“WannaCry” ransomware attack

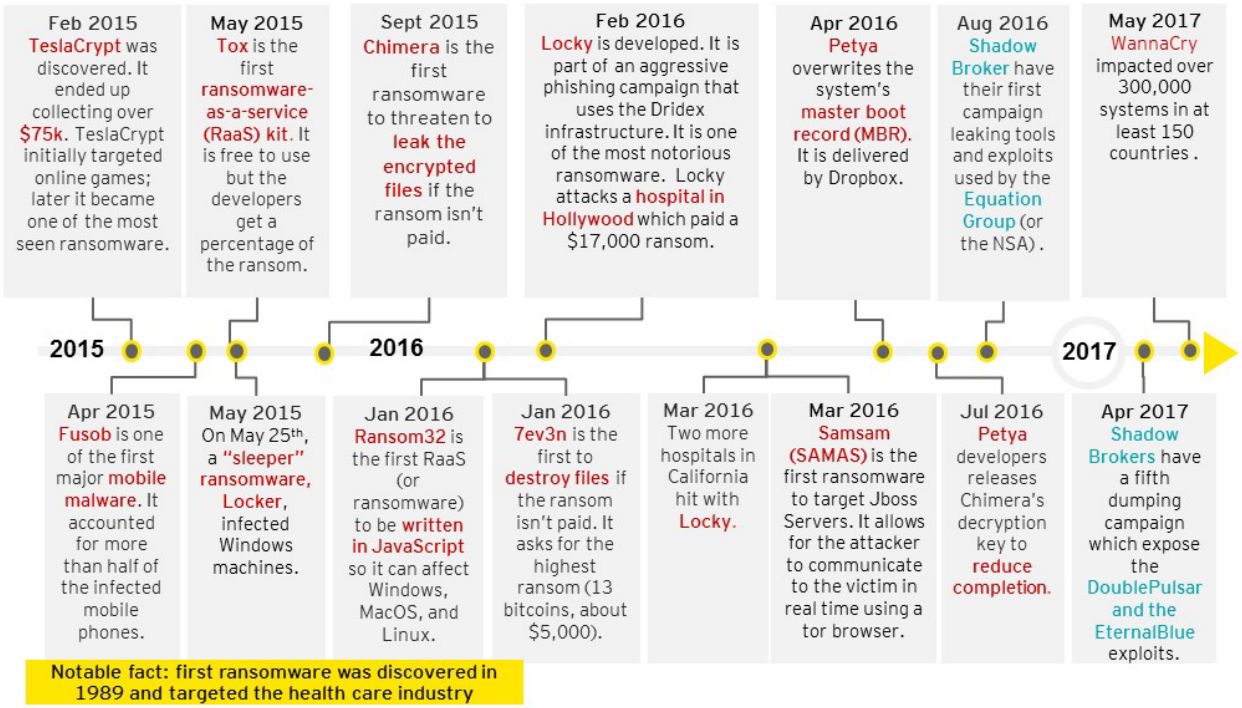
Technical intelligence analysis
May 2017

Building a better working world

Executive summary

On 12 May 2017, a massive ransomware attack occurred across a wide range of sectors, including health care, government, telecommunications and gas. To date, WannaCry has spread to over 300,000 systems in over 150 countries. The countries that appear to be the most affected are Russia and China, probably because of the high percentage of legacy software, with significant impacts elsewhere, notably to the UK National Health Service. The spread of the ransomware reportedly slowed in the two days following the launch of the attack, in part due to the discovery of a "kill switch" in its code. However, there are reports of new variants of the malware (such as Uiwix) which do not have this kill switch. Data on new variants is unconfirmed and limited at the moment, and EY wil publish updates as more information becomes available.

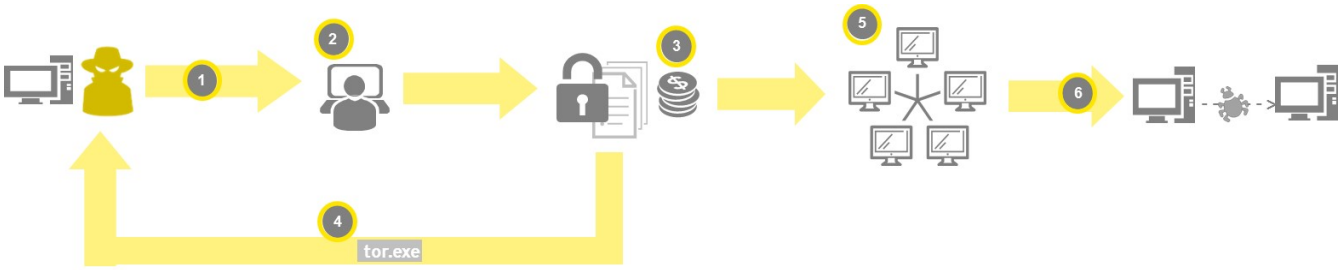
Recap of notable ransomware events



Overview of WannaCry

WannaCry is a type of ransomware, or extortive malware, that encrypts files, disks and locks computers. The malware demands a ransom of ~$300-600 to be paid to one of three bitcoin accounts within three days in return for decrypting the files.

WannaCry spreads via SMB, the Server Message Block protocol operating over ports 445 and 139, typically used by Windows machines to communicate with file systems over a network. Once successfully installed, this ransomware scans for and propogates to other at-risk devices. WannaCry checks to see if backdoors (like DoublePulsar) are already on previously infected machines. Both DoublePulsar and the EternalBlue exploit the SMB vulnerability that was made public by the Shadows Brokers hacking group in April.



1. Attacker uses a yet-to-be-confirmed intial attack vector
2. WannaCry encrypts files in the victim's machine using AES-128 cypher, deletes shadow copies. It then displays a ransom note requesting $300 or $600 in bitcoin
3. Tor.exe is used by wannadecryptor.exe, initiating connections to tor nodes in order to connect back to the attacker (therefore making this extremely difficult, if not impossible, to track)
4. IP address of the infected machine is checked; then IP addresses of the same subnet are scanned for additional vulnerable machines and connected to via port 445 TCP
5. When a machine is successfully connected, data containing the exploit payload is transferred

Global impact of WannaCry

There are approximately 30–40 publicly named companies among the likely thousands that were impacted by this ransomware. Examples include the Russian Interior Ministry, Telefonica (Spain's largest telecommunications company) and FedEx. The UK National Health Service (NHS) was badly hit, with 16 of the 47 NHS trusts being affected, and routine surgery and doctor appointments being canceled as the service recovers. There are reports that in China over 40,000 organizations have been affected, including over 60 academic institutions.

Figure 1. Distribution of attacks as of 14 May
(source: *Twitter Malware Tech - Ransomware country target mapping,* https://twitter.com/MalwareTechBlog/status/863054943632187392)

Russia appears to be the heaviest hit by the WannaCry attack. Kaspersky Labs attributes this to Russian organizations running a relatively large proportion of dated and unpatched systems. WannaCry appears to be specifically designed for an international attack: it can demand the ransom in 28 languages (see Appendix I).

Risk mitigation consideration

Organizations can help mitigate their risk exposure by considering the following actions:

- Ensure that vulnerability management (including patch management and vulnerability scanning/remediation) is a robust and mature enterprise-level program
- Maintain backups that account for critical data and the rate of data generation
  - Align timeline and procedures for restoring system backups with your business continuity plan (BCP)
  - Review the organization's incident response and disaster preparedness plans to verify that they adequately address recovery from a ransomware event
- Implement endpoint monitoring, giving teams visibility into malicious behavior occurring at that level
- Ensure that the organization has a comprehensive security awareness training program in place
- Maintain an effective enterprise incident response plan that is regularly tested and measured for effectiveness against ransomware, as well as regularly updated to reflect the current cyber threat environment
- Confirm that critical systems are not unnecessarily connected to/accessible from the internet

How WannaCry works and why it was so successful

The initial vector of delivery for this malware was originally widely reported to be phishing emails, however data to validate this has not been confirmed and other reports suggest other vectors, such as the use of public-accessible vulnerable SMB (Server Message Block) to spread the malware in a worm-life fashion. Once an infection takes place, WannaCry beacons out to the kill switch URL in order to determine if the malware is in a sandbox environment. If the URL does not respond, then the malware starts to encrypt the victim's files using an AES-128 cipher. Files encrypted by WannaCry are appended with a file extension of .wncry as well as others. Unlike other ransomware families, WannaCry continues to encrypt victim files following any name changes and any new files created following infection. A ransom note is then displayed on the victim's machine, which is completed using text from a library of rich text format (RTF) files, in multiple languages and chosen based on machine location. Observed ransom demands require victims to pay either US$300 or US$600 worth of bitcoin (BTC) for a decryption key. Once infected, the user will see a screen (see Figure 2) with instructions on how to pay the ransom.

Figure 2. Ransomware screen

WannaCry utilizes the exploit Eternal Blue, created by NSA and released by Shadow Brokers (full details in Appendix IV) on 14 April 2017. Of note, the malware also checks for existing backdoors via Double Pulsar, also released by Shadow Brokers, in order to help propogate through client networks. It should also be stated that the kill switch will not pause the attack if an organization is routing through a proxy for internet access.

How a UK malware tech researcher stalled the spread of WannaCry

Shortly after the first reports of NHS hospitals being hit with ransomware, the EY Cyber Threat Intelligence (CTI) team began following a UK researcher who was tweeting about the attack using the handle @malwaretechblog. The researcher obtained a copy of the malware, which he analyzed and discovered a reference to an unregistered domain called www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com. He registered this domain and inadvertently paused the spread of the worm-like attack. This is because WannaCry attempts to connect to the web domain. If it cannot do so, it will proceed with the infection — however, if it does connect, the malware will cease the attack, believing it is being run in an antivirus "sandbox" environment. The registration of the website triggered the malware's kill switch. However, this kill switch is not proxy aware — it did not help organizations that use a proxy to access the internet, as the attack would execute as designed. It is significant to note that most organizations use a proxy in order to access the internet, so the kill switch would have minimal impact in those cases.

What we expect next

CTI expects to see more further variants and copycats of WannaCry, and new variants have been spotted already, reportedly without the kill switch.

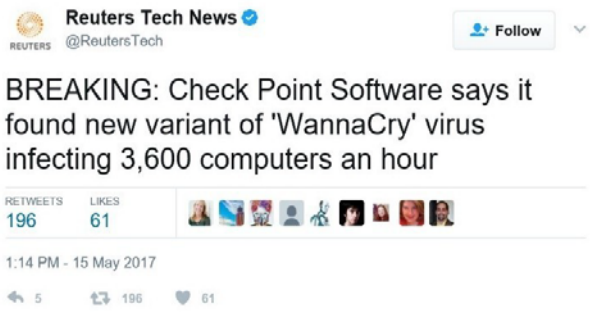


Figure 3. Twitter screenshot Reuters Tech News

Over the coming days and weeks, we anticipate that cyber criminals will release malware variants that leverage other and newer exploits, especially once more organizations patch systems to prevent EternalBlue. We expect that there could be more weaponization of the NSA's exploits that were leaked by Shadow Brokers.

We also expect that cyber criminals will try to copy the highly-effective worm-like propagation techniques of WannaCry, creating malware that can move laterally within an infected system without the need for human intervention.

Significant ransomware attacks tend to be industry agnostic, as they are criminal in nature, seeking to maximize revenue by hitting as wide a range of targets as possible. Industries that use legacy systems are at an elevated risk posture.

Appendix I: What you can do about it?

If you notice the screen shown in Figure 2 on your computer or changes to the file extensions of important files to one of those specified at the end of this advisory, then you are possibly a victim of this ransomware. Following the steps below immediately can help to reduce the impact.

- Disconnect all network connections and external storage immediately
- Shut down the computer and inform your IT teams
- Do not pay any ransom to the hacker, as this fuels the illegal ecosystem and there is no guarantee that you will get the data back
- Safeguard and keep your backups ready before experts assist you

Company-level recommendations:

- Block SMB port access and RDP (Remote Desktop Protocol) to all computers from the internet; Port 445 and 139 for SMB and 3389 for RDP should be blocked
- Block SMB for the time being within the company through a group policy or other endpoint security solution
- Stop granting any privilege escalation requests to users who want to run an unknown program as an administrator
- Ensure that all Windows OS and Microsoft software are patched, especially the MS17-010; any unsupported or outdated operating systems should either be upgraded or reconfigured to stop SMB and RDP
- Issue a notice to all employees to not open unknown attachments and emails; if in doubt, they should read emails on their mobile devices without opening the attachments
- Disable office macros through a group policy
- Enable scanning of all attachments at your endpoints and email gateways; see a list of file hashes and IP addresses to block and observe at the end of this advisory
- Disable uPNP on all your gateways, firewalls, routers and proxy servers
- Maintain backups that account for critical data and the rate of data generation
  - Align timeline and procedures for restoring system backups with your business continuity plan (BCP)
  - Review the organization's incident response and disaster preparedness plans to verify that they adequately address recovery from a ransomware event
- Endpoint monitoring: tools that give a team visibility into the behavior occurring on the endpoint are tremendously useful in combating ransomware
  - Antivirus tools lag behind in detection of ransomware due to their nature
  - Endpoint monitoring solutions allow visibility into processes and network traffic running on endpoints
  - Endpoint monitoring solutions can block rogue processes pending further verification
- Email filtering: Filtering extensions in email will stop a lot of malware attacks, including the Locky ransomware, in its tracks
  - Recommend blocking executable and zip file attachments, and filtering all other attachments for manual review
  - It is safer to block attachments and use a secure transfer option than to allow attachments that may harbor malicious software
- Security awareness training: In the long run, it doesn't matter what tools are implemented if a user is actively clicking on malicious attachments or taking actions that violate the acceptable use policy for a network
  - Security awareness training is an effective method of reducing the susceptibility of people to ransomware campaigns

- Maintain an effective enterprise incident response plan that is tested and measured for effectiveness against ransomware, as well as updated to reflect the current cyber threat environment
  - Confirm critical systems are not unnecessarily connected to/accessible from internet
- Ensure vulnerability management is a robust and mature enterprise-level program

Employee recommendations:

- Disconnect from the internet and take a backup of all your data on an encrypted, removable hard drive; disconnect the hard drive and keep it at a secure location after the backup is completed
- Do not open attachments from unknown sources, and do not download or open unauthorized software
- Do not check your personal email on a company computer, as most free email services will not have advanced security scanning of attachments
- If you suspect any unusual hard drive activity on your computer, immediately shut it down and notify your IT administrator
- Do not enable macros on office documents

IT administrator recommendations:

- Disconnect all network shares from idle computers and servers
- Recheck network shares with write permissions
- Change passwords of and safeguard all common domain administrator accounts; refrain from logging in using these accounts; and use these accounts to only authorize specific actions as per standard operating procedures
- Make sure backup solutions provide write access to only accounts that are hard configured in the backup solution
- User accounts should only have read access
- Enable volume shadow copy if possible through group policy and enforce it
- Update the endpoint security solution and enable anti-malware or anti-ransomware modules
- Prevent privilege escalation of unknown programs and processes
- Create a manual signature on your endpoint security solution and monitor for file hashes and extensions specific in this advisory; in case of any such findings on a user computer, disconnect it from the network and shut it down

Read about more recommendations here.

Appendix II: Indicator of compromise (IOCs) for WannaCry

Hashes

ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
c365ddaa345cfcaff3d629505572a484cff5221933d68e4a52130b8bb7badaf9
09a46b3e1be080745a6d8d88d6b5bd351b1c7586ae0dc94d0c238ee36421cafa
0a73291ab5607aef7db23863cf8e72f55bcb3c273bb47f00edf011515aeb5894
428f22a9afd2797ede7c0583d34a052c32693cbb55f567a60298587b6e675c6f
5c1f4f69c45cff9725d9969f9ffcf79d07bd0f624e06cfa5bcbacd2211046ed6
62d828ee000e44f670ba322644c2351fe31af5b88a98f2b2ce27e423dcf1d1b1
72af12d8139a80f317e851a60027fdf208871ed334c12637f49d819ab4b033dd
85ce324b8f78021ecfc9b811c748f19b82e61bb093ff64f2eab457f9ef19b186
a1d9cd6f189beff28a0a49b10f8fe4510128471f004b3e4283ddc7f78594906b
a93ee7ea13238bd038bcbec635f39619db566145498fe6e0ea60e6e76d614bd3
b43b234012b8233b3df6adb7c0a3b2b13cc2354dd6de27e092873bf58af2693c
eb47cd6a937221411bb8daf35900a9897fb234160087089a064066a65f42bcd4
24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c
24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c
2c2d8bc91564050cf073745f1b117f4ffdd6470e87166abdfcd10ecdff040a2e
7a828afd2abf153d840938090d498072b7e507c7021e4cdd8c6baf727cafc545
a897345b68191fd36f8cefb52e6a77acb2367432abb648b9ae0a9d708406de5b
fb0b6044347e972e21b6c376e37e1115dab494a2c6b9fb28b92b1e45b45d0ebc
9588f2ef06b7e1c8509f32d8eddfa18041a9cc15b1c90d6da484a39f8dcdf967
b43b234012b8233b3df6adb7c0a3b2b13cc2354dd6de27e092873bf58af2693c
4186675cb6706f9d51167fb0f14cd3f8fcfb0065093f62b10a15f7d9a6c8d982
09a46b3e1be080745a6d8d88d6b5bd351b1c7586ae0dc94d0c238ee36421cafa
d41d8cd98f00b204e9800998ecf8427e
666c806b76568adb5a6c3d34c434820e
a8d30fd8ffd02886818a89ebdd8e7502
6faeaf98d0eaf6671d74bc8e468bddc8ed1e0597
09a46b3e1be080745a6d8d88d6b5bd351b1c7586ae0dc94d0c238ee36421cafa
11d0f63c06263f50b972287b4bbd1abe0089bc993f73d75768b6b41e3d6f6d49
149601e15002f78866ab73033eb8577f11bd489a4cea87b10c52a70fdf78d9ff
16493ecc4c4bc5746acbe96bd8af001f733114070d694db76ea7b5a0de7ad0ab
190d9c3e071a38cb26211bfffeb6c4bb88bd74c6bf99db9bb1f084c6a7e1df4e
24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c
2584e1521065e45ec3c17767c065429038fc6291c091097ea8b22c8a502c41dd
4186675cb6706f9d51167fb0f14cd3f8fcfb0065093f62b10a15f7d9a6c8d982
593bbcc8f34047da9960b8456094c0eaf69caaf16f1626b813484207df8bd8af
043e0d0d8b8cda56851f5b853f244f677bd1fd50f869075ef7ba1110771f70c2
5d26835be2cf4f08f2beeff301c06d05035d0a9ec3afacc71dff22813595c0b9
76a3666ce9119295104bb69ee7af3f2845d23f40ba48ace7987f79b06312bbdf
be22645c61949ad6a077373a7d6cd85e3fae44315632f161adc4c99d5a8e6844
f7c7b5e4b051ea5bd0017803f40af13bed224c4b0fd60b890b6784df5bd63494
fc626fe1e0f4d77b34851a8c60cdd11172472da3b9325bfe288ac8342f6c710a

aee20f9188a5c3954623583c6b0e6623ec90d5cd3fdec4e1001646e27664002c
b9c5d4339809e0ad9a00d4d3dd26fdf44a32819a54abf846bb9b560d81391c25

URLs

http://146.0.32.144:9001
http://188.166.23.127:443
http://193.23.244.244:443
http://2.3.69.209:9001
http://50.7.161.218:9001P
gx7ekbenv2riucmf.onion
hxxp://iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
57g7spgrzlojinas.onion
easysupport.us
www.leadhacker.ru
bctxawdt.us
w5q7spejg96n.com
nnnlafqfnrbynwor.us
lkbsxkitgxttgaobxu.us
depuisgef.us
gxrytjoclpvv.us
peuwdchnvn.us
frullndjtkojlu.us
iouenviwrc.us
gcidpiuvamynj.us
kuuelejkfwk.us
xmqlcikldft.us
pvbeqjbqrslnkmashlsxb.us
pxyhybnyv.us
enyeikruptiukjorq.com
cokfqwjmferc.us
yobvyjmjbsgdfqnh.us
rkhlkmpfpoqxmlqmkf.us
yrwgugricfklb.us
cxbenjiikmhjcerbj.us
srwcjdfrtnhnjekjerl.us
ryitsfeogisr.us
hanoluexjqcf.us
udrgtaxgdyv.us
thstlufnunxaksr.us
iarirjjrnuornts.us
ns768.com
ywpvqhlqnssecpdemq.us
ifbjoosjqhaeqjjwaerri.us
qkkftmpy.us
agrdwrtj.us

ofdwcjnko.us
edoknehyvbl.us
mbfce24rgn65bx3g.jktew0.com
mbfce24rgn65bx3g.lfsjkad.net
mbfce24rgn65bx3g.yio3lvx.com
7gie6ffnkrjykggd.2kzm0f.com
mbfce24rgn65bx3g.2kzm0f.com
7gie6ffnkrjykggd.jktew0.com
7gie6ffnkrjykggd.jpo2z1.net
mbfce24rgn65bx3g.6t4u2p.net
mbfce24rgn65bx3g.jpo2z1.net
000o9jtv2.ru
yio3lvx.com
lfsjkad.net
jktew0.com
ww1.000o9jtv2.ru
882ybcdzjwi1.ru

IPs
91.121.65.179
89.40.71.149
86.59.21.38
83.169.6.12
81.30.158.223
81.19.88.103
79.172.193.32
62.138.7.171
51.255.203.235
51.15.36.164
50.7.161.218
47.91.107.213
46.101.166.19
217.79.179.177
217.69.133.148
213.61.66.116
212.47.232.237
2.3.69.209
199.254.238.52
197.231.221.211
193.23.244.244
193.11.114.43
192.42.113.102
188.166.23.127
178.208.83.16
176.9.80.202

176.9.39.218
167.114.35.28
163.172.149.155
158.69.92.127
149.202.160.69
146.0.32.144
128.31.0.39
94.23.204.175
91.134.139.207
84.80.80.69
81.30.158.223
79.172.193.32
79.172.193.32
51.254.115.225
5.9.158.75
46.101.140.16
217.79.179.177
217.160.13.173
213.61.66.116
212.47.232.237
198.199.90.205
194.109.206.212
188.42.216.83
151.80.42.103
144.76.42.239
141.20.103.25
138.201.132.17
131.188.40.189
128.31.0.39
128.31.0.39
104.238.167.111
212.47.232.237
79.172.193.32
38.229.72.16
2.3.69.209
217.79.179.177
188.166.23.127
193.23.244.244
81.30.158.223
50.7.161.218
128.31.0.39
213.61.66.116
146.0.32.144
89.45.235.21
188.138.33.220

217.79.179.77
86.59.21.38
83.169.6.12
104.131.84.119
178.254.44.135
198.199.64.217
163.172.25.118
192.42.115.102
2.3.69.209
50.7.161.218
146.0.32.144
188.166.23.127
193.23.244.244
104.155.67.78
52.11.100.253
35.164.244.192
79.172.193.32
144.217.254.3
79.137.66.14

File names
wcry.exe
WanAcry.exe
wanacry.exe
@WanaDecryptor@.exe
@Please_Read_Me@.txt
*.wncry.
%windows%\wanacry.exe
%windows%\@WanaDecryptor@.exe
%userprofile%\Desktop\wanacry.exe
%userprofile%\Desktop\@WanaDecryptor@.exe
%LocalLow%\wanacry.exe
%LocalLow%\@WanaDecryptor@.exe
%Local%\wanacry.exe
%Local%\@WanaDecryptor@.exe
%homedrive%\wanacry.exe
%homedrive%\@WanaDecryptor@.exe
%AppData%\wanacry.exe
%AppData%\@WanaDecryptor@.exe
gx7ekbenv2riucmf.onion
Xxlvbrloxvriy2c5.onion
cwwnhwhlz52maqm7.onion
sqjolphimrr7jqw6.onion
57g7spgrzlojinas.onion
76jdd2ir2embyv47.onion

diskpart.exe
wannacry.exe
lhdfrgui.exe
@WanaDecryptor@.exe
taskse.exe
b.wnry
taskdl.exe
u.wnry
r.wnry
s.wnry
c.wnry
t.wnry

Targeted 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

Appendix III: Languages targeted

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

Appendix IV: The ShadowBrokers issue

The Shadow Brokers (TSB) is a hacker group that first appeared in the summer of 2016. It published several leaks containing alleged NSA hacking tools, including several zero-day exploits. Specifically, these exploits and vulnerabilities targeted enterprise firewalls, antivirus products and Microsoft products. The Shadow Brokers originally attributed the leaks to the Equation Group threat actor.

First leak: "Equation Group Cyber Weapons Auction – Invitation"

While the exact date is unclear, reports suggest that preparation of the leak started at least in the beginning of August, and that the initial publication occurred 13 August 2016 with a tweet from a Twitter account @shadowbrokerss announcing a Pastebin page and a GitHub repository containing references and instructions for obtaining and decrypting the content of a file supposedly containing tools and exploits used by Equation Group.

The Pastebin includes various references for obtaining the file, named EQGRP-Auction-Files.zip. This zip file contains seven files, two of which are the GPG-encrypted archives eqgrp-auction-file.tar.xz.gpg and eqgrp-free-file.tar.xz.gpg. The eqgrp-free-file.tar.xz.gpg archive's password was revealed in the original Pastebin to be theequationgroup. The eqgrp-auction-file.tar.xz archive's password was revealed in a later Medium post to be CrDj"(;Va.*NdlnzB9M?@K2)#>deB7mN.

Second leak: "Message #5 - TrickOrTreat"

This publication, made on 31 October 2016, contains a list of servers, supposedly compromised by Equation Group as well as references to seven supposedly undisclosed tools (DEWDROP, INCISION, JACKLADDER, ORANGUTAN, PATCHICILLIN, RETICULUM, SIDETRACK AND STOCSURGEON) also used by the threat actor.

Third leak: "Message #6 - BLACK FRIDAY / CYBER MONDAY SALE"

This leak contains 60 folders named in a way to serve as a reference to tools likely used by Equation Group. The leak doesn't contain executable files, but rather screenshots of the tools' file structure. While the leak could be a fake, the overall cohesion between previous and future leaks and references as well as the work required to fake such a fabrication gives credibility to the theory that the referenced tools are genuine.

Fourth leak: "Don't Forget Your Base"

On 8 April 2017, the Medium account used by The Shadow Brokers posted a new update. The post released the password to encrypted files released last year to be CrDj"(;Va.*NdlnzB9M?@K2)#>deB7mN. Those files allegedly reveal more NSA hacking tools. This posting explicitly stated that the post was partially in response to President Donald Trump's attack against a Syrian airfield, which was also used by Russian forces.

Fifth leak: "Lost in Translation"

On 14 April 2017, the Twitter account used by The Shadow Brokers posted a tweet with a link to a Steemit story. Herein was a message with a link to the leak files, encrypted with the password Reeeeeeeeeeeeee.

The overall content is based around three folders: "oddjob," "swift" and "windows." The fifth leak is suggested to be the "… most damaging release yet," and CNN quoted Matthew Hickey as saying, "This is quite possibly the most damaging thing I've seen in the last several years."

The leak includes, among other things, the tools and exploits codenamed DANDERSPIRITZ, ODDJOB, FUZZBUNCH, DOUBLEPULSAR, ETERNALSYNERGY, ETERNALROMANCE, ETERNALBLUE, EXPLODINGCAN and EWOKFRENZY.

Some of the exploits targeting the Windows operating system, such as ETERNALBLUE and DOUBLEPULSAR, had been patched in a Microsoft Security Bulletin on 14 March 2017, one month before the leak occurred.

ETERNALBLUE: (CVE-2017-044) is an exploit that is believed to have been created by NSA and released publically by Shadow Brokers on 14 April. Microsoft relased a patch for this vulnerability on 14 March 2017. To date, CTI has not seen any reporting on a business being impacted that implemented the patch.

DOUBLEPULSAR: This is not an exploit; it is an implant that would be delivered via some exploit. The implant then allows for delivery of a malicious DLL from a remote system and then injects that DLL into memory on the compromised system. Think of an implant as a specialized back door. As such, there is no patch for DOUBLEPULSAR, just the exploits that were used to deliver it.

Appendix V: Microsoft alert for EternalBlue

Microsoft Security Bulletin MS17-010 - Critical
Security Update for Microsoft Windows SMB Server (4013389) Published: 14 March 2017
Version: 1.0

Executive Summary
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.

This security update is rated Critical for all supported releases of Microsoft Windows. For more information, see the Affected Software and Vulnerability Severity Ratings section.

The security update addresses the vulnerabilities by correcting how SMBv1 handles specially crafted requests.

For more information about the vulnerabilities, see the Vulnerability Information section.

For more information about this update, see Microsoft Knowledge Base Article 4013389.

Vulnerability Information
Multiple Windows SMB Remote Code Execution Vulnerabilities
Remote code execution vulnerabilities exist in the way that the Microsoft Server Message Block 1.0 (SMBv1) server handles certain requests. An attacker who successfully exploited the vulnerabilities could gain the ability to execute code on the target server.

To exploit the vulnerability, in most situations, an unauthenticated attacker could send a specially crafted packet to a targeted SMBv1 server.

The security update addresses the vulnerabilities by correcting how SMBv1 handles these specially crafted requests.

The following table contains links to the standard entry for each vulnerability in the Common Vulnerabilities and Exposures list:

Vulnerability title	CVE number	Publicly disclosed	Exploited
Windows SMB Remote Code Execution Vulnerability	CVE-2017-0143	No	No
Windows SMB Remote Code Execution Vulnerability	CVE-2017-0144	No	No
Windows SMB Remote Code Execution Vulnerability	CVE-2017-0145	No	No
Windows SMB Remote Code Execution Vulnerability	CVE-2017-0146	No	No
Windows SMB Remote Code Execution Vulnerability	CVE-2017-0148	No	No

Mitigating Factors
Microsoft has not identified any mitigating factors for these vulnerabilities.

Workarounds
The following workarounds may be helpful in your situation:
▸ Disable SMBv1 For customers running Windows Vista and later

See Microsoft Knowledge Base Article 2696547.

Alternative method for customers running Windows 8.1 or Windows Server 2012 R2 and later
For client operating systems:
1. Open Control Panel, clickPrograms, and then click Turn Windows features on or off.
2. In the Windows Features window, clear the SMB1.0/CIFS File Sharing Support checkbox, and then click OK to close the window.
3. Restart the system.

For server operating systems:
1. Open Server Manager and then click the Manage menu and select Remove Roles and Features.
2. In the Features window, clear the SMB1.0/CIFS File Sharing Support check box, and then click OK to close the window.
3. Restart the system.

Impact of workaround. The SMBv1 protocol will be disabled on the target system.

How to undo the workaround. Retrace the workaround steps, and select the SMB1.0/CIFS File Sharing Support check box to restore the SMB1.0/CIFS File Sharing Support feature to an active state.

See the full bulletin: Microsoft Bulletin MS17-010 - Eternal Blue Exploit

Appendix VI: Sourcing

- *The Daily Express,* http://www.express.co.uk/news/uk/803821/NHS-cyber-attack-hospital-trusts-hacked-cyber-security-hack-virus-patient-details, accessed 15 May 2017
- *The Verge (UK hospitals hit with massive ransomware attack),* https://www.theverge.com/2017/5/12/15630354/nhs-hospitals-ransomware-hack-wannacry-bitcoin, accessed 15 May 2017
- *Gizmodo*, http://gizmodo.com/theres-a-massive-ransomware-attack-spreading-globally-r-1795168952, accessed 15 May 2017
- *Twitter Malware Tech (Ransomware country target mapping),* https://twitter.com/MalwareTechBlog/status/863054943632187392, accessed 15 May 2017
- *Talos, http://blog.talosintelligence.com/2017/05/wannacry.html,*
- *Troy Hunt blog, https://www.troyhunt.com/everything-you-need-to-know-about-the-wannacrypt-ransomware/*, accessed 15 May 2017
- *New York Times, https://www.nytimes.com/interactive/2017/05/12/world/europe/wannacry-ransomware-map.html?_r=2*, accessed 17 May 2017
- *Kalb,* http://www.kalb.com/content/news/Huge-Cyberattack-Hits-Nearly-100-Countries-With-Wanna-Decryptor-Malware-422167474.html, accessed 13 May 2017
- *New York Times,* https://www.nytimes.com/2017/05/12/world/europe/uk-national-health-service-cyberattack.html?_r=0, accessed 17 May 2017
- *Telefonica,* https://www.telefonica.com/en/web/press-office/-/cibersecurity-incident,
- *Twitter Jakub Kroustek,* https://twitter.com/JakubKroustek/status/863045197663490053, accessed 13 May 2017
- *New York Times,* https://www.nytimes.com/2017/05/12/world/europe/uk-national-health-service-cyberattack.html?_r=0, accessed 17 May 2017
- *New York Times,* https://www.nytimes.com/interactive/2017/05/12/world/europe/wannacry-ransomware-map.html?_r=1, accessed 16 May 2017
- *Centro Criptologico Nacional,* https://www.ccn-cert.cni.es/seguridad-al-dia/comunicados-ccn-cert/4464-ataque-masivo-de-ransomware-que-afecta-a-un-elevado-numero-de-organizaciones-espanolas.html\, accessed 16 May 2017
- *Microsoft TecNet,* https://blogs.technet.microsoft.com/msrc/2017/04/14/protecting-customers-and-evaluating-risk/, accessed 17 May 2017
- *McAfee,* https://securingtomorrow.mcafee.com/executive-perspectives/analysis-wannacry-ransomware-outbreak/, accessed 17 May 2017
- *McAfee,* https://securingtomorrow.mcafee.com/executive-perspectives/analysis-wannacry-ransomware-outbreak/., accessed 17 May 2017
- *Cisco's Talos Intelligence Group Blog,* http://blog.talosintelligence.com/2017/05/wannacry.html
- *Rapid 7 Vulnerability & Exploit Database,* https://www.rapid7.com/db/modules/auxiliary/scanner/smb/smb_ms17_010, accessed 17 May 2017
- *Microsoft,* 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, accessed 17 May 2017
- *McAfee,* https://securingtomorrow.mcafee.com/executive-perspectives/analysis-wannacry-ransomware-outbreak/, accessed 17 May 2017
- *Sophos,* https://www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/Troj~Sage-P/detailed-analysis.aspx, accessed 17 May 2017
- *Securelist,* https://securelist.com/blog/incidents/78351/wannacry-ransomware-used-in-widespread-attacks-all-over-the-world/, accessed 17 May 2017
- *International Business Times,* http://www.ibtimes.co.uk/wannacry-list-major-companies-networks-hit-by-deadly-ransomware-around-globe-1621587, accessed 17 May 2017

EY | Assurance | Tax | Transactions | Advisory

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

EYG no. 03390-173Gbl
ED None

ey.com/cybersecurity
ey.com/ransomware