FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

11 JULY 2016

Alert Number

MC-000076-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.*

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 to guard against the persistent malicious actions of cyber criminals.

This FLASH has been released **TLP: GREEN:** The information in this product is useful for the awareness off all participating organizations within their sector or community, but not via publicly accessible channels.

Identification of ransomware variant called Locky

Summary

The 'Locky' malware is a ransomware variant, which has extensively utilized spam campaigns to distribute malicious files that download and execute code capable of encrypting numerous critical file types on both local and networked file stores. Encrypted files are renamed with a unique hexadecimal filename and receive the ".locky" extension. Each directory containing encrypted files contains instructions on how to utilize Bitcoin in order to pay a ransom for file recovery, and the system's computer background is also changed to contain payment instructions. Recovery of encrypted files is impossible without data backup or acquisition of the private key due to the well-implemented, strong encryption. Historically, while payment of the ransom may result in receipt of the valid private key, enabling decryption of the targeted files, the FBI does not recommended the victim pay the ransom.

Technical Details

In early 2016, a destructive ransomware variant, Locky, was observed infecting business computers in the United States, New Zealand, Australia, Germany, and the United Kingdom. It propagates through spam e-mails that include malicious Microsoft Office documents and JavaScript or compressed attachments (e.g., .rar, .zip). The infection vectors are similar to the Dridex banking Trojan and Pony loader. The malicious attachments contain macros or JavaScript files to download the Locky files. Locky has also been distributed via the Neutrino and Nuclear exploit kits. Locky is based on an affiliate model. The developers of Locky offer it

as a service, and the FBI currently assesses that it is the responsibility of the individual affiliate to distribute the malware, resulting in the variety of attack vectors mentioned above.

The malicious Microsoft Office documents contain macros with obfuscated Visual Basic Script (VBS) and/or batch files, which result in the download and execution of the Locky executable. The malicious JavaScript files are delivered via zip files in e-mail, which results in the download and execution of the Locky executable. Once executed, Locky establishes persistence via a Run key within the registry and attempts to delete shadow copies using the vssadmin command, and encrypt user space files, such as documents, media files, archives, source code, and other critical files.

Locky communicates with a hard coded command and control server to inform the operators of a successful infection and to obtain encryption keys and a unique victim identifier. Additionally, Locky contains a domain generation algorithm, which will generate additional domains for communication with the command and control infrastructure. Network requests typically include http POSTs to files, such as main.php, submit.php, or most recently, userinfo.php, and updated Locky variants encrypt command and control communications.

An updated complete list of indicators for known domains, e-mail subject lines, URLs, Hash data, and associated files is attached to this e-mail.

Recommended Steps for Prevention

- Implement an awareness and training program. Because end users are targeted, employees and individuals should be made aware of the threat of ransomware and how it is delivered.
- 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 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.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Implement application whitelisting; only allow systems to execute programs known and permitted by security policy.
- Categorize data based on organizational value, and implement physical/logical separation of networks and data for different organizational units.

Recommended Steps for Remediation

- Isolate the infected computer(s) immediately. Infected systems should be removed from the network as soon as possible to prevent ransomware from attacking network or share drives.
- Do not clean or re-image the infected computer(s) until you have completely recovered from the event. It may be critical to have the infected computer to recover from the incident if other avenues of recovery fail or are not available.
- Contact law enforcement. We strongly encourage you to contact a local FBI field office upon discovery to report a ransomware event and request assistance.
- Implement your security incident response and business continuity plan. Ideally, organizations should ensure they have appropriate backups, so that their response is simply to restore the data from a known clean backup.

The following information is being requested of victims of Locky infections when reporting to law enforcement:

1. Detailed victim information, to include organization name, sector, and technical POC.
2. Original e-mail(s) with full headers and any attachments (assuming phishing attack vector) or network traffic information from exploit kit attack vectors.
3. Copies of any executables or other files dropped onto the system after accessing malicious attachments.
4. Any domains or IP addresses communicated with just prior to or during infection.
5. The "personal identification ID" as specified in the ransom text/image.
6. The Bitcoin wallet ID to which payment is requested, and the amount being requested.
7. If a ransom was paid, the amount, and the Bitcoin wallet ID from which the payment was made.
8. If available, any forensic analysis or incident response reports completed.
9. If available, any memory captures taken during execution of the malware.
10. Status of the infection.

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 people, and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact.

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.