Cisco Talos Blog

Player 3 Has Entered the Game: Say Hello to 'WannaCry'

By Cisco Talos

FRIDAY, MAY 12, 2017 18:09

RANSOMWARE

By Martin Lee, Warren Mercer, Paul Rascagneres, and Craig Williams.

Executive Summary

A major ransomware attack has affected many organizations across the world reportedly including Telefonica in Spain, the National Health Service in the UK, and FedEx in the US. The malware responsible for this attack is a ransomware variant known as 'WannaCry'.

The malware then has the capability to scan heavily over TCP port 445 (Server Message Block/SMB), spreading similar to a worm, compromising hosts, encrypting files stored on them then demanding a ransom payment in the form of Bitcoin. It is important to note that this is not a threat that simply scans internal ranges to identify where to spread, it is also capable of spreading based on vulnerabilities it finds in other externally facing hosts across the internet.

Additionally, Talos has observed WannaCry samples making use of DOUBLEPULSAR which is a persistent backdoor that is generally used to access and execute code on previously compromised systems. This allows for the installation and activation of additional software, such as malware. This backdoor is typically installed following successful exploitation of SMB vulnerabilities addressed as part of Microsoft Security Bulletin MS17-010. This backdoor is associated with an offensive exploitation framework that was released as part of the Shadow Brokers cache that was recently released to the public. Since its release it has been widely analyzed and studied by the security industry as well as on various underground hacking forums.

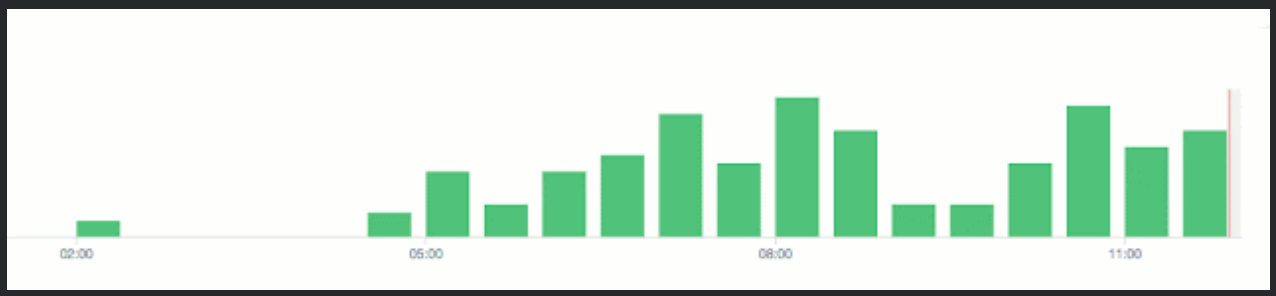
WannaCry appears to primarily utilize the ETERNALBLUE modules and the DOUBLEPULSAR backdoor. The malware uses ETERNALBLUE for the initial exploitation of the SMB vulnerability. If successful it will then implant the DOUBLEPULSAR backdoor and utilize it to install the malware. If the DOUBLEPULSAR backdoor is already installed the malware will still leverage this to install the ransomware payload. This is the cause of the worm-like activity that has been widely observed across the internet

Organizations should ensure that devices running Windows are fully patched and deployed in accordance with best practices. Additionally, organizations should have SMB ports (139, 445) blocked from all externally accessible hosts.

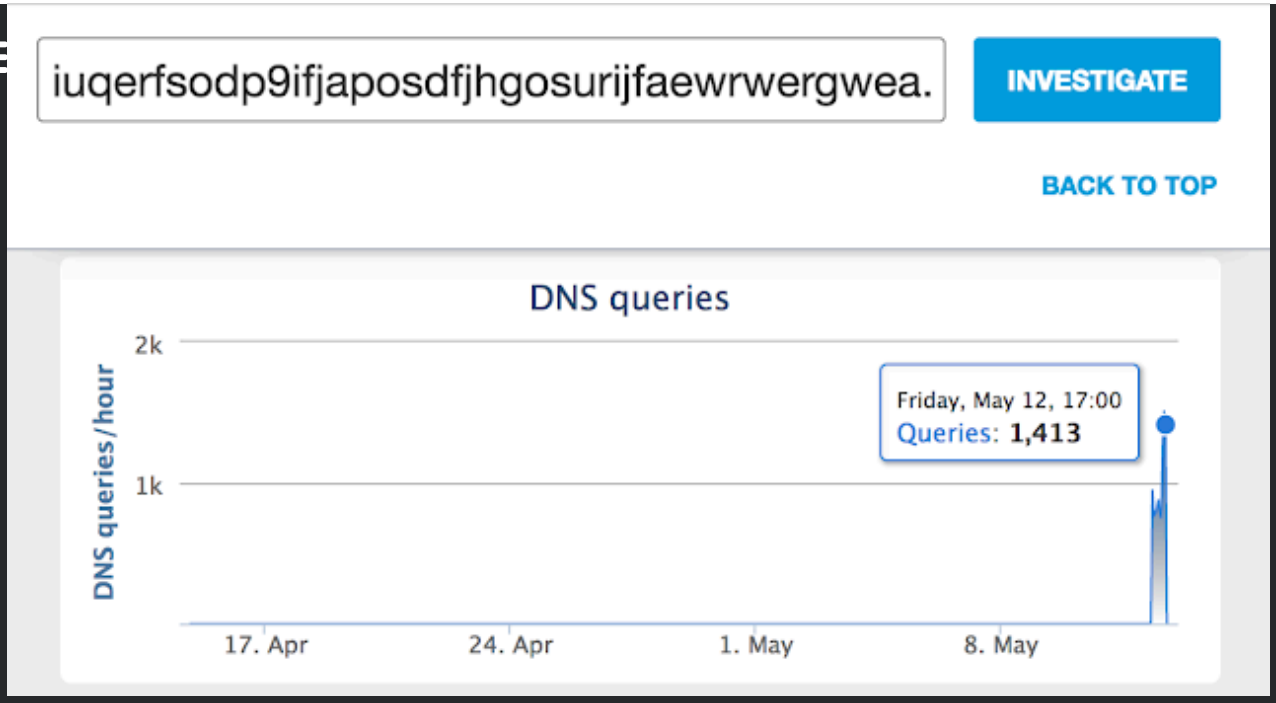
Please note this threat is still under active investigation, the situation may change as we learn more or as our adversary responds to our actions. Talos will continue to actively monitor and analyze this situation for new developments and respond accordingly. As a result, new coverage may be developed or existing

coverage adapted and/or modified at a later date. For current information, please refer to your Firepower Management Center or Snort.org.

Campaign Details We observed an uptick in scanning of our internet facing honeypots starting shortly before 5am EST (9am UTC).



Infrastructure Analysis Cisco Umbrella researchers first observed requests for one of WannaCry's killswitch domains (iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com) starting at 07:24 UTC, then rising to a peak of just over 1,400 nearly 10 hours later.



The domain composition looks almost human typed, with most characters falling into the top and home rows of a keyboard.

Communication to this domain might be categorized as a kill switch domain due to its role in the overall execution of the malware:

```
v4 = InternetOpenA(0, 1u, 0, 0, 0);
v5 = InternetOpenUrlA(v4, &szUrl, 0, 0, 0x84000000, 0);// ; "http://www.iuqerfsodp9ifjaposdfjhgosuri"...
if ( v5 )
{
  InternetCloseHandle(v4);
  InternetCloseHandle(v5);
  result = 0;
}
else
{
  InternetCloseHandle(v4);
  InternetCloseHandle(0);
  sub_408090();
  result = 0;
}
return result;
```

The above subroutine attempts an HTTP GET to this domain, and if it fails, continues to carry out the

infection. However if it succeeds, the subroutine exits. The domain is registered to a well known sinkhole, effectively causing this sample to terminate its malicious activity.

Email Address	Associated Domains	Email Type	Last Observed
BotnetSinkhole@gmail.com	36 Total - 35 malicious	Administrative, Registrant, Technical	Current

Nameserver	Associated Domains	Last Observed
ns2.sinkhole.tech	46 Total - 35 malicious	Current
ns4.sinkhole.tech	36 Total - 34 malicious	Current
ns1.sinkhole.tech	48 Total - 37 malicious	Current
ns3.sinkhole.tech	38 Total - 36 malicious	Current

The raw registration information re-enforces this as it was registered on 12 May 2017:

```
Domain Name: IUQERFSODP9IFJAPOSDFJHGOSURIJFAEWRWERGWEA.COM
Registrar: NAMECHEAP INC.
Sponsoring Registrar IANA ID: 1068
Whois Server: whois.namecheap.com
Referral URL: http://www.namecheap.com
Name Server: NS1.SINKHOLE.TECH
Name Server: NS2.SINKHOLE.TECH
Name Server: NS3.SINKHOLE.TECH
Name Server: NS4.SINKHOLE.TECH
Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Updated Date: 12-may-2017
Creation Date: 12-may-2017
Expiration Date: 12-may-2018
```

Malware Analysis An initial file "mssecsvc.exe" drops and executes "tasksche.exe", this exe tests the kill switch domains. One complete, the service mssecsvc2.0 is created, this is a method of persistance for the malware. This service executes "mssecsvc.exe" with a different entry point than the initial

execution. This second execution executes 2 threads. The first thread checks the IP address of the infected machine and attempts to connect to TCP445 (SMB) of each host/IP address in the same subnet and second thread generates random IP address on the Internet to perform the same action. When the malware successfully connects to a machine, a connection is initiated and data is transferred. The malware exploits the SMB vulnerability addressed by Microsoft in the bulletin MS17-010 (ETERNALBLUE) in order to implant the DOUBLEPULSAR backdoor. The backdoor is used to execute WANNACRY on the new compromised system.

The file tasksche.exe checks for disk drives, including network shares and removable storage devices mapped to a letter, such as 'C:/', 'D:/' etc. The malware then checks for files with a file extension as listed in the appendix and encrypts these using 2048-bit RSA encryption. While the files are being encrypted, the malware creates a new file directory 'Tor/' into which it drops tor.exe and nine dll files used by tor.exe. Additionally, it drops two further files: taskdl.exe & taskse.exe. The former deletes temporary files while the latter launches @wanadecryptor@.exe to display the ransom note on the desktop to the end user. The @wanadecryptor@.exe is not in and of itself the ransomware, only the ransom note. The encryption is performed in the background by tasksche.exe.

The tor.exe file is executed by @wanadecryptor@.exe. This newly executed process initiates network connections to Tor nodes. This allows WannaCry to attempt to preserve anonymity by proxying their traffic through the Tor network.

Typical of other ransomware variants, the malware also deletes any shadow copies on the victim's machine in order to make recovery more difficult. It achieve this by using WMIC.exe, vssadmin.exe and cmd.exe.

Process ID	Process Name	Command Line
29 (cmd.exe)	cmd.exe	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
30 (vssadmin.exe)	vssadmin.exe	vssadmin delete shadows /all /quiet
35 (WMIC.exe)	WMIC.exe	wmic shadowcopy delete

WannaCry uses various methods to attempt to aid its execution by leveraging both attrib.exe to modify the +h flag (hide) and also icacls.exe to allow full access rights for all users, "icacls . /grant Everyone:F /T /C /Q"

The malware has been designed as a modular service. It appears to us that the executable files associated with the ransomware have been written by a different individual than whomever developed the service module. Potentially, this means that the structure of this malware can be used to deliver and run different malicious payloads.

After encryption is complete, the malware displays the following ransomware note. One interesting aspect of this ransomware variant is that the ransom screen is actually an executable and not an image, HTA file, or text file.

Organisations should be aware that there is no obligation for criminals to supply decryption keys following the payment of a ransom. Talos strongly urges anyone who has been compromised to avoid paying the ransom if possible as paying the ransom directly funds development of these malicious campaigns.

Mitigation and Prevention Organizations looking to mitigate the risk of becoming compromised should follow the following recommendations:

- Ensure all Windows-based systems are fully patched. At a very minimum, ensure Microsoft bulletin MS17-010 has been applied.
- In accordance with known best practices, any organization who has SMB publically accessible via the internet (ports 139, 445) should immediately block inbound traffic.
  Additionally, organizations should strongly consider blocking connections to TOR nodes and TOR traffic on network. Known TOR exit nodes are listed within the Security Intelligence feed of ASA

Firepower devices. Enabling this to be blocklisted will prevent outbound communications to TOR networks.

In addition to the mitigations listed above, Talos strongly encourages organizations take the following industry-standard recommended best practices to prevent attacks and campaigns like this and similar ones.

- Ensure your organization is running an actively supported operating system that receives security updates.
- Have effective patch management that deploys security updates to endpoints and other critical parts of your infrastructure in a timely manner.
- Run anti-malware software on your system and ensure you regularly receive malware signature updates.
- Implement a disaster recovery plan that includes backing up and restoring data from devices that are kept offline. Adversaries frequently target backup mechanisms to limit the possibilities a user may be able to restore their files without paying the ransom.

Coverage Snort Rule: 42329-42332, 42340, 41978

Open Source Snort Subscriber Rule Set customers can stay up to date by downloading the latest rule pack available for purchase on Snort.org. Additional ways our customers can detect and block this threat are listed below.

Advanced Malware Protection (AMP) is ideally suited to prevent the execution of the malware used by these threat actors.

CWS or WSA web scanning prevents access to malicious websites and detects malware used in these attacks.

Network Security appliances such as NGFW, NGIPS, and Meraki MX can detect malicious activity associated with this threat.

AMP Threat Grid helps identify malicious binaries and build protection into all Cisco Security products.

Umbrella prevents DNS resolution of the domains associated with malicious activity.

Stealthwatch detects network scanning activity, network propagation, and connections to CnC infrastructures, correlating this activity to alert administrators.

IoCs

File names

- d5e0e8694ddc0548d8e6b87c83d50f4ab85c1debadb106d6a6a794c3e746f4fa b.wnry
- 055c7760512c98c8d51e4427227fe2a7ea3b34ee63178fe78631fa8aa6d15622 c.wnry
- 402751fa49e0cb68fe052cb3db87b05e71c1d950984d339940cf6b29409f2a7c r.wnry
- e18fdd912dfe5b45776e68d578c3af3547886cf1353d7086c8bee037436dff4b s.wnry
- 4a468603fdcb7a2eb5770705898cf9ef37aade532a7964642ecd705a74794b79 taskdl.exe
- 2ca2d550e603d74dedda03156023135b38da3630cb014e3d00b1263358c5f00d taskse.exe
- 97ebce49b14c46bebc9ec2448d00e1e397123b256e2be9eba5140688e7bc0ae6 t.wnry
- b9c5d4339809e0ad9a00d4d3dd26fdf44a32819a54abf846bb9b560d81391c25 u.wnry

Observed IPs

- 188[.]166[.]23[.]127:443 - Tor Exit Node
- 193[.]23[.]244[.]244:443 - Tor Exit Node
- 2[.]3[.]69[.]209:9001 - Tor Exit Node
- 146[.]0[.]32[.]144:9001 - Tor Exit Node
- 50[.]7[.]161[.]218:9001 - Tor Exit Node
- 128.31.0[.]39 - Tor Exit Node
- 213.61.66[.]116 - Tor Exit Node
- 212.47.232[.]237 - Tor Exit Node
- 81.30.158[.]223 - Tor Exit Node
- 79.172.193[.]32 - Tor Exit Node

Tor C2s

- xxlvbrloxvriy2c5.onion
- cwwnhwhlz52maqm7.onion
- gx7ekbenv2riucmf.onion
- 57g7spgrzlojinas.onion
- 76jdd2ir2embyv47.onion

Observed hash values

- ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
- c365ddaa345cfcaff3d629505572a484cff5221933d68e4a52130b8bb7badaf9
- 09a46b3e1be080745a6d8d88d6b5bd351b1c7586ae0dc94d0c238ee36421cafa
- 0a73291ab5607aef7db23863cf8e72f55bcb3c273bb47f00edf011515aeb5894
- 428f22a9afd2797ede7c0583d34a052c32693cbb55f567a60298587b6e675c6f
- 5c1f4f69c45cff9725d9969f9ffcf79d07bd0f624e06cfa5bcbacd2211046ed6
- 62d828ee000e44f670ba322644c2351fe31af5b88a98f2b2ce27e423dcf1d1b1
- 72af12d8139a80f317e851a60027fdf208871ed334c12637f49d819ab4b033dd
- 85ce324b8f78021ecfc9b811c748f19b82e61bb093ff64f2eab457f9ef19b186
- a1d9cd6f189beff28a0a49b10f8fe4510128471f004b3e4283ddc7f78594906b
- a93ee7ea13238bd038bcbec635f39619db566145498fe6e0ea60e6e76d614bd3
- b43b234012b8233b3df6adb7c0a3b2b13cc2354dd6de27e092873bf58af2693c
- eb47cd6a937221411bb8daf35900a9897fb234160087089a064066a65f42bcd4
- 24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c
- 2c2d8bc91564050cf073745f1b117f4ffdd6470e87166abdfcd10ecdff040a2e
- 7a828afd2abf153d840938090d498072b7e507c7021e4cdd8c6baf727cafc545
- a897345b68191fd36f8cefb52e6a77acb2367432abb648b9ae0a9d708406de5b

- fb0b6044347e972e21b6c376e37e1115dab494a2c6b9fb28b92b1e45b45d0ebc
- 9588f2ef06b7e1c8509f32d8eddfa18041a9cc15b1c90d6da484a39f8dcdf967
- b43b234012b8233b3df6adb7c0a3b2b13cc2354dd6de27e092873bf58af2693c
- 4186675cb6706f9d51167fb0f14cd3f8fcfb0065093f62b10a15f7d9a6c8d982
- 09a46b3e1be080745a6d8d88d6b5bd351b1c7586ae0dc94d0c238ee36421cafa Tor Artifacts
  There will be odd looking domains which are artifacts from Tor visible in network PCAPs, these domains are not considered IOCs and should not be considered malicious.

Appendix List of file names encrypted by the ransomware:

```
.der, .pfx, .key, .crt, .csr, .p12, .pem, .odt, .sxw, .stw, .3ds, .max, .3dm, .ods,
.sxc, .stc, .dif, .slk, .wb2, .odp, .sxd, .std, .sxm, .sqlite3, .sqlitedb, .sql,
.accdb, .mdb, .dbf, .odb, .mdf, .ldf, .cpp, .pas, .asm, .cmd, .bat, .vbs, .sch, .jsp,
.php, .asp, .java, .jar, .class, .mp3, .wav, .swf, .fla, .wmv, .mpg, .vob, .mpeg, .asf,
.avi, .mov, .mp4, .mkv, .flv, .wma, .mid, .m3u, .m4u, .svg, .psd, .tiff, .tif, .raw,
.gif, .png, .bmp, .jpg, .jpeg, .iso, .backup, .zip, .rar, .tgz, .tar, .bak, .ARC,
.vmdk, .vdi, .sldm, .sldx, .sti, .sxi, .dwg, .pdf, .wk1, .wks, .rtf, .csv, .txt, .msg,
.pst, .ppsx, .ppsm, .pps, .pot, .pptm, .pptx, .ppt, .xltm, .xltx, .xlc, .xlm, .xlt,
.xlw, .xlsb, .xlsm, .xlsx, .xls, .dotm, .dot, .docm, .docx, .doc,
```

RELATED CONTENT

Akira ransomware continues to evolve

OCTOBER 21, 2024 12:50

As the Akira ransomware group continues to evolve its operations, Talos has the latest research on the group's attack chain, targeted verticals, and potential future TTPs.

Threat actor believed to be spreading new MedusaLocker variant since 2022

OCTOBER 3, 2024 06:00

The malware, called "BabyLockerKZ," has primarily affected users in Europe and South America.

GhostSec's joint ransomware operation and evolution of their arsenal

MARCH 5, 2024 08:00

Cisco Talos observed a surge in GhostSec, a hacking group's malicious activities since this past year. GhostSec has evolved with a new GhostLocker 2.0 ransomware, a Golang variant of the GhostLocker ransomware.

Microsoft Advisories

INCIDENT RESPONSE

Talos IR Capabilities

Emergency Support

SECURITY RESOURCES

Open Source Security Tools

Intelligence Categories Reference

Secure Endpoint Naming Reference

MEDIA

Talos Intelligence Blog

Threat Source Newsletter

Beers with Talos Podcast

Talos Takes Podcast

Talos Videos

SUPPORT

Support Documentation

COMPANY

About Talos

Careers

Cisco Security

FOLLOW US