Threat Intelligence

WannaCry Ransomware Campaign: Threat Details and Risk Management

May 15, 2017

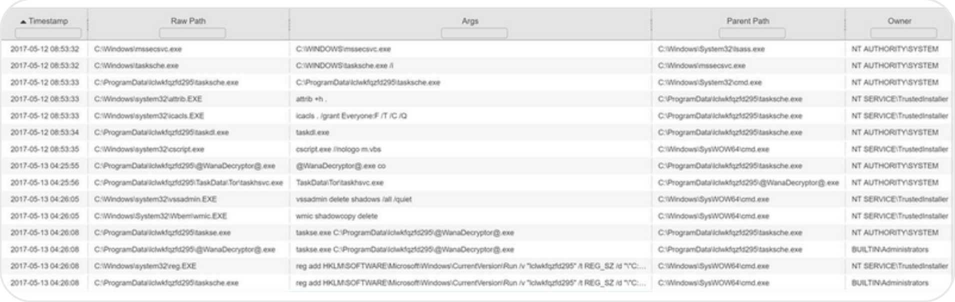
Mandiant

We observed the emergence of a new WannaCry variant with the internet-check URL www.ifferfsodp9ifjaposdfjhgosurijfaewrwergwea[.]testing . A bug in the code logic causes the malware to actually query www.ifferfsodp9ifjaposdfjhgosurijfaewrwergwea[.]test. The malware will encrypt your files only if it cannot contact this domain (specifically, if it cannot make a successful HTTP request to the resolution of the domain). Security researchers were able to register these “killswitch” domains for previous variants to stop encryption; however, this particular domain cannot be registered, since the .test TLD is reserved by the Internet Engineering Task Force (IETF) for testing purposes only. So, if this malware infects a system, the infrastructure killswitch approach used to date cannot be applied to stop encryption.

Organizations seeking to protect themselves from this latest variant can still “locally” sinkhole the domain by adding a DNS A-record to their DNS server and translating the domain to any of the existing sinkhole IPs.

We are currently investigating how widely this new variant

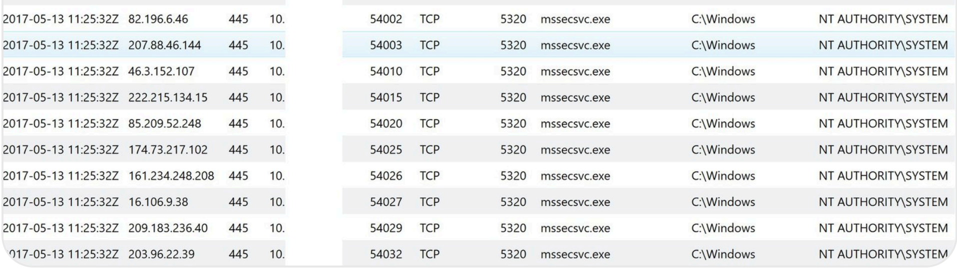
FireEye has analyzed a number of systems infected with WannaCry. Figure 2 depicts the real-time process execution events from a Windows 7 system infected with WannaCry via the EternalBlue SMB exploit. Of particular note is that the parent process of the mssecsvc.exe dropper is lsass.exe (which indicates that the system was compromised by the SMB exploit that injects a dll into lsass.exe). Additionally, all malware specific processes are owned by system accounts (e.g. NT AUTHORITY\SYSTEM and BUILTIN\Administrators) and not the primary user of the system.



▲ Timestamp	Raw Path	Args	Parent Path	Owner
2017-05-12 08:53:32	C:\Windows\mssecsvc.exe	C:\WINDOWS\mssecsvc.exe	C:\Windows\System32\lsass.exe	NT AUTHORITY\SYSTEM
2017-05-12 08:53:32	C:\Windows\tasksche.exe	C:\WINDOWS\tasksche.exe /i	C:\Windows\mssecsvc.exe	NT AUTHORITY\SYSTEM
2017-05-12 08:53:33	C:\ProgramData\iclwkfqzfd295\tasksche.exe	C:\ProgramData\iclwkfqzfd295\tasksche.exe	C:\Windows\System32\cmd.exe	NT AUTHORITY\SYSTEM
2017-05-12 08:53:33	C:\Windows\system32\attrib.EXE	attrib +h .	C:\ProgramData\iclwkfqzfd295\tasksche.exe	NT SERVICE\TrustedInstaller
2017-05-12 08:53:33	C:\Windows\system32\icacls.EXE	icacls . /grant Everyone:F /T /C /Q	C:\ProgramData\iclwkfqzfd295\tasksche.exe	NT SERVICE\TrustedInstaller
2017-05-12 08:53:34	C:\ProgramData\iclwkfqzfd295\taskdl.exe	taskdl.exe	C:\ProgramData\iclwkfqzfd295\tasksche.exe	NT AUTHORITY\SYSTEM
2017-05-12 08:53:35	C:\Windows\system32\cscript.exe	cscript.exe //nologo m.vbs	C:\Windows\SysWOW64\cmd.exe	NT SERVICE\TrustedInstaller
2017-05-13 04:25:55	C:\ProgramData\iclwkfqzfd295\@WanaDecryptor@.exe	@WanaDecryptor@.exe co	C:\ProgramData\iclwkfqzfd295\tasksche.exe	NT AUTHORITY\SYSTEM
2017-05-13 04:25:56	C:\ProgramData\iclwkfqzfd295\TaskData\Tor\taskhsvc.exe	TaskData\Tor\taskhsvc.exe	C:\ProgramData\iclwkfqzfd295\@WanaDecryptor@.exe	NT AUTHORITY\SYSTEM
2017-05-13 04:26:05	C:\Windows\system32\vssadmin.EXE	vssadmin delete shadows /all /quiet	C:\Windows\SysWOW64\cmd.exe	NT SERVICE\TrustedInstaller
2017-05-13 04:26:05	C:\Windows\System32\Wbem\wmic.EXE	wmic shadowcopy delete	C:\Windows\SysWOW64\cmd.exe	NT SERVICE\TrustedInstaller
2017-05-13 04:26:08	C:\ProgramData\iclwkfqzfd295\taskse.exe	taskse.exe C:\ProgramData\iclwkfqzfd295\@WanaDecryptor@.exe	C:\ProgramData\iclwkfqzfd295\tasksche.exe	NT AUTHORITY\SYSTEM
2017-05-13 04:26:08	C:\ProgramData\iclwkfqzfd295\@WanaDecryptor@.exe	taskse.exe C:\ProgramData\iclwkfqzfd295\@WanaDecryptor@.exe	C:\ProgramData\iclwkfqzfd295\tasksche.exe	BUILTIN\Administrators
2017-05-13 04:26:08	C:\Windows\system32\reg.EXE	reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v "iclwkfqzfd295" /t REG_SZ /d "\"C:...	C:\Windows\SysWOW64\cmd.exe	NT SERVICE\TrustedInstaller
2017-05-13 04:26:08	C:\ProgramData\iclwkfqzfd295\tasksche.exe	reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v "iclwkfqzfd295" /t REG_SZ /d "\"C:...	C:\Windows\SysWOW64\cmd.exe	BUILTIN\Administrators

Figure 2: Real-time process execution events

Systems successfully infected with WannaCry will scan random IP addresses very rapidly (about 25 IP addresses per second) for open TCP 445 ports (the port used for SMB communications) and if open will attempt to spread



2017-05-13 11:25:32Z	82.196.6.46	445	10.	54002	TCP	5320	mssecsvc.exe	C:\Windows	NT AUTHORITY\SYSTEM
2017-05-13 11:25:32Z	207.88.46.144	445	10.	54003	TCP	5320	mssecsvc.exe	C:\Windows	NT AUTHORITY\SYSTEM
2017-05-13 11:25:32Z	46.3.152.107	445	10.	54010	TCP	5320	mssecsvc.exe	C:\Windows	NT AUTHORITY\SYSTEM
2017-05-13 11:25:32Z	222.215.134.15	445	10.	54015	TCP	5320	mssecsvc.exe	C:\Windows	NT AUTHORITY\SYSTEM
2017-05-13 11:25:32Z	85.209.52.248	445	10.	54020	TCP	5320	mssecsvc.exe	C:\Windows	NT AUTHORITY\SYSTEM
2017-05-13 11:25:32Z	174.73.217.102	445	10.	54025	TCP	5320	mssecsvc.exe	C:\Windows	NT AUTHORITY\SYSTEM
2017-05-13 11:25:32Z	161.234.248.208	445	10.	54026	TCP	5320	mssecsvc.exe	C:\Windows	NT AUTHORITY\SYSTEM
2017-05-13 11:25:32Z	16.106.9.38	445	10.	54027	TCP	5320	mssecsvc.exe	C:\Windows	NT AUTHORITY\SYSTEM
2017-05-13 11:25:32Z	209.183.236.40	445	10.	54029	TCP	5320	mssecsvc.exe	C:\Windows	NT AUTHORITY\SYSTEM
017-05-13 11:25:32Z	203.96.22.39	445	10.	54032	TCP	5320	mssecsvc.exe	C:\Windows	NT AUTHORITY\SYSTEM

Figure 3: Real-time TCPv4 network connection events

UPDATE (May 16 – 8:00 p.m. ET)

On May 15, we observed at least two new killswitch domains being used by WannaCry variants, ayylmaotjhsstasdfasdfasdfasdfasdfasdfasdf[.]com (This domain matches the format of WannaCry-associated domains, but has not yet been clearly linked to a specific sample. Organizations wish to maintain awareness of this domain in the event that it is associated with WannaCry activity.) and iuqssfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com. These domains were also sinkholed. Again, we currently lack visibility as to whether these changes were implemented by the original distributors or a third party modifying distributed samples.

Attribution

Financially motivated cyber criminals are typically responsible for ransomware operations, with many such actors operating independently worldwide; however, as of yet, none of these actors have been identified as a strong candidate for attributing the WannaCry operation.

Some aspects of the WannaCry operation suggest the operators may not be highly sophisticated and may not have anticipated the malware would spread as widely as it has. One of these aspects is the aforementioned killswitch functionality. Sophisticated malware developers experienced with combatting security countermeasures might have anticipated this functionality would constitute a threat to the malware’s success. Another aspect is that identified ransom payments have been reported to be relatively low thus far, suggesting the operators’ payment system may not have been equipped to handle the outcome of worldwide infections.

Numerous open-source reports allege potential North Korean involvement in this campaign. Based on FireEye’s initial analysis, the code similarities cited between allegedly North Korea-linked malware and WannaCry constitute a potential lead worth further investigation, but are not unique enough independent of other evidence to be clearly indicative of common operators.

Since May 12, 2017, a highly prolific WannaCry ransomware campaign has been observed impacting organizations globally. WannaCry (aka WCry or WanaCryptor) malware is self-propagating (worm-like) ransomware that spreads through internal networks and over the public internet by exploiting a vulnerability in Microsoft Server Message Block (SMB) protocol. The malware appends encrypted data files with the .WCRY extension, drops and executes a decryptor tool, and demands $300 or $600 USD (via Bitcoin) to decrypt the data. The malware uses encrypted Tor channels for command and control (C2) communications.

Based on our analysis, malicious binaries associated with WannaCry activity are comprised of two distinct components, one that provides ransomware functionality – acting very similar to WannaCry malware samples reported before May 12 – and a component used for propagation, which contains functionality to enable the discussed scanning and SMB exploitation capabilities.

Given the rapid and prolific distribution of this ransomware, FireEye iSIGHT Intelligence considers this activity to pose a significant risk to all organizations using potentially vulnerable Windows machines.

environment. This propagation mechanism can distribute the malware both within the compromised network and over the public internet. The exploit used is codenamed "EternalBlue" and was leaked by Shadow Brokers. The exploited vulnerability, was patched in Microsoft MS17-010.

Based on our analysis, the malware spawns two threads. The first thread enumerates the network adapters and determines which subnets the system is on. The malware then generates a thread for each IP on the subnet. Each of these threads attempt to connect to the IP on TCP port 445 and, if successful, attempt exploitation of the system. An example of an attempt to exploit a remote system can be seen in Figure 1.

Figure 1: WannaCry network traffic attempting SMB exploit

In response to the use of this exploited vulnerability, Microsoft has provided [specific risk management steps for WannaCry](#).

While WannaCry ransomware has spread primarily through SMB exploitation, its operators may also use other distribution methods. Early reports suggested to ransomware activity, such as malicious documents, malvertising, or compromises of high-traffic sites. In light of this campaign's high impact thus far and the uncertainties as to early distribution vectors, organizations should consider any common malware delivery vector a potential source of WannaCry infection.

Malware Characteristics

Each of the WannaCry variants identified to date (that had worm-like functionality) included a killswitch that a number of security researchers have used to prevent the malware from encrypting files. However, operators could eliminate or modify this feature, as demonstrated by the emergence of multiple variants with new a domain.

- Upon infecting a victim machine, the WannaCry package that began spreading on May 12 attempts to contact: www[.]iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com. If the malware could successfully reach this domain, based on FireEye's testing, it would not perform encryption or self-propagation (some organizations have reported the malware will continue to self-propagate in this case, but we have not confirmed this behavior in test environments). This

- On May 14, a variant surfaced with a new killswitch domain: www[.]ifferfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com. This domain was also sinkholed, ostensibly causing the killswitch behavior to disable any WannaCry infections that contacted the domain. Whether this domain contact change was implemented by the original distributors or a third party modifying distributed samples is unclear.
- Also on May 14, a new variant was identified that does not contain the domain contact killswitch functionality. However, this change may have been implemented by a third party after the malware was compiled rather than by the operators. The ransomware component of this variant appears corrupted and does not function in test environments.

Impact

Despite encouraging reports of waning threat activity, WannaCry continues to pose significant risks. Given this malware's effective repropagation mechanisms, virtually any organization that hasn't applied Microsoft's recommended mitigation mechanisms is at potential risk of attempted WannaCry propagation. Furthermore, the

Risk Management

Organizations seeking to protect themselves from this threat should read Microsoft's blog on addressing the associated SMB exploitation.

The rapid, prolific distribution of this ransomware has influenced swift, proactive updates to FireEye’s entire portfolio of detection technologies, threat intelligence analysis and recommendations and consulting services.

FireEye’s Network, Email, and Endpoint products have ransomware detection capabilities that can proactively detect and, if deployed inline, or with Exploit Guard enabled, can block new ransomware (including WannaCry) distributed through web and email infection vectors. WannaCry operators could leverage these popular delivery mechanisms at any time. Should this occur, FireEye product customers would be alerted by the following alerts:

- HX: WMIC SHADOWCOPY DELETE, WANNACRY RANSOMWARE, *Ransom.WannaCryptor.*, or Trojan.Generic*. Exploit Guard and Anti-Virus alert names will depend on delivery mechanism and

FireEye products also detect later stage WannaCry activity, such as command and control communications and host indicators for existing WannaCry infections. Additionally, FireEye PX (Network Forensics) sensors deployed internally and monitored by FireEye as a Service (FaaS) can detect SMB propagation traffic. Customers can leverage confirmed indicators to hunt for possible infections. These indicators have been deployed to FireEye HX (Endpoint) customers and are available on the MySIGHT intelligence portal for iSIGHT subscription customers.

Network proxies and other enterprise network security features may prevent the malware from contacting its killswitch domain and inadvertently trigger encryption. Organizations may wish to adjust their proxy configurations or other network configurations to avoid this problem.

Additionally, organizations can leverage the following indicators of compromise to identify potentially related activity. These have been obtained during preliminary analysis of associated samples and continuing investigation.

Related Sample MD5s:

06e235714dfa46e0ef3d15e45331ebe1

09431f379fc1914685f93f56c2400133

0cb40a8a51539e2c5727c3ec87af8a56

0fb1ce09b168987ce7f47bcd82fa034d

1177e33203cb8b1d71fe9147364328fe

13d702666bb8eadcd60d0c3940c39228

16aa3809de7a2a87d97de34ed7747638

18ad48cf2ed0cfeda8636187169ab181

1c615bf80a47848f17f935e689ae7ee2

246c2781b88f58bc6b0da24ec71dd028

2822abbaff89f989a4377b3c54067540

29365f675b69ffa0ec17ad00649ce026

2b4e8612d9f8cdcf520a8b2e42779ffa

3600607ab080736dd31859c02eaff188

36ebcf590480009be4c9c2259982a71a

38089fd3b6f1faa54cfe974fd1e29f0a

3c1ab42f5dd52f217ec57d270ffc8960

3c6375f586a49fc12a4de9328174f0c1

42fcf5f97f224c53a0434856016c706c

4362e287ca45a4862b7fe9ecaf46e985

468d1f5e0b048c16fd6d5364add58640

46d140a0eb13582852b5f778bb20cf0e

4e1f1183a31740618213f4e4c619b31c

4fef5e34143e646dbf9907c4374276f5

509c41ec97bb81b0567b059aa2f50fe8

546c1d3e78d9a0c676648e1230b8d454

5982d0ca85b00f59a44c0d1e9114da5e

59815ca85fa772753ca37fa0399c668c

59fc71209d74f2411580f6e1b6daf8d8

5bef35496fcbdbe841c82f4d1ab8b7c2

638f9235d038a0a001d5ea7f5c5dc4ae

6a4041616699ec27b42f98bbf111a448

707282fc5832e4674a2b5904b4115202

775a0631fb8229b2aa3d7621427085ad

7bf2b57f2a205768755c07f238fb32cc

7ecd842a3e9b1bcb3bb70b98220a563b

7f7ccaa16fb15eb1c7399d422f8363e8

80a2af99fd990567869e9cf4039edf73

82fc5885862b097be5ec9ec2176e30f1

82fd8635ff349f2f0d8d42c27d18bcb7

835fff032e51075e0e37946f6cbd64a2

8d8e6512155651953lff64c1ed0bfe09

8dd63adb68ef053e044a5a2f46e0d2cd

8ff9c908dea430ce349cc922cee3b7dc

92cc807fa1ff0936ef7bcd59c76b123b

93ebec8b34a4894c34c54cca5039c089

947d69c0531504ee3f7821574ea405a7

9503af3b691e22149817edb246ea7791

96714005ac1ddd047a8eda781249d683

96dff36b5275c67e35097d77a120d0d4

998ea85d3e72824a8480d606d33540a6

a0a46b3ea8b643acd8b1b9220701d45d

a155e4564f9ec62d44bf3ea2351fd6ce

a2ded86d6ddc7d1fca74925c111d6a95

b675498639429b85af9d70be1e8a8782

b6ded2b8fe83be35341936e34aa433e5

b77288deb5e9ebced8a27c5ea533d029

b7f7ad4970506e8547e0f493c80ba441

b8a7b71bfbde9901d20ab179e4dead58

bdda04ebcc92840a64946fc222edc563

be70ee98253ae9ebbf91af35da829ee0

be74e91f1ef8b4cb9e3918911e429124

bec0b7aff4b107edd5b9276721137651

c2559b51cfd37bdbd5fdb978061c6c16

c39ed6f52aaa31ae0301c591802da24b

c61256583c6569ac13a136bfd440ca09

cb97641372f4e31670574cc4faa5df59

d724d8cc6420f06e8a48752f0da11c66

db349b97c37d22f5ea1d1841e3c89eb4

df535dcb74ab9e2ba0a63b3519eee2bb

e16b903789e41697ecab21ba6e14fa2b

e372d07207b4da75b3434584cd9f3450

eb7009df4951e18ccbe4f035985b635c

efa8cda6aa188ef8564c94a58b75639f

f0d9ffefa20cdadf5b47b96b7f8d1f60

f107a717f76f4f910ae9cb4dc5290594

f351e1fcca0c4ea05fc44d15a17f8b36

f4856b368dc74f04adb9c4548993f148

f529f4556a5126bba499c26d67892240

f9992dfb56a9c6c20eb727e6a26b0172

Related URLs:

iuqssfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com

ifferfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com

iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com

Ayylmaotjhsstasdfasdfasdfasdfasdfasdfasdf[.]com (This domain matches the format of WannaCry-associated domains, but has not yet been clearly linked to a specific sample. Organizations wish to maintain awareness of this domain in the event that it is associated with WannaCry activity.)

Related Tor Sites:

57g7spgrzlojinas[.]onion

76jdd2ir2embyv47[.]onion

cwwnhwhlz52maqm7[.]onion

gx7ekbenv2riucmf[.]onion

sqjolphimrr7jqw6[.]onion

Xxlvbrloxvriy2c5[.]onion

Related Registry Keys:

HKEY_LOCAL_MACHINE\Software\WanaCrypt0r

Related Files Created:

%TEMP%\m.vbs

%TEMP%\b.wrny

%TEMP%\c.wrny

taskse.exe

taskdl.exe

@Please_Read_Me@.txt

@WanaDecryptor@.exe

Related File Strings:

Wanna Decryptor 1.0

Wana Decrypt0r

Wana Decryptor

WANNACRY

Note: Additional files with .wnry extensions may be created.

Related Processes Started:

cscript.exe //nologo m.vbs

Related SNORT Signatures:

The following SNORT signatures may be useful for identifying SMB exploitation activity related to this threat.

Posted in Threat Intelligence—Security & Identity

Related articles

Compromise Ukrainian Military Recruits and Deliver Anti-Mobilization Narratives

By Google Threat Intelligence Group • 10-minute read

By Mandiant • 19-minute read

Threat Intelligence

How Low Can You Go? An Analysis of 2023 Time-to-Exploit Trends

By Mandiant • 10-minute read

Threat Intelligence

capa Explorer Web: A Web-Based Tool for Program Capability Analysis

By Mandiant • 6-minute read