03 July 2017

Alert Number

MI-000082-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.*

The following information is being provided by the FBI for potential use at the sole discretion of recipients to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber criminals.

This FLASH has been released **TLP:WHITE** and may be distributed without restriction, subject to copyright controls.

Indicators Associated with Ransomware Attack Potentially Modeled after Petya

Summary

According to numerous open-source reports, a widespread ransomware campaign is affecting various organizations in the United States, France, India, Russia, Spain, Ukraine, and the United Kingdom. Initial open-source reporting detailed a potential variant of the Petya ransomware was being utilized in the attack and demanded a ransom of $300 US worth of bitcoin.

Technical Details

Open-source reports indicate the new ransomware employs the same EternalBlue exploit used by WannaCry ransomware, allowing it to spread quickly and infect additional systems. Published by the Shadow Brokers in April 2017, the vulnerability targets Windows' SMB file-sharing system. Microsoft issued a patch for the MS17-010 SMB vulnerability on March 14, 2017. In addition to leveraging the Service Message Block (SMB) vulnerability, the ransomware also uses wmic/PSExec to move between computers on a local network.

A variant of the Petya ransomware was potentially used in the attack, according to open-source reporting. Petya ransomware was first discovered in 2016 and operated atypically from previous known ransomware variants by overwriting the Master Boot Record (MBR)

and encrypting the Master File Table (MFT), instead of encrypting individual files. While using a very similar method to overwrite the MBR and load a custom boot loader, the new variant also performs user mode encryption of select file extensions on individual files. Further open-source reporting indicated the ransomware attack could be the result of a new ransomware variant, different from Petya.

Confirmed Indicators

Hashes
34f917aaba5684fbe56d3c57d48ef2a1aa7cf06d

9717cfdc2d023812dbc84a941674eb23a2a8ef06

38e2855e11e353cedf9a8a4f2f2747f1c5c07fcf

56c03d8e43f50568741704aee482704a4f5005ad

Contact Email
wowsmith123456@posteo.net

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 of this document to report information concerning suspicious or criminal activity 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 people, and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact. Press inquiries should be directed to the FBI's National Press Office at npo@ic.fbi.gov or (202) 324-3691.

Administrative Note

This product is marked **TLP:WHITE** and may be distributed without restriction, subject to copyright controls.

For comments or questions related to the content or dissemination of this product, contact CyWatch.

FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

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.