wannacrypt ransomware worm targets out-of-date systems

Autor:
Data de publicació: 13-10-2023

YSTEMS

?????

????

???

??

?

msft-mmpc May 12, 2017 48

911
1588

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.

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 Antivirus 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.

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:

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

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

www[.]iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com
www[.]ifferfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com

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.

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”

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@2ol7”.

When run, WannaCrypt creates the following registry keys:

HKLMSOFTWAREMicrosoftWindowsCurrentVersionRun<random string> = “<malware working directory>tasksche.exe”
HKLMSOFTWAREWanaCrypt0rwd = “<malware working directory>”

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

HKCUControl PanelDesktopWallpaper: “<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
msgm_bulgarian.wnry
msgm_chinese (simplified).wnry
msgm_chinese (traditional).wnry
msgm_croatian.wnry
msgm_czech.wnry
msgm_danish.wnry
msgm_dutch.wnry
msgm_english.wnry
msgm_filipino.wnry
msgm_finnish.wnry
msgm_french.wnry
msgm_german.wnry
msgm_greek.wnry
msgm_indonesian.wnry
msgm_italian.wnry
msgm_japanese.wnry
msgm_korean.wnry
msgm_latvian.wnry
msgm_norwegian.wnry
msgm_polish.wnry
msgm_portuguese.wnry
msgm_romanian.wnry
msgm_russian.wnry
msgm_slovak.wnry
msgm_spanish.wnry
msgm_swedish.wnry
msgm_turkish.wnry
msgm_vietnamese.wnry
r.wnry
s.wnry
t.wnry
TaskDataTorlibeay32.dll
TaskDataTorlibevent-2-0-5.dll
TaskDataTorlibevent_core-2-0-5.dll
TaskDataTorlibevent_extra-2-0-5.dll

TaskDataTorlibgcc_s_sjlj-1.dll
TaskDataTorlibssp-0.dll
TaskDataTorssleay32.dll
TaskDataTortaskhsvc.exe
TaskDataTortor.exe
TaskDataTorzlib1.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 , .xltm , .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:

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

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 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.

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. Download this playbook to see how you can leverage Windows Defender ATP to detect, investigate, and mitigate ransomware in networks: Windows Defender Advanced Threat Protection – Ransomware response playbook.

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

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:

HKLMSOFTWAREWanaCrypt0rwd

Karthik Selvaraj, Elia Florio, Andrea Lelli, and Tanmay Ganacharya
Microsoft Malware Protection Center

Tags exploit ransomware SMB EternalBlue vulnerability WanaCrypt0r WannaCry WannaCrypt WCRY WCrypt Windows Defender Antivirus worm

Comments (48)

Name *

Email *

Website

Bob B.

May 13, 2017 at 06:38

Thanks for this very informative write-up. A couple of questions that I have:
1. The computers I manage are set up so that the users always operate as a standard user. They do not have the ability to elevate to administrator. For this specific malware, would operating as a standard user prevent either the encryption part or the worm part from functioning?

2. I also have all web traffic directed thru a web proxy. Would a web proxy prevent this malware from functioning? The write-up only mentions one URL that is contacted, and that one, if successfully reached, PREVENTS the encryption from taking place. That seems like an unusual arrangement. Other ransomware contacts a host to download a unique encryption key, and if unsuccessful, cannot encrypt the user's files. So if the malware is not able to find and use the web proxy, this would mitigate the effects. Does a web proxy mitigate the effects of WannaCrypt?

Reply

msft-mmpc

May 14, 2017 at 23:31

Hi, Bob.
1. No, it would not. Due to the nature of the vulnerability being exploited, the worm mechanism will work even if the user is not signed in. The best solution is to patch.
2. 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.

Reply

Robert Carleton

May 13, 2017 at 06:53

I've tried many ways to get an answer to the question: "Has my p.c. downloaded the protection against "Wanna Decrypt0r 2.0??" and I get nothing in return except extended technical discussions that are way beyond anything I can even imagine. Why not provide a simple answer in a really easy-to-locate place?

Reply

P. S.

May 15, 2017 at 05:42

Hi Robert, this technical post is mostly directed at system administrators. The easy advise is to make sure your system is as up-to-date as possible and to install security patches when they become available.
A hopefully easier article can be found on https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/#sm.00017eeq5n109mcufsatfm76hcu3l and also the article on https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/ is easier than this one.

Reply

Tim Miller Dyck

May 13, 2017 at 07:19

Can you address attack effectiveness against Windows Server 2008 R2? This statement in the blog post is ambiguous if it refers to Windows Server 2008 R1 only. "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."

Reply

msft-mmpc

May 14, 2017 at 23:33

Hi, Tim. You can refer to Microsoft Security Bulletin MS17-010 (https://technet.microsoft.com/en-us/library/security/ms17-010.aspx) for the list of affected software.

Reply

Nik

May 15, 2017 at 06:35

To be honest, the reference to MS17-010 is confusing at best in my opinion. It lists all MS OSes up to Windows Server 2016 as critically vulnerable to CVE-2017-0145, but the vulnerability itself as not exploited. Would you please clarify/correct this (including an explanation for what's the difference between 2008/7 and 2012/8/10 with regard to CVE-2017-0145) and also answer Tim's question whether Server 2008 R2 is affected or not. Thanks!

Reply

mahelsay

May 13, 2017 at 07:49

Thanks for this good article. bottom line is patch magmt is critical to any organization!.
thanks also for the steps mentioned

Reply

John F Kohler

May 13, 2017 at 08:01

May I view the Windows7 patches that have downloaded and installed in my Dell desktop PC?

Reply

durgesh7(MCTS, MCP)

May 14, 2017 at 18:43

Pls go to Control Panel > Programs and Features > View Installed Updates

Reply

Robert Scroggins

May 13, 2017 at 08:36

Thank you for providing IOCs–especially hashes.

Reply

Stefan Kanthak

May 13, 2017 at 09:15

As always, you forgot Software Restriction Policies, available in ALL editions of Windows since 15+ years.
Use SRP alias SAFER to deny execution of every file unprivileged users can write/create, allow execution only for files installed by an administrator into the safe directories %SystemRoot% and %ProgramFiles%.
See https://skanthak.homepage.t-online.de/SAFER.html
BUT: beware of the loopholes!
See https://skanthak.homepage.t-online.de/appcert.html

Reply

Carlos C.

May 13, 2017 at 13:01

Don’t appear patches for windows-7, from windows update catalog.

Reply

msft-mmpc

May 14, 2017 at 23:33

You can refer to https://support.microsoft.com/en-us/help/4013389/title for further details.

Reply

Michael Koziewicz

May 13, 2017 at 16:40

I just read an AP article that said: “Microsoft took the unusual step late Friday of making free patches available for older Windows systems, such as Windows XP from 2001. Before, Microsoft had made such fixes available only to mostly…” I have a couple of old XP systems in use. If the article is true, how can I down load the patch? Please advise

Reply

durgesh7(MCTS, MCP)

May 14, 2017 at 18:42

here is the microsoft update catalog link to download patch for XP
http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012598

Reply

Khaled

May 13, 2017 at 18:31

that is very helpful but can you guarantee that windows 10 enterprise can’t be affected

Reply

blank

May 13, 2017 at 18:43

To protect yourself, upgrade to Windows 10. This is stupid advice. Tell people to keep their Windows and Antiviruses up to date. Windows 10 sucks and if I could work with it, I would.

Reply

blank2

May 15, 2017 at 04:29

You don’t seem to know what you’re talking about.

Reply

Alexander Thomas

May 13, 2017 at 23:52

Important message to All Computer Systems Administartors

Reply

Raffaele Rialdi

May 14, 2017 at 06:24

Would you launch from a flying airplane just because someone tells you the parachute is on your back?
Or you would rather want to see with your eyes that you really weared it and it is setup correctly?

During an emergency, just running Windows Update on all the machine is not something that I am interested in.
From this kind of articles I would expect a command line to have the *proof* the patch is there!
Hint: the command line is: wmic qfe get hotfixid
Which one should everyone verify?
According to the bullettin there is a different KB for each OS version, this is not good.

Reply

noneofyourbiz

May 14, 2017 at 08:25

I WannaCry… MS massive fail… People HEALTH has been at stake because of YOUR greedy and irresponsible attitude towards legacy systems.

What's more, you KNEW it beforehand as you offered (after a great resistance) to give PAID support to some of the massive organizations that depend on XP… And now you want us to believe you are SOOOOO concerned about our well-being that you FINALLY deploy a patch for something you KNEW about in March?!?!?!?????! What's more, you prove that when you decide to do it it takes just ONE f$%%?&*ing day to do it, why SO LATE?

WOW! Thumbs up, greedy bastards, I can't wait for a world where you simply disappear from the surface of this planet, you are an insult to humanity. Making billions on dollars of profit while evading taxes AND putting the health of human being in danger is simply bad, you know, as in good vs bad as any child on this planet would understand it…

Reply

Ruaim

May 15, 2017 at 01:42

The patch was released back in March. Unfortunately the patch was not deployed in many organizations

Please can you be constructive in your comments next time? Your comment was totally pointless.

Reply

Martin S.

May 15, 2017 at 03:31

@noneofyourbiz — Thank you very much for your valuable comment. What’s wrong? Did someone rattle your cage?

Reply

Download Game Android Apk

May 14, 2017 at 08:25

Is this stuff can attack windows 10 ?

Reply

Jagan Jami

May 14, 2017 at 11:04

Can you suggest steps if already attacked by wannacry ransomware?

Reply

msft-mmpc

May 14, 2017 at 23:36

You can refer to our Ransomware FAQ (https://www.microsoft.com/en-us/security/portal/mmpc/shared/ransomware.aspx) for more info.

Reply

Still Fightingalosingbattle

May 14, 2017 at 12:42

Press reports claim that many users do not update often enough or correctly, yet my 64-bit Windows 7 will NOT update correctly. It does not download or even run Update as it should. Your Update package does not work and I cannot get the various Update remediation fixes to install or work.

Reply

msft-mmpc

May 14, 2017 at 23:37

You can refer to our dedicated Support for Windows 7: https://technet.microsoft.com/en-us/windows/bb187457.aspx

Reply

XP Mode User

May 14, 2017 at 17:17

Like others, I can't tell whether I'm protected. I have a patched WIn 7 system, but running XP Mode in a virtual PC. All my email comes through Outlook Express running under XP Mode.

Am I protected using XP Mode with just a patched Win 7 system?

Reply

msft-mmpc

May 14, 2017 at 23:44

Make sure your virtual PC has all the required patches applied. Refer to the relevant KBs listed: http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012598

Reply

Matthew Maa

May 14, 2017 at 21:20

Technically accurate, yet practically useless. When I get sick, I need a cure. When I am deadly sick, I need a cure fast. When someone tells me all the information how I get affected by the virus and how it break down different part of my body to the cellular level while I am dying, I would like to strangler the messenger.

Reply

Matt S

May 15, 2017 at 05:39

I think you misunderstand the purpose of this particular blog post then.

Reply

Ricko

May 14, 2017 at 22:55

Wow thanks for your time to create this post, this virus is booming in my country and national television talk about it too.

And in my neighbourhood people talk about it, a lot of people look scared, even the old ladies who usually trash talk about celebrity gossip. lol.

But I don't know why, I'm cool, I never dealing with virus since maybe 2004 (at that time internet very expensive and I can't afford it, so my antivirus rarely updated). Now, all of my softwares original, I didn't use pirates software, I'm using paid premium antivirus, windows firewall active. I never open "bad" website, even I only open website using SSL.

Windows 10 auto update, antivirus auto update, so I only need to drink my coffee, working, and forget about that ransomware.

Reply

Bill Gates III

May 15, 2017 at 02:23

Nob

Reply

Alexander

May 15, 2017 at 04:26

Yes, but sometimes users in large environments receive an email from “known” address with malicious code, and then you can imagine hell for the administrators.

Reply

Arpan Thakrar

May 14, 2017 at 23:49

Thanks for this good article. But it’s not true Windows 10 PCs are not affected by this attack. I found Windows 10 is also affected by this attack. Actually it’s more affected than Windows 7 & 8.

Reply

Dasoman

May 15, 2017 at 05:15

It says Windows 10 is not affected by the SMB exploit. It doesn’t say Windows 10 systems can’t be infected by running an infected e-mail attachment.