NTT Security Monthly Threat Report

May 2017

Contents

1 Introduction

In April 2017, cybercriminal group Shadow Brokers leaked supposed NSA hacking tools. This leak included zero-day exploits, custom hacking frameworks, backdoor implants, scanning tools and more. This leak led directly to global distribution of the WannaCry ransomware.

One of the backdoor implants included in this release is DOUBLEPULSAR. This backdoor is the primary payload in Server Message Block (SMB) and Remote Desktop Protocol (RDP) vulnerabilities leveraged by the NSA's FuzzBunch software, an exploitation framework similar to Metasploit.

This backdoor, if successfully installed, is designed to remain undetected. It can be used to conduct further operations on infected systems, including leveraging leaked zero-days, exfiltrating data and moving laterally through a network.

The NTT Security Global Threat Intelligence Center (GTIC) identified several detections for the signatures and indicators of compromise (IOCs) related to WannaCry. This report details the results of the GTIC's data analysis.

The GTIC has also provided high-level analysis of the WannaCry campaign, with emphasis on both the challenges with definitive attribution, as well as the long road to recovery if infected with WannaCry (or any other ransomware).

2 Multiple SMB Vulnerabilities – MS17-010

Threat Status: Critical

CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0147

Severity: **Critical** (CVSS: 10.0)

Date: May 13, 2017

Remediation Details: Microsoft released a patch to address these vulnerabilities. If patching is not possible, disable SMBv1 as a temporary workaround.

Affected Versions:

- Windows Vista x64 Edition Service Pack 2
- Windows Server 2008 for 32-bit Systems Service Pack 2
- Windows Server 2008 for x64-based Systems Service Pack 2
- Windows Server 2008 for Itanium-based Systems Service Pack 2
- Windows 7 for 32-bit Systems Service Pack 1
- Windows 7 for x64-based Systems Service Pack 1
- Windows Server 2008 R2
- Windows Server 2008 R2 for x64-based Systems Service Pack 1
- Windows Server 2008 R2 for Itanium-based Systems Service Pack 1
- Windows 8.1 for 32-bit Systems
- Windows 8.1 for x64-based Systems
- Windows Server 2012 and Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows RT 8.1
- Windows 10 for 32-bit Systems
- Windows 10 for x64-based Systems
- Windows 10 Version 1511 for 32-bit Systems
- Windows 10 Version 1511 for x64-based Systems
- Windows 10 Version 1607 for 32-bit Systems
- Windows 10 Version 1607 for x64-based Systems
- Windows Server 2016 for x64-based Systems
- Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
- Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)

- Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2 (Server Core installation)
- Windows Server 2016 for x64-based Systems (Server Core installation)

Analyst Note:
Microsoft released a patch to address multiple vulnerabilities found in the Microsoft Server Message Block (SMB) server**. All listed vulnerabilities are rated as critical, and remote code execution is possible.** Exploitation relies on an unauthenticated attacker sending a malformed packet targeting the SMBv1 server.

The hacker group Shadow Brokers leaked several NSA tools, and ETERNALBLUE was one of the exploits that disclosed during the leak. ETERNALBLUE takes advantage of the vulnerabilities patched with Microsoft Security Bulletin MS17-010. On May 12 2017, a global ransomware campaign targeted endpoints around the world. This ransomware variant, dubbed WannaCry or WCry, used the ETERNALBLUE exploit to compromise machines. The WannaCry ransomware is a worm which self propagates using the ETERNALBLUE vulnerability. The WannaCry ransomware is only the beginning, as several variants are emerging as of the time of this writing.

Microsoft patched all vulnerabilities related to ETERNALBLUE in March 2017. Due to the threat of these vulnerabilities Microsoft has released an out-of-band patch for operating systems like Windows XP which Microsoft no longer officially supports.

A workaround to this vulnerability exists. Disable SMB ports 139 and 445 if disabling those ports will not adversely affect your operations. **If SMB is being used in your environment, block inbound traffic over ports 139 and 445.**

3 WannaCry: More Questions Than Answers

Over 98 percent of WannaCry victims were running unpatched versions of Windows 7.

This is likely due in part to the fact that ETERNALBLUE never worked properly on XP, and it appears the tool's worm-like ability to infect additional computers on the same network without human intervention was designed for Windows 7. WannaCry was also discovered to be unsuccessful in propagating on older versions of the Windows OS, including XP.

Please note the common denominator of those infected, irrespective of Windows version: they were UNPATCHED. Systems that had applied the patches from Microsoft Security Bulletin MS17-010 were unaffected by the exploits associated with the distribution of WannaCry.

WannaCry rapidly became one of the largest cyberattacks to date, having infected over 200,000 hosts around the globe, WannaCry appears to have spread through internet-wide SMB (file shares) rather than phishing emails, as initially thought.

And the saga continues. As of this writing, there appear to be many more questions than answers – particularly with regards to motivation and attribution.

On the surface, this attack bears the hallmarks of a cybercriminal campaign designed to make money. This campaign has only netted a fraction of the amount expected, considering the number of infected machines. Also, with the way the ransom demands are hard-coded into the WannaCry ransomware, the motivation behind the campaign is in question. As of this writing, less than $121,000 has been paid to the attackers.

Attribution is also under intense investigation from government as well as private sector security researchers around the globe. Threat actors often reuse code available in the wild, especially as a cover and to deflect blame, making definitive attribution even more difficult.

In addition, conducting cyber operations to meet objectives are increasingly used by ALL threat actors (e.g., cybercriminals, nation-state actors, etc.). Cyber operations are often designed to be:

- Cost-effective.
- Asymmetric. Or, put another way, they are a means to obtaining a "level playing field" when targeting those of significantly greater capabilities.
- Deniable. Deniability limits the possibility of punishment (e.g., arrest in the case of the cybercriminal, sanctions in the case of the nation-state actor).

So, "obvious clues" aren't necessarily all they appear to be.

Initial reporting, shortly following the Shadow Brokers leak on April 14, suggested cybercriminals from Russia and China were quickly jumping to take advantage these sophisticated offensive cyber weapons, including several zero-day exploits. Attempts to leverage tools as soon as possible after discovery is nothing new. When zero-day vulnerabilities or older vulnerabilities remain unpatched on systems, threat actors of all levels will try to take full advantage.

Researchers are continuing to investigate whether these Chinese and Russian threat actors were state-sponsored, but the speed at which tools were weaponized and deployed do indicate capabilities which are on the more advanced side of the scale.

A question researchers continue to ask is, "Which threat actors were ultimately responsible for the WannaCry campaign?"

Preliminary findings suggest that the Lazarus Group, widely believed to be associated with North Korean threat actors, may have had a hand in the WannaCry campaign. Researchers have found evidence of commonalities in the code, as well as in the techniques *and* infrastructure used. These techniques include additional tools (e.g., Destover, Volgmer) used in attacks previously attributed to the Lazarus Group.

Some researchers found evidence of chatter related to these attacks in dark web forums before they happened, as is often the case. Open source and dark web analysis identified chatter about these tools, which indicates researchers (and likely actors with malicious intent), are downloading and analyzing these tools. It is possible that additional tools are being primed for deployment, as many more experienced threat actors are quick to weaponize these types of tools.

As a case in point, WannaCry was not the only campaign targeting vulnerabilities in SMB to emerge from the leaked NSA tools.

In fact, one tool dubbed Adylkuzz hit the proverbial streets three weeks before WannaCry. Designed to generate "digital cash" via Monero cryptocurrency mining operations, Adylkuzz, unlike WannaCry, wasn't quickly discovered, as it allowed the computer to operate almost normally (a slight degradation of server performance was noted) while mining operations ran in the background. In addition, it blocked other SMB exploits –including WannaCry – perhaps even limiting WannaCry's infection rate. Since Adylkuzz was mining Monero specifically, this operation could be efforts to bump up the value of this cryptocurrency. Monero is similar to Bitcoin, but is not as popular and has enhanced anonymity capabilities.

EternalRocks was yet another campaign which leveraged seven NSA tools exploiting SMB weaknesses. Part of the beauty of this malware was that it disguised itself as WannaCry to fool mitigation efforts, though instead of dropping ransomware, it gains an unauthorized foothold on a victim host for future exploitation. (Note: The EternalRocks author has discontinued development and had taken the code offline.)

Although both Adylkuzz and EternalRocks can be detected with the same signatures as WannaCry, they are more difficult for the end user, as they do not encrypt the file system and display a ransom note.

Culpability and motives may be unknown for WannaCry, but patches are available for these exploits. These patches, along with best practices – at a very minimum – are your best defense against these tools at this time. There is good news though, should you become infected: the Wanakiwi decryption tool is available, potentially allowing victims to recover files without paying a ransom. This decryptor is reportedly effective on all Windows operating systems. There is one catch, though – it works only on systems that have not been rebooted post-infection. **(NOTE: NTT SECURITY MAKES NO GUARANTEES AS TO THE EFFECTIVENESS OF DECRYPTION TOOL, AND USERS SHOULD PROCEED WITH CAUTION AND LEVERAGE THESE TOOLS AT THEIR OWN RISK.)**

As an additional precaution, please note that there are several fake decryption tools which exist as mentioned in the GTIC's separate article in this report, WannaCry: Road to Recovery.

In addition to the recommendations outlined in *WannaCry: Road to Recovery*, it may also be worthwhile to blacklist known Tor IPs, and, needless to say, immediately remove any infected computer from the network. Full indicators for WannaCry and associated attacks can be found in this report in section 7: Characteristics, Indicators and Signatures.

In addition, even if you have your SMB and CIFS applications hardened, be aware that the same malware can be distributed via alternate means, so ensure your systems are up to date on all patches and all best practices for security measures are followed.

The moral of the story is this: opportunistic hackers WILL take advantage of the tools from these continued leaks, along with all other vulnerabilities which they discover their targets have not yet patched. There are many reasons why organizations and individuals do not patch their systems, but threat actors don't really care exactly why those systems are unpatched, just that they are.

Expect more classified tools (including zero-day vulnerabilities) to be released via outlets such as the Shadow Brokers and WikiLeaks. A variety of threat actors will quickly acquire newly released tools, weaponize, and deploy them. In fact, Shadow Brokers authored a blog post where they promised to release tools each month, beginning in June 2017, to anyone willing to pay for access. Given the successes we saw with WannaCry and the other exploits which took advantage of the unpatched SMB vulnerability, we should not be surprised to see Shadow Brokers have some success in selling future access.

NTT Security fully expects continued repurposing of these tools, especially as systems worldwide remain unpatched.

The bad guys are counting on it.

4 WannaCry: Road to Recovery

Beginning on Friday, May 12, the WannaCry ransomware campaign blanketed over 200,000 workstations around the world with an image similar to this one:

Figure 1. WannaCry/WCry ransom demand page

The attack left individuals and enterprises reeling as the staggering implications settled in. Sadly, many organizations were not prepared for a ransomware attack, and even worse, for some victims, the ransom message “Send $300 worth of bitcoin” might as well have been in an unintelligible language.

While blockchain experts may think nothing of purchasing cryptocurrency, to the everyday employee, this task sounds daunting, if not impossible. NTT Security evaluated whether obtaining $300 worth of bitcoin was even possible in the timeframe allotted by the WannaCry ransomware.

To test this, NTT Security ran an experiment measuring the amount of time it would take someone to buy the required cryptocurrency. The experiment would be conducted by someone with a thorough knowledge of cryptocurrency and the blockchain, then repeated by someone with virtually no knowledge of the blockchain. In each iteration, users would perform the same tasks.

Upon completion of the experiment, the times would be compared to evaluate whether obtaining $300 worth of bitcoin was possible.

1. First, the test subject would need to set up an account at a (legitimate) cryptocurrency exchange.
2. Second, he would be required to complete all verification and setup procedures.
3. Third, he would have to add a (real) funding source.
4. And finally, the test subject would need to verify his identity to increase his buy limits.

Once all four steps are complete, the user should then be at a point where he can purchase enough bitcoin to pay the ransom demand.

The blockchain expert completed all tasks in 9 minutes, 28 seconds.

Unfortunately, the end user who was unfamiliar with the blockchain was **unable to complete the task**, having made mistakes while in the process of account verification. This resulted in a 24-hour hold on the user's cryptocurrency exchange account.

Once the user was finally able to log in to the exchange, he would not have been able to purchase the appropriate amount of bitcoin in the time allotted (seven days), as the test subject had linked his bank account as opposed to a credit card (Purchasing bitcoin via bank transfer, as opposed to purchase with credit card, can take 7-14 days).

Most cybersecurity experts will tell you that paying the ransom is not recommended, and with WannaCry, this is *certainly* the case. The GTIC was unable to verify that *any* files had been decrypted, even after affected users paid the ransom. In fact, the WannaCry ransomware campaign has significant flaws, and researchers wonder if the attackers ever planned to decrypt *any* of the computers infected.

So why run the test?

We wanted to simulate the difficulty (and frustration) involved with recovering from a ransomware attack, especially one for which the end user (or organization) is not prepared.

The test was conducted in a controlled environment and the end user test subject was likely not as stressed as, say, a business owner would be had he lost all his critically important files. It is important to communicate how crucial it is to be prepared for such an attack. Beyond the frustration of trying to learn a new technology (i.e., blockchain), and the follow-on concern of making the payment, a ransomware attack saddles the victim with much more "to pay" than simply $300.

And the uninformed end user may be more apt to rely on search engine query results for gathering information on how to pay the ransom. These results can lead users to fake decryptors, potentially exacerbating the problem.

4.1 Loss of Operational Capability

WannaCry infected entire networks, rendering some them all but useless. For those organizations not prepared for a ransomware attack, operations came to a grinding halt.

When an organization loses operational capability due to a ransomware attack, employees can't work, the organization cannot sell their products and services, cannot pay for materials and services needed to keep their organization running and they are "dead in the water." If the business cannot continue to function, cashflow stops, which is bad for any business.

4.2 Data Loss

In the event of a ransomware attack, it's probably best to assume that your data is gone forever.

Honoring the demand to "Pay us $300 in bitcoin" does not guarantee you will receive a decryption key to unlock your files, and the chance of getting *all* your data back is slim.

And let's not forget how expensive data loss, by its very nature, can be. If your organization completely loses data, expect the following:

1. You're going to lose customers.
    a. This could be for a variety of reasons:
        i. You lost invoice data, meaning you don't know which customers owe you what amount of money for your goods and services.
        ii. You lost personally identifiable information (PII), violating your customers' trust.
2. You're going to have to pay to get your files back.
    a. While NTT Security does not recommend paying the ransom, that may be the "cheapest" way to unlock your files – that is, if the criminal comes through on their promise to provide a decryption key. In the case of WannaCry, you would simply be out your $300 (or $600 if you waited until three days had passed since the infection).
    b. To reiterate, there is *no guarantee* you will receive the key to decrypt your files, so paying the extortion may just be throwing away money.

4.3 Ransomware is a "Breach"

Whether or not you pay the ransom, your organization needs to treat the ransomware as a breach. At the very least, you have identified malware on organizational resources. You cannot simply pay the ransom and move on. And you obviously cannot ignore that the ransomware is present.

Regardless of other outcomes, the organization must reimage systems, and treat the infrastructure as if it has been compromised. That may mean outsourced services, it may mean restoring from backups, and it may mean reinstalling systems, but the organization needs to take actions to purge the malware and associated breach from its environment. After all, the ransomware you know about may not be the only malware installed in your environment.

And if industry breach notification rules apply to you, they kick in the second you get that internal notification or the second that "pay bitcoins" notice pops up.

4.4 An Ounce of Prevention Only Gets You an Ounce of Protection

There is no *single* solution to be prepared for a ransomware attack. If your organization falls victim to ransomware, you will be glad you were prepared, but it will take work to ensure you are prepared, and this work must take place *before* the attack happens.

Implement only one or two of the below recommendations, and you will have an incomplete preparation model.

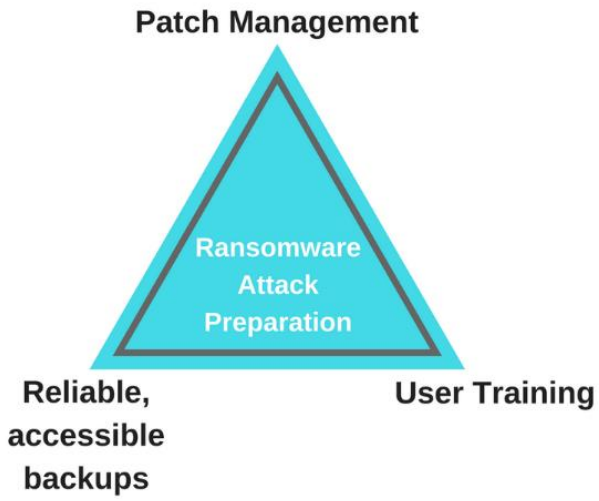

Figure 2. Ransomware attack preparation model

4.5 Ransomware Recommendations

1. Ensure you establish a feasible patch management (and upgrade) program.
    a. In the example of WannaCry, the campaign targeted vulnerabilities in many systems that had reached end-of-life (EOL) and were no longer supported by the original

manufacturer. In other words, part of your patch management program must include periodic audits of the systems in your environment to determine whether those systems can be patched or if they should be deprecated.

b. When it comes to patching, install patches in your environment as soon as is feasible.

2. Implement a complete backup solution.
    a. Store backups both on-site and off-site.
    b. Remember backups are not JUST about the data. While the data is important, the organization must consider the ability to access and use that data. That means ensuring the organization retains backup copies of any applications being used, as well as required operating systems and any keys or licenses upon which those things rely.
    c. When selecting a backup solution, keep in mind the "CIA triad".
        i. Confidentiality – Is the data protected and accessible only to those who require access?
        ii. Integrity – Can the data be trusted?
        iii. Availability – If reverting to a backup is needed, how accessible are those backups? How long will it take to be operational if reverting to backups is required?
    d. And, remember that your backup is only as good as what you can restore. Organizations should test their backup AND RESTORE process to ensure that the data and systems are recoverable.
3. Train (and test) your end users.
    a. WannaCry, though it infected over 200,000 systems, was likely not delivered via a phishing email; however, *most* ransomware variants *are* delivered via phishing emails.
    b. Train your end users to spot the most common signs of phishing emails.
        i. If possible, train users with phishing emails which targeted your company, or an industry peer.
    c. Test your users' ability to identify and report phishing emails.
        i. This is not a "gotcha" to see who falls for it. It is a self-correcting action that will allow your organization to determine the effectiveness of this part of your end user training.

Remember, security is not always convenient, as every recommendation above will be "inconvenient" in some way, but *when* you're attacked, you'll be glad you were ready.

5 WannaCry Attack Analysis

5.1 Summary

The WannaCry ransomware is a worm-like malware which spreads by exploiting the leaked NSA exploit ETERNALBLUE. The group known as the Shadow Brokers released the malware into the wild. The malware encrypts files, drops and executes a decryptor tool, displays a ransom notice for either $300 or $600 payable with Bitcoin, and uses Tor for C2 channels. It became extremely prevalent in May 2017

and crippled many organizations for several days. Windows systems which have been fully patched with MS17-010 are not exploitable.

5.2 WannaCry Characteristics

GTIC researchers took a detailed look at WannaCry and the files which make it up. GITC also used several Snort and Palo Alto signatures in the malware and data analysis as well as ongoing monitoring. These characteristics appear in this report in section 7: Characteristics, Indicators and Signatures.

As part of this analysis, GTIC researchers analyzed the progression of a WannaCry attack.

5.3 WannaCry Installation Details

1. WannaCry starts by trying to access a kill switch domain. If access to the domain succeeds, then the malware immediately exits. If access to the domain fails, then command line arguments are checked. If no arguments were passed, then the malware continues with installation; otherwise, it enters service mode.
2. In service mode, WannaCry scans the subnet it is on, then attempts to spread itself to available hosts via ETERNALBLUE. For installation, the malware creates a service named *mssecsvc2.0* with a binary path pointing to the running module with arguments "-m security". Once created, the malware starts the created service. The malware then writes *tasksche.exe* to C:\WINDOWS, executes it with "/i" argument then moves C:\WINDOWS\tasksche.exe to C:\WINDOWS\<random>.
3. Running with the /i argument, the malware will try to create the mutex Global\MsWinZonesCacheCounterMutexA0. If it fails to create the mutex, it will reinstall itself and try again. If that fails, it will continue as normal. Without the /i command, WannaCry will drop its encryption component and begin the process of encrypting the machine's files.
4. Once the malware completes encrypting the desktop and documents folder, it executes the following commands:

    - taskkill.exe /f /im Microsoft.Exchange.*
    - taskkill.exe /f /im MSExchange*
    - taskkill.exe /f /im sqlserver.exe
    - taskkill.exe /f /im sqlwriter.exe
    - taskkill.exe /f /im mysqld.exe

5. It then starts encrypting files found on logical drives attached to the system. The malware executes "cmd.exe /c start /b @WanaDecryptor@.exe vs", copying the decryptor to each users' desktop folder.
6. The desktop wallpaper is set to a @WanaDecryptor@.bmp image, and the following dialogue box is displayed:

Figure 3. WannaCry dialogue box

7. Communication with the threat actors is accomplished via an onion router using a Tor server running on the local host port 9050.

6 WannaCry/WCry Threat Research Report

With the public leak of these NSA Tools, the GTIC analyzed logs provided by security appliances in clients' networks to identify detections correlating to the NSA leak. With this approach, the GTIC gathered data detailing several Snort, Fortigate and Palo Alto alerts, as well as alerts including IP addresses from WannaCry IoCs. The GTIC analyzed the raw data and included the important findings in this document. Please be aware: This is ongoing analysis, as NTT Security researchers are continuing to analyze several of the payloads acquired from Snort and other sources.

6.1 Analysis Findings

6.1.1 Preliminary Data Statistics

GTIC researchers have observed WannaCry related activity with the context shown in this table.

Subject	Summary
Affected Industries	Finance Manufacturing Government Education Health Care Business Services Technology Energy & Utilities Retail Non-Profit Hospitality Food/Beverage Construction/Real Estate
Timeframe	February 7 – May 23
Security Appliances	Snort Palo Alto Fortigate Cisco ASA Sonic Firewall Juniper Networks JunOS Plixer Scrutinizer Trend Micro Deep Discovery
Direction of Traffic	Inbound, Outbound

Subject	Summary
Well-Known Ports Identified	445 (Server Message Block) 80 (HTTP) 123 (NTP) 9001 (TOR) 9090 53 (DNS) 443 (HTTPS) 137 (NetBIOS) 139 (NetBIOS) 22 (SSH)
Number of Foreign IP Addresses	386
Types of Traffic/Attacks	Successful SMB Ping Responses Process Injection Commands Successful Process Injection Responses Sinkhole Connections
Protocols	TCP ICMP UDP

The GTIC has included all signatures and indicators related to WannaCry in this report in section 7: Characteristics, Indicators and Signatures.

6.1.2 Signature Detection Findings and Analysis

WannaCry leverages ETERNALBLUE to exploit a vulnerability in Microsoft's SMB protocol. While GTIC analysis of ETERNALBLUE did not detect WannaCry-specific activity, analysts did observe and analyze several signatures related to ETERNALBLUE and DOUBLEPULSAR. Detection of these signatures is highlighted in *Figure 4*.

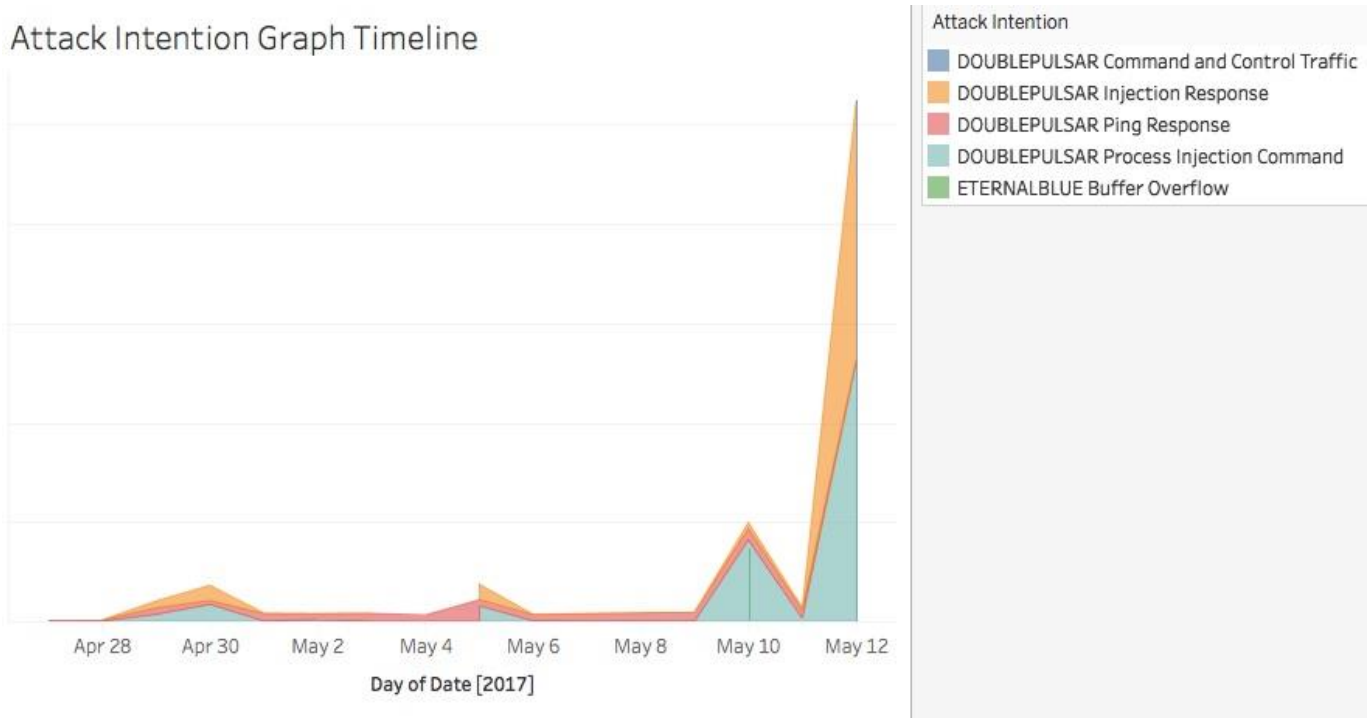

Figure 4. Attack intention graph timeline

As shown in *Figure 4,* the use of DOUBLEPULSAR was consistent from late April through May 10, followed by a significant increase in detections on May 12. These detections include SMB ping responses, which were detected while threat actors conducted reconnaissance, attempting to identify publicly available systems with the backdoor already installed.

From April 28-May 1 and on May 5, analysts observed detections for both SMB process injection commands and successful injection responses, indicating threat actors were attempting to leverage those existing backdoors.

On May 10, attempts to use the ETERNALBLUE exploit (CVE-2017-0144, CVE-2017-0146) were briefly detected, with nearly 400 attempts observed before subsiding. On May 11 and 12, the GTIC observed significant spikes in SMB process injection commands and responses leveraging DOUBLEPULSAR.

Although analysts did not observe specific WannaCry infections via IDS/IPS implementations, this activity suggests threat actors are continuing attempts to identify compromised systems and leverage the backdoor for nefarious purposes.

6.1.3 Indicators of Compromise (IOC) Detections and Analysis

The GTIC collected several different IOCs related to WannaCry infections. These included hashes, domains, C2 domains, registry keys, filenames, IPv4 addresses, and more. Analysts identified and evaluated several IP addresses based on MSSP detections. These indicators are collected in this report in section 7: Characteristics, Indicators and Signatures.

Figure 5 provides an overview of IOC IPv4 address per MSSP data. Please note, 195.22.26.248 was removed due to its sheer log count and since it was identified as a sinkhole, that IP address was used as a focal point to redirect malicious traffic to for analysis.

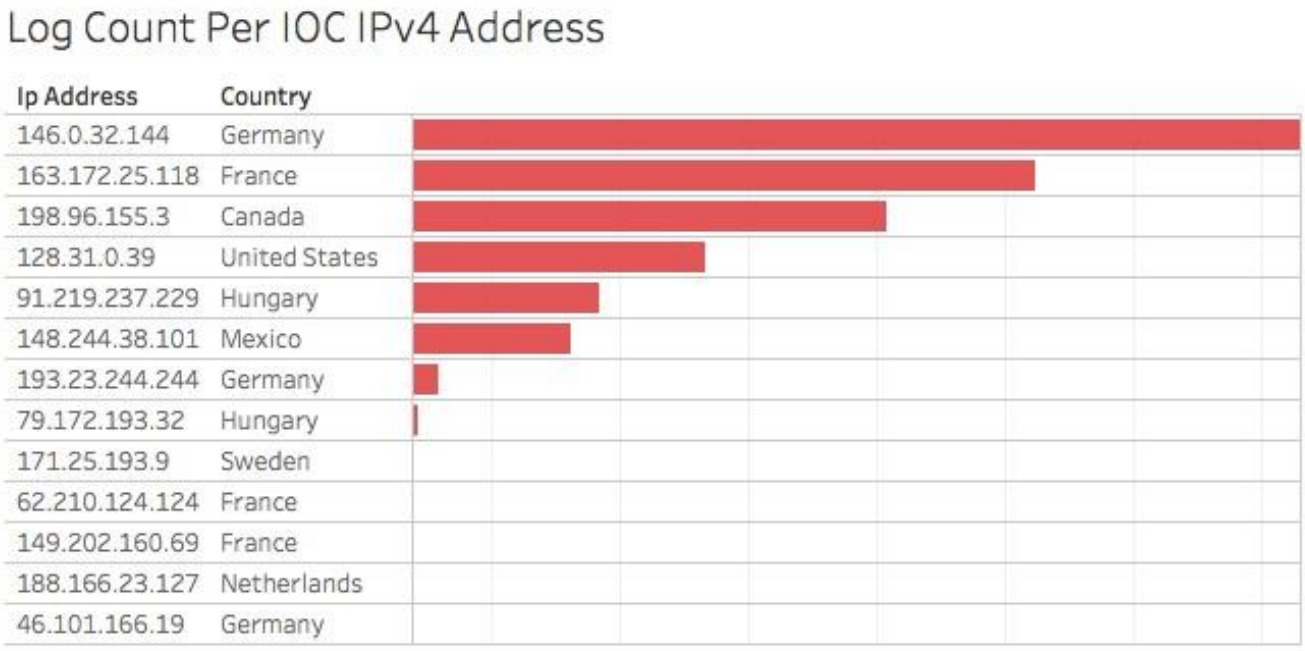

Figure 5. Log count per IOC IPv4 address

Analysis indicates none of these IPv4 addresses conducted activity related to the use of DOUBLEPULSAR or ETERNALBLUE; however, the GTIC focused on requests to 7319[.]m8374[.]net/0.0.9 and p45pfvm2fhnvx23yiddqrrm[.]com[:]9001.

The 7319[.]m8374[.]net/0.0.9 domain resolves to 195.22.26.248, which belongs Claranet Portugal Telecomunicacoes S.A. of Portugal. 43 percent of outbound traffic was destined to this specific URL. According to passive DNS and Shodan results, this IP appears to be a security researcher sinkhole. The GTIC determined DNS was the primary protocol for traffic sent to this IP or a resolving domain. This indicator was gathered from ISC SANS Center. As shown in *Figure 5*, most of the detections related to the IPv4 IOCs were directed at the sinkhole, 195.22.26.248. The bubble chart (*Figure 6*), is used to describe the purpose of the server with the specific IPv4 address found in both MSSP detections and the WannaCry IOC list provided by the GTIC.

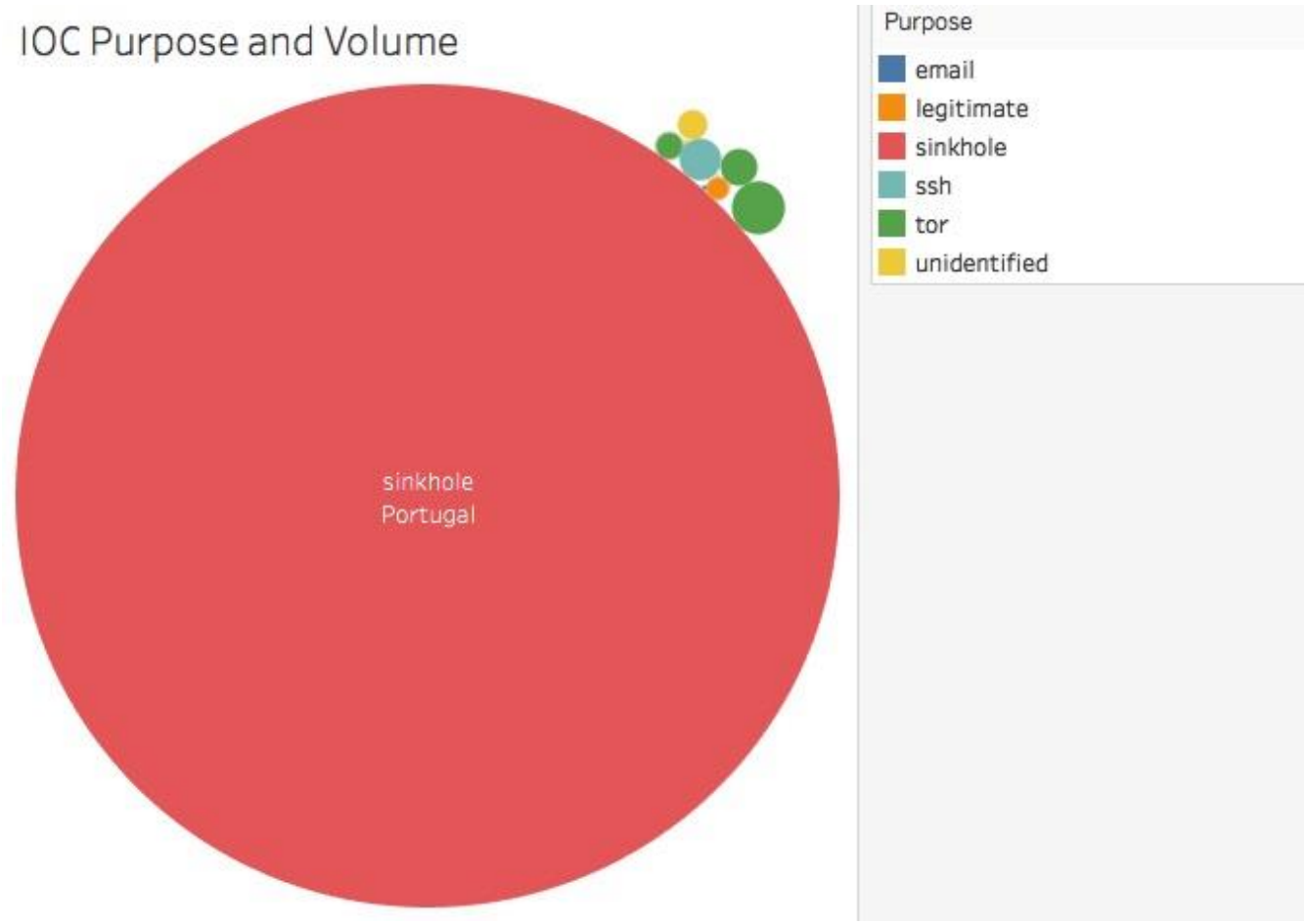

Figure 6. IOC purpose and volume

Additionally, traffic to p45pfvm2fhnvx23yiddqrrm[.]com caught our attention because the destination port specified was 9001, typically used for Tor traffic. Traffic for this was caught by a firewall and did not indicate any further malicious activity; however, the GTIC discovered that WannaCry uses Tor addresses for C2 channels, also noting that this domain resolves to 149.202.160.69, identified as a WannaCry C2 server.

6.2 Conclusion

Based on the data analyzed, the GTIC did not identify specific WannaCry detections; however, GTIC did analyze detections related to activity generated prior to or after WannaCry infections. Please be aware that traffic to 195.22.26.248 does not automatically suggest a WannaCry infection but may indicate different malware or potentially unwanted programs (PUPs). As of this writing, leveraging of SMB and SAMBA exploits continued to rise with the release of WannaCry spin-off EternalRocks and CVE-2017-7494 before the developer pulled it from release. Organizations are highly encouraged to review and implement the recommendations below.

6.3 Recommendations

6.3.1 Mitigation, Identification and Eradication

Deploying patch MS17-010 is essential to mitigating this threat, as it addresses several of the exploits leaked by Shadow Brokers earlier this year, including ETERNALBLUE. There is reportedly a decryption program available for WannaCry which works for users running Windows 7 or earlier. The instructions for the decryptor direct the user to not restart their machine. This decryption program, Wanakiwi, rebuilds the encryption key from prime numbers left in memory on Windows versions XP through 7. The program can be found at https://github.com/gentilkiwi/wanakiwi.

Countercept has also created a Python script (available on Github) to identify and eradicate the DOUBLEPULSAR backdoor if dropped during the ETERNALBLUE exploit. **(NOTE: NTT SECURITY MAKES NO GUARANTEES AS TO THE EFFECTIVENESS OF EITHER OF THE ABOVE TOOLS, AND USERS SHOULD PROCEED WITH CAUTION AND LEVERAGE THESE TOOLS AT THEIR OWN RISK.)**

7 Characteristics, Indicators and Signatures

7.1 WannaCry File Characteristics

FILE NAME	24d004a104d4d54034dbcffc2a4b19a04703480b1022c.exe
FILE SIZE	3723264 bytes
FILE TYPE	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	db349b97c37d22f5ea1d1841e3c89eb4
SHA1	e889544aff85ffaf8b0d0da705105dee7c97fe26
SHA256	24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c
SHA512	d6c60b8f22f89cbd1262c0aa7ae240577a82002fb149e9127d4edf775a25abcda4e585b6113e79ab4a24bb65f4280532529c2f06f7ffe4d5db45c0caf74fea38
CRC32	1457555570
SSDEEP	98304:wDqPoBhz1aRxcSUDk36SAEdhvxWa9P593R8yAVp2g3R:wDqPe1Cxcxk3ZAEUadzR8yc4gB
Compile Time	03:08.0
Version	6.1.7601.17514 (win7sp1_rtm.101119-1850)
Original Filename	lhdfrgui.exe
Author	Microsoft Corporation
Description	Microsoft® Disk Defragmenter

FILE NAME	tasksche.exe
FILE SIZE	3514368 bytes
FILE TYPE	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	84c82835a5d21bbcf75a61706d8ab549
SHA1	5ff465afaabcbf0150d1a3ab2c2e74f3a4426467
SHA256	ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
SHA512	90723a50c20ba3643d625595fd6be8dcf88d70ff7f4b4719a88f055d5b3149a4231018ea30d375171507a147e59f73478c0c27948590794554d031e7d54b7244
CRC32	1154904451
SSDEEP	98304:QqPoBhz1aRxcSUDk36SAEdhvxWa9P593R8yAVp2g3x:QqPe1Cxcxk3ZAEUadzR8yc4gB
Compile Time	05:05.0
Version	6.1.7601.17514 (win7sp1_rtm.101119-1850)
Original Filename	diskpart.exe
Author	Microsoft Corporation
Description	DiskPart

FILE NAME	f351e1fcca0c4ea05fc44d15a17f8b36.exe
FILE SIZE	65536 bytes
FILE TYPE	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
MD5	f351e1fcca0c4ea05fc44d15a17f8b36
SHA1	7d36a6aa8cb6b504ee9213c200c831eb8d4ef26b
SHA256	1be0b96d502c268cb40da97a16952d89674a9329cb60bac81a96e01cf7356830
SHA512	c139bddae3571cac3d832535e0c3bc6d817b86fb3f7b68864d1b94e9c37b38856f2eeeb49c16f2fb8fee45e6a7c95bc67072443b7428034b6def10d3f724ca22
CRC32	2897727361
SSDEEP	768:edWOTdghGl7Lu/qGrN5r5UF9sBaho9S4AJKqBz8MZK8IgpkCamlniZfO:PGdghGleSGh5resN9S4A3jHaqniZfO
Compile Time	12:55.0
Version	6.1.7600.16385 (win7_rtm.090713-1255)
Original Filename	kbdlv.dll

Author	Microsoft Corporation
Description	Latvia Keyboard Layout

FILE NAME	**@WanaDecryptor@.exe**
FILE SIZE	245760 bytes
FILE TYPE	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	7bf2b57f2a205768755c07f238fb32cc
SHA1	45356a9dd616ed7161a3b9192e2f318d0ab5ad10
SHA256	b9c5d4339809e0ad9a00d4d3dd26fdf44a32819a54abf846bb9b560d81391c25
SHA512	91a39e919296cb5c6eccba710b780519d90035175aa460ec6dbe631324e5e5753bd8d87f395b5481bcd7e1ad623b31a34382d81faae06bef60ec28b49c3122a9
CRC32	4211736213
SSDEEP	3072:Rmrhd5U1eigWcR+uiUg6p4FLlG4tlL8z+mmCeHFZjoHEo3m:REd5+lZiZhLlG4AimmCo
Compile Time	19:35.0
Version	6.1.7601.17514 (win7sp1_rtm.101119-1850)
Original Filename	LODCTR.EXE
Author	Microsoft Corporation
Description	Load PerfMon Counters

7.2 WannaCry Configuration Details

	24d004a104d4d54034dbcffc2a4b19a04703480b1022c.exe – Loader and Worm Component
Hash:	MD5 - db349b97c37d22f5ea1d1841e3c89eb4
Action	Writes loader to disk
Process	Creates mssecvc2.0 service for persistence C:\Users\Emily\AppData\Local\Temp\24d004a104d4d54034dbcffc2a4b19a04703480b1022c.exe -m security

	tasksche.exe – Loader
Hash:	MD5 - 84c82835a5d21bbcf75a61706d8ab549
Action	Written to C:\ProgramData\<random>\tasksche.exe
Process 1	Creates service for persistence cmd.exe /c "C:\ProgramData\<random>\tasksche.exe" Service Name is the same as the random value
Process 2	C:\Logs\@WanaDecryptor@.exe Creates a registry value for persistence Key: HKLM\SOFTWARE\WANACRYPTOR Value: Wd Data: C:\ProgramData\<wanacrypt name>

	Unavailable – Encryptor
Hash:	MD5 – f351e1fcca0c4ea05fc44d15a17f8b36

	@WanaDecryptor@.exe – Decryptor
Hash:	MD5 – 7bf2b57f2a205768755c07f238fb32cc

7.3 WannaCry Technical Indicators

The following technical indicators provide details about characteristics of this malware. These indicators can be used to enhance detection capabilities of network devices if detection signatures are created and implemented.

IP addresses and those using them are typically transient in nature, so while blocking offending IP addresses is a small step toward improving security, you cannot afford to just “block it and forget it.”

IP ADDRESSES		
2.3.69.209	148.244.38.101	213.61.66.117
50.7.161.218	149.202.160.69	46.101.142.174
193.23.244.244	163.172.149.155	46.101.166.19
188.166.23.127	171.25.193.9	62.210.124.124
146.0.32.144	195.22.26.248	91.121.65.179

IP ADDRESSES		
128.31.0.39	197.231.221.221	91.219.237.229
144.76.92.176	198.96.155.3	

C2 IP ADDRESSES AND PORTS		
188.166.23.127:443	193.23.244.244:443	2.3.69.209:9001
146.0.32.144:9001	50.7.161.218:9001	62.138.10.60:9001
82.94.251.227:443	213.239.216.222:443	51.255.41.65:9001
86.59.21.38:443	198.199.64.217:443	83.169.6.12:9001
192.42.115.102:9004	104.131.84.119:443	178.254.44.135:9001
163.172.25.118:22	217.79.179.77	128.31.0.39
213.61.66.116	212.47.232.237	81.30.158.223
79.172.193.32	89.45.235.21	38.229.72.16
188.138.33.220		

DOMAINS		
gx7ekbenv2riucmf.onion	bcbnprjwry2.net	xanznp2kq.com
57g7spgrzlojinas.onion	bqmvdaew.net	chy4j2eqieccuk.com
xxlvbrloxvriy2c5.onion	sxdcmua5ae7saa2.net	lkry2vwbd.com
76jdd2ir2embyv47.onion	rbacrbyq2czpwnl5.net	ju2ymymh4zlsk.com
cwwnhwhlz52maqm7.onion	ow24dxhmuhwx6uj.net	43bwabxrduicndiocpo.net
graficagbin.com.br	fa3e7yyp7slwb2.com	sdhjjekfp4k.com
dyc5m6xx36kxj.net	wwld4ztvwurz4.com	iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
gurj5i6cvyi.net	bqkv73uv72t.com	sqjolphimrr7jqw6.onion

CURRENTLY KNOWN KILLSWITCH DOMAINS
www.lazarusse.suiche.sdfjhgosurijfaqwqwqrgwea.com

CURRENTLY KNOWN KILLSWITCH DOMAINS
www.iuqerxxxdp9ifjaposdfjhgosurijfaewrwergwea.com
www.ayylmaotjhsstasdfasdfasdfasdfasdfasdfasdf.com
www.udhridhfowhgibe9vheiviehfiehbfvieheifheih.com
www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
www.ifferfsodp9ifjaposdfjhgosurijfaewrwergwea.com

FILE HASHES
0345782378ee7a8b48c296a120625fd439ed8699ae857c4f84befeb56e727366
09a46b3e1be080745a6d8d88d6b5bd351b1c7586ae0dc94d0c238ee36421cafa
11d0f63c06263f50b972287b4bbd1abe0089bc993f73d75768b6b41e3d6f6d49
149601e15002f78866ab73033eb8577f11bd489a4cea87b10c52a70fdf78d9ff
16493ecc4c4bc5746acbe96bd8af001f733114070d694db76ea7b5a0de7ad0ab
190d9c3e071a38cb26211bfffeb6c4bb88bd74c6bf99db9bb1f084c6a7e1df4e
201f42080e1c989774d05d5b127a8cd4b4781f1956b78df7c01112436c89b2c9
24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c
2584e1521065e45ec3c17767c065429038fc6291c091097ea8b22c8a502c41dd
2ca2d550e603d74dedda03156023135b38da3630cb014e3d00b1263358c5f00d
4186675cb6706f9d51167fb0f14cd3f8fcfb0065093f62b10a15f7d9a6c8d982
4A468603FDCB7A2EB5770705898CF9EF37AADE532A7964642ECD705A74794B79
57c12d8573d2f3883a8a0ba14e3eec02ac1c61dee6b675b6c0d16e221c3777f4
593bbcc8f34047da9960b8456094c0eaf69caaf16f1626b813484207df8bd8af
2584e1521065e45ec3c17767c065429038fc6291c091097ea8b22c8a502c41dd
5ad4efd90dcde01d26cc6f32f7ce3ce0b4d4951d4b94a19aa097341aff2acaec
6bf1839a7e72a92a2bb18fbedf1873e4892b00ea4b122e48ae80fac5048db1a7
78e3f87f31688355c0f398317b2d87d803bd87ee3656c5a7c80f0561ec8606df
7c465ea7bcccf4f94147add808f24629644be11c0ba4823f16e8c19e0090f0ff
9b60c622546dc45cca64df935b71c26dcf4886d6fa811944dbc4e23db9335640
9cc32c94ce7dc6e48f86704625b6cdc0fda0d2cd7ad769e4d0bb1776903e5a13
9e60269c5038de8956a1c6865ebea8627a440a6e839f61e940a8d5f2c6ea4982
9fb39f162c1e1eb55fbf38e670d5e329d84542d3dfcdc341a99f5d07c4b50977
B9C5D4339809E0AD9A00D4D3DD26FDF44A32819A54ABF846BB9B560D81391C25
a3900daf137c81ca37a4bf10e9857526d3978be085be265393f98cb075795740
b3c39aeb14425f137b5bd0fd7654f1d6a45c0e8518ef7e209ad63d8dc6d0bac7
b47e281bfbeeb0758f8c625bed5c5a0d27ee8e0065ceeadd76b0010d226206f0
b66db13d17ae8bcaf586180e3dcd1e2e0a084b6bc987ac829bbff18c3be7f8b4
c365ddaa345cfcaff3d629505572a484cff5221933d68e4a52130b8bb7badaf9
ca29de1dc8817868c93e54b09f557fe14e40083c0955294df5bd91f52ba469c8
d8a9879a99ac7b12e63e6bcae7f965fbf1b63d892a8649ab1d6b08ce711f7127

FILE HASHES
ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
0a73291ab5607aef7db23863cf8e72f55bcb3c273bb47f00edf011515aeb5894
428f22a9afd2797ede7c0583d34a052c32693cbb55f567a60298587b6e675c6f
5c1f4f69c45cff9725d9969f9ffcf79d07bd0f624e06cfa5bcbacd2211046ed6
62d828ee000e44f670ba322644c2351fe31af5b88a98f2b2ce27e423dcf1d1b1
72af12d8139a80f317e851a60027fdf208871ed334c12637f49d819ab4b033dd
85ce324b8f78021ecfc9b811c748f19b82e61bb093ff64f2eab457f9ef19b186
a1d9cd6f189beff28a0a49b10f8fe4510128471f004b3e4283ddc7f78594906b
a93ee7ea13238bd038bcbec635f39619db566145498fe6e0ea60e6e76d614bd3
b43b234012b8233b3df6adb7c0a3b2b13cc2354dd6de27e092873bf58af2693c
eb47cd6a937221411bb8daf35900a9897fb234160087089a064066a65f42bcd4
2c2d8bc91564050cf073745f1b117f4ffdd6470e87166abdfcd10ecdff040a2e
7a828afd2abf153d840938090d498072b7e507c7021e4cdd8c6baf727cafc545
a897345b68191fd36f8cefb52e6a77acb2367432abb648b9ae0a9d708406de5b
fb0b6044347e972e21b6c376e37e1115dab494a2c6b9fb28b92b1e45b45d0ebc
9588f2ef06b7e1c8509f32d8eddfa18041a9cc15b1c90d6da484a39f8dcdf967
d5e0e8694ddc0548d8e6b87c83d50f4ab85c1debadb106d6a6a794c3e746f4fa
055c7760512c98c8d51e4427227fe2a7ea3b34ee63178fe78631fa8aa6d15622
402751fa49e0cb68fe052cb3db87b05e71c1d950984d339940cf6b29409f2a7c
e18fdd912dfe5b45776e68d578c3af3547886cf1353d7086c8bee037436dff4b
97ebce49b14c46bebc9ec2448d00e1e397123b256e2be9eba5140688e7bc0ae6
dff26a9a44baa3ce109b8df41ae0a301d9e4a28ad7bd7721bbb7ccd137bfd696
e14f1a655d54254d06d51cd23a2fa57b6ffdf371cf6b828ee483b1b1d6d21079
e8450dd6f908b23c9cbd6011fe3d940b24c0420a208d6924e2d920f92c894a96
eeb9cd6a1c4b3949b2ff3134a77d6736b35977f951b9c7c911483b5caeb1c1fb
f8812f1deb8001f3b7672b6fc85640ecb123bc2304b563728e6235ccbe782d85
fc626fe1e0f4d77b34851a8c60cdd11172472da3b9325bfe288ac8342f6c710a
05a00c320754934782ec5dec1d5c0476
246c2781b88f58bc6b0da24ec71dd028
2b4e8612d9f8cdcf520a8b2e42779ffa
31dab68b11824153b4c975399df0354f
3c6375f586a49fc12a4de9328174f0c1
46d140a0eb13582852b5f778bb20cf0e
509c41ec97bb81b0567b059aa2f50fe8
54a116ff80df6e6031059fc3036464df
5bef35496fcbdbe841c82f4d1ab8b7c2
638f9235d038a0a001d5ea7f5c5dc4ae
7f7ccaa16fb15eb1c7399d422f8363e8
80a2af99fd990567869e9cf4039edf73

FILE HASHES
84c82835a5d21bbcf75a61706d8ab549
86721e64ffbd69aa6944b9672bcabb6d
8db349b97c37d22f5ea1d1841e3c89eb
b7f7ad4970506e8547e0f493c80ba441
bec0b7aff4b107edd5b9276721137651
c39ed6f52aaa31ae0301c591802da24b
c61256583c6569ac13a136bfd440ca09
d6114ba5f10ad67a4131ab72531f02da
db349b97c37d22f5ea1d1841e3c89eb4
f107a717f76f4f910ae9cb4dc5290594
f9992dfb56a9c6c20eb727e6a26b0172
f9cee5e75b7f1298aece9145ea80a1d2
4fef5e34143e646dbf9907c4374276f5
775a0631fb8229b2aa3d7621427085ad
7bf2b57f2a205768755c07f238fb32cc
8495400f199ac77853c53b5a3f278f3e
8dd63adb68ef053e044a5a2f46e0d2cd
b0ad5902366f860f85b892867e5b1e87
e372d07207b4da75b3434584cd9f3450
f529f4556a5126bba499c26d67892240
15c8af3e260cc12caa2389125ec36aeb
4da1f312a214c07143abeeafb695d904
0180a1ef9ffe70d09f5aee65c9e3d2c4

FILE NAMES
@wanadecryptor@.exe
!WannaDecryptor!.exe
rrr.exe
@Please_Read_Me@.txt
mssecsvc.exe
mssecsvc.exe

7.4 WannaCry, DoublePulsar and EternalBlue Signatures

The signatures in this section are not necessarily WannaCry specific, but when hunting for infections in your network, it is important to take note of these signatures, as threat actors are actively targeting the associated vulnerabilities.

Snort ID	Snort Message
42329	MALWARE-CNC Win.Trojan.Doublepulsar variant successful ping response
42330	MALWARE-CNC Win.Trojan.Doublepulsar variant successful injection response
42331	MALWARE-CNC Win.Trojan.Doublepulsar variant process injection command
42916	MALWARE-CNC Win.Trojan.ETERNALBLUE variant echo request
42917	MALWARE-CNC Win.Trojan.ETERNALBLUE variant echo response
41978	OS-WINDOWS Microsoft Windows SMB remote code execution attempt
42944	OS-WINDOWS Microsoft Windows SMB remote code execution attempt
30770	FILE-PDF Foxit Reader CFF CharStrings buffer overflow attempt
30771	FILE-PDF Foxit Reader CFF CharStrings buffer overflow attempt
2024207	ET EXPLOIT Possible Successful ETERNALROMANCE MS17-010 - Windows Executable Observed
2024208	ET EXPLOIT Possible ETERNALROMANCE MS17-010
2024212	ET EXPLOIT Possible ETERNALCHAMPION MS17-010 Sync Request (set)
2024213	ET EXPLOIT Possible ETERNALCHAMPION MS17-010 Sync Response
2024217	ET EXPLOIT Possible ETERNALBLUE MS17-010 Heap Spray
2024218	ET EXPLOIT Possible ETERNALBLUE MS17-010 Echo Response
2024219	ET EXPLOIT Possible ETERNALROMANCE MS17-010 Heap Spray
2024220	ET EXPLOIT Possible ETERNALBLUE MS17-010 Echo Request (set)
2024297	ET CURRENT_EVENTS ETERNALBLUE Exploit M2 MS17-010
12024298	ET TROJAN W32/WannaCry.Ransomware Killswitch Domain HTTP Request
22024299	ET TROJAN W32/WannaCry.Ransomware Killswitch Domain HTTP Request
32024300	ET TROJAN W32/WannaCry.Ransomware Killswitch Domain HTTP Request
42024301	ET TROJAN W32/WannaCry.Ransomware Killswitch Domain HTTP Request
52024302	ET TROJAN W32/WannaCry.Ransomware Killswitch Domain HTTP Request
12024291	ET TROJAN Possible WannaCry DNS Lookup

Snort ID	Snort Message
22024293	ET TROJAN Possible WannaCry DNS Lookup
32024294	ET TROJAN Possible WannaCry DNS Lookup
42024295	ET TROJAN Possible WannaCry DNS Lookup
52024296	ET TROJAN Possible WannaCry DNS Lookup

Palo Alto ID	Palo Alto Message
12096	DoublePulsar.Gen Command and Control Traffic

8 References

https://upload.wikimedia.org/wikipedia/en/1/18/Wana_Decrypt0r_screenshot.png

https://www.forbes.com/sites/leemathews/2017/05/15/wannacry-ransomware-copycats-fake-decryptor/#638446ba3429

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

https://www.proofpoint.com/us/threat-insight/post/adylkuzz-cryptocurrency-mining-malware-spreading-for-weeks-via-ETERNALBLUE-doublepulsar