KPMG

WannaCry

Технический бюллетень
17 мая 2017 года

В пятницу, 12 мая 2017 года, начал свое распространение так называемый вирус-вымогатель WannaCry. В данном документе содержится как общее описание этого вируса, так и техническая информация о механизмах его действия.

Ключевая информация

Вирус-вымогатель (ransomware) WannaCry в случае невыплаты определенной суммы выкупа шифрует жесткий диск компьютера/сервера жертвы. Вирус уже затронул несколько десятков тысяч компаний во многих странах. Среди жертв называются крупные российские компании и государственные структуры.

Название

WannaCry, WNCry, WanaCrypt0r, Wana Decrypt0r, WannaCrypt, WCrypt, WCRY.

Вектор распространения

Вредоносная программа использует программную уязвимость в операционных системах Microsoft Windows (используемая уязвимость фигурирует под названием MS17-010 или ETERNALBLUE).

Подверженные системы

Windows Vista SP2, Windows 2008 R2, Windows 7, Windows 8.1, Windows 2012 R2, Windows 10, Windows Server 2016 (и другие Windows-системы, подверженные уязвимости MS17-010).

Нахождение в системе

Вредоносное ПО запускает себя под каждой из открытых в системе RDP-сессий в контексте пользователя.

Что делает вирус

Программа-вымогатель зашифровывает данные на компьютере и требует выкупа (обычно 300$ в биткоинах) в установленный промежуток времени, в противном случае удаляет данные.

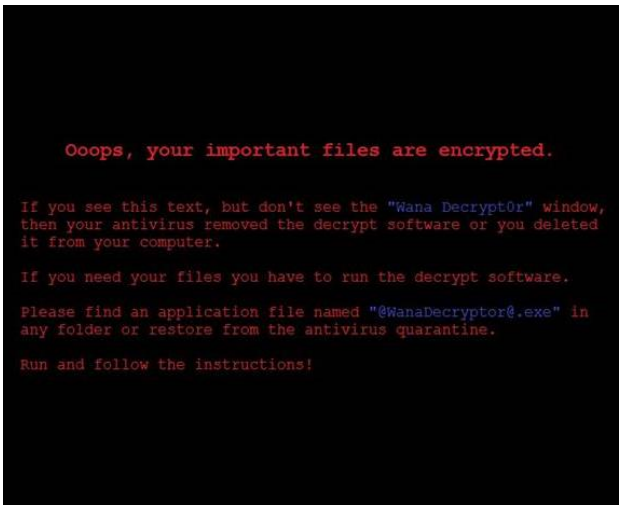
Возможность расшифрования

Вредонос использует криптостойкое шифрование (RSA-2048 и AES-128), и на текущий момент вирусным аналитикам не удалось найти недостатков в реализации криптоалгоритма.

Важно

Патч для устранения данной уязвимости был выпущен в марте 2017 года как часть MS17-010 / CVE-2017-0147. В настоящий момент исправление данной уязвимости доступно также и для не поддерживаемых больше систем Windows: XP и 2003 (https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/).

Внешний вид зараженной машины



Процесс заражения

Вредонос проверяет состояние системы и наличие заражения. Если WannaCry не присутствует на машине, то первым этапом заражения является установка WannaCry как сервиса mssecsvc2.0. Полное имя в системе – *Microsoft Security Center (2.0).* Сервис использует TOR Browser Bundle и программу шифрования файлов на диске. Если машина заражена, вредонос работает в режиме червя, эксплуатируя **уязвимость** MS17-010.

Исполняемый файл вредоноса представляет собой распаковщик ZIP-архива. При запуске вредонос распаковывает свои компоненты в директорию, где он был запущен из архива с использованием пароля «WNcry@2ol7».

```
HGLOBAL EternalBlue_Worm()
{
  HGLOBAL result; // eax@1
  void *v1; // eax@2
  signed int v2; // esi@4
  void *v3; // eax@5

  result = Init_EternalBlue_Worm();
  if ( result )
  {
    v1 = (void *)beginthreadex(0, 0, EternalBlue_scan_LAN, 0, 0, 0);
    if ( v1 )
      CloseHandle(v1);
    v2 = 0;
    do
    {
      v3 = (void *)beginthreadex(0, 0, EternalBlue_scan_inet, v2, 0, 0);
      if ( v3 )
        CloseHandle(v3);
      Sleep(0x7D0u);
      ++v2;
    }
    while ( v2 < 128 );
    result = 0;
  }
  return result;
}
```

Компоненты вредоноса

b.wnry	Обои для рабочего стола, индикатор заражения
c.wnry	Конфигурационный файл, содержащий адреса C&C серверов, адреса биткоин-кошельков и прочее
r.wnry	Q&A файл, содержащий информацию о процессе работы с биткоинами
s.wnry	ZIP-архив с клиентом сети TOR
t.wnry	Модуль шифрования, который зашифрован с использованием специального формата WannaCry; может быть дешифрован с использованием приватного ключа, находящегося в исполняемом файле вредоноса
u.wnry	Исполняемый файл, использующийся для дешифрования файлов пользователя в случае поступления оплаты от пользователя
Taskdl.exe	Исполняемый файл, удаляющий все временные файлы, созданные во время процесса шифрования (.WNCRYT)
Taskse.exe	Исполняемый файл, запускающий вредонос в контексте всех пользователей с RDP-сессией (основан на TSCON)
msg*	Языковые файлы (на текущий момент вредонос поддерживает 28 различных языков)

Вредонос создает несколько дополнительных файлов в ходе своего выполнения

00000000.eky	Ключ шифрования для файла t.wnry, который в свою очередь содержит действительный модуль шифрования вредоноса.
00000000.pky	Публичный ключ, используемый вредоносом для шифрования сгенерированной пары AES-ключей, которыми в свою очередь шифруются файлы пользователей.
00000000.res	Результаты взаимодействия с управляющим C&C (command and control) сервером.

Вредонос меняет права на ряд файлов и взаимодействует с C&C сервером в сети TOR

```
attrib +h .
icacls . /grant Everyone:F /T /C /Q
C:\Users\xxx\AppData\Local\Temp\taskdl.exe
@WanaDecryptor@.exe fi
300921484251324.bat
```

Вредонос создает мьютекс «Global\MsWinZonesCacheCounterMutexA» и запускает команду

```
cmd.exe /c vssadmin delete shadows /all /quiet & wmic shadowcopy delete & bcdedit /set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no & wbadmin delete catalog –quiet
```

Данная команда удаляет резервные копии, отключает возможность перезагрузки в режим восстановления системы и прочее.

Что привело к массовому заражению?

1. Отсутствие налаженного процесса менеджмента обновлений прикладного и системного программного обеспечения компании.
2. Отсутствие постоянного контроля внешнего периметра сети на наличие избыточных сервисов с публичным доступом.
3. Отсутствие сегментирования и межсетевого экранирования внутри корпоративных сетей.
4. В случае заражения через фишинг – недостаточная осведомленность пользователей в вопросах информационной безопасности.
5. Отсутствие проактивной позиции специалистов по информационной безопасности в отношении актуальных угроз.

Процесс заражения

- После заражения вредонос начинает работать в режиме червя, инициализирует криптографические библиотеки для шифрования файлов пользователей.
- Вредонос содержит две версии библиотек dll – для 32- и 64-битных версий операционной системы.
- Запуск dll приводит к размещению на диске файла C:\WINDOWS\mssecsvc.exe.

```
.text:10001114                  public PlayGame
.text:10001114 PlayGame         proc near               ; DATA XREF: .rdata:off_100021B8↓o
.text:10001114                  push    offset aMssecsvc_exe ; "mssecsvc.exe"
.text:10001119                  push    offset aWindows ; "WINDOWS"
.text:1000111E                  push    offset Format   ; "C:\\%s\\%s"
.text:10001123                  push    offset payload_drop_location ; Dest
.text:10001128                  call    ds:sprintf
.text:1000112E                  add     esp, 10h
.text:10001131                  call    drop_payload_from_resources
.text:10001136                  call    execute_payload
.text:1000113B                  xor     eax, eax
.text:1000113D                  retn
.text:1000113D PlayGame         endp
```

Какие данные шифруются вредоносом?

На всех локальных дисках и доступных сетевых ресурсах шифруются файлы со следующими расширениями:

1. Офисные файлы			
.ppt	.doc	.docx	.xlsx
.sxi	.sxw	.odt	.hwp

2. Архивы и мультимедийные файлы			
.zip	.rar	.tar	.bz2
.mp4	.mkv	.vsd	.odg
.raw	.nef	.svg	.psd

3. Файлы писем и почтовых программ			
.eml	.msg	.ost	.pst
.edb			

4. Файлы баз данных			
.sql	.accdb	.mdb	.dbf
.odb	.myd		

5. Файлы проектов и исходные коды			
.php	.java	.cpp	.pas
.asm			

6. Ключи шифрования и сертификаты			
.key	.pfx	.pem	.p12
.csr	.gpg	.aes	

7. Файлы виртуальных машин			
.vmx	.vmdk	.vdi	

Полный перечень

.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

Индикаторы компрометации

Для обнаружения заражения серверов и рабочих станций можно использовать хеши файлов, которые обеспечивают выполнение вредоносного кода, а также пути файлов и DNS-имена, связанные с атакой. Основные индикаторы вредоноса представлены ниже, в последующих разделах дополнительно представлена информация по всем индикаторам компрометации, доступным на текущий момент.

Тип идентификатора	Идентификатор
FileHash-SHA256	09a46b3e1be080745a6d8d88d6b5bd351b1c7586ae0dc94d0c238ee36421cafa
FileHash-SHA256	24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c
FileHash-SHA256	2584e1521065e45ec3c17767c065429038fc6291c091097ea8b22c8a502c41dd
FileHash-SHA256	2ca2d550e603d74dedda03156023135b38da3630cb014e3d00b1263358c5f00d
FileHash-SHA1	45356a9dd616ed7161a3b9192e2f318d0ab5ad10
FileHash-SHA256	4a468603fdcb7a2eb5770705898cf9ef37aade532a7964642ecd705a74794b79
FileHash-MD5	509c41ec97bb81b0567b059aa2f50fe8
FileHash-SHA1	51e4307093f8ca8854359c0ac882ddca427a813c
FileHash-MD5	7bf2b57f2a205768755c07f238fb32cc
FileHash-MD5	7f7ccaa16fb15eb1c7399d422f8363e8
FileHash-MD5	84c82835a5d21bbcf75a61706d8ab549
FileHash-SHA1	87420a2791d18dad3f18be436045280a4cc16fc4
FileHash-SHA256	b9c5d4339809e0ad9a00d4d3dd26fdf44a32819a54abf846bb9b560d81391c25
FileHash-SHA1	bd44d0ab543bf814d93b719c24e90d8dd7111234
FilePath	C:\Windows\mssecsvc.exe
FilePath	C:\WINDOWS\tasksche.exe
FileHash-MD5	db349b97c37d22f5ea1d1841e3c89eb4
FileHash-SHA1	e889544aff85ffaf8b0d0da705105dee7c97fe26
FileHash-SHA256	ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
FileHash-MD5	f107a717f76f4f910ae9cb4dc5290594
FileHash-SHA256	f8812f1deb8001f3b7672b6fc85640ecb123bc2304b563728e6235ccbe782d85
Hostname	iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com
Hostname	ifferfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com

Индикаторы компрометации в реестре

Ниже перечислены индикаторы, позволяющие определить активность вредоноса в системе по ключам реестра и их содержимому. Следует обратить внимание, что некоторые участки ключей реестра генерируются случайным образом.

HKLM\SOFTWARE\WanaCrypt0r

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\<random>: “”<ransomware directory>\tasksche.exe””

HKLM\SOFTWARE\WanaCrypt0r\wd: “<ransomware directory>”

HKU\S-1-5-21-677641349-3533616285-3951951702-1000\Control Panel\Desktop\Wallpaper: “%APPDATA%\Microsoft\Windows\Themes\TranscodedWallpaper.jpg”

HKU\S-1-5-21-677641349-3533616285-3951951702-1000\Control Panel\Desktop\Wallpaper: “<ransomware directory>\@WanaDecryptor@.bmp”

Индикаторы компрометации в файловой системе

Ниже перечислены индикаторы, позволяющие определить активность вредоноса по названиям файлов на локальных дисках пользователей и сетевых ресурсах. Следует обратить внимание, что часть адреса зависит от директории, где был запущен вредонос.

@Please_Read_Me@.txt – размещается во всех папках, содержащих зашифрованные файлы.

@WanaDecryptor@.exe.lnk – размещается во всех папках, содержащих зашифрованные файлы.

%DESKTOP%\@WanaDecryptor@.bmp

%DESKTOP%\@WanaDecryptor@.exe

%APPDATA%\tor\cached-certs

%APPDATA%\tor\cached-microdesc-consensus

%APPDATA%\tor\cached-microdescs.new

%APPDATA%\tor\lock

%APPDATA%\tor\state

<ransomware directory>\00000000.eky

<ransomware directory>\00000000.pky

<ransomware directory>\00000000.res

<ransomware directory>\@WanaDecryptor@.bmp

<ransomware directory>\@WanaDecryptor@.exe

<ransomware directory>\b.wnry

<ransomware directory>\c.wnry

<ransomware directory>\f.wnry

<ransomware directory>\msg\m_bulgarian.wnry

<ransomware directory>\msg\m_chinese (simplified).wnry

<ransomware directory>\msg\m_chinese (traditional).wnry

<ransomware directory>\msg\m_croatian.wnry

<ransomware directory>\msg\m_czech.wnry

<ransomware directory>\msg\m_danish.wnry

<ransomware directory>\msg\m_dutch.wnry

<ransomware directory>\msg\m_english.wnry

<ransomware directory>\msg\m_filipino.wnry

<ransomware directory>\msg\m_finnish.wnry

<ransomware directory>\msg\m_french.wnry

<ransomware directory>\msg\m_german.wnry

<ransomware directory>\msg\m_greek.wnry

<ransomware directory>\msg\m_greek.wnry

<ransomware directory>\msg\m_indonesian.wnry

<ransomware directory>\msg\m_italian.wnry

<ransomware directory>\msg\m_japanese.wnry

<ransomware directory>\msg\m_korean.wnry

<ransomware directory>\msg\m_latvian.wnry

<ransomware directory>\msg\m_norwegian.wnry

<ransomware directory>\msg\m_polish.wnry

<ransomware directory>\msg\m_portuguese.wnry

<ransomware directory>\msg\m_romanian.wnry

<ransomware directory>\msg\m_russian.wnry

<ransomware directory>\msg\m_slovak.wnry

<ransomware directory>\msg\m_spanish.wnry

<ransomware directory>\msg\m_swedish.wnry

<ransomware directory>\msg\m_turkish.wnry

<ransomware directory>\msg\m_vietnamese.wnry

<ransomware directory>\r.wnry

<ransomware directory>\s.wnry

<ransomware directory>\t.wnry

<ransomware directory>\TaskData\Tor\libeay32.dll

<ransomware directory>\TaskData\Tor\libevent-2-0-5.dll

<ransomware directory>\TaskData\Tor\libevent_core-2-0-5.dll

<ransomware directory>\TaskData\Tor\libevent_extra-2-0-5.dll

<ransomware directory>\TaskData\Tor\libgcc_s_sjlj-1.dll

<ransomware directory>\TaskData\Tor\libssp-0.dll

<ransomware directory>\TaskData\Tor\ssleay32.dll

<ransomware directory>\TaskData\Tor\taskhsvc.exe

<ransomware directory>\TaskData\Tor\tor.exe

<ransomware directory>\TaskData\Tor\zlib1.dll

<ransomware directory>\taskdl.exe

<ransomware directory>\taskse.exe

<ransomware directory>\u.wnry

C:\@WanaDecryptor@.exe

Индикаторы компрометации по обращениям к узлам Интернет и TOR

Ниже перечислены индикаторы, позволяющие определить активность вредоноса в системе по обращениям к ресурсам сетей Интернет и TOR. Следует обратить внимание, что последние представленные адреса не следует добавлять в черные списки. Данные URL используются для аварийного отключения вредоноса (при установке в систему в первых версиях вредоносная программа проверяла доступность указанного узла и, если он доступен, не заражала систему).

- 197.231.221.221:9001
- 128.31.0.39:9191
- 149.202.160.69:9001
- 46.101.166.19:9090
- 91.121.65.179:9001
- 2.3.69.209:9001
- 146.0.32.144:9001
- 50.7.161.218:9001
- 217.79.179.177:9001
- 213.61.66.116:9003
- 212.47.232.237:9001
- 81.30.158.223:9001
- 79.172.193.32:443
- 38.229.72.16:443
- Rphjmrpwmfv6v2e[dot]onion
- Gx7ekbenv2riucmf[dot]onion
- 57g7spgrzlojinas[dot]onion
- xxlvbrloxvriy2c5[dot]onion
- 76jdd2ir2embyv47[dot]onion
- cwwnhwhlz52maqm7[dot]onion
- iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com (sinkholed)
- ifferfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com (sinkholed)

Индикаторы компрометации новых версий вредоноса

На текущий момент обнаружено множество новых версий данного вредоноса. Некоторые образцы индикаторов компрометации представлены ниже.

Первый экземпляр

MD5	D724D8CC6420F06E8A48752F0DA11C66
SHA2	07C44729E2C570B37DB695323249474831F5861D45318BF49CCF5D2F5C8EA1CD

Второй экземпляр

MD5	DB349B97C37D22F5EA1D1841E3C89EB4
SHA2	24D004A104D4D54034DBCFFC2A4B19A11F39008A575AA614EA04703480B1022C

Третий экземпляр

MD5	D724D8CC6420F06E8A48752F0DA11C66
SHA2	07C44729E2C570B37DB695323249474831F5861D45318BF49CCF5D2F5C8EA1CD

Для получения более полного перечня актуальных индикаторов компрометации можно воспользоваться публичными источниками threat intelligence.

Рекомендации

1. Ограничить доступ к портам TCP 139/445 на граничных брандмауэрах и провести внешнее сканирование всех корпоративных публичных диапазонов IP-адресов на предмет их наличия.
2. Установить обновление MS17-010 на серверы/АРМ.
3. Отключить поддержку устаревшего протокола SMBv1.
4. Блокировать какие-либо коммуникации с узлами TOR-сетей на граничных брандмауэрах.
5. Существуют отчеты, в которых отражено, что первичное заражение происходило при помощи рассылки вредоносных документов по электронной почте. В случае невозможности митигирования рисков в короткий срок (обширная инфраструктура и пр.) следует рассмотреть подход по временному отключению возможностей использования пересылки файлов в почтовых сообщениях.

Нужна помощь? asksecurity@kpmg.ru

Наша команда в России – это специалисты мирового уровня, обладающие такими сертификатами, как CISA, CISM, CISSP, C|EH, OSCP, CRISC, ISO 27001 LA (a). У нас есть возможность сочетать локальный опыт с лучшей международной практикой, привлекая наших коллег – экспертов КПМГ по защите информации и кибербезопасности во всем мире. Мы комплексно подходим к решению вопросов информационной безопасности, уделяя внимание как организационным, так и техническим аспектам.

kpmg.ru/cyber

Download on the App Store

kpmg.com/app