Alert (TA17-132A)

Indicators Associated With WannaCry Ransomware

Original release date: May 12, 2017 | Last revised: May 15, 2017

Systems Affected

Microsoft Windows operating systems

Overview

According to numerous open-source reports, a widespread ransomware campaign is affecting various organizations with reports of tens of thousands of infections in as many as 74 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 either through Remote Desktop Protocol (RDP) compromise or 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 is via phishing emails.

Technical Details

Indicators of Compromise (IOC)

IOCs are provided within the accompanying .xlsx file of this report.

Yara Signatures

```
rule Wanna_Cry_Ransomware_Generic {

       meta:

              description = "Detects WannaCry Ransomware on Disk and in Virtual Page"

              author = "US-CERT Code Analysis Team"

              reference = "not set"

              date = "2017/05/12"

       hash0 = "4DA1F312A214C07143ABEEAFB695D904"

       strings:

              $s0 = {410044004D0049004E0024}

              $s1 = "WannaDecryptor"

              $s2 = "WANNACRY"

              $s3 = "Microsoft Enhanced RSA and AES Cryptographic"

              $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 = {7461736B736368652E657865000000005461736B5374617274000000742E776E7279000069636163}

            $s12 = {6C73202E202F6772616E742045766572796F6E653A46202F54202F43202F5100617474726962202B68}
```

```
             $s13 = "WNcry@2ol7"

             $s14 = "wcry@123"

             $s15 = "Global\\MsWinZonesCacheCounterMutexA"

       condition:

              $s0 and $s1 and $s2 and $s3 or $s4 and $s5 and $s6 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 (http://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 dropping 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 = "h6agLCqPqVyXi2VSQ8O6Yb9ijBX54j"

              $wannacry_payload_substr2 = "h54WfF9cGigWFEx92bzmOd0UOaZlM"

              $wannacry_payload_substr3 = "tpGFEoLOU6+5I78Toh/nHs/RAP"

       condition:

              all of them

}
```

Initial Analysis

The WannaCry ransomware received and analyzed by US-CERT is a loader that contains an AES-encrypted DLL. During runtime, the loader writes a file to disk named “t.wry”. The malware then uses an embedded 128-bit key to decrypt this file. This DLL, which is then loaded into the parent process, is the actual Wanna Cry Ransomware responsible for encrypting the user’s files. Using this cryptographic loading method, the WannaCry DLL is never directly exposed on disk and not vulnerable to antivirus software scans.

The newly loaded DLL immediately begins encrypting files on the victim’s system and encrypts the user’s files with 128-bit AES. A random key is generated for the encryption of each file.

The malware also attempts to access the IPC$ shares and SMB resources the victim system has access to. This access permits the malware to spread itself laterally on a compromised network. However, the malware never attempts to attain a password from the victim’s account in order to access the IPC$ share.

This malware is designed to spread laterally on a network by gaining unauthorized access to the IPC$ share on network resources on the network on which it is operating.

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 e-mails from reaching the end users and authenticate in-bound e-mail using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent e-mail spoofing.
    - Scan all incoming and outgoing e-mails 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 e-mail. Consider using Office Viewer software to open Microsoft Office files transmitted via e-mail instead of full Office suite applications.
- Develop, institute and practice employee education programs for identifying scams, malicious links, and attempted social engineering.
- Have regular penetration tests run against the network. No less than once a year. Ideally, as often as possible/practical.
- Test your backups to ensure they work correctly upon use.

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 e-mails, and do not open attachments included in unsolicited e-mails.
- 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)

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