National Cyber Awareness System:

TA13-309A: CryptoLocker Ransomware Infections

11/05/2013 10:58 AM EST

Original release date: November 05, 2013 | Last revised: November 06, 2013

Systems Affected

Microsoft Windows systems running Windows 7, Vista, and XP operating systems

Overview

US-CERT is aware of a malware campaign that surfaced in 2013 and is associated with an increasing number of ransomware infections. CryptoLocker is a new variant of ransomware that restricts access to infected computers and demands the victim provide a payment to the attackers in order to decrypt and recover their files. As of this time, the primary means of infection appears to be phishing emails containing malicious attachments.

Description

CryptoLocker appears to have been spreading through fake emails designed to mimic the look of legitimate businesses and through phony FedEx and UPS tracking notices. In addition, there have been reports that some victims saw the malware appear following after a previous infection from one of several botnets frequently leveraged in the cyber-criminal underground.

Impact

The malware has the ability to find and encrypt files located within shared network drives, USB drives, external hard drives, network file shares and even some cloud storage drives. If one computer on a network becomes infected, mapped network drives could also become infected. CryptoLocker then connects to the attackers' command and control (C2) server to deposit the asymmetric private encryption key out of the victim's reach.

Victim files are encrypted using asymmetric encryption. Asymmetric encryption uses two different keys for encrypting and decrypting messages. Asymmetric encryption is a more secure form of encryption as only one party is aware of the private key, while both sides know the public key.

While victims are told they have three days to pay the attacker through a third-party payment method (MoneyPak, Bitcoin), some victims have claimed online that they paid the attackers and did not receive the promised decryption key. US-CERT and DHS encourage users and administrators experiencing a ransomware infection NOT to respond to extortion attempts by attempting payment and instead to report the incident to the FBI at the Internet Crime Complaint Center (IC3).

Solution

Prevention

US-CERT recommends users and administrators take the following preventative measures to protect their computer networks from a CryptoLocker infection:

- Do not follow unsolicited web links in email messages or submit any information to webpages in links
- Use caution when opening email attachments. Refer to the Security Tip Using Caution with Email Attachments for more information on safely handling email attachments
- Maintain up-to-date anti-virus software
- Perform regular backups of all systems to limit the impact of data and/or system loss
- Apply changes to your Intrusion Detection/Prevention Systems and Firewalls to detect any known malicious activity
- Secure open-share drives by only allowing connections from authorized users
- Keep your operating system and software up-to-date with the latest patches
- Refer to the Recognizing and Avoiding Email Scams (pdf) document for more information on avoiding email scams
- Refer to the Security Tip Avoiding Social Engineering and Phishing Attacks for more information on social engineering attacks

Mitigation

US-CERT suggests the following possible mitigation steps that users and administrators can implement, if you believe your computer has been infected with CryptoLocker malware:

- Immediately disconnect the infected system from the wireless or wired network. This may prevent the malware from further encrypting any more files on the network
- Users who are infected should change all passwords AFTER removing the malware from their system
- Users who are infected with the malware should consult with a reputable security expert to assist in removing the malware, or users can retrieve encrypted files by the following methods:
    - Restore from backup,
    - Restore from a shadow copy or
    - Perform a system restore.

References

- CryptoLocker Virus: New Malware Holds Computers For Ransom, Demands $300 Within 100 Hours And Threatens To Encrypt Hard Drive
- CryptoLocker Wants Your Money!
- CryptoLocker ransomware – see how it works, learn about prevention, cleanup and recovery
- Microsoft Support – Description of the Software Restriction Policies in Windows XP
- Microsoft Software Restriction Policies Technical Reference – How Software Restriction Policies Work
- CryptoLocker Ransomware Information Guide and FAQ