ООО Агентство
комплексной
безопасности «Барьер»
www.saveit.pro

394018, г. Воронеж,
ул. Никитинская, д. 42,
оф. 509
т/ф.: +7 (473) 202-24-64
info@saveit.pro

ИНН 3664091561
КПП 366401001
ОГРН 1083668024175

WannaCrypt 2.0

Классификация, Общие сведения, Принцип работы, Меры защиты

Бруданин Артём
Лаборатория анализа защищенности
@hackzard

Воронеж, 2017

Классификация

WannaCrypt (также известный как Wcry и WanaCrypt0r 2.0) — компьютерный вирус, поразивший в мае 2017 года большое количество компьютеров под управлением операционной системы Microsoft Windows. Одними из первых были атакованы компьютеры Испании, потом вирус распространился на другие страны. От вируса пострадали компьютеры частных лиц, коммерческих организаций и правительственных учреждений. Используется как средство вымогательства.

По состоянию на 14:00 13 мая 2017 года инфицированы 131000 компьютеров из 99 стран. Текст требования о переводе денежных средств переведён на 28 языков мира. Россия больше других стран пострадала от атаки этого вируса.[1]

Тип	Загрузочный вирус, RansomWare
Время появления	Февраль 2017г.
Используемые ПО/Службы/Протоколы	Уязвимость в SMBv1
Уязвимые ОС	Все версии Windows до версии: Windows 10
Уязвимость	Критическая уязвимость MS17-010[2]
Возможность восстановления файлов	**Не найдено (15.05.2017)**
Возможность защиты от уязвимости	**Бюллетень Windows MS17-010**

1 https://ru.wikipedia.org/wiki/WannaCry
2 https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

Общие сведения

Данный компьютерный вирус представляет собой вирус-вымогатель, использующий процедуру шифрования файлов, на основе двух криптоалгоритмов: Rijndael (AES 128) + RSA 256. Заражая компьютер, вирус зашифровывает все пользовательские данные на жестком диске и требует выкуп за их расшифровку. Отличительной особенностью вируса является стихийность – неуправляемое распространение вируса в сети Интернет.

Вирус затрагивает следующие расширения файлов:

.doc, .docx, .xls, .xlsx, .ppt, .pptx, .pst, .ost, .msg, .eml, .vsd, .vsdx, .txt, .csv, .rtf, .123, .wks, .wk1, .pdf, .dwg, .onetoc2, .snt, .jpeg, .jpg, .docb, .docm, .dot, .dotm, .dotx, .xlsm, .xlsb, .xlw, .xlt, .xlm, .xlc, .xltx, .xltm, .pptm, .pot, .pps, .ppsm, .ppsx, .ppam, .potx, .potm, .edb, .hwp, .602, .sxi, .sti, .sldx, .sldm, .sldm, .vdi, .vmdk, .vmx, .gpg, .aes, .ARC, .PAQ, .bz2, .tbk, .bak, .tar, .tgz, .gz, .7z, .rar, .zip, .backup, .iso, .vcd, .bmp, .png, .gif, .raw, .cgm, .tif, .tiff, .nef, .psd, .ai, .svg, .djvu, .m4u, .m3u, .mid, .wma, .flv, .3g2, .mkv, .3gp, .mp4, .mov, .avi, .asf, .mpeg, .vob, .mpg, .wmv, .fla, .swf, .wav, .mp3, .sh, .class, .jar, .java, .rb, .asp, .php, .jsp, .brd, .sch, .dch, .dip, .pl, .vb, .vbs, .ps1, .bat, .cmd, .js, .asm, .h, .pas, .cpp, .c, .cs, .suo, .sln, .ldf, .mdf, .ibd, .myi, .myd, .frm, .odb, .dbf, .db, .mdb, .accdb, .sql, .sqlitedb, .sqlite3, .asc, .lay6, .lay, .mml, .sxm, .otg, .odg, .uop, .std, .sxd, .otp, .odp, .wb2, .slk, .dif, .stc, .sxc, .ots, .ods, .3dm, .max, .3ds, .uot, .stw, .sxw, .ott, .odt, .pem, .p12, .csr, .crt, .key, .pfx, .der

Предпосылкой создания данного вируса послужил взлом серверов АНБ хакерской группировкой «The Shadow Brokers», с последующей массовой публикацией, созданных АНБ, эксплоитов[3] (в частности: EternalBlue и DoublePulsar).

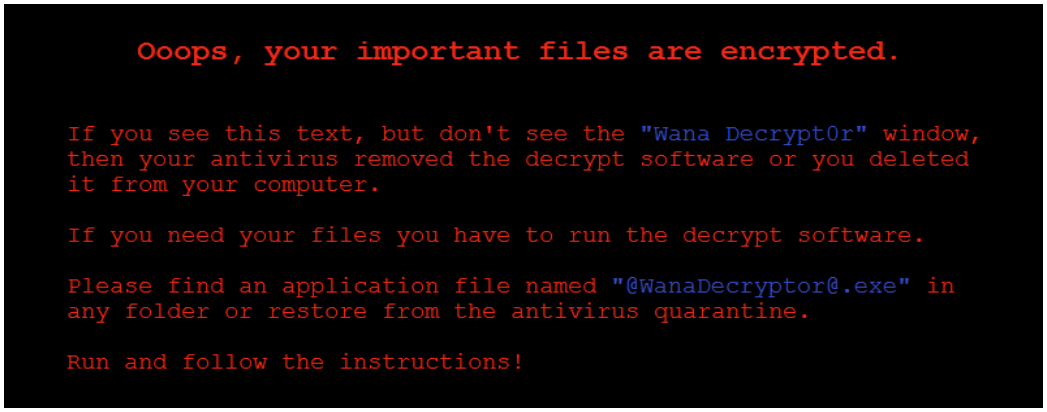
Вирус использует уязвимость в протоколе SMBv1 (Server Message Block 1.0) — «EternalBlue», позволяющую удаленно выполнить на ПК жертвы любой программный код.

Уязвимость была исправлена два месяца назад компанией Microsoft выпуском бюллетени обновления Windows: MS17-010[4].

3 https://ru.wikipedia.org/wiki/Эксплойт
4 https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

Принцип работы

1. Вирус сканирует сеть Интернет на наличие узлов, имеющих открытый порт 445 (используется протоколом SMB);
2. Используя уязвимость MS17-010, WannaCrypt подключается к компьютерам жертвы через найденный порт и создаёт односторонний «тоннель» для выполнения команд;
3. Вирус взаимодействует с каждой RDP сессией на компьютере и устанавливает в каждую из них свои копии для автоматического запуска;
4. Используя пейлоад[5] (полезная нагрузка) «DoublePulsar», вирус устанавливает бэкдор[6] на компьютер жертвы и устанавливает вредоносное ПО, которое находит и шифрует данные.
5. Вирус удаляет теневые хранилища операционной системы, для предотвращения возможности восстановления исходных файлов;
6. Меняется фон рабочего стола:



7. Появляется окно вируса-вымогателя:

5 https://ru.wikipedia.org/wiki/Полезная_нагрузка
6 https://ru.wikipedia.org/wiki/Бэкдор

Меры защиты

1. Исключить «выход» портов, использующих SMB в сеть Интернет;
2. Установить последние обновления Windows, включая бюллетень безопасности MS17-010;
3. При возникновении проблем с установкой обновлений MS Windows необходимо отключить поддержку протокола SMBv1:

   - С помощью PowerShell на стороне сервера:

Set-SmbServerConfiguration -EnableSMB1Protocol $false -Force

   - С помощью PowerShell на стороне клиента:

sc.exe config lanmanworkstation depend= bowser/mrxsmb20/nsi

sc.exe config mrxsmb10 start= disabled

   - Через реестр Windows:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters

Параметру SMB1 задать значение типа DWORD = 0

или

Создать параметр DWORD SMB1 со значением = 0

4. При обнаружении подозрительных процессов на компьютере: отключить ПК от сети Интернет для предотвращения дальнейшего распространения вируса;

Файлы обновлений MS Windows

Windows XP	http://download.windowsupdate.com/d/msdownload/update/softwa…
Windows XP x64	http://download.windowsupdate.com/d/csa/csa/secu/2017/02/win...
Windows Server 2003 x86	http://download.windowsupdate.com/c/csa/csa/secu/2017/02/win...
Windows Server 2003 x64	http://download.windowsupdate.com/c/csa/csa/secu/2017/02/win...
Windows Vista x86	http://download.windowsupdate.com/d/msdownload/update/softwa...
Windows Vista x64	http://download.windowsupdate.com/d/msdownload/update/softwa...
Windows Server 2008 x86	http://download.windowsupdate.com/d/msdownload/update/softwa...
Windows Server 2008 x64	http://download.windowsupdate.com/d/msdownload/update/softwa...
Windows 7 x86	http://download.windowsupdate.com/d/msdownload/update/softwa...
Windows 7 x64	http://download.windowsupdate.com/d/msdownload/update/softwa...
Windows Server 2008 R2	http://download.windowsupdate.com/d/msdownload/update/softwa...
Windows 8 x86	http://download.windowsupdate.com/c/msdownload/update/softwa...
Windows 8 x64	http://download.windowsupdate.com/c/msdownload/update/softwa...
Windows Server 2012	http://download.windowsupdate.com/c/msdownload/update/softwa...
Windows 8.1 x86	http://download.windowsupdate.com/c/msdownload/update/softwa...
Windows 8.1 x64	http://download.windowsupdate.com/c/msdownload/update/softwa...
Windows Server 2012 R2	http://download.windowsupdate.com/c/msdownload/update/softwa...
Windows 10 x86	http://download.windowsupdate.com/c/msdownload/update/softwa...
Windows 10 x64	http://download.windowsupdate.com/c/msdownload/update/softwa...
Windows 10 (1511) x86	http://download.windowsupdate.com/c/msdownload/update/softwa...
Windows 10 (1511) x64	http://download.windowsupdate.com/c/msdownload/update/softwa...
Windows 10 (1607) x86	http://download.windowsupdate.com/c/msdownload/update/softwa...
Windows 10 (1607) x64	http://download.windowsupdate.com/d/msdownload/update/softwa...
Windows Server 2016	http://download.windowsupdate.com/d/msdownload/update/softwa...