TLP:WHITE

Alert (TA17-132A)

Indicators Associated With WannaCry Ransomware

Original release date: May 12, 2017 | Last revised: June 07, 2018

Systems Affected

Microsoft Windows operating systems

Overview

This Alert has been updated to reflect the U.S. Government's public attribution of the "WannaCry" ransomware variant to the North Korean government. Additional information on the attribution may be found in a press briefing from the White House. For more information related to WannaCry activity, go to https://www.us-cert.gov/hiddencobra.

According to numerous open-source reports, a widespread ransomware campaign is affecting various organizations with reports of tens of thousands of infections in over 150 countries, including the United States, United Kingdom, Spain, Russia, Taiwan, France, and Japan. The software can run in as many as 27 different languages.

The latest version of this ransomware variant, known as WannaCry, WCry, or Wanna Decryptor, was discovered the morning of May 12, 2017, by an independent security researcher and has spread rapidly over several hours, with initial reports beginning around 4:00 AM EDT, May 12, 2017. Open-source reporting indicates a requested ransom of .1781 bitcoins, roughly $300 U.S.

This Alert is the result of efforts between the Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center (NCCIC) and the Federal Bureau of Investigation (FBI) to highlight known cyber threats. DHS and the FBI continue to pursue related information of threats to federal, state, and local government systems and as such, further releases of technical information may be forthcoming.

Description

Initial reports indicate the hacker or hacking group behind the WannaCry campaign is gaining access to enterprise servers through the exploitation of a critical Windows SMB vulnerability. Microsoft released a security update for the MS17-010 vulnerability on March 14, 2017. Additionally, Microsoft released patches for Windows XP, Windows 8, and Windows Server 2003 operating systems on May 13, 2017.

According to open sources, one possible infection vector may be through phishing.

Technical Details

Indicators of Compromise (IOC)

TLP:WHITE

See TA17-132A_WannaCry.xlsx and TA17-132A_WannaCry_stix.xml for IOCs developed immediately after WannaCry ransomware appeared. These links contain identical content in two different formats.

See TA17-132A_stix.xml for IOCs developed after further analysis of the WannaCry malware.

Analysis

Three files were submitted to US-CERT for analysis. All files are confirmed as components of a ransomware campaign identified as "WannaCry", a.k.a "WannaCrypt" or ".wnCry". The first file is a dropper, which contains and runs the ransomware, propagating via the MS17-010/EternalBlue SMBv1.0 exploit. The remaining two files are ransomware components containing encrypted plug-ins responsible for encrypting the victim users files. For a list of IOCs found during analysis, see the STIX file.

Displayed below are YARA signatures that can be used to detect the ransomware:

Yara Signatures

```
rule Wanna_Cry_Ransomware_Generic {

       meta:

              description = "Detects WannaCry Ransomware on Dis
k and in Virtual Page"

              author = "US-CERT Code Analysis Team"

              reference = "not se
t"

              date = "2017/05/12"

       hash0 = "4DA1F312A214C07143ABEEAFB695D904"

       strings:

              $s0 = {410044004D0049004E0024}

              $s1 = "WannaDecryptor"

              $s2 = "WANNACRY"

              $s3 = "Microsoft Enhanced RSA and AES Cryptograph
ic"

              $s4 = "PKS"

              $s5 = "StartTask"

              $s6 = "wcry@123"

              $s7 = {2F6600002F72}

              $s8 = "unzip 0.15 Copyrigh"

              $s9 = "Global\\WINDOWS_TASKOSHT_MUTEX"

             $s10 = "Global\\WINDOWS_TASKCST_MUTEX"
```

```
            $s11 = {7461736B736368652E65786500000005461736B53
74617274000000742E776E7279000069636163}

            $s12 = {6C73202E202F6772616E742045766572796F6E653A
46202F54202F43202F5100617474726962202B68}

            $s13 = "WNcry@2ol7"

            $s14 = "wcry@123"

            $s15 = "Global\\MsWinZonesCacheCounterMutexA"

      condition:

             $s0 and $s1 and $s2 and $s3 or $s4 and $s5 and $s
6 and $s7 or $s8 and $s9 and $s10 or $s11 and $s12 or $s13 or
$s14 or $s15

}

/*The following Yara ruleset is under the GNU-GPLv2 license (ht
tp://www.gnu.org/licenses/gpl-2.0.html) and open to any user or
organization, as long as you use it under this license.*/

rule MS17_010_WanaCry_worm {

      meta:

            description = "Worm exploiting MS17-010 and dropp
ing WannaCry Ransomware"

            author = "Felipe Molina (@felmoltor)"

            reference = "https://www.exploit-db.com/exploits/
41987/"

            date = "2017/05/12"

      strings:

            $ms17010_str1="PC NETWORK PROGRAM 1.0"

            $ms17010_str2="LANMAN1.0"

            $ms17010_str3="Windows for Workgroups 3.1a"

            $ms17010_str4="__TREEID__PLACEHOLDER__"

            $ms17010_str5="__USERID__PLACEHOLDER__"

            $wannacry_payload_substr1 = "h6agLCqPqVyXi2VSQ8O6
Yb9ijBX54j"

            $wannacry_payload_substr2 = "h54WfF9cGigWFEx92bzm
Od0UOaZlM"

            $wannacry_payload_substr3 = "tpGFEoLOU6+5I78Toh/n
Hs/RAP"

      condition:
```

```
                all of them

}
```

Dropper

This artifact (5bef35496fcbdbe841c82f4d1ab8b7c2) is a malicious PE32 executable that has been identified as a WannaCry ransomware dropper. Upon execution, the dropper attempts to connect to the following hard-coded URI:

```
http[:]//www[.]iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com.
```

Displayed below is a sample request observed:

```
--Begin request—

GET / HTTP/1.1
Host: www[.]iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
Cache-Control: no-cache

--End request--
```

If a connection is established, the dropper will terminate execution. If the connection fails, the dropper will infect the system with ransomware.
When executed, the malware is designed to run as a service with the parameters “-m security”. During runtime, the malware determines the
number of arguments passed during execution. If the arguments passed are less than two, the dropper proceeds to install itself as the
following service:

```
--Begin service--

ServiceName = "mssecsvc2.0"
DisplayName = "Microsoft Security Center (2.0) Service"
StartType = SERVICE_AUTO_START
BinaryPathName = "%current
directory%5bef35496fcbdbe841c82f4d1ab8b7c2.exe -m security"

--End service--
```

Once the malware starts as a service named mssecsvc2.0, the dropper attempts to create and scan a list of IP ranges on the local network
and attempts to connect using UDP ports 137, 138 and TCP ports 139, 445. If a connection to port 445 is successful, it creates an additional
thread to propagate by exploiting the SMBv1 vulnerability documented by Microsoft Security bulliten MS17-010. The malware then extracts &
installs a PE32 binary from it's resource section named "R". This binary has been identified as the ransomware component of WannaCrypt.
The dropper installs this binary into "C:\WINDOWS\tasksche.exe." The dropper executes tasksche.exe with the following command:

```
--Begin command--

"C:\WINDOWS\tasksche.exe /i"

--End command—
```

Note:
=====
When this sample was initially discovered, the domain "iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com" was not registered, allowing the malware to run and propagate freely. However within a few days, researchers learned that by registering the domain and allowing the
malware to connect, it's ability to spread was greatly reduced. At this time, all traffic to "iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com" is
re-directed to a monitored, non-malicious server, causing the malware to terminate if it is allowed to connect. For this reason, we recommend
that administrators and network security personnel not block traffic to this domain.

Impact

Ransomware not only targets home users; businesses can also become infected with ransomware, leading to negative consequences, including

- temporary or permanent loss of sensitive or proprietary information,
- disruption to regular operations,
- financial losses incurred to restore systems and files, and
- potential harm to an organization’s reputation.

Paying the ransom does not guarantee the encrypted files will be released; it only guarantees that the malicious actors receive the victim’s money, and in some cases, their banking information. In addition, decrypting files does not mean the malware infection itself has been removed.

Solution

Recommended Steps for Prevention

- Apply the Microsoft patch for the MS17-010 SMB vulnerability dated March 14, 2017.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate in-bound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching the end users.
- Ensure anti-virus and anti-malware solutions are set to automatically conduct regular scans.
- Manage the use of privileged accounts. Implement the principle of least privilege. No users should be assigned administrative access unless absolutely needed. Those with a need for administrator accounts should only use them when necessary.
- Configure access controls including file, directory, and network share permissions with least privilege in mind. If a user only needs to read specific files, they should not have write access to those files, directories, or shares.
- Disable macro scripts from Microsoft Office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full Office suite applications.
- Develop, institute, and practice employee education programs for identifying scams, malicious links, and attempted social engineering.
- Run regular penetration tests against the network, no less than once a year. Ideally, run these as often as possible and practical.

- Test your backups to ensure they work correctly upon use.

Recommendations for Network Protection

Apply the patch (MS17-010). If the patch cannot be applied, consider:

- Disabling SMBv1 and
- blocking all versions of SMB at the network boundary by blocking TCP port 445 with related protocols on UDP ports 137-138 and TCP port 139, for all boundary devices.

Note: *disabling or blocking SMB may create problems by obstructing access to shared files, data, or devices. The benefits of mitigation should be weighed against potential disruptions to users.*

Review US-CERT's Alert on The Increasing Threat to Network Infrastructure Devices and Recommended Mitigations and consider implementing the following best practices:

1. Segregate networks and functions.
2. Limit unnecessary lateral communications.
3. Harden network devices.
4. Secure access to infrastructure devices.
5. Perform out-of-band network management.
6. Validate integrity of hardware and software.

Recommended Steps for Remediation

- Contact law enforcement. We strongly encourage you to contact a local FBI field office upon discovery to report an intrusion and request assistance. Maintain and provide relevant logs.
- Implement your security incident response and business continuity plan. Ideally, organizations should ensure they have appropriate backups so their response is simply to restore the data from a known clean backup.

Defending Against Ransomware Generally

Precautionary measures to mitigate ransomware threats include:

- Ensure anti-virus software is up-to-date.
- Implement a data back-up and recovery plan to maintain copies of sensitive or proprietary data in a separate and secure location. Backup copies of sensitive data should not be readily accessible from local networks.
- Scrutinize links contained in emails, and do not open attachments included in unsolicited emails.
- Only download software—especially free software—from sites you know and trust.
- Enable automated patches for your operating system and Web browser.

Report Notice

DHS and FBI encourages recipients who identify the use of tool(s) or techniques discussed in this document to report information to DHS or law enforcement immediately. We encourage you to contact DHS's National Cybersecurity and Communications Integration Center (NCCIC) (NCCICcustomerservice@hq.dhs.gov or 888-282-0870), or the FBI through a local field office or the FBI's Cyber Division (CyWatch@ic.fbi.gov or 855-292-3937) to report an intrusion and to request incident response resources or technical assistance.

References

- Malwarebytes LABS: WanaCrypt0r ransomware hits it big just before the weekend
- Malwarebytes LABS: The worm that spreads WanaCrypt0r
- Microsoft: Microsoft Security Bulletin MS17-010
- Forbes: An NSA Cyber Weapon Might Be Behind A Massive Global Ransomware Outbreak
- Reuters: Factbox: Don't click - What is the 'ransomware' WannaCry worm?
- GitHubGist: WannaCry|WannaDecrypt0r NSA-Cyberweapon-Powered Ransomware Worm
- Microsoft: Microsoft Update Catalog: Patches for Windows XP, Windows 8, and Windows Server 2003, (KB4012598)
- Cisco: Player 3 Has Entered the Game: Say Hello to 'WannaCry'
- Washington Post: More than 150 countries affected by massive cyberattack, Europol says

Revisions

- May 12, 2017: Initial post
- May 14, 2017: Corrected Syntax in the second Yara Rule
- May 14, 2017: Added Microsoft link to patches for Windows XP, Windows 8, and Windows Server 2003
- May 14, 2017: Corrected Syntax in the first Yara Rule
- May 16, 2017: Provided further analysis and new IOCs in STIX format
- May 18, 2017: Provided initial IOCs in a STIX format
- June 7, 2018: Added attribution of the WannaCry malware variant to the North Korean government and link to White House press briefing