УДК 004.056

ВРЕДОНОСНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ДЛЯ ВЫМОГАТЕЛЬСТВА И МЕТОДЫ БОРЬБЫ С НИМ

Кот Л.Л., Кручинин А.В.
ГВУЗ «Национальный горный университет», http://bit.nmu.org.ua/,E-mail: leon.k91@yandex.ua

В данных тезисах рассматривается вредоносное программное обеспечение для вымогательства, особенности его функционирования, способы его проникновения в систему и методы борьбы с ним.

Ключевые слова – вредоносное программное обеспечение для вымогательства, ransomware, cerber, teslacrypt, cryptxxx, malvertising.

ВВЕДЕНИЕ

Программное обеспечение (ПО) для вымогательства или Ransomware – такой вид вредоносного ПО, который при попадании в компьютер или мобильное устройство блокирует доступ или шифрует хранящиеся файлы, а для восстановления управления компьютером или файлами пользователю необходимо отправить требуемую сумму на указанный счет.

Средняя сумма выкупа – 679 долларов США [3]. Распространенный способ оплаты выкупа – в биткоинах.

Среди общего количества обнаруженного ПО для вымогательства 64% составляет криптографическое ПО [1].

Между 2013 и 2014 годами количество видов криптографического ПО для вымогательства увеличилось на 250% [1].

Согласно данным Лаборатории Касперского, статистика по этому виду угрозы выглядит следующим образом [2]:

- процент пострадавших от программ, шифрующих файлы, вырос на 25%, с 6.6% в 2014 – 2015 гг. до 31.6% в 2015 – 2016;
- количество пользователей, столкнувшихся с программами блокировки компьютера снизился на 13.03%, с 1836673 в 2014-2015 годах до 1597395 в 2015-2016 годах;
- количество пользователей, столкнувшихся с ПО для вымогательства при пользовании мобильными устройствами, выросло в 4 раза: с 35413 пользователей в 2014-2015 до 136532 в 2015-2016 гг.

ВИДЫ ВРЕДОНОСНОГО ПО ДЛЯ ВЫМОГАТЕЛЬСТВА

На данный момент существуют 2 вида программного обеспечения для вымогательства [1], [2]:

- блокирующее ПО (computer locker);
- вредоносное ПО с криптографическими функциями (data locker).

БЛОКИРУЮЩЕЕ ВРЕДОНОСНОЕ ПО ДЛЯ ВЫМОГАТЕЛЬСТВА (COMPUTER LOCKER)

Данный вид ПО разработан с целью блокировки доступа пользователя к компьютеру. Как правило, функциональность заблокированного компьютера ограничена, мышь может быть отключена, а на клавиатуре могут работать только цифровые клавиши для ввода платежного кода [1].

ВРЕДОНОСНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ С КРИПТОГРАФИЧЕСКИМИ ФУНКЦИЯМИ

Данный тип вредоносного ПО разработан с целью поиска и шифрования файлов, хранящихся на атакуемом компьютере.

Доступ к файлам возможен только в случае использования ключа расшифрования, который можно получить только после оплаты суммы, указанной в всплывающем окне при работе компьютера.

Количество пользователей, атакованных криптографическим ПО для вымогательства в Украине в 2014 - 2015 году составило 1.34%, в то время как в 2015 – 2016 году было зарегистрировано уже 28.86% атак [2].

Для шифрования используются такие алгоритмы шифрования, как RSA – 1024, 3DES, AES [1].

СЕМЕЙСТВА ВРЕДОНОСНОГО ПО ДЛЯ ВЫМОГАТЕЛЬСТВА

На данный момент самыми распространенными семействами вредоносного ПО для вымогательства являются: Teslacrypt, Cerber, CryptXXX [2], [3];

Для контактов с жертвами злоумышленники используют сеть Tor, предоставляющую анонимное сетевое соединение, защищённое от прослушивания.

Некоторые семейства вирусов имеют дополнительные функции. CryptXXX способен добавить инфицированный компьютер в ботнет, и этот компьютер может быть затем использован для осуществления DDoS – атак [3].

СПОСОБЫ ПРОНИКНОВЕНИЯ ВРЕДОНОСНОГО ПО ДЛЯ ВЫМОГАТЕЛЬСТВА В СИСТЕМУ

Существуют следующие способы проникновения данного вредоносного ПО в систему:

- спам и социальная инженерия (письма электронной почты от Интернет-провайдера, счет по коммунальным платежам, письмо от банка, при переходе по ссылке, указанной в письме или загрузке

прикрепленного файла, вирус попадает в систему [3], [4]).

- через уязвимости операционной системы [4];
- скачивание вредоносного контента с заражённых веб-сайтов (вредоносное ПО, встроенное в бесплатное ПО, аудио и др. файлы) [1];
- malvertising – распространение через рекламные сети Yahoo!, YouTube, Skype [4].

СПОСОБЫ ПРЕДОТВРАЩЕНИЯ ПРОНИКНОВЕНИЯ ВРЕДОНОСНОГО ПО ДЛЯ ВЫМОГАТЕЛЬСТВА В СИСТЕМУ И МЕТОДЫ БОРЬБЫ С НИМ

1. Включение в настройках системы отображения расширения файлов, это поможет определить, например, не был ли загружен файл аудиозаписи .mp3 с расширением .exe [2].
2. Использование обновляемого антивирусного ПО.
3. Регулярное обновление ОС и установленного ПО (Adobe Flash, Java, Chrome, Firefox, Internet Explorer, Microsoft Windows, Office) [2].
4. Создание образа системы средствами ОС или с помощью специализированных программ.
5. Регулярное создание резервных копий ценных файлов или на внешнем носителе, или с помощью OneDrive for Business компании Microsoft [5].
6. Не открывать письма электронной почты от незнакомых отправителей.
7. Компании Лаборатория Касперского, Intel, Symantec разработали инструменты для определения типа угрозы и ее устранения [6], [7].

ВЫВОДЫ

В данных тезисах представлена информация о вредоносном ПО для вымогательства, способах его проникновения в систему, способах предотвращения проникновения и методах борьбы с ним.

Среди указанных в тезисах способов предотвращения проникновения вредоносного программного обеспечения и борьбы с ним следует выделить основные: использование антивирусного программного обеспечения, резервное копирование файлов на съемный носитель. Антивирусными средствами, обладающими функциями обнаружения и удаления вредоносного ПО для вымогательства являются: Kaspersky Internet Security, Kaspersky Anti-Ransomware Tool for Business, Bitdefender Total Security Multi-Device (предоставляет защиту для Windows, Mac OC и Android), Norton Power Eraser.

Резервное копирование может быть организовано:

- стандартными средствами в системе;
- программой Acronis True Image;

Учитывая увеличение разнообразия устройств, подключаемых к Интернет, все они могут быть подвержены атакам вредоносного программного обеспечения, следовательно, уязвимыми могут оказаться: часы, системы Smart Home (Умный дом), телевизоры, кондиционеры, стиральные машины, холодильники и другая бытовая техника, транспортные средства. Это влечет за собой необходимость в создании и применении дополнительных методов, способов и средств защиты от вредоносного ПО для вымогательства, ориентированных на конкретное защищаемое устройство.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Kevin Savage, Peter Coogan, Hon Lau - «Эволюция вредоносного программного обеспечения для вымогательства» [Электронный ресурс] – [Веб-сайт] - Режим доступа: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-evolution-of-ransomware.pdf
2. Securelist.com - «Отчет сетевой безопасности Касперского: Вредоносное программное обеспечение в 2014 – 2016 годах» [Электронный ресурс] – [Веб-сайт] – Режим доступа: https://securelist.com/files/2016/06/KSN_Report_Ransomware_2014-2016_final_ENG.pdf
3. Symantec.com - «Специальный отчет об угрозах безопасности в Интернет: Ransomware и бизнес» [Электронный ресурс] – [Веб-сайт] - Режим доступа: https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/ISTR2016_Ransomware_and_Businesses.pdf
4. Владимир Безмалый: «Деньги или данные? Что такое Ransomware.» [Электронный ресурс] – [Веб-сайт] - Режим доступа: https://www.pcweek.ru/security/article/detail.php?ID=175237
5. Alexs Pena – «Как справиться с Ransomware» [Электронный ресурс] – [Веб-сайт] - Режим доступа: https://blogs.technet.microsoft.com/office365security/how-to-deal-with-ransomware/
6. Проект «Больше никакого выкупа» инструменты для расшифрования файлов [Электронный ресурс] – [Веб-сайт] - Режим доступа: https://www.nomoreransom.org/decryption-tools.html
7. Программы для расшифрования файлов, разработанные Лабораторией Касперского [Электронный ресурс] – [Веб-сайт] - Режим доступа: https://noransom.kaspersky.com