Global WannaCry ransomware outbreak uses known NSA exploits

blog.emsisoft.com/2017/05/12/wcry-ransomware-outbreak/

Holger

May 12, 2017

EMSISOFT

Following the emergence of the Jaff ransomware attack campaign earlier this week, another, even bigger outbreak is making headlines. The culprit? A new ransomware family called WannaCry or WCry.

Spotted earlier today, WCry caught the attention of the team due to it being spread via the recently exposed NSA shadow broker exploits. WCry took many businesses and public institutions by surprise, including telco giant Telefonica in Spain and the National Health Service in the United Kingdom, and has already infected tens of thousands of systems across the globe.

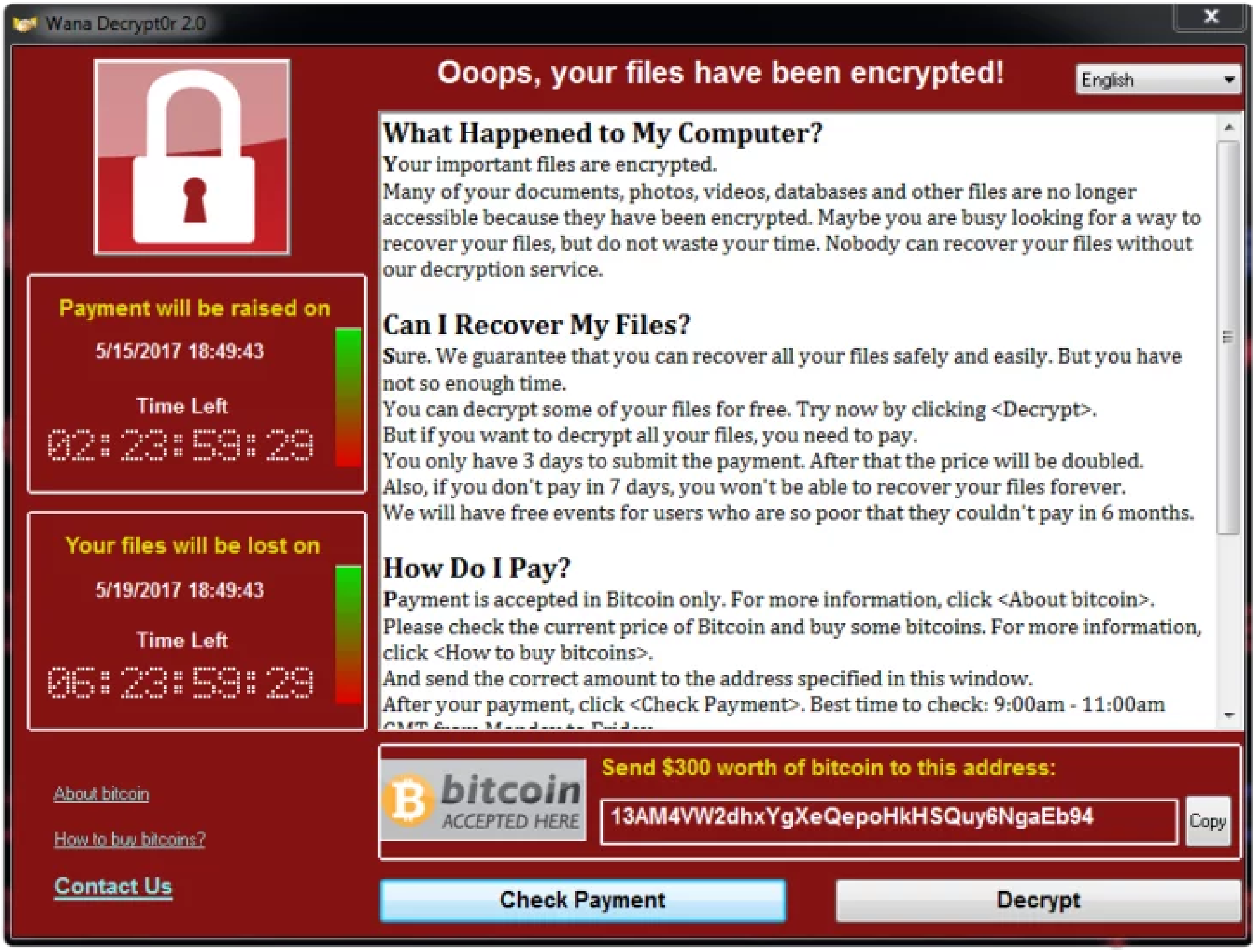
Security researcher MalwareTech created a map of overall infections and a real time map of infections to visualise the number of WCry infections, which has surpassed the 350,000 infection mark across more than 100 countries worldwide.

Meet WannaCry Ransomware

The WCry ransomware, also referred to as WNCry, WannaCry, WanaCrypt0r or Wana Decrypt0r, was originally spotted in campaigns in early February 2017, with more campaigns following in March. But it wasn't until now that a global attack had been registered.

It has been written in C++ and no attempts have been made to hide the majority of the code. Like most ransomware families, WCry renames files it encrypts, adding the .WNCRY extension.

When infecting a system, it presents a ransom screen asking to pay $300 worth of bitcoins:



Ooops, your files have been encrypted!

Payment will be raised on
5/15/2017 18:49:43
Time Left
02:23:59:29

Your files will be lost on
5/19/2017 18:49:43
Time Left
06:23:59:29

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 GMT from Monday to Friday.

Send $300 worth of bitcoin to this address:
13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94

Unlike most ransomware campaigns, which usually target specific regions, WCry is targeting systems around the globe. So it comes as no surprise that the ransomware authors provide localised ransomware message for more than 20 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

How do you get infected with WCry ransomware?

At the moment, WCry is primarily spreading via the leaked NSA exploits that the Shadow Brokers group released recently. More specifically, French researcher Kaffine was the first to suspect that WCry was being spread via the ETERNALBLUE exploit.

ETERNALBLUE exploits a vulnerability in the Microsoft SMBv1 protocol, allowing an attacker to take control over systems which:

- have the SMBv1 protocol enabled
- are accessible from the internet and

- have not been patched by the MS17-010 fix released back in March 2017

In addition, it appears that the malware authors are also taking advantage of DOUBLESPEAR, a backdoor that is usually installed via the ETERNALBLUE exploit and persisting on the system. So if your system was compromised by ETERNALBLUE previously, chances are your system is still vulnerable, even if the initial SMBv1 vulnerability was patched.

The ransomware executable itself can be best described as a dropper that contains all the different ransomware components in form of a password protected ZIP archive within its file. When run, it will start unpacking its components to the directory it was executed in using the hardcoded password "[email protected]". Closer inspection of the ZIP archive reveals the following files:

- **b.wnry** – Ransom desktop wallpaper
- **c.wnry** – Configuration file containing C2 server addresses, BitCoin Wallet etc.
- **r.wnry** – Ransom note
- **s.wnry** – ZIP archive containing the TOR client
- **t.wnry** – The encryption part of the ransomware encrypted using a WanaCry specific format; can be decrypted using the private key embedded inside the ransomware executable.
- **u.wnry** – Decrypter executable
- **Taskdl.exe** – Deletes all temporary files created during encryption (.WNCRYT)
- **Taskse.exe** – Runs given program in all user sessions
- **msg*** – Language files (currently 28 different languages)

In addition the ransomware creates a couple of additional files during its execution:

- **00000000.eky** – Encryption key for the t.wnry file which stores the actual file encryption component used by the ransomware. It is encrypted using the public key that belongs to a private key embedded inside the ransomware.
- **00000000.pky** – Public key used by the ransomware to encrypt the generated AES keys that are used to encrypt the user's files
- **00000000.res** – Command & Control Server (C2) communication results

A list of all changes made by the ransomware to an infected system, can be found in the "Indicators of Compromise" section below.

WCry key generation and encryption

WCry ransomware uses a combination of RSA and AES-128-CBC to encrypt the victim's data. To facilitate this process, is uses the Windows CryptoAPI for RSA, but a custom implementation for the AES encryption.

Interestingly, the encryption routine is stored in a separate component within the *t.wnry* file, and is itself encrypted using the same method used by the ransomware to encrypt user files. This was likely done to make the malware analysis more difficult. The module is loaded into memory using a custom loader and executed from there, without ever being written to the victim's disk unencrypted.

When WCry arrives on a system, it will first import a hardcoded private RSA key that is used to decrypt the file encryption component stored within "t.wnry". Once done, the ransomware will generate a new private RSA key. That RSA key is then submitted to the malware's command and control server and a copy of the generated public key is stored on the system.

The ransomware then searches all available drives and network shares for files with one of 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, .db, .dbf, .odb, .frm, .myd, .myi, .ibd, .mdf, .ldf, .sln, .suo, .cs, .cpp, .pas, .asm, .js, .cmd, .bat, .ps1, .vbs, .vb, .pl, .dip, .dch, .sch, .brd, .jsp, .php, .asp, .rb, .java, .jar, .class, .sh, .mp3, .wav, .swf, .fla, .wmv, .mpg, .vob, .mpeg, .asf, .avi, .mov, .mp4, .3gp, .mkv, .3g2, .flv, .wma, .mid, .m3u, .m4u, .djvu, .svg, .ai, .psd, .nef, .tiff, .tif, .cgm, .raw, .gif, .png, .bmp, .jpg, .jpeg, .vcd, .iso, .backup, .zip, .rar, .7z, .gz, .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, .c, .h

Once done, the malware will generate a new 128 bit AES key for every file it found, which is encrypted using the public RSA key generated earlier and the RSA-encrypted AES key is stored within the header of the encrypted file, together with the file marker "WANACRY!". The AES key is then used to encrypt the file's content.

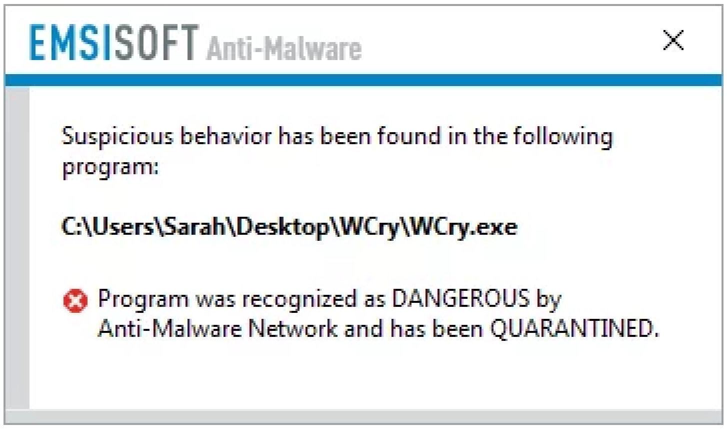
Unfortunately, after evaluating the way WCry performs its encryption, there is no way to restore encrypted files without access to the private key generated by the ransomware. So it's not likely a free WCry ransomware decrypter will be available for victims.

How can I protect myself from WannaCry?

As an emergency measure, make sure to have the latest security updates installed on your Windows computers and servers. Given the scale of the attack, Microsoft even took the unusual step to release security patches for "unsupported systems" such as Windows XP and Windows Server 2003.

As explained in our ransomware article, the best protection still remains a reliable and proven backup strategy, especially since the encryption used by WCry ransomware is secure. The only way to get the data back is through the help of the ransomware author or via restoring from backups. Making sure to install critical windows updates is also a very important step in protecting a system, as WCry only seems to be spreading via the SMBv1 exploit currently, which has been patched for 2 months already.

Apart from regular backups, you will be glad to hear that the Behavior Blocker technology used by Emsisoft Anti-Malware has proven to be the next best defense, as it has caught the ransomware before the file could execute and thus once again keeping our users protected from this and hundreds of other ransomware families without the need for signatures.



Suspicious behavior has been found in the following program:

C:\Users\Sarah\Desktop\WCry\WCry.exe

☒ Program was recognized as DANGEROUS by Anti-Malware Network and has been QUARANTINED.

Emsisoft Anti-Malware users are protected from WannaCry ransomware by our Behavior Blocker.

We consider ransomware one of the biggest threats of the past year and plan to do our best to continue our excellent track record in the next year, to keep our users as protected as possible.

It seems to be an impossible puzzle yet it’s easy to solve the Rubik’ Cube using algorithms.

Download now: Emsisoft Anti-Malware free trial.

Antivirus software from the world’s leading ransomware experts. Get your free trial today. Try It Now

Indicators of Compromise

Registry:

- HKLMSOFTWAREWanaCrypt0r
- HKLMSOFTWAREMicrosoftWindowsCurrentVersionRun<random>: “”<ransomware directory>tasksche.exe””
- HKLMSOFTWAREWanaCrypt0rwd: “<ransomware directory>”
- HKUS-1-5-21-677641349-3533616285-3951951702-1000Control PanelDesktopWallpaper: “%APPDATA%MicrosoftWindowsThemesTranscodedWallpaper.jpg”
- HKUS-1-5-21-677641349-3533616285-3951951702-1000Control PanelDesktopWallpaper: “<ransomware directory>@[email protected]”

File system:

- @[email protected] – Placed inside every folder that contains encrypted files
- @[email protected] – Placed inside every folder that contains encrypted files
- %DESKTOP%@[email protected]
- %DESKTOP%@[email protected]
- %APPDATA%torcached-certs
- %APPDATA%torcached-microdesc-consensus
- %APPDATA%torcached-microdescs.new
- %APPDATA%torlock
- %APPDATA%torstate
- <ransomware directory>0000000.eky
- <ransomware directory>0000000.pky
- <ransomware directory>0000000.res
- <ransomware directory>@[email protected]
- <ransomware directory>@[email protected]
- <ransomware directory>b.wnry
- <ransomware directory>c.wnry
- <ransomware directory>f.wnry
- <ransomware directory>msgm_bulgarian.wnry
- <ransomware directory>msgm_chinese (simplified).wnry
- <ransomware directory>msgm_chinese (traditional).wnry
- <ransomware directory>msgm_croatian.wnry
- <ransomware directory>msgm_czech.wnry
- <ransomware directory>msgm_danish.wnry
- <ransomware directory>msgm_dutch.wnry
- <ransomware directory>msgm_english.wnry
- <ransomware directory>msgm_filipino.wnry
- <ransomware directory>msgm_finnish.wnry

- <ransomware directory>msgm_french.wnry
- <ransomware directory>msgm_german.wnry
- <ransomware directory>msgm_greek.wnry
- <ransomware directory>msgm_indonesian.wnry
- <ransomware directory>msgm_italian.wnry
- <ransomware directory>msgm_japanese.wnry
- <ransomware directory>msgm_korean.wnry
- <ransomware directory>msgm_latvian.wnry
- <ransomware directory>msgm_norwegian.wnry
- <ransomware directory>msgm_polish.wnry
- <ransomware directory>msgm_portuguese.wnry
- <ransomware directory>msgm_romanian.wnry
- <ransomware directory>msgm_russian.wnry
- <ransomware directory>msgm_slovak.wnry
- <ransomware directory>msgm_spanish.wnry
- <ransomware directory>msgm_swedish.wnry
- <ransomware directory>msgm_turkish.wnry
- <ransomware directory>msgm_vietnamese.wnry
- <ransomware directory>r.wnry
- <ransomware directory>s.wnry
- <ransomware directory>t.wnry
- <ransomware directory>TaskDataTorlibeay32.dll
- <ransomware directory>TaskDataTorlibevent-2-0-5.dll
- <ransomware directory>TaskDataTorlibevent_core-2-0-5.dll
- <ransomware directory>TaskDataTorlibevent_extra-2-0-5.dll
- <ransomware directory>TaskDataTorlibgcc_s_sjlj-1.dll
- <ransomware directory>TaskDataTorlibssp-0.dll
- <ransomware directory>TaskDataTorssleay32.dll
- <ransomware directory>TaskDataTortaskhsvc.exe
- <ransomware directory>TaskDataTortor.exe
- <ransomware directory>TaskDataTorzlib1.dll
- <ransomware directory>taskdl.exe
- <ransomware directory>taskse.exe
- <ransomware directory>u.wnry
- C:@[email protected]