Э. А. Гайдукевич, К. Е. Чечеба

АЛГОРИТМЫ РАБОТЫ ВИРУСА-ШИФРОВАЛЬЩИКА

Рассматривается алгоритм работы вирусов-шифровальщиков на примере вируса-вымогателя «Petya».

Введение

Вирусы-шифровальщики – особый вид программного обеспечения, который обычно осуществляет шифрование всех файлов на жестком диске, после чего мошенники требуют выкуп за ключ расшифрования или специальную программу-декриптор. Однако существуют вирусы-вымогатели, разработчики которых достигают своей цели немного иным образом.

I. Краткое описание вируса «Petya»

Одним из наиболее примечательных представителей вредоносных программ такого типа является вирус-вымогатель «Petya». Его особенность заключается в том, что вместо того, чтобы шифровать файлы один за другим, он запрещает доступ ко всей системе, атакуя низкоуровневые структуры на диске. Главная загрузочная запись заражённой системы перезаписывается специальным загрузчиком, который загружает вредоносное ядро, что затем приступает к дальнейшему шифрованию.

II. Алгоритм работы программы-вымогателя

Алгоритм работы вируса состоит из двух этапов.

Первый этап начинается с .exe файла. Во-первых, генерируется уникальный ключ, который будет использоваться для дальнейшей блокировки. Случайные значения генерируются функцией «Windows Crypto API: CryptGenRandom». Ключ шифруется по методу ECC и отображается жертве в качестве личного номера, который предлагается отправить злоумышленникам. Во-вторых, вредоносный код записывается в начало диска, куда помещаются важные для системы файлы, после чего программа намеренно выводит систему из строя.

Второй этап начинается с кода, прежде записанного в начало диска. Его исполнение происходит во время загрузки системы. Программа запускает фальшивую проверку жёсткого диска на наличие ошибок. Во время такой «проверки» главная файловая таблица шифруется с помощью алгоритма «Salsa20». По завершению отображается экран, сообщающий пользователю о том, что все файлы зашифрованы, и доступ к ним невозможен.

III. Алгоритм заражения главной загрузочной записи

Сначала сектор жёсткого диска под номером 0 (прежде содержавший стандартные код и данные) шифруется при помощи простой операции исключающего «или» (гаммирование) по блоку параметров в BIOS с номером 0x37, после чего результат шифрования записывается в сектор номер 56. Далее, аналогичным образом шифруются секторы 1-33. После этого генерируются настройки для вредоносной программы, которые потом записываются в сектор 54. Затем создаётся проверочный сектор 55, заполненный повторяющимся блоком 0x37. Потом копируется сигнатура диска, определяющая диск в операционной системе, и таблица разделов в свой загрузчик; на диск же записывается вредоносный загрузчик в сектор 0 и вредоносный код в секторы 34-50. Наконец, вызывается функция «NTRaiseHardError», приводящая к аварийному завершению работы машины.

IV. Выводы

Из всего описанного можно сделать вывод, что вирус «Petya», являющийся вирусом-вымогателем, имеет отличную от других программ подобного типа схему нанесения вреда машине: помимо препятствия загрузки ОС, он блокирует доступ к файлам, расположенным на жёстких дисках атакуемой системы. Именно это делает его особенно опасным.

1. AVAST [Электронный ресурс]. – Режим доступа: `https://blog.avast.com/ru/vse-chto-nuzhno-znat-o-petna-viruse-vymogatele-semejstva-petya`. – Дата доступа: 03.04.2022
2. MalwarebytesLABS [Электронный ресурс]. – Режим доступа: `https://blog.malwarebytes.com/threat-analysis/2016/04/petya-ransomware`. – Дата доступа: 04.04.2022
3. SecureList by Kaspersky [Электронный ресурс]. – Режим доступа: `https://securelist.com/petya-the-two-in-one-trojan/74609`. – Дата доступа: 05.04.2022

Гайдукевич Эмили Андреевна, студент 1 курса ФИТиУ БГУИРа, gureensaradu@gmail.com.
Чечеба Карина Евгеньевна, студент 1 курса ФИТиУ БГУИРа, koryatch@gmail.com.
Научный руководитель: Шатилова Ольга Олеговна, старший преподаватель кафедры вычислительных методов и программирования БГУИР, магистр технических наук, o.shatilova@bsuir.by.