УДК 004.7.056.53

ВИРУСЫ – ВЫМОГАТЕЛИ. АНАЛИЗ И РЕКОМЕНДАЦИИ ПО СНИЖЕНИЮ РИСКОВ И УГРОЗ

Матвеев И.В.

к.физ.-мат.н., доцент,

Поволжский государственный университет телекоммуникаций и информатики,

Самара, Россия

Андреев А.А.

студент,

Поволжский государственный университет телекоммуникаций и информатики,

Самара, Россия

Аннотация. В современном информационном обществе информация становится очень ценным ресурсом. Все чаще появляются желающие заполучить её незаконным путём или уничтожить, преследуя финансовую выгоду, удержание влияния компании или целого государства. В статье рассматривается угроза в мире информационной безопасности в лице вирусов – вымогателей. Проблема актуальна в наше время. Во время пандемии 2020 года число кибератак стало резко возрастать. Многие организации практически парализованы самой пандемией COVID, а еще одна эпидемия шифровальщиков может их полностью уничтожить. Научная новизна предложена в виде методов и рекомендаций по борьбе и предотвращению атак подобных вирусов – вымогателей.

Ключевые слова: вирус, шифровальщик, информационная безопасность, сети, программа – шифровальщик.

RANSOMWARE VIRUSES. ANALYSIS AND RECOMMENDATIONS TO REDUCE RISKS AND LOSSES

Matveev I.V.

PhD, Associate Professor,

Povolzhky State University of Telecommunications and Informatics,

Samara, Russia

Andreev A.A.

Student,

Povolzhky State University of Telecommunications and Informatics,

Samara, Russia

Abstract. In today's information society, information is becoming a very valuable resource. Increasingly, there are those who want to get it illegally or destroy it, in pursuit of financial gain, retention of the influence of a company or an entire country. The article examines the threat in the world of information security in the face of ransomware viruses. During the 2020 pandemic, the number of cyberattacks began to increase sharply. Many organizations are practically paralyzed by the COVID pandemic itself, and yet another ransomware epidemic could wipe them out completely. Scientific novelty is offered in the form of methods and methods to combat and prevent attacks ransomware viruses.

Keywords: virus, encrypter, information security, networks, ransomware.

Введение

Наше общество в данный момент находится в постиндустриальной эпохе, главным продуктом в которой является информация с использованием высококаче-

ственных и инновационных технологий. С появлением информационных технологий в повседневное использование всех структур общества появились и угрозы несанкционированного доступа к информации, находящейся в информационных системах и использования ее в целях получения собственной выгоды, финансового и репутационного вреда. В более крупных масштабах этот момент можно рассмотреть, как новый способ создания и удержания влияния государств, используя информационную среду. Можем заметить, что проходит время обычных в нашем понимание войн. Теперь наступила эпоха войн в информационной среде (или же кибервойн). В этой статье мы рассмотрим угрозу в киберпространстве, называемую вирусами – шифровальщиками, они же ransomware (англ. ransom – выкуп, software – программное обеспечение) [1-3]. Обсудим их пагубные последствия и рекомендации по снижению рисков и ожидаемых потерь [4-10]. Хотя многие могут сказать, что время шифровальщиков прошло, так как злоумышленники за дни этой эпидемии заработали сравнительно небольшие деньги относительно, например, киберпреступников, ориентированных на банковскую сферу, нельзя игнорировать тот факт, что распространившийся в сети такой вирус может парализовать практически полностью работу от одной организации или учреждения(например медицинского – инцидент в Дюссельдорфе) до какой – либо важной государственной структуре, что может повлечь за собой не только огромные экономические потери, но и потери человеческих жизней. По подсчётам Лаборатории Касперского средняя потеря для организации от атаки 99,000$. Чтобы понять, как бороться с вирусами – шифровальщики, рассмотрим самые популярные подвиды.

WannaCry

Вполне можно считать, что это самый нашумевший червь – шифровальщик, который начал свое массовое распространение в мае 2017 года. Первыми жертвами червя стали жители Испании. В течение короткого времени вирус заразил около 500 тысяч компьютеров по всему миру.

Рис.1 – WannaCry[3]

WannaCry использует для своего распространения эксплойт EternalBlue и бэкдор DoublePulsar. При помощи EternalBlue эксплуатировалась уязвимость TCP – порта 445, который используется в операционных системах семейства Windows для совместной работы с файлами внутри сети, в дальнейшем с помощью эксплойта загружался DoublePulsar (уязвимость в реализации протокола SMB (Server Message Block) – протокол удаленного доступа к файлам и принтерам. Бэкдор работает на уровне ядра, позволяющий злоумышленникам иметь высокий доступ к устройству. Появляется доступ к командам kill, ping, exec. Командой exec происходит выполнение исполняемого файла вируса. В отличие от прочих шифровальщиков WannaCry распространяется полностью без участия пользователя, так как он сканирует порт 445 не только в локальной, но и в глобальной сети. Исправление EternalBlue было реализовано в обновлении Windows MS17-010, что остановило быстрое распространение вируса. Но не стоит думать, что после установки обновления операционной системы вы в безопасности. Пользователь так же может заразиться, запустив исполняемый файл вручную,

патч лишь предотвратит его распространение через ранее уязвимый порт. Общие потери достигают около 8 миллиардов долларов.

NotPetya

Вслед за нашумевшей эпидемией Wannacry 27 июня 2017 года началась новая волна. Её спровоцировал шифровальщик NotPetya. Жертвами стали в основном компании из России и Украины. По результатам анализа, предоставленным компанией Positive Technologies, вирус NotPetya для распространения использует TCP-порты 135,139,445, используя при этом службы SMB, WMI, PsExec

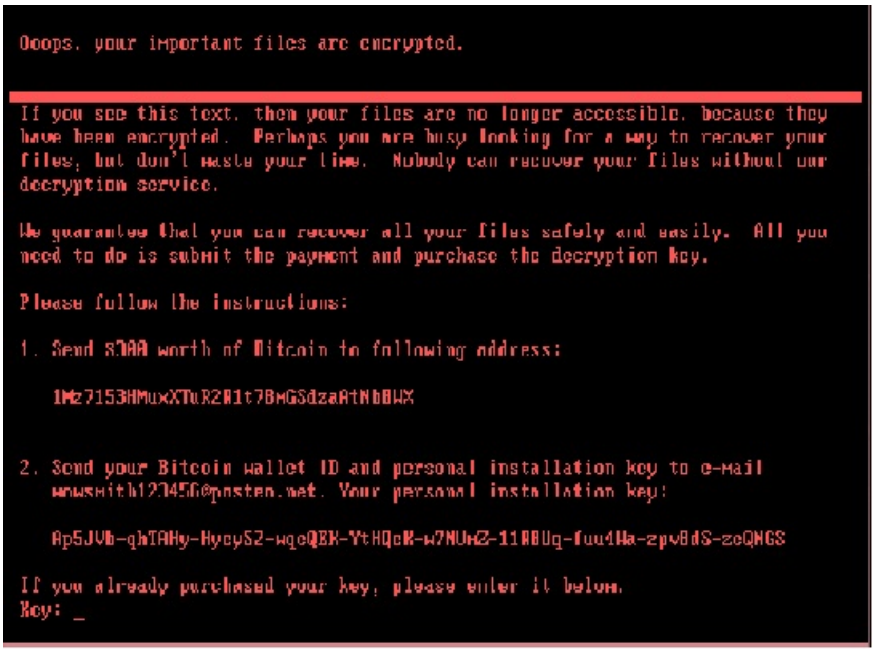

Рис.2 – NotPetya[11]

Windows Management Instrumentation (WMI) – инструмент, предназначенный для централизированного администрирования работы различных частей компьютерных инфраструктур под управлением операционной системы Windows. PsExec – инструмент администрирования для выполнения процессов в удаленных системах. Использование этих утилит требует права администратора. В этом вредоносной программе помогает эксплойт EternalBlue. В случае наличия

обновленной версии Windows вирус использует утилиту Mimikatz для получения логинов и паролей всех учётных записей внутри сети в открытом виде. Общие потери достигают около 10 миллиардов долларов.

BadRabbit

Вечером 24 октября началась новая массовая атака вируса – шифровальщика под названием BadRabbit, его сравнили с предшественниками WannaCry и NotPetya.

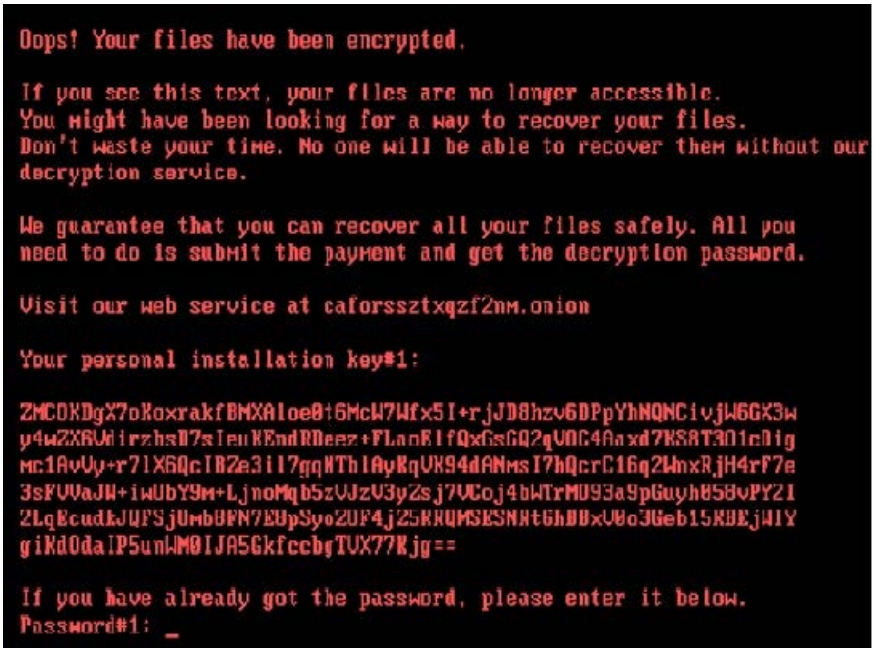

Рис. 3 – BadRabbit[11]

Основными жертвами вируса стали Россия, Украина, Турция и Германия. Предполагается, что распространение BadRabbit началось с некоторых взломанных крупных сайтов СМИ, на которых был внедрен JavaScript код. Код показывал пользователям сайта уведомления о необходимости обновить Adobe Flash Player. В случае соглашения пользователя, с серверов злоумышленников начинается скачивание вредоносного файла install_flash_player.exe. Для успешного внедрения на компьютер пользователь должен иметь права администратора. Шифровальщик создает исполняемый файл dispci.exe, после создает задание в

планировщике Windows для его запуска и перезагрузки компьютера. Для распространения по локальной сети вирус сканирует её перебором IP адресов. Для получения доступа к компьютерам в остальной сети BadRabbit выполняет перебор логинов и паролей по жестко вшитому в код словарю или раннее упомянутую утилиту Mimikatz. В случае успеха вирус распространяет себя через протоколы SMB и WebDAV

Рекомендации по снижению рисков и потерь

Рассмотрев некоторые из видов шифровальщиков, приступим к рассмотрению рекомендаций по борьбе с ними. При анализе приведённых выше вредоносных программ можно сделать вывод, что все они размножаются, используя уязвимости в получении прав администратора, что естественно наталкивает на следующие действия. Первым делом необходимо устранить уязвимость EternalBlue, обновив Windows, это уберет при этом возможность получить максимальные права доступа к системе злоумышленниками. Далее необходимо ограничить извлечения паролей в открытом или зашифрованном состоянии учетных записей из памяти утилитой Mimikatz и ей подобных. Утилита LAPS(Local admin password solution) позволит централизованно управлять паролями администраторов на всех компьютерах сети, с её помощью можно создавать уникальные пароли для каждой учетной записи администратора и периодически обновлять их(в обычном режиме период – 30 дней). Однако эти рекомендации могут оказаться бесполезными, если не используются базовые правила обеспечения безопасности административных учётных записей. В этом деле главное – максимально ограничить права административных привилегий для учётных записей администраторов и рядовых пользователей. Необходимо оставить только те права, что требуются для выполнения повседневных задач организации. Так же полезным будут ограничения запуска исполняемых файлов по их имени и хэшу. Но главной

проблемой в информационной безопасности всегда оставался человеческий фактор. Проводите регулярные учения персонала по безопасной работе с технологиями, составьте грамотную политику безопасности. Не стоит забывать и о резервных копиях баз данных.

Заключение

В статье мы рассмотрели некоторые примеры ransomware – подобных программ и обсудили рекомендации по противодействию их распространения и снижения последствий от удачного проникновения в систему. Специалисты по информационной безопасности всегда должны уделать должное внимание своим системам, устанавливая и применяя современные, доступные на данный момент меры обеспечения безопасности. Ошибки, безответственность сотрудника может привести к серьёзному ущербу организации или даже целому государству. Ежедневно происходят тысячи атак на важнейшие инфраструктуры страны. От осведомлённости и своевременного решения проблем зависят судьбы не только целых организаций, но и государств.

Библиографический список:

1. Мохурл С., Патил М. Краткое исследование Wannacry-угрозы: атака программ-вымогателей, 2017 г. // Международный журнал перспективных исследований в области компьютерных наук. – 2017. – Т. 8. – №. 5. – С. 1938-1940.

2. Маккуэйд М. Нерассказанная история NotPetya, самой разрушительной кибератаки в истории. - 2018.

3. Захра С. Р., Чишти М. А. Программы-вымогатели и Интернет вещей: новый кошмар безопасности // 9-я Международная конференция по облачным вычислениям, науке о данных и инженерии (Confluence), 2019 г. - IEEE, 2019. - С. 551-555.

4. Панин Д.Н., Филиппова Д.Н., Пирогов Д.С., Афонин А.М. ОБЛАЧНАЯ БЕЗОПАСНОСТЬ - РЕКОМЕНДАЦИИ ПО СНИЖЕНИЮ УГРОЗ // Информатизация и связь. - 2020. - №2. - С. 73-76.

5. Ли С., Ким Х. К., Ким К. Защита от программ-вымогателей с использованием перспективы защиты с использованием подвижных целей// Компьютеры и электротехника. - 2019. - Т. 78. - С. 288-299.

6. Мохаммад А. Х. Эволюция, рост и рекомендации по обнаружению программ-вымогателей // Современная прикладная наука. - 2020. - Т. 14. - №3. - С. 68-74

7. Парра Г. Д. Л. Т. и др. Обнаружение атак Интернета вещей с помощью распределенного глубокого обучения // Журнал сетевых и компьютерных приложений. - 2020. - С. 102662.

8. Чу К. Дж. У., Кумар В. Обнаружение программ-вымогателей на основе поведения // Материалы 34-й Международной конференции. о компьютерах и их приложениях. - 2019. – Т. 58. - С. 127-136.

9. Зайнудин Ф. К. М. и др. Обнаружение вредоносных программ с использованием технологии Lebahnet // Журнал кибербезопасности OIC-CERT. - 2020. - Т. 2. - №1. - С. 69-76.

10. Чукилла, Алехандро, Тереза Гуарда и Джованни Нинахуальпа Кинья. «Защита от выкупа WannaCry принадлежит каждому». 2019 14-я Иберийская конференция по информационным системам и технологиям (CISTI). IEEE, 2019. - стр. 1-4.

11. Дэвис С. Р., Макфарлейн Р., Бьюкенен У. Дж. Оценка реальных криминалистических методов в борьбе с атаками программ-вымогателей // Forensic Science International: Digital Investigation. - 2020. - Т. 33. - С. 300979.

Оригинальность 98%