

WannaCrypt ransomware worm targets out-of-date systems

microsoft.com/security/blog/2017/05/12/wannacrypt-ransomware-worm-targets-out-of-date-systems/

May 13, 2017

On May 12, 2017 we detected a new ransomware that spreads like a worm by leveraging vulnerabilities that have been previously fixed. While security updates are automatically applied in most computers, some users and enterprises may delay deployment of patches. Unfortunately, the ransomware, known as [WannaCrypt](#), appears to have affected computers that have not applied the patch for these vulnerabilities. While the attack is unfolding, we remind users to install [MS17-010](#) if they have not already done so.

The trend towards increasingly sophisticated malware behavior, highlighted by the use of exploits and other attack vectors, makes older platforms so much more susceptible to ransomware attacks. From June to November 2017, Windows 7 devices were 3.4 times more likely to encounter ransomware compared to Windows 10 devices.

Read our latest report: [A worthy upgrade: Next-gen security on Windows 10 proves resilient against ransomware outbreaks in 2017](#)

Microsoft antimalware telemetry immediately picked up signs of this campaign. Our expert systems gave us visibility and context into this new attack as it happened, allowing [Windows Defender Advanced Threat Protection \(ATP\)](#) to deliver real-time defense. Through automated analysis, machine learning, and predictive modeling, we were able to rapidly protect against this malware.

In this blog, we provide an early analysis of the end-to-end ransomware attack. Please note this threat is still under investigation. The attack is still active, and there is a possibility that the attacker will attempt to react to our detection response.

To test how Windows Defender ATP can help your organization detect, investigate, and respond to advanced attacks, [sign up for a free trial](#).

Attack vector

Ransomware threats do not typically spread rapidly. Threats like WannaCrypt (also known as WannaCry, WanaCrypt0r, WCRypt, or WCRY) usually leverage social engineering or email as primary attack vector, relying on users downloading and executing a malicious payload. However, in this unique case, the ransomware perpetrators used publicly available exploit code for the patched SMB “[EternalBlue](#)” vulnerability, [CVE-2017-0145](#), which can be triggered by sending a specially crafted packet to a targeted SMBv1 server. This vulnerability was fixed in security bulletin [MS17-010](#), which was released on March 14, 2017.

WannaCrypt’s spreading mechanism is borrowed from [well-known public SMB exploits](#), which armed this regular ransomware with worm-like functionalities, creating an entry vector for machines still unpatched even after the fix had become available.

The exploit code used by WannaCrypt was designed to work only against unpatched Windows 7 and Windows Server 2008 (or earlier OS) systems, so [Windows 10 PCs are not affected by this attack](#).

We haven’t found evidence of the exact initial entry vector used by this threat, but there are two scenarios that we believe are highly possible explanations for the spread of this ransomware:

- Arrival through social engineering emails designed to trick users to run the malware and activate the worm-spreading functionality with the SMB exploit
- Infection through SMB exploit when an unpatched computer is addressable from other infected machines

Dropper

The threat arrives as a dropper Trojan that has the following two components:

1. A component that attempts to exploit the SMB CVE-2017-0145 vulnerability in other computers
2. The ransomware known as WannaCrypt

The dropper tries to connect the following domains using the API `InternetOpenUrlA()`:

- `www[.]iuqerfsodp9ifjaposdfjhgosurijfaewrwegwea[.]com`
- `www[.]jifferfsodp9ifjaposdfjhgosurijfaewrwegwea[.]com`
- `www[x].iuqerfsodp9ifjaposdfjhgosurijfaewrwegwea[.]test`

If connection to the domains is successful, the dropper does not infect the system further with ransomware or try to exploit other systems to spread; it simply stops execution. However, if the connection fails, the threat proceeds to drop the ransomware and creates a service on the system.

In other words, unlike in most malware infections, **IT Administrators should NOT block these domains**. Note that the malware is not proxy-aware, so a local DNS record may be required. This does not need to point to the Internet, but can resolve to any accessible server which will accept connections on TCP 80.

```
mov     esi, eax
push    0           ; lpszHeaders
push    ecx         ; http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwegwea.com
push    esi         ; hInternet
call    ds:InternetOpenUrlA
mov     edi, eax
push    esi         ; hInternet
mov     esi, ds:InternetCloseHandle
test    edi, edi
jnz     short exit
call    esi ; InternetCloseHandle
push    0           ; hInternet
call    esi ; InternetCloseHandle
call    dropper_main
pop     edi
xor     eax, eax
pop     esi
add     esp, 50h
retn   10h

; -----
exit:
call    esi ; InternetCloseHandle ; CODE XREF: WinMain(x,x,x,x)+65↑j
push    edi         ; hInternet
call    esi ; InternetCloseHandle
```

The threat creates a service named `mssecsvc2.0`, whose function is to exploit the SMB vulnerability in other computers accessible from the infected system:

Service Name: mssecsvc2.0

Service Description: (Microsoft Security Center (2.0) Service)

Service Parameters: "-m security"

```

push    offset Format    ; "%s -m security"
push    eax              ; Dest
call    ds:sprintf
add     esp, 0Ch
push    0F003Fh          ; dwDesiredAccess
push    0                ; lpDatabaseName
push    0                ; lpMachineName
call    ds:OpenSCManagerA
mov     edi, eax
test    edi, edi
jz     short loc_407CCA
push    ebx
push    esi
push    0                ; lpPassword
push    0                ; lpServiceStartName
push    0                ; lpDependencies
push    0                ; lpdwTagId
lea    ecx, [esp+120h+Dest]
push    0                ; lpLoadOrderGroup
push    ecx              ; lpBinaryPathName
push    1                ; dwErrorControl
push    2                ; dwStartType
push    10h              ; dwServiceType
push    0F01FFh         ; dwDesiredAccess
push    offset DisplayName ; "Microsoft Security Center (2.0) Service"
push    offset ServiceName ; "msseccsvc2.0"
push    edi              ; hSCManager
call    ds:CreateServiceA
mov     ebx, ds:CloseServiceHandle
mov     esi, eax

```

WannaCrypt ransomware

The ransomware component is a dropper that contains a password-protected .zip archive in its resource section. The document encryption routine and the files in the .zip archive contain support tools, a decryption tool, and the ransom message. In the samples we analyzed, the password for the .zip archive is "WNCry@2o17".

When run, WannaCrypt creates the following registry keys:

- `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\<random string> = "<malware working directory>\tasksche.exe"`
- `HKLM\SOFTWARE\WanaCrypt0r\lwd = "<malware working directory>"`

It changes the wallpaper to a ransom message by modifying the following registry key:

`HKCU\Control Panel\Desktop\Wallpaper: "<malware working directory>\@WanaDecryptor@.bmp"`

It creates the following files in the malware's working directory:

- `00000000.eky`
- `00000000.pky`
- `00000000.res`
- `274901494632976.bat`
- `@Please_Read_Me@.txt`
- `@WanaDecryptor@.bmp`
- `@WanaDecryptor@.exe`
- `b.wnry`
- `c.wnry`
- `f.wnry`
- `m.vbs`
- `msg\m_bulgarian.wnry`

- *msg\m_chinese (simplified).wnry*
- *msg\m_chinese (traditional).wnry*
- *msg\m_croatian.wnry*
- *msg\m_czech.wnry*
- *msg\m_danish.wnry*
- *msg\m_dutch.wnry*
- *msg\m_english.wnry*
- *msg\m_filipino.wnry*
- *msg\m_finnish.wnry*
- *msg\m_french.wnry*
- *msg\m_german.wnry*
- *msg\m_greek.wnry*
- *msg\m_indonesian.wnry*
- *msg\m_italian.wnry*
- *msg\m_japanese.wnry*
- *msg\m_korean.wnry*
- *msg\m_latvian.wnry*
- *msg\m_norwegian.wnry*
- *msg\m_polish.wnry*
- *msg\m_portuguese.wnry*
- *msg\m_romanian.wnry*
- *msg\m_russian.wnry*
- *msg\m_slovak.wnry*
- *msg\m_spanish.wnry*
- *msg\m_swedish.wnry*
- *msg\m_turkish.wnry*
- *msg\m_vietnamese.wnry*
- *r.wnry*
- *s.wnry*
- *t.wnry*
- *TaskData\Tor\libeay32.dll*
- *TaskData\Tor\libevent-2-0-5.dll*
- *TaskData\Tor\libevent_core-2-0-5.dll*
- *TaskData\Tor\libevent_extra-2-0-5.dll*
- *TaskData\Tor\libgcc_s_sjlj-1.dll*
- *TaskData\Tor\libssp-0.dll*
- *TaskData\Tor\ssleay32.dll*
- *TaskData\Tor\taskhsvc.exe*
- *TaskData\Tor\tor.exe*
- *TaskData\Tor\zlib1.dll*
- *taskdl.exe*
- *taskse.exe*
- *u.wnry*

WannaCrypt may also create the following files:

- *%SystemRoot%\tasksche.exe*
- *%SystemDrive%\intel\<random directory name>\tasksche.exe*
- *%ProgramData%\<random directory name>\tasksche.exe*

It may create a randomly named service that has the following associated ImagePath: *"cmd.exe /c "<malware working directory>\tasksche.exe"*.

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

WannaCrypt encrypts all files it finds and renames them by appending .WNCRY to the file name. For example, if a file is named *picture.jpg*, the ransomware encrypts and renames the file to *picture.jpg.WNCRY*.

This ransomware also creates the file *@Please_Read_Me@.txt* in every folder where files are encrypted. The file contains the same ransom message shown in the replaced wallpaper image (see screenshot below).

After completing the encryption process, the malware deletes the volume shadow copies by running the following command:

```
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
```

It then replaces the desktop background image with the following message:

Oops, your important files are encrypted.

If you see this text, but don't see the "Wana Decrypt0r" window, then your antivirus removed the decrypt software or you deleted it from your computer.

If you need your files you have to run the decrypt software.

Please find an application file named "@WanaDecryptor@.exe" in any folder or restore from the antivirus quarantine.

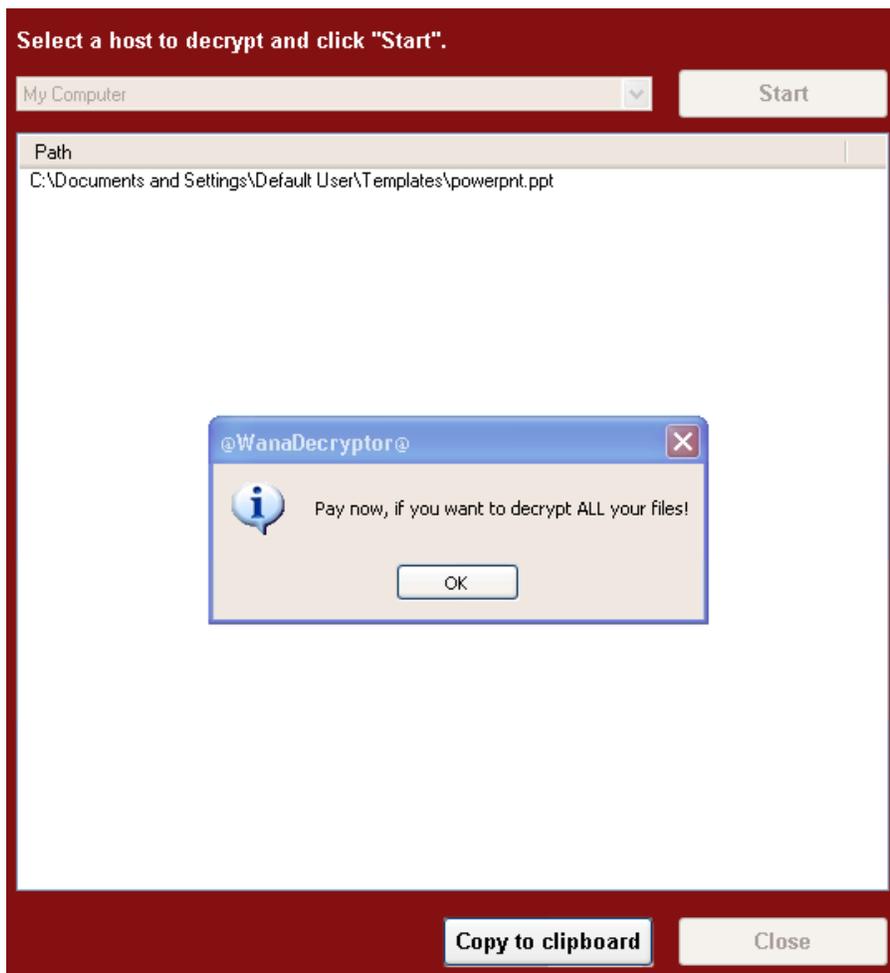
Run and follow the instructions!

It also runs an executable showing a ransom note which indicates a \$300 ransom in Bitcoins as well as a timer:

The screenshot shows a ransomware interface with a dark red background. At the top, a title bar reads "Ooops, your files have been encrypted!" with a language dropdown set to "English". On the left, there is a large white padlock icon. Below it, two boxes indicate payment deadlines: "Payment will be raised on 5/15/2017 16:50:06" with a timer at "02:23:34:22", and "Your files will be lost on 5/19/2017 16:50:06" with a timer at "06:23:34:22". The main content area contains several sections: "What Happened to My Computer?" explaining file encryption; "Can I Recover My Files?" offering a free decryption trial and a 3-day payment deadline; and "How Do I Pay?" detailing Bitcoin payment instructions. At the bottom, there is a Bitcoin logo with "ACCEPTED HERE", a text box containing the address "115p7UMMngoj1pMvkpHjicRdfJNXj6LrLn" with a "Copy" button, and two buttons labeled "Check Payment" and "Decrypt".

The text is localized into the following languages: Bulgarian, Chinese (simplified), Chinese (traditional), Croatian, Czech, Danish, Dutch, English, Filipino, Finnish, French, German, Greek, Indonesian, Italian, Japanese, Korean, Latvian, Norwegian, Polish, Portuguese, Romanian, Russian, Slovak, Spanish, Swedish, Turkish, and Vietnamese.

The ransomware also demonstrates the decryption capability by allowing the user to decrypt a few random files, free of charge. It then quickly reminds the user to pay the ransom to decrypt all the remaining files.



Spreading capability

The worm functionality attempts to infect unpatched Windows machines in the local network. At the same time, it also executes massive scanning on Internet IP addresses to find and infect other vulnerable computers. This activity results in large SMB traffic from the infected host, which can be observed by SecOps personnel, as shown below.

The screenshot displays a network traffic analysis interface. The top section shows hex data with corresponding ASCII characters. A red box highlights a sequence of IP addresses: .157.11, .157.12, and .157.13. Below this, a table lists captured packets. A red box highlights the destination IP addresses in the table, which match the highlighted sequence. The bottom section shows the details of a selected packet, highlighting the destination port 445.

No.	Time	Source	Destination	Protocol
200618	217.566696		.157.11	TCP
202094	218.633911		.157.12	TCP
203140	219.441199		.157.12	TCP
203455	219.695544		.157.13	TCP
204356	220.488082		.157.13	TCP
204779	220.800093		.157.14	TCP
206453	221.883475		.157.15	TCP

Packet details for Transmission Control Protocol (TCP):
 Source Port: 50041
 Destination Port: 445

The Internet scanning routine randomly generates octets to form the IPv4 address. The malware then targets that IP to attempt to exploit CVE-2017-0145. The threat avoids infecting the IPv4 address if the randomly generated value for first octet is 127 or if the value is equal to or greater than 224, in order to skip local loopback interfaces. Once a vulnerable machine is found and infected, it becomes the next hop to infect other machines. The vicious infection cycle continues as the scanning routing discovers unpatched computers.

When it successfully infects a vulnerable computer, the malware runs kernel-level shellcode that seems to have been copied from the public backdoor known as DOUBLEPULSAR, but with certain adjustments to drop and execute the ransomware dropper payload, both for x86 and x64 systems.

```

    cmp     [esp+128h+var_0], 20h
    jge    short loc_407908
    call   Rand_cryptgen_random_number_for_ip_selection ; Crypt CrSec
    xor    edx, edx
    mov    ecx, 0FFh
    div    ecx
    mov    [esp+128h+var_110], edx

loc_407908:
    ; CODE XREF: Ws2_thread2+AA↑j
    ; Ws2_thread2+B4↑j
    call   Rand_cryptgen_random_number_for_ip_selection ; Crypt CrSec
    xor    edx, edx
    mov    ecx, 0FFh
    div    ecx
    mov    ebx, edx
    call   Rand_cryptgen_random_number_for_ip_selection ; Crypt CrSec
    xor    edx, edx
    mov    ecx, 0FFh
    div    ecx
    lea   eax, [esp+128h+Dest]
    push  edx
    mov   edx, [esp+12Ch+var_110]
    push  ebx
    push  edx
    push  ebp
    push  offset IP_address_string_format ; "%d.%d.%d.%d"
    push  eax ; Dest
    call  ds:sprintf
    add   esp, 18h
    lea   ecx, [esp+128h+Dest]
    push  ecx ; cp
    call  inet_addr
    push  eax

```

```

call   Rand_cryptgen_random_number_for_ip_selection ;
xor    edx, edx
mov    ecx, 0FFh
div    ecx
mov    ebp, edx
cmp    ebp, 127
jz     short try_next_random_number
cmp    ebp, 224
jge    short try_next_random_number

```

Protection against the WannaCrypt attack

To get the latest protection from Microsoft, upgrade to [Windows 10](#). Keeping your computers up-to-date gives you the benefits of the latest features and proactive mitigations built into the latest versions of Windows.

We recommend customers that have not yet installed the security update [MS17-010](#) do so as soon as possible. Until you can apply the patch, we also recommend two possible workarounds to reduce the attack surface:

- Disable SMBv1 with the steps documented at [Microsoft Knowledge Base Article 2696547](#) and as [recommended previously](#).
- Consider adding a rule on your router or firewall to block incoming SMB traffic on port 445

[Windows Defender Antivirus](#) detects this threat as [Ransom:Win32/WannaCrypt](#) as of the 1.243.297.0 update. Windows Defender Antivirus uses cloud-based protection, helping to protect you from the latest threats.

For enterprises, use [Device Guard](#) to lock down devices and provide kernel-level virtualization-based security, allowing only trusted applications to run, effectively preventing malware from running.

Use [Office 365 Advanced Threat Protection](#), which has machine learning capability that blocks dangerous email threats, such as the emails carrying ransomware.

Monitor networks with [Windows Defender Advanced Threat Protection](#), which alerts security operations teams about suspicious activities.

To test how Windows Defender ATP can help your organization detect, investigate, and respond to advanced attacks, [sign up for a free trial](#).

Resources

Download English language security updates: [Windows Server 2003 SP2 x64](#), [Windows Server 2003 SP2 x86](#), [Windows XP SP2 x64](#), [Windows XP SP3 x86](#), [Windows XP Embedded SP3 x86](#), [Windows 8 x86](#), [Windows 8 x64](#)

Download localized language security updates: [Windows Server 2003 SP2 x64](#), [Windows Server 2003 SP2 x86](#), [Windows XP SP2 x64](#), [Windows XP SP3 x86](#), [Windows XP Embedded SP3 x86](#), [Windows 8 x86](#), [Windows 8 x64](#)

MS17-010 Security Update: <https://technet.microsoft.com/en-us/library/security/ms17-010.aspx>

Customer guidance for WannaCrypt attacks: <https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/>

General information on ransomware: <https://www.microsoft.com/en-us/security/portal/mmpc/shared/ransomware.aspx>

Next-generation ransomware protection with Windows 10 Creators Update: <https://blogs.technet.microsoft.com/mmpc/2017/06/08/windows-10-creators-update-hardens-security-with-next-gen-defense/>

Indicators of compromise

SHA1 of samples analyzed:

- 51e4307093f8ca8854359c0ac882ddca427a813c
- e889544aff85ffaf8b0d0da705105dee7c97fe26

Files created:

- %SystemRoot%\mssecsvc.exe
- %SystemRoot%\tasksche.exe
- %SystemRoot%\qeriuwjhrf
- b.wnry
- c.wnry
- f.wnry
- r.wnry
- s.wnry
- t.wnry
- u.wnry
- taskdl.exe
- taskse.exe
- 00000000.eky
- 00000000.res
- 00000000.pky
- @WanaDecryptor@.exe
- @Please_Read_Me@.txt
- m.vbs
- @WanaDecryptor@.exe.lnk

- @WanaDecryptor@.bmp
- 274901494632976.bat
- taskdl.exe
- Taskse.exe
- Files with “.wnry” extension
- Files with “.WNCRY” extension

Registry keys created:

HKLM\SOFTWARE\WanaCrypt0r\wd

*Karthik Selvaraj, Elia Florio, Andrea Lelli, and Tanmay Ganacharya (@tanmayg)
Microsoft Malware Protection Center (@msftmpc)*

Related blog entries:

[Windows 10 Creators Update provides next-gen ransomware protection](#)

[Analysis of the ETERNALBLUE and ETERNALROMANCE exploits leaked by Shadow Brokers](#)

Updates:

June 20, 2017 – added reference to analysis of exploits leaked by Shadow Brokers



Talk to us

Questions, concerns, or insights on this story? Join discussions at the [Microsoft community](#) and [Windows Defender Security Intelligence](#).