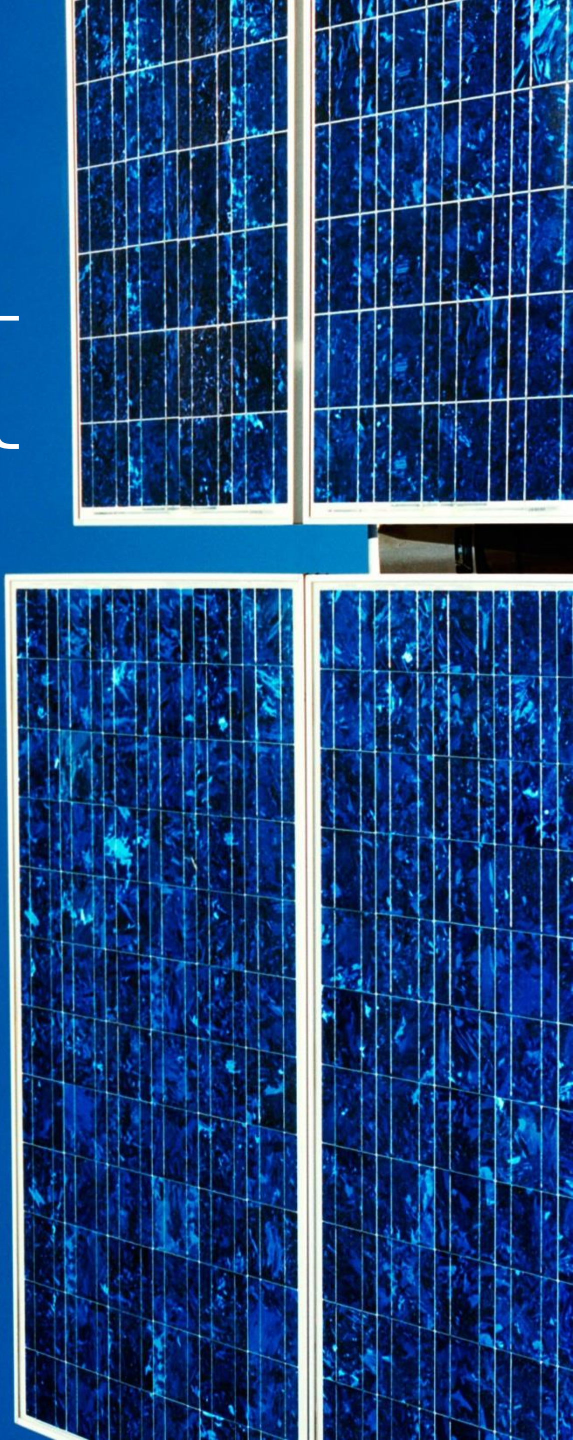
WannaCry/ WannaCrypt Ransomware A synopsis by KPMG



Malware analysis credit to: KPMG (UK) LLP

Recommendations by: KPMG UK, India, Australia, Greece

—

May 2017

Key Points

Virus Name: WannaCrypt, WannaCry, WanaCrypt0r, WCrypt, WCRY

Affected Systems: Windows – Vista SP2, Windows 2008 R2, Windows 7, Windows 8.1, Windows 2012 R2, Windows 10, Windows Server 2016 (other Windows versions affected by ETERNALBLUE *may* be vulnerable – see below).

Vector: It uses ETERNALBLUE (SMBv1) MS17-010 to propagate**.** *Windows XP and Windows 2003 did NOT have the MS17-010 patch and were vulnerable, but as of Monday 15 May, a patch has been issued by Microsoft.*

Ransom Amount: Between $300 to $600. There is code to 'rm' (delete) files in the virus. Seems to reset if the virus crashes.

Persistence Techniques: Malware loops through every open RDP session on a system to run the ransomware as that user (using tscon.exe equivalent as SYSTEM). Various reports that variants also install the in-memory DOUBLEPULSAR backdoor.

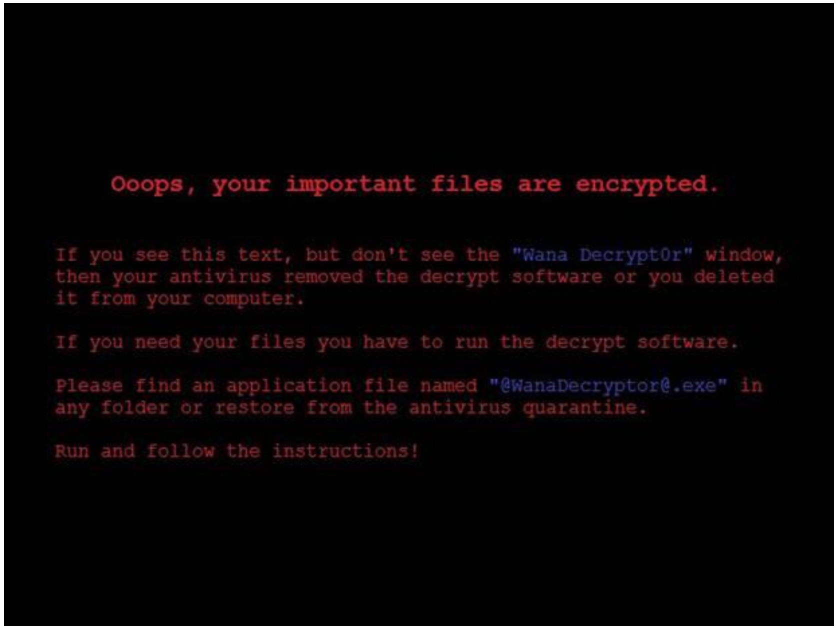
Example Infections: NHS (UK), Telefonica (Spain), FedEx (US), University of Waterloo (US), Russia interior ministry & Megafon (Russia), Shaheen Airlines (India), Neustadt station (Germany), University of Milan (Italy) amongst others.

Spread so far: Over 425,000 attacks in 150 countries.

Kill switches: Domains such as www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com if are registered and sinkholed, the spread of the worm is slowed down. We fear that WannaCry v2.0 will not have a kill switch.

Extent of attack

What you see…



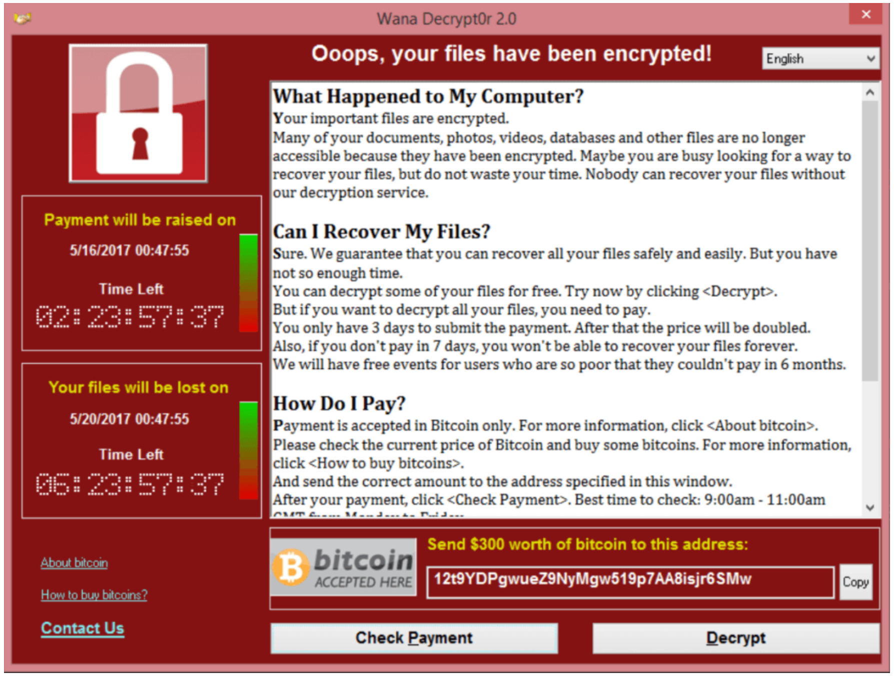
```
Ooops, your important files are encrypted.

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!
```



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.

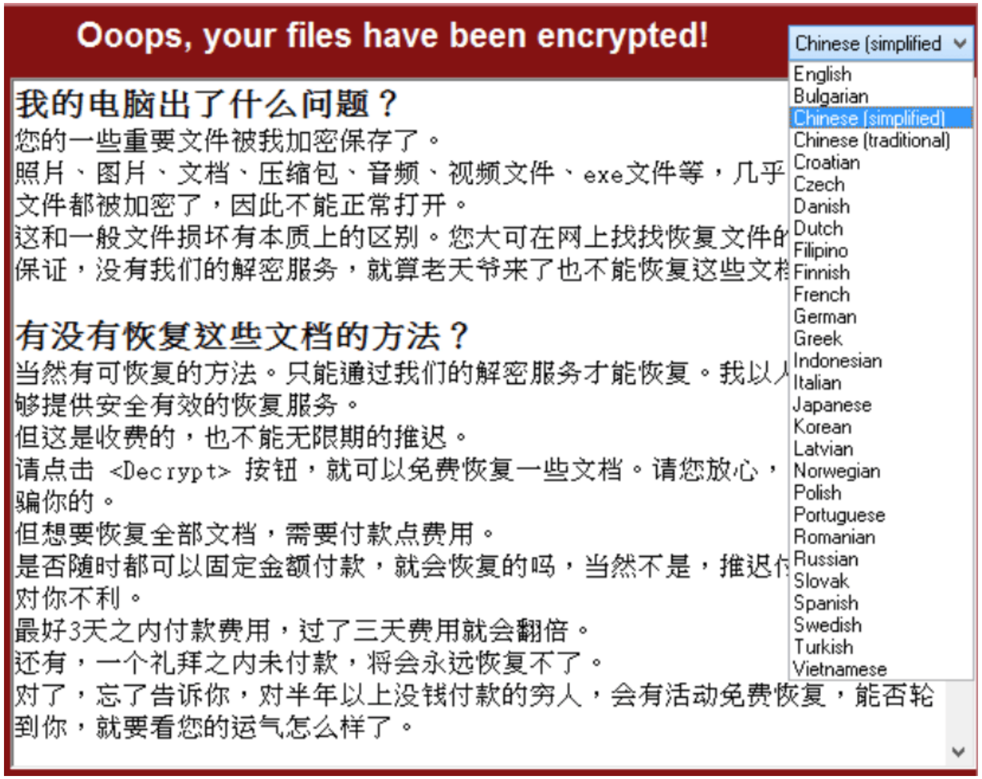
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

International Attack Coverage

Following languages by default:
Bulgarian, Chinese (simplified), Chinese (traditional), Croatian, Czech, Danish, Dutch, English, Filipino, Finish, French, German, Greek, Indonesian, Italian, Japanese, Korean, Latvian, Norwegian, Polish, Portuguese, Romanian, Russian, Slovak, Spanish, Swedish, Turkish, Vietnamese.



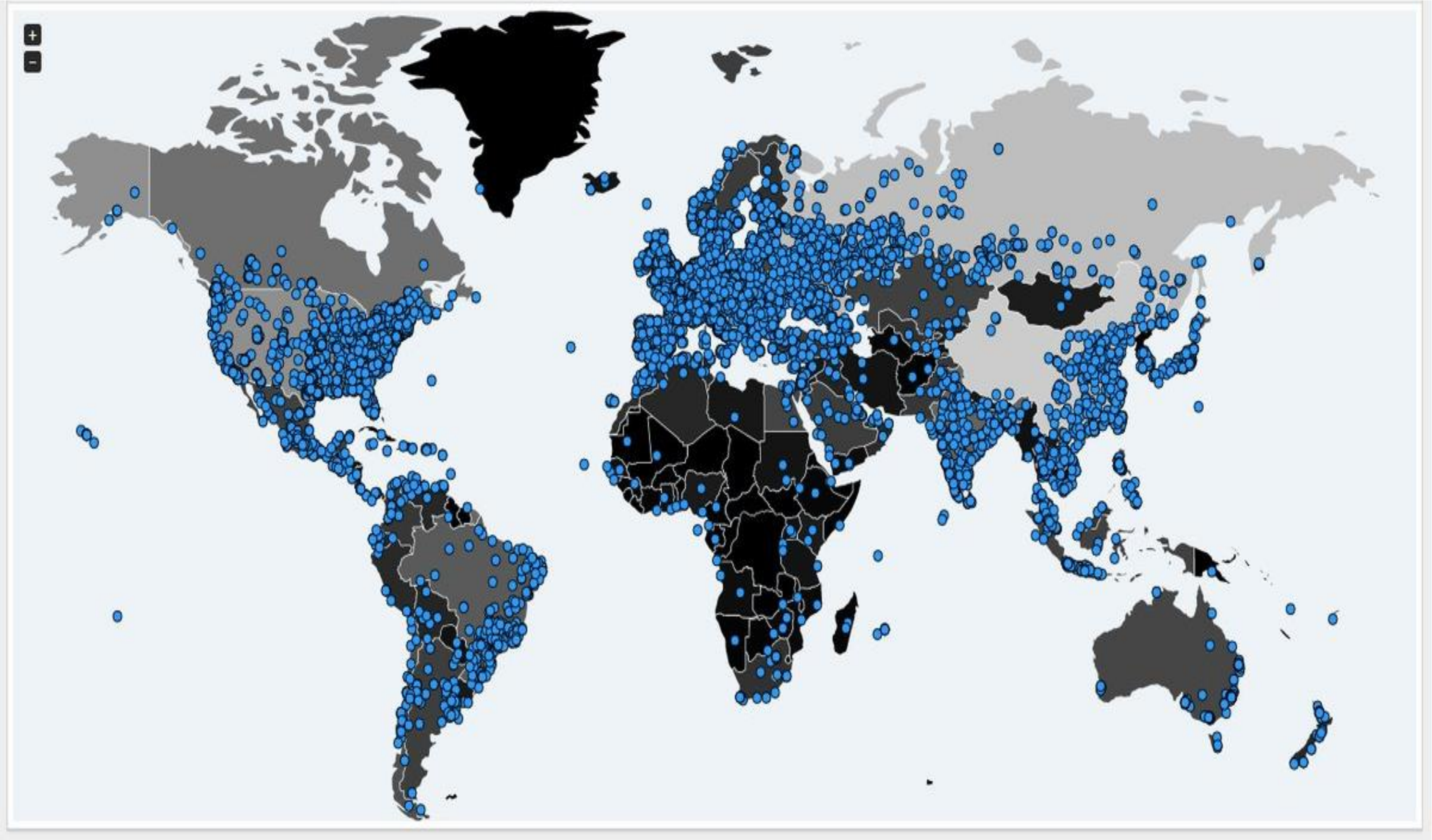
Ooops, your files have been encrypted!

Chinese (simplified

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的
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档

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。我以人
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，推迟付
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。

Infection Patterns



How it works

Exploit Conditions

Needs to get on to a machine initially:

Two routes:

- Phishing: “E-mail subjects: FILE_<5 numbers>, SCAN_<5 numbers> , PDF_<4 or 5 numbers> - attachment nm.pdf“ + others probably exist.

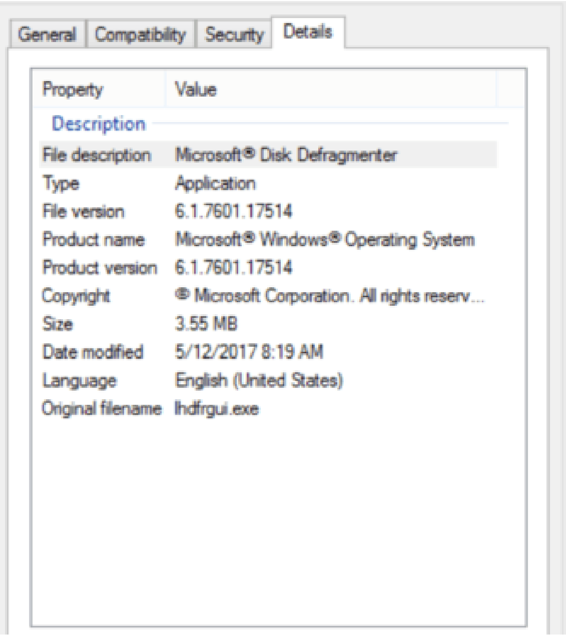
OR

- Uses ETERNALBLUE which 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 or internal LAN.
  - have not been patched by the MS17-010 fix released in March 2017.

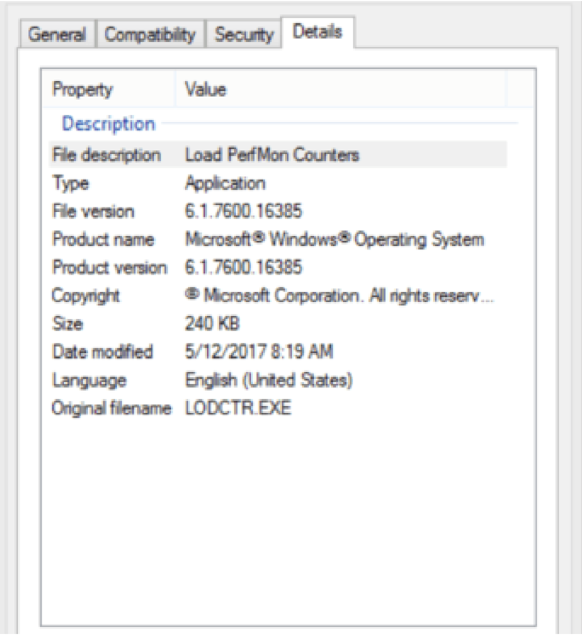
MS17-010:

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

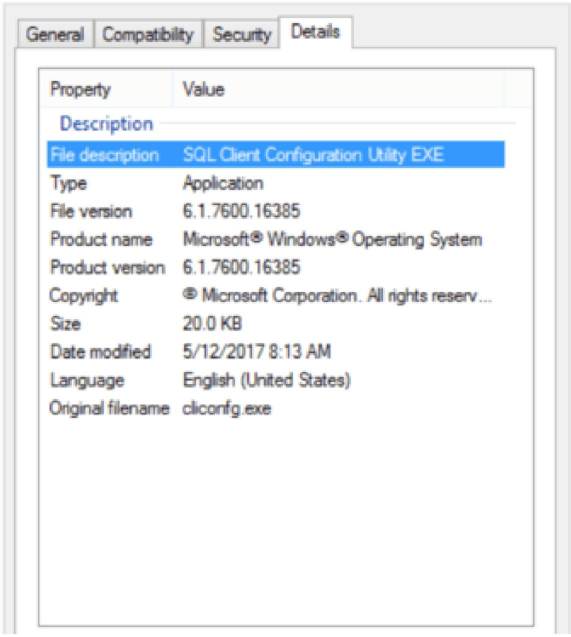
It wears a disguise!



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	Ihdfrgui.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

What does it encrypt?

All drives and network shares with:

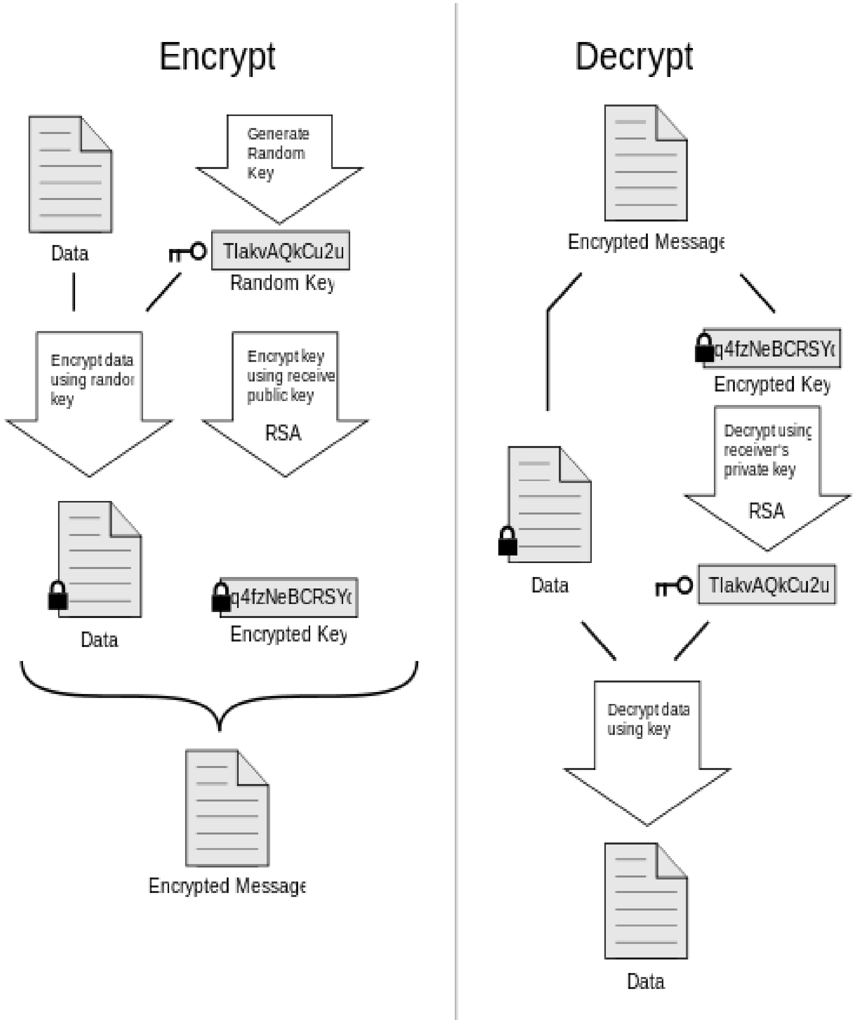
1. Commonly used office file extensions (.ppt, .doc, .docx, .xlsx, .sxi).
2. Less common and nation-specific office formats (.sxw, .odt, .hwp).
3. Archives, media files (.zip, .rar, .tar, .bz2, .mp4, .mkv).
4. Emails and email databases (.eml, .msg, .ost, .pst, .edb).
5. Database files (.sql, .accdb, .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).

Full List:

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

How does it encrypt?

- Files are encrypted via AES-128-CBC (custom implementation in the binary).
- The AES keys are generated with a CSPRNG, CryptGenRandom.
- The malware will generate a new 128 bit AES key for every file it finds!
- AES keys are wrapped/encrypted with RSA-2048 (Windows RSA implementation).
- The RSA-encrypted AES key is stored within the header of the encrypted file, together with the file marker “WANACRY!”.
- The master 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…. Pretty Standard.



Where do the decryption keys get sent?

The following C2 Servers have been identified (all TOR hidden servers):

- gx7ekbenv2riucmf.onion
- 57g7spgrzlojinas.onion
- xxlvbrloxvriy2c5.onion
- 76jdd2ir2embyv47.onion
- cwwnhwhlz52ma.onion
- sqjolphimrr7jqw6.onion

Where does the money go?

- 3 addresses hard coded into the malware.
- https://blockchain.info/address/13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94
- https://blockchain.info/address/12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
- https://blockchain.info/address/115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

Indicators of Compromise (IoC)

Indicators of Compromise

Type	Hash
FileHash-SHA256	09a46b3e1be080745a6d8d88d6b5bd351b1c7586ae0dc94d0c238ee36421cafa
FileHash-SHA256	24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c
FileHash-SHA256	2584e1521065e45ec3c17767c065429038fc6291c091097ea8b22c8a502c41dd
FileHash-SHA256	2ca2d550e603d74dedda03156023135b38da3630cb014e3d00b1263358c5f00d
FileHash-SHA1	45356a9dd616ed7161a3b9192e2f318d0ab5ad10
FileHash-SHA256	4a468603fdcb7a2eb5770705898cf9ef37aade532a7964642ecd705a74794b79
FileHash-MD5	509c41ec97bb81b0567b059aa2f50fe8
FileHash-SHA1	51e4307093f8ca8854359c0ac882ddca427a813c
FileHash-MD5	7bf2b57f2a205768755c07f238fb32cc
FileHash-MD5	7f7ccaa16fb15eb1c7399d422f8363e8

Indicators of Compromise

Type	Hash
FileHash-MD5	84c82835a5d21bbcf75a61706d8ab549
FileHash-SHA1	87420a2791d18dad3f18be436045280a4cc16fc4
FileHash-SHA256	b9c5d4339809e0ad9a00d4d3dd26fdf44a32819a54abf846bb9b560d81391c25
FileHash-SHA1	bd44d0ab543bf814d93b719c24e90d8dd7111234
FilePath	C:\Windows\mssecsvc.exe
FilePath	C:\WINDOWS\tasksche.exe
FileHash-MD5	db349b97c37d22f5ea1d1841e3c89eb4
FileHash-SHA1	e889544aff85ffaf8b0d0da705105dee7c97fe26
FileHash-SHA256	ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
FileHash-MD5	f107a717f76f4f910ae9cb4dc5290594
FileHash-SHA256	f8812f1deb8001f3b7672b6fc85640ecb123bc2304b563728e6235ccbe782d85
hostname	www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[dot]com

Registry indicators of Compromise

HKLM\SOFTWARE\WanaCrypt0r
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\<random>: “”<ransomware directory>\tasksche.exe””
HKLM\SOFTWARE\WanaCrypt0r\wd: “<ransomware directory>”
HKU\S-1-5-21-677641349-3533616285-3951951702-1000\Control Panel\Desktop\Wallpaper: “%APPDATA%\Microsoft\Windows\Themes\TranscodedWallpaper.jpg”
HKU\S-1-5-21-677641349-3533616285-3951951702-1000\Control Panel\Desktop\Wallpaper: “<ransomware directory>\@WanaDecryptor@.bmp

File System Indicators of Compromise

@Please_Read_Me@.txt – Placed inside every folder that contains encrypted files.

@WanaDecryptor@.exe.lnk – Placed inside every folder that contains encrypted files.

%DESKTOP%\@WanaDecryptor@.bmp

%DESKTOP%\@WanaDecryptor@.exe

%APPDATA%\tor\cached-certs

%APPDATA%\tor\cached-microdesc-consensus

%APPDATA%\tor\cached-microdescs.new

%APPDATA%\tor\lock

%APPDATA%\tor\state

<ransomware directory>\00000000.eky

<ransomware directory>\00000000.pky

<ransomware directory>\00000000.res

<ransomware directory>\@WanaDecryptor@.bmp

<ransomware directory>\@WanaDecryptor@.exe

File System Indicators of Compromise

<ransomware directory>\b.wnry

<ransomware directory>\c.wnry

<ransomware directory>\f.wnry

<ransomware directory>\msg\m_bulgarian.wnry

<ransomware directory>\msg\m_chinese (simplified).wnry

<ransomware directory>\msg\m_chinese (traditional).wnry

<ransomware directory>\msg\m_croatian.wnry

<ransomware directory>\msg\m_czech.wnry

<ransomware directory>\msg\m_danish.wnry

<ransomware directory>\msg\m_dutch.wnry

<ransomware directory>\msg\m_english.wnry

<ransomware directory>\msg\m_filipino.wnry

<ransomware directory>\msg\m_finnish.wnry

<ransomware directory>\msg\m_french.wnry

<ransomware directory>\msg\m_german.wnry

<ransomware directory>\msg\m_greek.wnry

File System Indicators of Compromise

<ransomware directory>\msg\m_greek.wnry

<ransomware directory>\msg\m_indonesian.wnry

<ransomware directory>\msg\m_italian.wnry

<ransomware directory>\msg\m_japanese.wnry

<ransomware directory>\msg\m_korean.wnry

<ransomware directory>\msg\m_latvian.wnry

<ransomware directory>\msg\m_norwegian.wnry

<ransomware directory>\msg\m_polish.wnry

<ransomware directory>\msg\m_portuguese.wnry

<ransomware directory>\msg\m_romanian.wnry

<ransomware directory>\msg\m_russian.wnry

<ransomware directory>\msg\m_slovak.wnry

<ransomware directory>\msg\m_spanish.wnry

<ransomware directory>\msg\m_swedish.wnry

File System Indicators of Compromise

<ransomware directory>\msg\m_turkish.wnry

<ransomware directory>\msg\m_vietnamese.wnry

<ransomware directory>\r.wnry

<ransomware directory>\s.wnry

<ransomware directory>\t.wnry

<ransomware directory>\TaskData\Tor\libeay32.dll

<ransomware directory>\TaskData\Tor\libevent-2-0-5.dll

<ransomware directory>\TaskData\Tor\libevent_core-2-0-5.dll

<ransomware directory>\TaskData\Tor\libevent_extra-2-0-5.dll

<ransomware directory>\TaskData\Tor\libgcc_s_sjlj-1.dll

<ransomware directory>\TaskData\Tor\libssp-0.dll

<ransomware directory>\TaskData\Tor\ssleay32.dll

<ransomware directory>\TaskData\Tor\taskhsvc.exe

<ransomware directory>\TaskData\Tor\tor.exe

<ransomware directory>\TaskData\Tor\zlib1.dll

File System Indicators of Compromise

<ransomware directory>\taskdl.exe

<ransomware directory>\taskse.exe

<ransomware directory>\u.wnry

C:\@WanaDecryptor@.exe

What can organizations do?

Mitigation Actions [1]

Various mitigation steps can be taken – these are by no means exhaustive:

- Securely backup your data on a frequent basis.
- Block all incoming connections from the Internet to services that should not be publicly available.
- Block all *.onion sites at edge firewalls.
- Do not open unsolicited emails and attachments.
- Disable AutoPlay to prevent the automatic launching of executable files .
- **Block ports TCP 445/139 at edge firewalls** and perform external scanning of all internet facing ranges to confirm ports are blocked.
- **Push out MS17-010 to every machine as a matter of priority.**
- For Windows XP/2003 machines consider using the inbuilt firewall to block ports TCP 445/139 (however this will have severe repercussions for domain joined machines).
- **Disable SMBv1**! https://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1,-smbv2,-and-smbv3-in-windows-vista,-windows-server-2008,-windows-7,-windows-server-2008-r2,-windows-8,-and-windows-server-2012

Mitigation Actions [2]

Various mitigation steps can be taken – these are by no means exhaustive

- Establish a security governance framework.
- Address security incidents response; internally or with the assistance of a third party.
- Update AV/SIEM/IPS/Everything!
- Start monitoring for IoCs if you have a SOC and/or the appropriate tools.
- Upgrade all end of life machines as a matter of priority.
- For systems without patches isolate them from the network as much as possible (strict VLAN's and Firewalls with very very tight ACLs, for example only allow 139/445 to FileServer and DC).
- Train employees to raise awareness.
- Quarantine all infected systems immediately.
- Visit AV vendors to obtain information. For example:
  - https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
  - https://securingtomorrow.mcafee.com/business/analysis-wannacry-ransomware-outbreak/ includes details on specific IP addresses to block and AV signature hashes to update, as well as Snort IDS rules

linkedin.com/company/kpmg-greece

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.