The WannaCry Malware Attack

Dear all,

This alert is to provide guidance regarding malware variously named WannaCrypt, WannaCry, WannaCryptor, or Wcry. Please share this with your IT and Security teams to ensure they are fully aware, prepared and protecting your organization against the attack.

On May 12, 2017, many of our customers around the world and the critical systems they depend on were victims of malicious "WannaCrypt" software. Microsoft is working to ensure we are taking all possible actions to protect our customers. Below we have given further details of the threat and steps every individual and business should take to stay protected. Additionally, we are taking the highly unusual step of providing a security update for all customers to protect Windows platforms that are in custom support only, including Windows XP, Windows 8, and Windows Server 2003. Customers running Windows 10 were not targeted by the attack today.

In March, we released a security update which addresses the vulnerability that these attacks are exploiting. Unfortunately, the malware 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 constantly monitors for such threats, and alerted us to this attack. These systems gave us the visibility and context around the attach, allowing Windows Defender Antivirus to deliver real-time defense. Through automated analysis, machine learning, and predictive modeling, we were able to protect many up-to-date systems against this malware.

Steps to prevent and protect against this threat

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 (Reboot Required)
- 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. Enable Windows Defender Antivirus to detect this ransomware. Windows Defender Antivirus uses cloud-based protection, helping to protect you from the latest threats.

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

Monitor your network 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.

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.

Below are Frequently Asked Questions to help you further understand the nature of this malware attack, and to answer some of the questions you might have. For more information on support options please visit our support site: https://support.microsoft.com/en-us/gp/support-options-for-business

In case you have any further questions or require any assistance from our side, please do not hesitate to let me know.

Regards,

-------- Add your Signature ----------

Frequently Asked Questions

1. Question: What is WannCrypt Ransomware and How does it attack my environment?
2. Question: How does the virus enter my systems?
3. Question: How does WannaCry takes control over my system?
4. Question: How does the virus spread further into my systems?
5. Question: What are the necessary steps to prevent from the attack?
6. Question: What Microsoft Malware Detection Tools can I use?
7. Question: Where Do I find an additional resources?

Attack vector

A ransomware threat does not normally spread so rapidly. Threats like WannaCrypt typically leverage social engineering or emails as primary attack vector, relying on users downloading and executing a malicious payload. However, in this unique case, the ransomware perpetrators incorporated 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, was fixed in security bulletin MS17-010, 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 in 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 we believe are highly possible for this ransomware family:

- 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 can be addressed in other infected machines

Dropper

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

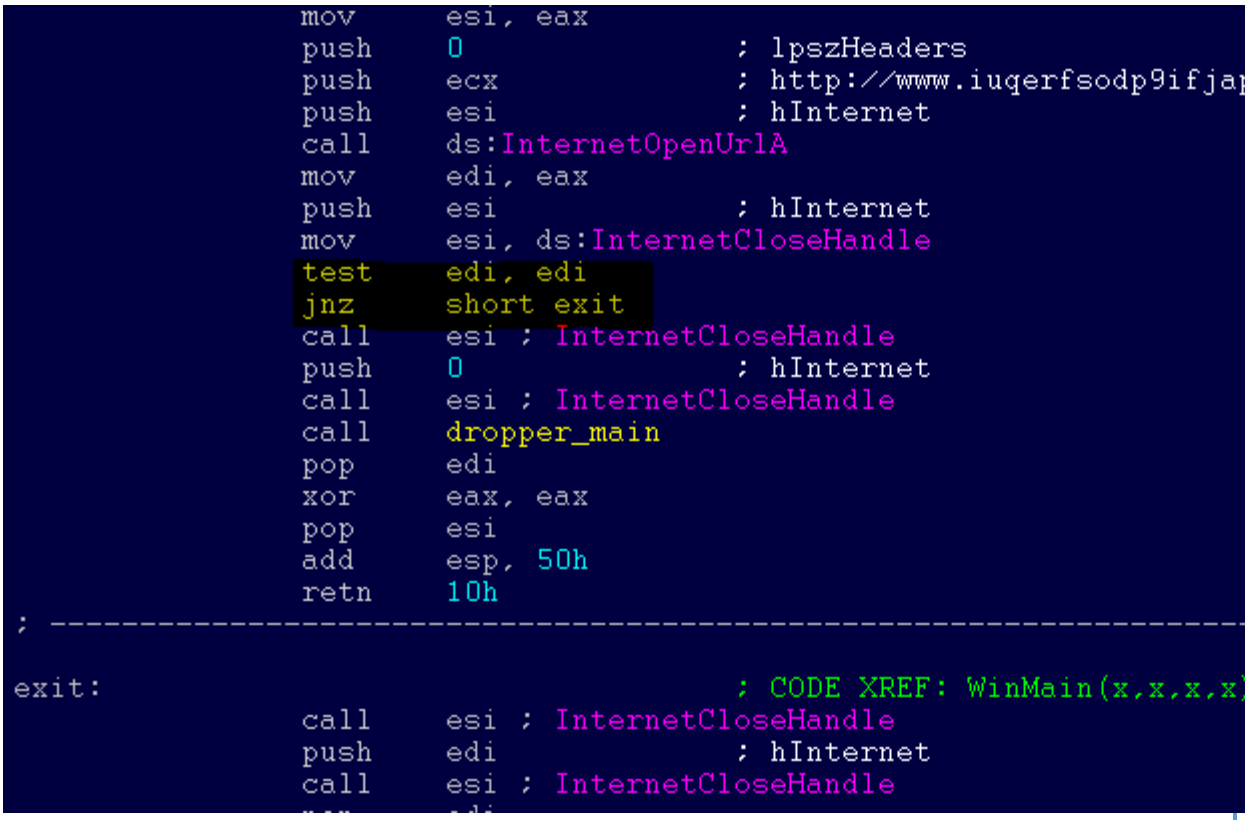
- Ccomponent that tries to exploit the SMB EternalBlue vulnerability in other computers
- Ransomware known as WannaCrypt

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

hxxp://www[.]iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com

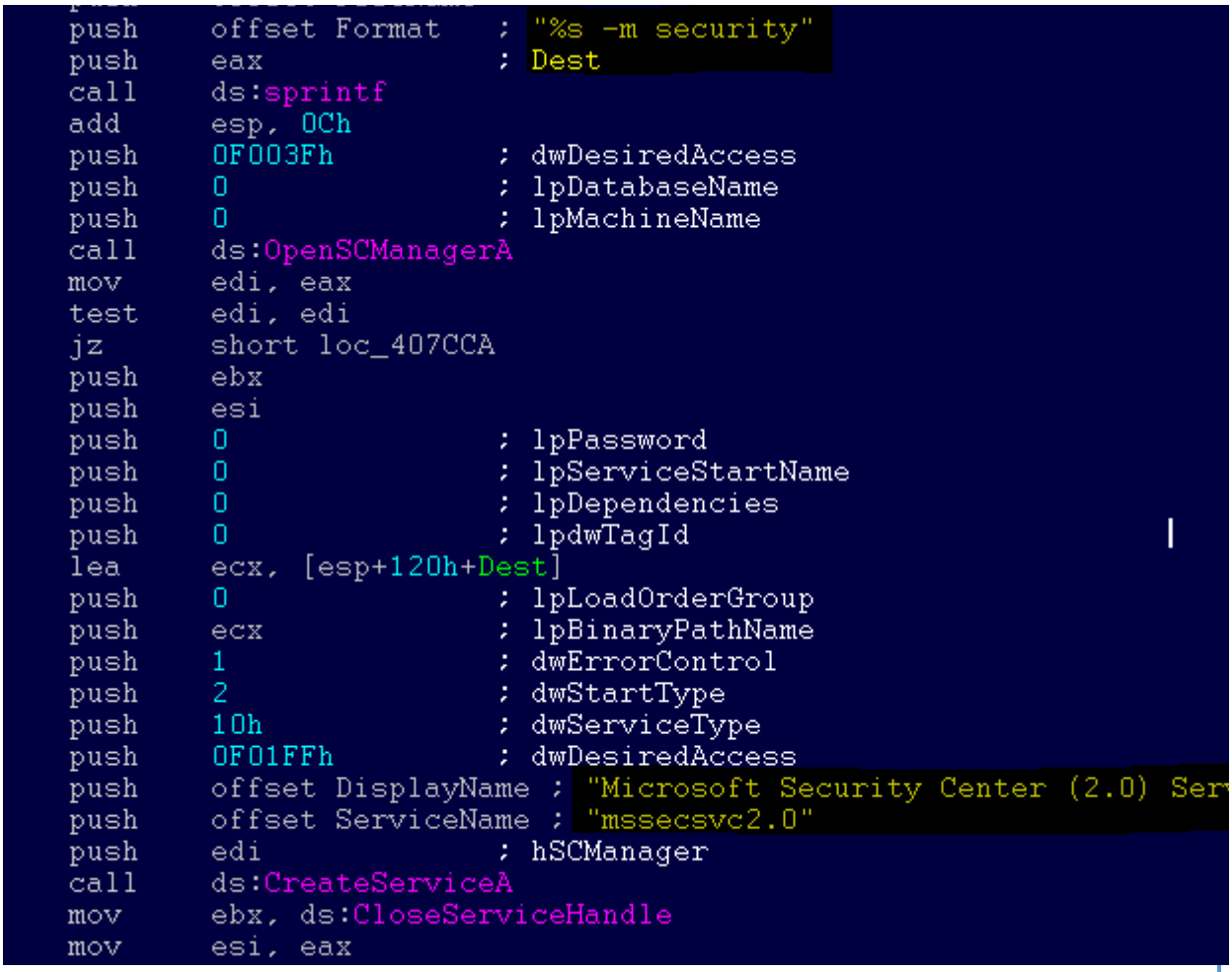
If connection is successful, the threat does not infect the system further with ransomware or try to exploit other systems to spread; it simply stops execution. However, if the connection fails, the dropper proceeds to drop the ransomware and creates a service on the system.

In other words, blocking the domain with firewall either at ISP or enterprise network level will cause the ransomware to continue spreading and encrypting files.



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 archive in its resource section. The document encryption routine and the files in the .zip archivecontain 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:

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

Then it 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

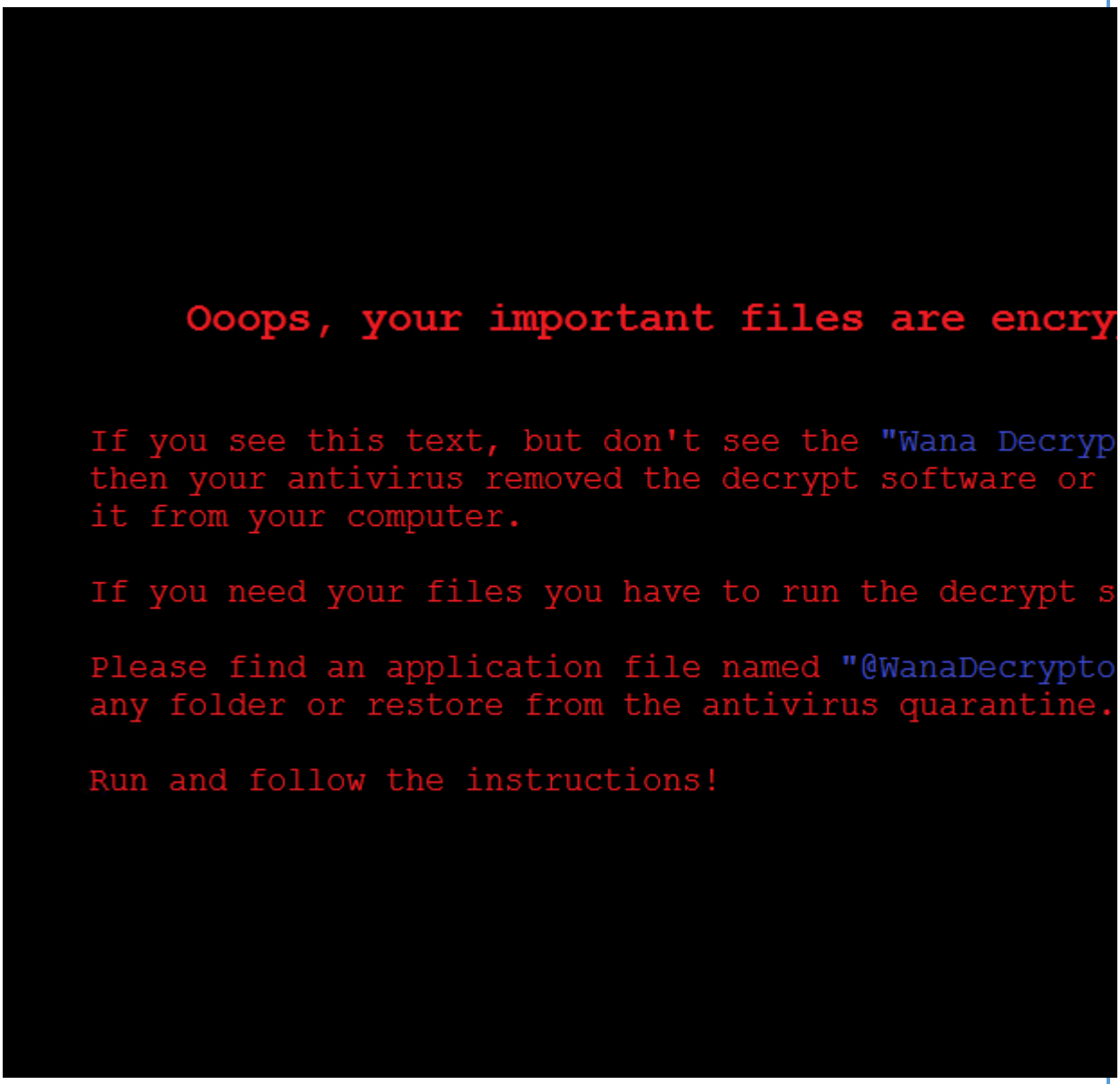
WannaCrypt encrypts all files it finds and renames them by appending ".WNCRY" to the file name. For example, if a file is named "picture.jpg", the ransomware encrypts and renames to "picture.jpg.WNCRY".

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 (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

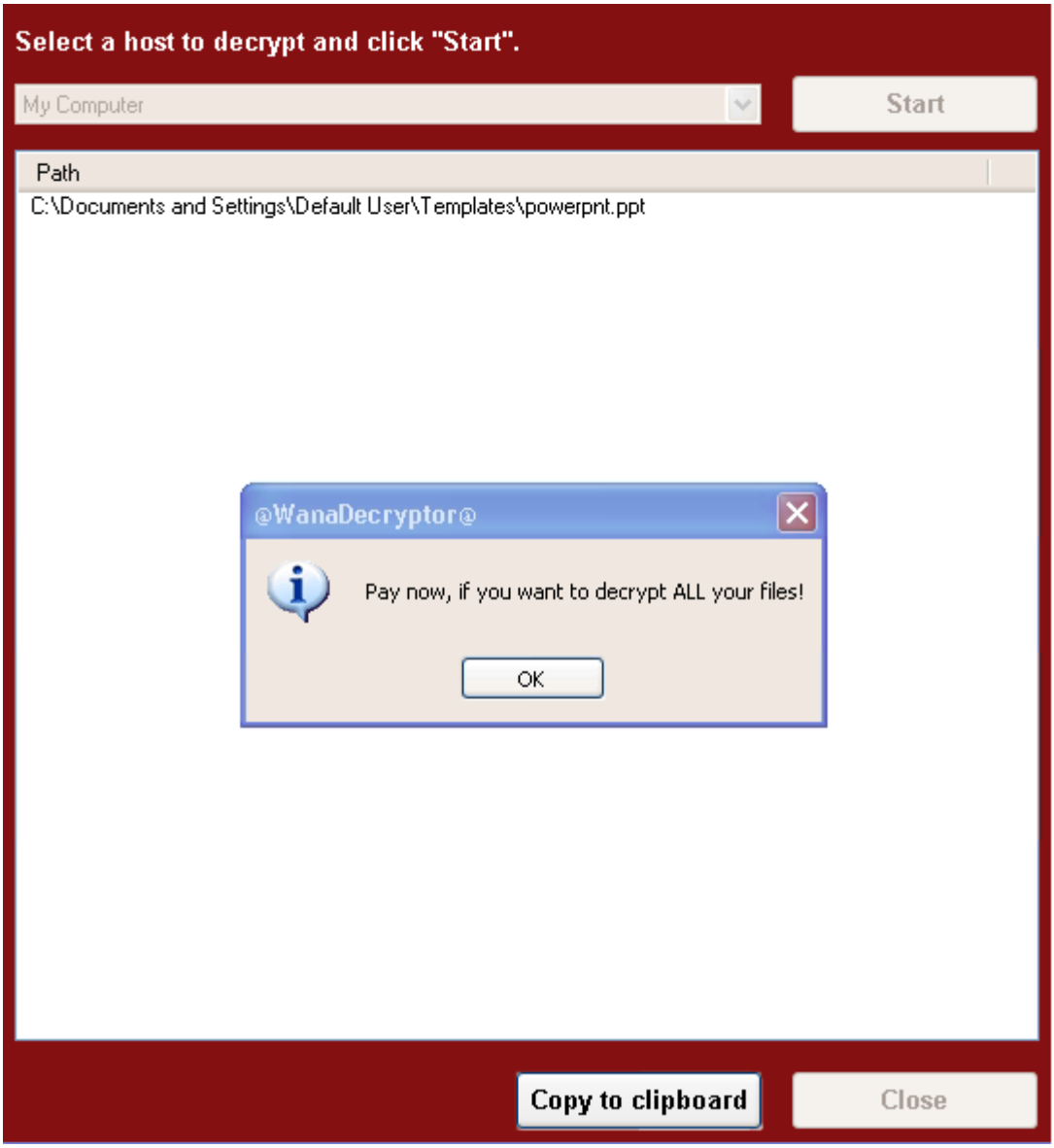
It then replaces the desktop background image with the following message:



It also runs an executable showing a ransom note which indicates a $300 ransom and a timer:

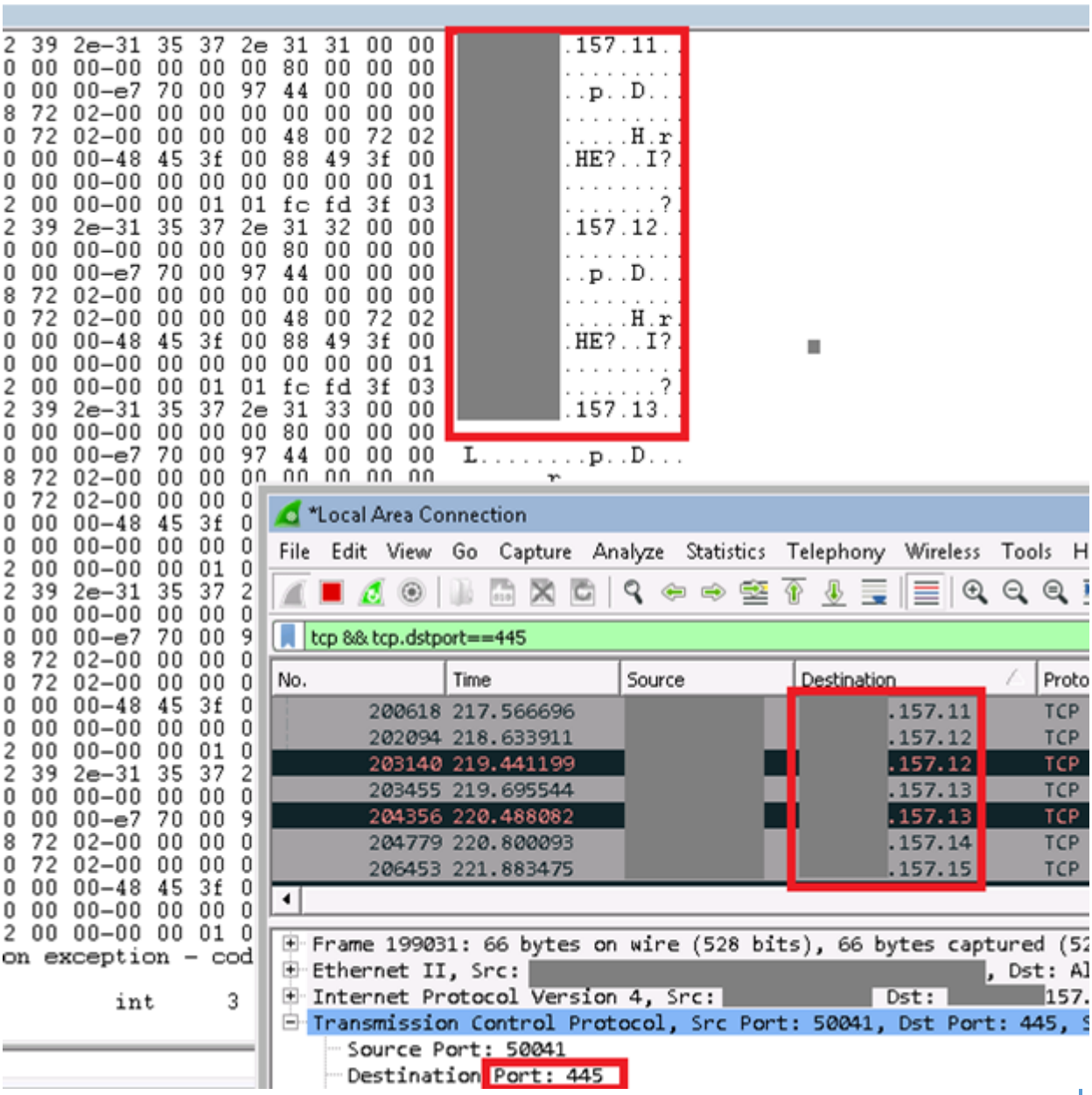
The text is localized into the following languages: Bulgarian, Chinese (simplified), Chinese (traditional), Croatian, Czech, Danish, Dutch, English, Filipino, Finnish, French, German, Greek, Indonesian, Italian, Japanese, Korean, Latvian, Norwegian, Polish, Portuguese, Romanian, Russian, Slovak, Spanish, 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 normally can be observed by SecOps personnel, as shown below.



The Internet scanning routine randomly generates octets to form the IPv4 address and targets that IP to attempt exploitation of 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 which 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+arg_0], 28h
                jge     short loc_407908
                call    Rand_cryptgen_random_number_for_ip_selection
                xor     edx, edx
                mov     ecx, 0FFh
                div     ecx
                mov     [esp+128h+var_110], edx

loc_407908:                             ; CODE XREF: Ws2_thread2+AA↑
                                        ; Ws2_thread2+B4↑j
                call    Rand_cryptgen_random_number_for_ip_selection
                xor     edx, edx
                mov     ecx, 0FFh
                div     ecx
                mov     ebx, edx
                call    Rand_cryptgen_random_number_for_ip_selection
                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.
                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
```

Microsoft Malware Detection and Removal Tools

Use the following free Microsoft tools to detect and remove this threat:

- Windows Defender: https://www.microsoft.com/en-us/windows/windows-defender
- Microsoft Safety Scanner: http://www.microsoft.com/security/scanner/

Additional Resources

- Microsoft Security Response Center Blog: http://blogs.technet.microsoft.com/msrc
- Microsoft Malware Protection Center Blog: http://blogs.technet.microsoft.com/mmpc
- Microsoft Safety and Security Center webpage: http://www.microsoft.com/security/default.aspx