Трубников А.Н., Губарев О. Защита информации в вычислительных системах : Учебное пособие для вузов / Москва, 2002.-192с. URL:https://elibrary.ru/item.asp?id=32762286 (Дата обращения 14.02.2019)
4. WannaCry (вирус - вымогатель) // URL:https://clck.ru/FrUV5 (Дата обращения 16.03.2019)
5. Khramov V.V., Trubnikov A.N. Analysis of the aggressiveness of a software product //Automatic Control and Computer Sciences. – 1999. – Т. 33, № 2. – С. 28-34. URL:https://elibrary.ru/item.asp?id=13328155 (Дата обращения 14.02.2019)
6. Храмов В.В., Трубников А.Н.Модель специальной программной закладки //Вопросы защиты информации. – 1998. – № 1-2 (40-41). – С. 36-37. URL:https://elibrary.ru/item.asp?id=36309954 (Дата обращения 14.02.2019)
7. WannaCry // URL:https://en.wikipedia.org/wiki/WannaCry/ (Дата обращения 16.02.2019)
8. The Shadow Brokers // URL:https://ru.wikipedia.org/wiki/The_Shadow_Brokers#cite_note-4/ (Дата обращения 14.02.2019)
9. Акперов И.Г. Об алгоритмах работы подсистемы мониторинга реформы образования в регионе // Дороги в общество третьего тысячелетия: сборник трудов преподавателей ИУБиП. Ростов-на-Дону, 2001. – С. 7-10. – URL:https://elibrary.ru/item.asp?id=35047645/ (Дата обращения 14.02.2019)
10. DoublePulsar // URL:https://en.wikipedia.org/wiki/DoublePulsar/ (Дата обращения 14.02.2019)
11. Храмов В.В. Принцип интеллатентности и его использование в задачах распознавания // Тематический научно-технический сборник. – Пущино, 1994. – С. 62-66. – URL:https://elibrary.ru/item.asp?id=32838003 (Дата обращения 14.02.2019)
12. Храмов В.В., Трубников А.Н. Модель элементарной защиты программного средства // Информационные технологии и проблемы микроэлектроники: Сборник научных статей /под ред. докт. тех. наук, проф. В.А. Бархоткина. – Москва, 1999. – С. 192-197. – URL:https://elibrary.ru/item.asp? id=327112590 (Дата обращения 14.02.2019)
13. Голубенко Е.В., Ковтун О.Г., Храмов В.В. Информационная безопасность и защита информации на транспорте Тестовые задания по дисциплине. – Ростов-на-Дону, 2015. – 104 с. – URL:https://elibrary.ru/item.asp?id=36311930 (Дата обращения 14.02.2019)
14. Храмов В.В., Хадыка А.С. Разработка принципов, методов и средств самоорганизации систем защиты информации // Транспорт-2006: Труды Всероссийской научно-практической конференции: в 3 частях. Ростовский государственный университет

путей сообщения. – 2006. – С. 230-232. . – URL:https://elibrary.ru/item.asp?id=32632220 (Дата обращения 14.02.2019)
15. Как обновить Windows, чтобы защититься от WannaCry // URL:https://www.kaspersky.ru/blog/wannacry-windows-update/17543/ (Дата обращения 7.03.2019)