HSIN-HPH Bulletin: Ransomware (Locky variant)

Date: 04/05/2016

The Department of Homeland Security National Cybersecurity and Communications Integration Center (NCCIC) has notified the Department of Health and Human Services (HHS) of an increase in ransomware incidents at some healthcare organizations in the U.S. This Bulletin provides Healthcare and Public Health (HPH) Partners with information regarding ransomware, mitigation strategies, as well as additional materials to reference located within the HSIN HPH Cyber Threat Library.

Information in this bulletin was developed in coordination with and for the benefit of the HPH Sector Critical Infrastructure Protection (CIP) Partnership. The HPH CIP Partnership operates under the National Infrastructure Protection Plan and is coordinated within HHS by the Office of the Assistant Secretary for Preparedness and Response. The partnership is dedicated to joint public and private sector efforts to protect the HPH Sector from all hazards through information sharing and collaborative risk management.

This bulletin is specific to the Locky variant of ransomware. Additional details of the Locky variant, and other variants, are available in a number of creditable products posted to the HSIN HPH Cyber Threat Library, the US-CERT Portal, and US-CERT Open Internet Website. If your organization, hospital, or facility experiences a similar cyber attack, please contact law enforcement immediately. You may also be able to find assistance from the DHS National Cybersecurity and Communications Integration Center (NCCIC) or an Information Sharing and Analysis Organization (ISAO) such as NH-ISAC or HITRUST. If you have any questions about which resources may be available to you or how to connect with them, please contact us at cip@hhs.gov.

Creditable Sources on Ransomware

- FBI FLASH MC-000068-MW
- US-CERT Alert (TA16-091A) Ransomware and Recent Variants
- FBI FLASH MC-000070-MW
- Samas.A_IOC_List
- HPH-HSIN Bulletin on Ransomware 03312016

Threat Details – Locky Ransomware variant

There is recent open source reporting that ties Locky Ransomware to the Dridex infrastructure. The malware seems to be most commonly delivered through mass phishing emails with malicious attachments. New discoveries suggest that recent Locky ransomware campaigns are using multiple types of attachments as the delivery mechanism. Unlike previous

variants, some of these instances no longer depend on the user enabling document macros to begin the encryption process.

Similarly, once the user opens the attachment, Locky attempts to download the encryption payload, looks for file extensions on the hard drive, and encrypts them. The token 'Ransom note image' is displayed with this message to the user: "All of your files are encrypted with RSA-2048 and AES-128 ciphers. Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server".

Below provides a list of recently discovered attachments along with their functionality:

- JavaScript files that download and execute a malicious binary which performs the encryption.
- .zip files which contain the malicious JavaScript files.
- Microsoft Word documents that contain macros that automatically create and execute a malicious .vbs file. This .vbs file then downloads and executes a malicious binary which performs the encryption.

Indicators of Compromise (IOC)
The hash values, associated domains, and internet protocol addresses appear to be constantly changing and are therefore not reliable.

Mitigation
Guidance at this point mirrors the mitigation advice for most ransomware:

- If IOCs are determined for a particular attack, monitor for other systems communicating with those IOCs. While IOCs change between attacks, observations indicate that individual emails associated with an attack share indicators.
- Monitor for unexpected emails containing .doc, .js, and .zip files.
- Monitor for the creation of malicious .js and .vbs files on file systems, particularly in users' Application Data and Temp folders.
- Patch applications to ensure antivirus, OS, and third party software products are up-to-date.
- Do not open suspicious attachments or follow suspicious links.
- Perform regular backups that are stored on non-network connected machines.