WannaCry ransomware used in widespread attacks all over the world

By GReAT on May 12, 2017. 5:30 pm

INCIDENTS

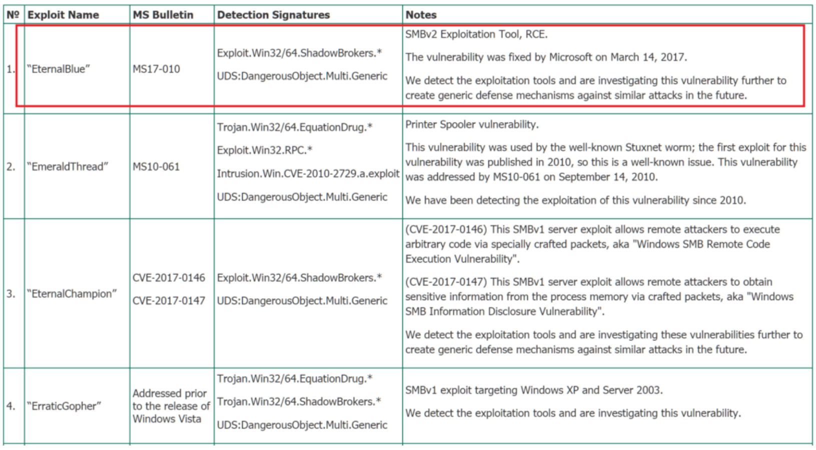
ENCRYPTION MALWARE DESCRIPTIONS RANSOMWARE VULNERABILITIES AND EXPLOITS

GReAT
Kaspersky Lab's Global Research & Analysis Team
@e_kaspersky/great

Earlier today, our products detected and successfully blocked a large number of ransomware attacks around the world. In these attacks, data is encrypted with the extension ".WCRY" added to the filenames.

Our analysis indicates the attack, dubbed "WannaCry", is initiated through an SMBv2 remote code execution in Microsoft Windows. This exploit (codenamed "EternalBlue") has been made available on the internet through the Shadowbrokers dump on April 14th, 2017 and patched by Microsoft on March 14.

Unfortunately, it appears that many organizations have not yet installed the patch.



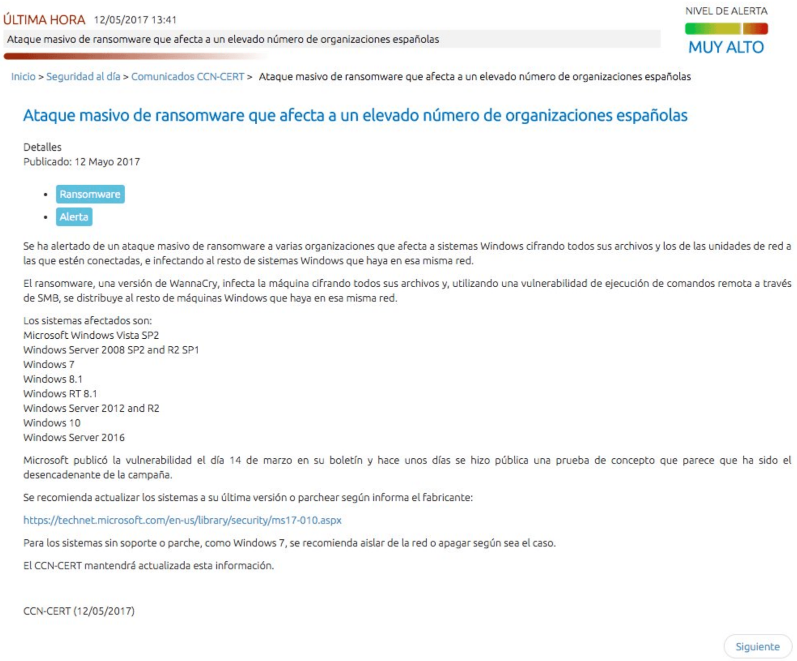
№	Exploit Name	MS Bulletin	Detection Signatures	Notes
1.	"EternalBlue"	MS17-010	Exploit.Win32/64.ShadowBrokers.* UDS:DangerousObject.Multi.Generic	SMBv2 Exploitation Tool, RCE. The vulnerability was fixed by Microsoft on March 14, 2017. We detect the exploitation tools and are investigating this vulnerability further to create generic defense mechanisms against similar attacks in the future.
2.	"EmeraldThread"	MS10-061	Trojan.Win32/64.EquationDrug.* Exploit.Win32.RPC.* Intrusion.Win.CVE-2010-2729.a.exploit UDS:DangerousObject.Multi.Generic	Printer Spooler vulnerability. This vulnerability was used by the well-known Stuxnet worm; the first exploit for this vulnerability was published in 2010, so this is a well-known issue. This vulnerability was addressed by MS10-061 on September 14, 2010. We have been detecting the exploitation of this vulnerability since 2010.
3.	"EternalChampion"	CVE-2017-0146 CVE-2017-0147	Exploit.Win32/64.ShadowBrokers.* UDS:DangerousObject.Multi.Generic	(CVE-2017-0146) This SMBv1 server exploit allows remote attackers to execute arbitrary code via specially crafted packets, aka "Windows SMB Remote Code Execution Vulnerability". (CVE-2017-0147) This SMBv1 server exploit allows remote attackers to obtain sensitive information from the process memory via crafted packets, aka "Windows SMB Information Disclosure Vulnerability". We detect the exploitation tools and are investigating these vulnerabilities further to create generic defense mechanisms against similar attacks in the future.
4.	"ErraticGopher"	Addressed prior to the release of Windows Vista	Trojan.Win32/64.EquationDrug.* Trojan.Win32/64.ShadowBrokers.* UDS:DangerousObject.Multi.Generic	SMBv1 exploit targeting Windows XP and Server 2003. We detect the exploitation tools and are investigating this vulnerability.

Source: https://support.kaspersky.com/shadowbrokers

A few hours ago, Spain's Computer Emergency Response Team CCN-CERT, posted an alert on their site about a massive ransomware attack affecting several Spanish organizations. The alert recommends the installation of updates in the Microsoft March 2017 Security Bulletin as a means of stopping the spread of the attack.

The National Health Service (NHS) in the U.K. also issued an alert and confirmed infections at 16 medical institutions. We have confirmed additional infections in several additional countries, including Russia, Ukraine, and India.

It's important to understand that while unpatched Windows computers exposing their SMB services can be remotely attacked with the "EternalBlue" exploit and infected by the WannaCry ransomware, the lack of existence of this vulnerability doesn't really prevent the ransomware component from working. Nevertheless, the presence of this vulnerability appears to be the most significant factor that caused the outbreak.



ÚLTIMA HORA 12/05/2017 13:41

Ataque masivo de ransomware que afecta a un elevado número de organizaciones españolas

Inicio > Seguridad al día > Comunicados CCN-CERT > Ataque masivo de ransomware que afecta a un elevado número de organizaciones españolas

Ataque masivo de ransomware que afecta a un elevado número de organizaciones españolas

Detalles
Publicado: 12 Mayo 2017

- Ransomware
- Alerta

Se ha alertado de un ataque masivo de ransomware a varias organizaciones que afecta a sistemas Windows cifrando todos sus archivos y los de las unidades de red a las que estén conectadas, e infectando al resto de sistemas Windows que haya en esa misma red.

El ransomware, una versión de WannaCry, infecta la máquina cifrando todos sus archivos y, utilizando una vulnerabilidad de ejecución de comandos remota a través de SMB, se distribuye al resto de máquinas Windows que haya en esa misma red.

Los sistemas afectados son:
Microsoft Windows Vista SP2
Windows Server 2008 SP2 and R2 SP1
Windows 7
Windows 8.1
Windows RT 8.1
Windows Server 2012 and R2
Windows 10
Windows Server 2016

Microsoft publicó la vulnerabilidad el día 14 de marzo en su boletín y hace unos días se hizo pública una prueba de concepto que parece que ha sido el desencadenante de la campaña.

Se recomienda actualizar los sistemas a su última versión o parchear según informa el fabricante:

https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

Para los sistemas sin soporte o parche, como Windows 7, se recomienda aislar de la red o apagar según sea el caso.

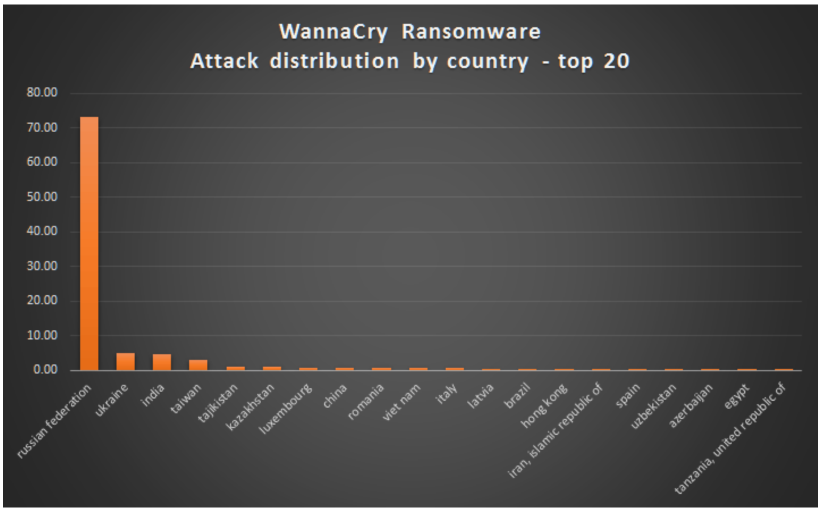
El CCN-CERT mantendrá actualizada esta información.

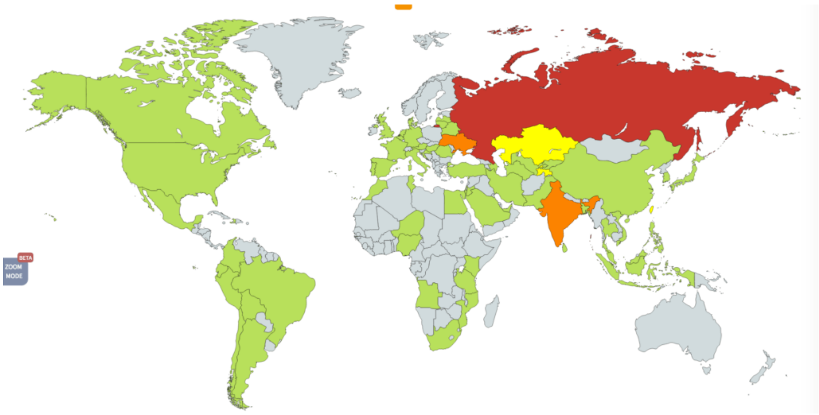
CCN-CERT (12/05/2017)

CCN-CERT alert (in Spanish)

Analysis of the attack

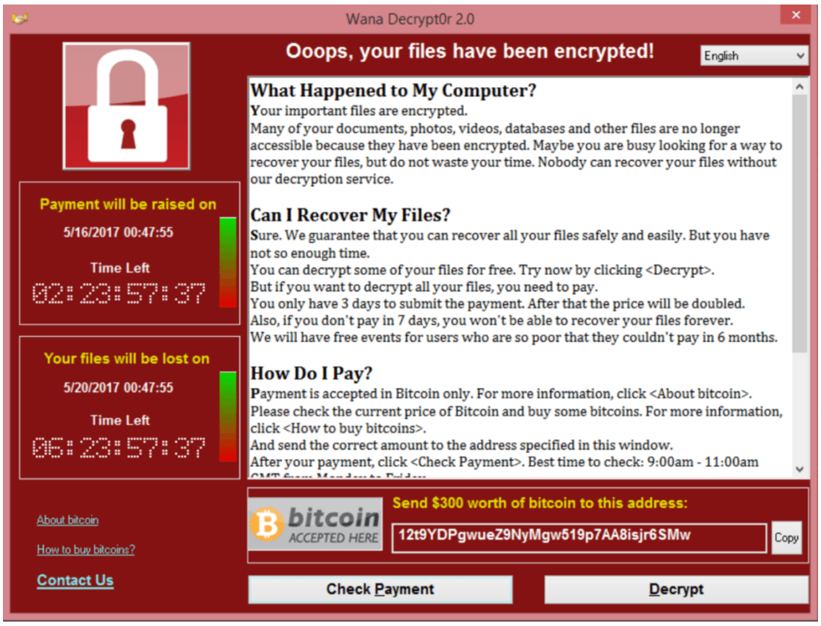
Currently, we have recorded more than 45,000 attacks of the WannaCry ransomware in 74 countries around the world, mostly in Russia. It's important to note that our visibility may be limited and incomplete and the range of targets and victims is likely much, much higher.





Geographical target distribution according to our telemetry for the first few hours of the attack

The malware used in the attacks encrypts the files and also drops and executes a decryptor tool. The request for $600 in Bitcoin is displayed along with the wallet. It's interesting that the initial request in this sample is for $600 USD, as the first five payments to that wallet is approximately $300 USD. It suggests that the group is increasing the ransom demands.



Ooops, your files have been encrypted!

What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

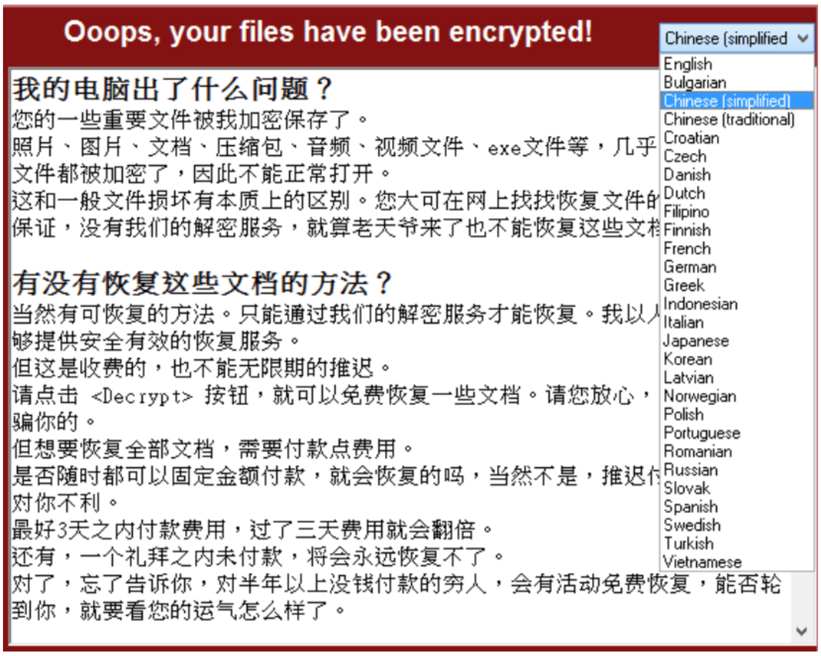
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

The tool was designed to address users of multiple countries, with translated messages in different languages.


Chinese (simplified
English
Bulgarian
Chinese (simplified)
Chinese (traditional)
Croatian
Czech
Danish
Dutch
Filipino
Finnish
French
German
Greek
Indonesian
Italian
Japanese
Korean
Latvian
Norwegian
Polish
Portuguese
Romanian
Russian
Slovak
Spanish
Swedish
Turkish
Vietnamese

Ooops, your files have been encrypted!

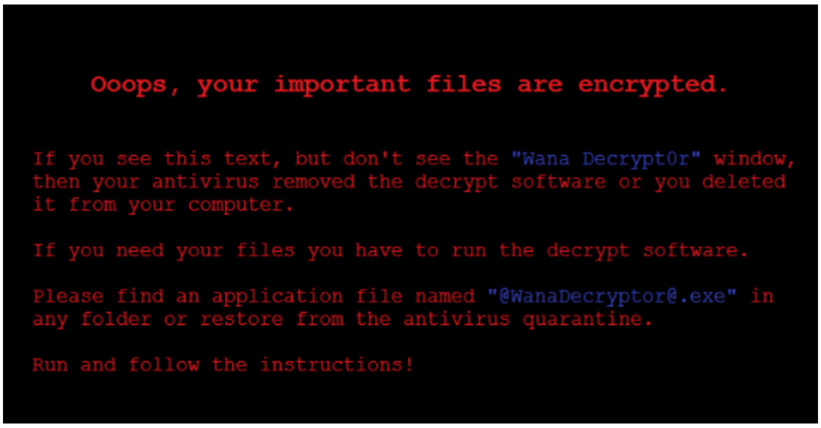
我的电脑出了什么问题？
您的一些重要文件被我加密保存了。
照片、图片、文档、压缩包、音频、视频文件、exe文件等，几乎
文件都被加密了，因此不能正常打开。
这和一般文件损坏有本质上的区别。您大可在网上找找恢复文件
保证，没有我们的解密服务，就算老天爷来了也不能恢复这些文

有没有恢复这些文档的方法？
当然有可恢复的方法。只能通过我们的解密服务才能恢复。我以
够提供安全有效的恢复服务。
但这是收费的，也不能无限期的推迟。
请点击 <Decrypt> 按钮，就可以免费恢复一些文档。请您放心，
骗你的。
但想要恢复全部文档，需要付款点费用。
是否随时都可以固定金额付款，就会恢复的吗，当然不是，推迟
对你不利。
最好3天之内付款费用，过了三天费用就会翻倍。
还有，一个礼拜之内未付款，将会永远恢复不了。
对了，忘了告诉你，对半年以上没钱付款的穷人，会有活动免费恢复，能否轮
到你，就要看您的运气怎么样了。

Language list that the malware supports

Note that the “payment will be raised” after a specific countdown, along with another display raising urgency to pay up, threatening that the user will completely lose their files after the set timeout. Not all ransomware provides this timer countdown.

To make sure that the user doesn’t miss the warning, the tool changes the user’s wallpaper with instructions on how to find the decryptor tool dropped by the malware.



Ooops, 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.

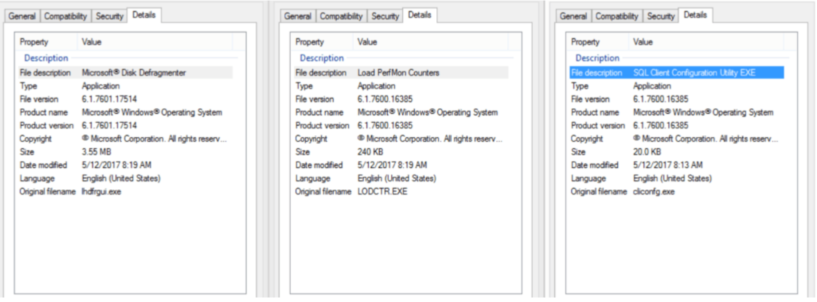
If you need your files you have to run the decrypt software.

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

Run and follow the instructions!

An image used to replace user’s wallpaper

Malware samples contain no reference to any specific culture or codepage other than universal English and Latin codepage CP1252. The files contain version info stolen from random Microsoft Windows 7 system tools:



Property	Value
Description	
File description	Microsoft® Disk Defragmenter
Type	Application
File version	6.1.7601.17514
Product name	Microsoft® Windows® Operating System
Product version	6.1.7601.17514
Copyright	© Microsoft Corporation. All rights reserv...
Size	3.55 MB
Date modified	5/12/2017 8:19 AM
Language	English (United States)
Original filename	lhdfrgui.exe

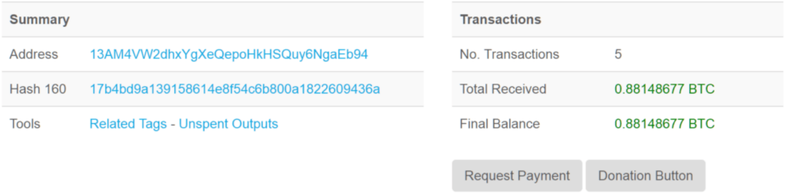
Property	Value
Description	
File description	Load PerfMon Counters
Type	Application
File version	6.1.7600.16385
Product name	Microsoft® Windows® Operating System
Product version	6.1.7600.16385
Copyright	© Microsoft Corporation. All rights reserv...
Size	240 KB
Date modified	5/12/2017 8:19 AM
Language	English (United States)
Original filename	LODCTR.EXE

Property	Value
Description	
File description	SQL Client Configuration Utility EXE
Type	Application
File version	6.1.7600.16385
Product name	Microsoft® Windows® Operating System
Product version	6.1.7600.16385
Copyright	© Microsoft Corporation. All rights reserv...
Size	20.0 KB
Date modified	5/12/2017 8:13 AM
Language	English (United States)
Original filename	cliconfg.exe

Properties of malware files used by WannaCry

For convenient bitcoin payments, the malware directs to a page with a QR code at btcfrog, which links to their main bitcoin wallet 13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94. Image metadata does not provide any additional info:

One of the Bitcoin wallets used by the attackers:
13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94

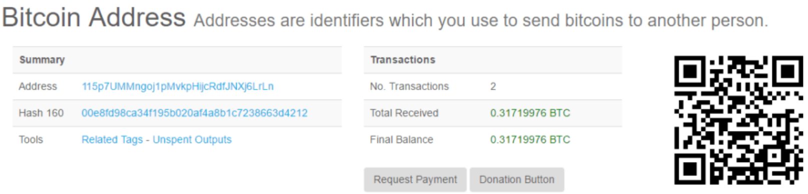


Summary	
Address	13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94
Hash 160	17b4bd9a139158614e8f54c6b800a1822609436a
Tools	Related Tags - Unspent Outputs

Transactions	
No. Transactions	5
Total Received	0.88148677 BTC
Final Balance	0.88148677 BTC

One of the attacker wallets received 0.88 BTC during the last hours

Another Bitcoin wallets included in the attackers' "readme.txt" from the samples are:
115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn – 0.32 BTC



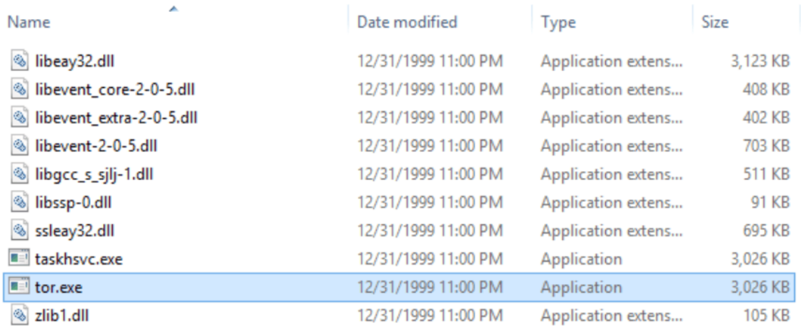
Bitcoin Address Addresses are identifiers which you use to send bitcoins to another person.

Summary	
Address	115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn
Hash 160	00e8fd98ca34f195b020af4a8b1c7238663d4212
Tools	Related Tags - Unspent Outputs

Transactions	
No. Transactions	2
Total Received	0.31719976 BTC
Final Balance	0.31719976 BTC

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw – 0.16 BTC
1QAc9S5EmycqjzzWDc1yiWzr9jJLC8sLiY

For command and control, the malware extracts and uses Tor service executable with all necessary dependencies to access the Tor network:



Name	Date modified	Type	Size
libeay32.dll	12/31/1999 11:00 PM	Application extens...	3,123 KB
libevent_core-2-0-5.dll	12/31/1999 11:00 PM	Application extens...	408 KB
libevent_extra-2-0-5.dll	12/31/1999 11:00 PM	Application extens...	402 KB
libevent-2-0-5.dll	12/31/1999 11:00 PM	Application extens...	703 KB
libgcc_s_sjlj-1.dll	12/31/1999 11:00 PM	Application extens...	511 KB
libssp-0.dll	12/31/1999 11:00 PM	Application extens...	91 KB
ssleay32.dll	12/31/1999 11:00 PM	Application extens...	695 KB
taskhsvc.exe	12/31/1999 11:00 PM	Application	3,026 KB
tor.exe	12/31/1999 11:00 PM	Application	3,026 KB
zlib1.dll	12/31/1999 11:00 PM	Application extens...	105 KB

A list of dropped files related to Tor service

In terms of targeted files, the ransomware encrypts files with the following extensions:

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

The file extensions that the malware is targeting contain certain clusters of formats including:

1. Commonly used office file extensions (.ppt, .doc, .docx, .xlsx, .sxi).
2. Less common and nation-specific office formats (.sxw, .odt, .hwp).
3. Archives, media files (.zip, .rar, .tar, .bz2, .mp4, .mkv)
4. Emails and email databases (.eml, .msg, .ost, .pst, .edb).
5. Database files (.sql, .accdb, .mdb, .dbf, .odb, .myd).
6. Developers’ sourcecode and project files (.php, .java, .cpp, .pas, .asm).
7. Encryption keys and certificates (.key, .pfx, .pem, .p12, .csr, .gpg, .aes).
8. Graphic designers, artists and photographers files (.vsd, .odg, .raw, .nef, .svg, .psd).
9. Virtual machine files (.vmx, .vmdk, .vdi).

The WannaCry dropper drops multiple “user manuals” on different 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, Vietnamese

The example of a “user manual” in English:

What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking .
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click .
Please check the current price of Bitcoin and buy some bitcoins.
For more information, click .
And send the correct amount to the address specified in this window.
After your payment, click . Best time to check: 9:00am - 11:00am GMT from Monday to Friday.
Once the payment is checked, you can start decrypting your files immediately.

Contact
If you need our assistance, send a message by clicking .

```
We strongly recommend you to not remove this
software, and disable your anti-virus for a
while, until you pay and the payment gets
processed. If your anti-virus gets
updated and removes this software automatically,
it will not be able to recover your files even
if you pay!
```

It also drops batch and VBS script files, and a “readme” (contents are provided in the appendix).

Just in case the user closed out the bright red dialog box, or doesn’t understand it, the attackers drop a text file to disk with further instruction. An example of their “readme” dropped to disk as “@Please_Read_Me@.txt” to many directories on the victim host. Note that the English written here is done well, with the exception of “How can I trust?”. To date, only two transactions appear to have been made with this 115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn bitcoin address for almost $300:

```
Q: What's wrong with my files?
```

A: Ooops, your important files are encrypted. It means you will not be able to access them anymore until they are decrypted.
If you follow our instructions, we guarantee that you can decrypt all your files quickly and safely!
Let's start decrypting!

Q: What do I do?

A: First, you need to pay service fees for the decryption.
Please send $300 worth of bitcoin to this bitcoin address:
115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

Next, please find an application file named
"@WanaDecryptor@.exe". It is the decrypt software.
Run and follow the instructions! (You may need to disable your antivirus for a while.)

Q: How can I trust?

A: Don't worry about decryption.
We will decrypt your files surely because nobody will trust us if we cheat users.

```
* If you need our assistance, send a message by
clicking on the decryptor window.
```

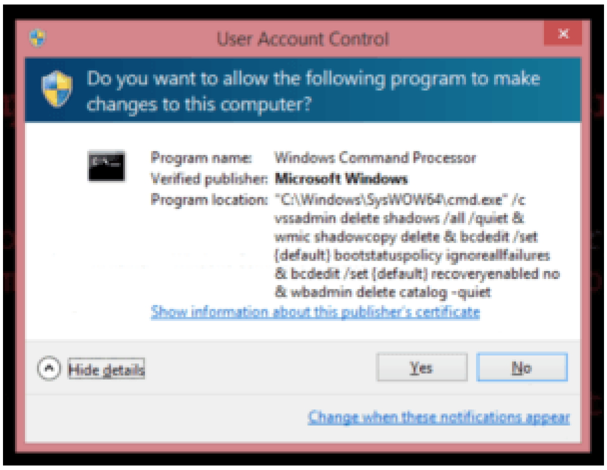
Once started it immediately spawns several processes to change file permissions and communicate with tor hidden c2 servers:

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

The malware creates mutex “Global\MsWinZonesCacheCounterMutexA” and runs the 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
```

This results in an UAC popup that user may notice.


User Account Control

Do you want to allow the following program to make changes to this computer?

Program name: Windows Command Processor
Verified publisher: **Microsoft Windows**
Program location: "C:\Windows\SysWOW64\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

Show information about this publisher's certificate
Hide details
Yes
No
Change when these notifications appear

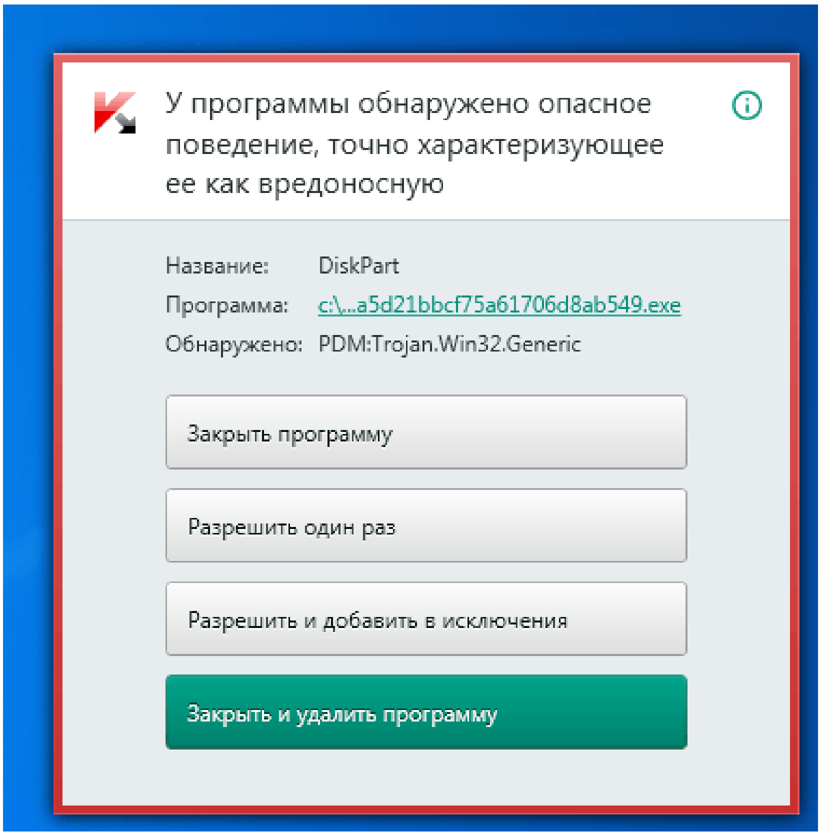
UAC popup to disable Volume Shadow Service (System Restore)

The malware use TOR hidden services for command and control. The list of .onion domains inside is as following:

- gx7ekbenv2riucmf.onion
- 57g7spgrzlojinas.onion
- Xxlvbrloxvriy2c5.onion
- 76jdd2ir2embyv47.onion
- cwwnhwhlz52maqm7.onion
- sqjolphimrr7jqw6.onion

Mitigation and detection information

Quite essential in stopping these attacks is the Kaspersky System Watcher component. The System Watcher component has the ability to rollback the changes done by ransomware in the event that a malicious sample managed to bypass other defenses. This is extremely useful in case a ransomware sample slips past defenses and attempts to encrypt the data on the disk.



У программы обнаружено опасное поведение, точно характеризующее ее как вредоносную

Название: DiskPart
Программа: c:\...a5d21bbcf75a61706d8ab549.exe
Обнаружено: PDM:Trojan.Win32.Generic

Закрыть программу
Разрешить один раз
Разрешить и добавить в исключения
Закрыть и удалить программу

System Watcher blocking the WannaCry attacks

Mitigation recommendations:

1. Make sure that all hosts are running and have enabled endpoint security solutions.
2. Install the official patch (MS17-010) from Microsoft, which closes the affected SMB Server vulnerability used in this attack.
3. Ensure that Kaspersky Lab products have the System Watcher component enabled.
4. Scan all systems. After detecting the malware attack as MEM:Trojan.Win64.EquationDrug.gen, reboot the system. Once again, make sure MS17-010 patches are installed.

Samples observed in attacks so far:

4fef5e34143e646dbf9907c4374276f5
5bef35496fcbdbe841c82f4d1ab8b7c2
775a0631fb8229b2aa3d7621427085ad
7bf2b57f2a205768755c07f238fb32cc
7f7ccaa16fb15eb1c7399d422f8363e8
8495400f199ac77853c53b5a3f278f3e
84c82835a5d21bbcf75a61706d8ab549
86721e64ffbd69aa6944b9672bcabb6d
8dd63adb68ef053e044a5a2f46e0d2cd
b0ad5902366f860f85b892867e5b1e87

d6114ba5f10ad67a4131ab72531f02da
db349b97c37d22f5ea1d1841e3c89eb4
e372d07207b4da75b3434584cd9f3450
f529f4556a5126bba499c26d67892240

Kaspersky Lab detection names:

Trojan-Ransom.Win32.Gen.djd
Trojan-Ransom.Win32.Scatter.tr
Trojan-Ransom.Win32.Wanna.b
Trojan-Ransom.Win32.Wanna.c
Trojan-Ransom.Win32.Wanna.d
Trojan-Ransom.Win32.Wanna.f
Trojan-Ransom.Win32.Zapchast.i
PDM:Trojan.Win32.Generic

Kaspersky Lab experts are currently working on the possibility of creating a decryption tool to help victims. We will provide an update when a tool is available.

Appendix

Batch file

```
@echo off
echo SET ow = WScript.CreateObject("WScript.Shell")> m.vbs
echo SET om = ow.CreateShortcut("C:\Users\ADMINI~1\AppData\Local\Temp\@WanaDecryptor@.exe.lnk")>> m.vbs

echo om.TargetPath = "C:\Users\ADMINI~1\AppData\Local\Temp\@WanaDecryptor@.exe">> m.vbs

echo om.Save>> m.vbs
cscript.exe //nologo m.vbs
del m.vbs
del /a %0
```

m.vbs

```
SET ow = WScript.CreateObject("WScript.Shell")
SET om = ow.CreateShortcut("C:\Users\ADMINI~1\AppData\Local\Temp\@WanaDecryptor@.exe.lnk")
```

```
om.TargetPath =
"C:\Users\ADMINI~1\AppData\Local\Temp\@WanaDecry
ptor@.exe"
om.Save
```

Related Posts

- SPAM AND PHISHING IN Q1 2017
- USE OF DNS TUNNELING FOR C&C COMMUNICATION
- HAJIME, THE MYSTERIOUS EVOLVING BOTNET

THERE ARE 23 COMMENTS

If you would like to comment on this article you must first login

c0den
Posted on May 12, 2017. 7:33 pm

You may have an error throughout this entry. You call out SMBv2 however based on MS17-010 and what I have read about wannacry, it is SMBv1 that is being used for lateral movement.

Reply

thesaint
Posted on May 13, 2017. 3:19 pm

exactly i have the same worry kaspersky and symantec said its smb v2 and they refer to MS17-010 which only mention SMB v1 ??!!!!!!!!!!!!!!!!!!

Reply

mullar
Posted on May 12, 2017. 7:54 pm

Useful

Reply

Fernando
Posted on May 12, 2017. 9:06 pm

Hello guys,

Kaspersky Security 10 for Windows Server (10.0.0.486) with Anti-Cryptor running will be block this attempt to encrypt?

Best regards,

Fernando.

Reply

DK
Posted on May 13, 2017. 9:19 am

KSWS (Kaspersky Security for Windows Servers) will monitor file shares on the server it is installed on using the Anti-Cryptor component if it is enabled. Should it detect an encryption algorithm being performed on contents of a file share by another endpoint, it will sever the network connection to that endpoint for an hour.

Reply

A Another
Posted on May 12, 2017. 9:24 pm

You guys are doing great.

I hope you manage do create a decryption device and take the opportunity to give it away free.

Good luck guys

Reply

Mn90
Posted on May 12, 2017. 9:30 pm

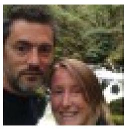
Hi,
Is it correct attack over SMBv2? The MS17-010 official description talks about SMBv1
”
This security update resolves vulnerabilities in Microsoft Windows. The most severe of the vulnerabilities could allow remote code execution if an attacker sends specially crafted messages to a Microsoft Server Message Block 1.0 (SMBv1) server.
“

Reply

E K
Posted on May 13, 2017. 9:24 am

It’s correct.

Reply



Richard Bartlett
Posted on May 13, 2017. 3:23 pm

You’ll need to provide a bit more validation than an anonymous assertion! Given that no other source in the world (other than people quoting this page) are identifying an SMB v2 flaw this has to be considered a typo someone doesn’t want to back down from.

Reply

Brian N
Posted on May 13, 2017. 3:41 am

Phew, good thing I have Kaspersky installed ☺

Reply

Khaled Ahmad
Posted on May 13, 2017. 8:58 am

Thanks

Reply

KenWhelp
Posted on May 13, 2017. 10:17 am

Surely the people at fault here are those that did not install the March Windows update?
We are now nearly halfway through May.
I can’t think of any excuse not to keep updated with security vulnerability patches!
Keep up the good work, guys!

Reply

Narcísio Jose Mula
Posted on May 13, 2017. 10:49 am

Thank you

Reply

Arnaud
Posted on May 13, 2017. 12:39 pm

Does KIS 2017 protects against Wanna Cry virus ?

Reply

Mark
Posted on May 13, 2017. 2:19 pm

Enable System Watcher tool if its not and Also INSTALL THE PATCH

Reply

B.ChinasubbaRao
Posted on May 13, 2017. 2:55 pm

yes, I am used Kaspersky internet security-2017 past 4 years. it is everthing ok. well protected my computer.

Reply

Anil Murlidhar Jangam
Posted on May 13, 2017. 1:11 pm

Please do create a decryption device as early as possible and take the opportunity to give it away free.

Thanking You.

Reply

DK
Posted on May 13, 2017. 3:09 pm

To decrypt files changed by ransomware is not an easy task. It usually requires access to the encryption key. Whether someones shares this key, they find it during analysis, or just due to sloppy programming from the ransomwares author.
Either way, if a key is found, Kaspersky Lab makes decryption tools and they are all free. You can find existing ones on the website nomoreransom.org

Reply

SUN
Posted on May 13, 2017. 1:40 pm

I am a Kaspersky user. Do I get protected even I didn’t update the Windows patch? I tried to update but it kept saying ‘searching for updates on this computer’ for more than half an hour.

Reply

Mark
Posted on May 13, 2017. 2:21 pm

Kaspersky will do what it can do… however this doesn't guarantee that the attackers are not going to release another modification of the same. Install the Microsoft patch as advised to be safe.

Reply

DK
Posted on May 13, 2017. 3:16 pm

Regarding protection from this malware using Kaspersky Lab solutions. Yes, you are protected. On top of this, this malware normally gains access to a computer via the user opening an attachment in a spam email. If you don't know the sender, don't open the attachment. Even if you know the sender, if you aren't expecting a file, don't open it.
The other way it can infect your machine is if you are unpatched and someone else using the same network opens the email. Say a family member for example.
Keep persisting with Windows Updates, they can take a while, but should work eventually.
If your windows updates were applied and you had up to date Kaspersky Lab software, you had nothing at all to worry about.

Reply

Lovshak
Posted on May 13, 2017. 4:58 pm

I'm a die-hard Win XP SP3 user (there's a lot of us out there). Needless to say, Microsoft has long ago abandoned us and refuses to patch Win XP.

I count on KIS 2017; I keep it up-to-date, and 'Settings' clearly shows "System Watcher" enabled.

Am I "WannaCry" safe? Is there anything else I should do (short of replacing my PC and it's vintage OS)?

Reply

Xx
Posted on May 13, 2017. 7:17 pm

MS did patch for XP

Reply