FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

Indicators Associated With WannaCry Ransomware

13 May 2017

Alert Number
MC-000081-MW

WE NEED YOUR HELP!

If you find any of these indicators on your networks, or have related information, please contact FBI CYWATCH immediately.

Email:
cywatch@ic.fbi.gov

Phone:
1-855-292-3937

*Note: By reporting any related information to FBI CyWatch, you are assisting in sharing information that allows the FBI to track malicious actors and coordinate with private industry and the United States Government to prevent future intrusions and attacks.

This is a joint product with the Department of Homeland Security.

In furtherance of public-private partnerships, the FBI routinely advises private industry of various cyber threat indicators observed during the course of our investigations. This data is provided in order to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber criminals.

This FLASH has been released **TLP: WHITE**: This information may be distributed without restriction.

Summary

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 99 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.

Technical Details

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. According to open sources, one possible infection vector is via phishing emails.

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.

Confirmed indicators:

SHA-256 Hashes:
24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c

043e0d0d8b8cda56851f5b853f244f677bd1fd50f869075ef7ba1110771f70c2
5d26835be2cf4f08f2beeff301c06d05035d0a9ec3afacc71dff22813595c0b9
76a3666ce9119295104bb69ee7af3f2845d23f40ba48ace7987f79b06312bbdf
be22645c61949ad6a077373a7d6cd85e3fae44315632f161adc4c99d5a8e6844
f7c7b5e4b051ea5bd0017803f40af13bed224c4b0fd60b890b6784df5bd63494
fc626fe1e0f4d77b34851a8c60cdd11172472da3b9325bfe288ac8342f6c710a
09a46b3e1be080745a6d8d88d6b5bd351b1c7586ae0dc94d0c238ee36421cafa
aee20f9188a5c3954623583c6b0e6623ec90d5cd3fdec4e1001646e27664002c
c365ddaa345cfcaff3d629505572a484cff5221933d68e4a52130b8bb7badaf9
ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
b9c5d4339809e0ad9a00d4d3dd26fdf44a32819a54abf846bb9b560d81391c25

File name:
@WanaDecryptor@.exe

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"
        condition:
                $s0 and $s1 and $s2 and $s3 or $s4 or $s5 or $s6 or $s7 or $s8
}
/*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
}
```

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, and 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.

Reporting Notice

The FBI encourages recipients who identify the use of tool(s) or techniques discussed in this document to report information to their local FBI field office or the FBI's 24/7 Cyber Watch (CyWatch). Field office contacts can be identified at www.fbi.gov/contact-us/field. CyWatch can be contacted by phone at 855-292-3937 or by e-mail at CyWatch@ic.fbi.gov. When available, each report submitted should include: the date; time; location; type of activity; number of infected users; type of equipment used for the activity; name of the submitting company or organization; and a designated point of contact.

Your Feedback on the Value of this Product Is Critical

Was this product of value to your organization? Was the content clear and concise? Your comments are very important to us and can be submitted anonymously. Please take a moment to complete the survey at the link below. Feedback should be specific to your experience with our written products to enable the FBI to make quick and continuous improvements to such products. Feedback may be submitted online here:
https://www.ic3.gov/PIFSurvey

Please note that this survey is for feedback on content and value only. Reporting of technical information regarding FLASH reports must be submitted through FBI CYWATCH.