Ransomware and Recent Variants | CISA

Published: 2016-09-29 · Archived: 2026-04-05 22:38:39 UTC

Systems Affected

Networked Systems

Overview

In early 2016, destructive ransomware variants such as Locky and Samas were observed infecting computers belonging to individuals and businesses, which included healthcare facilities and hospitals worldwide. Ransomware is a type of malicious software that infects a computer and restricts users' access to it until a ransom is paid to unlock it.

The United States Department of Homeland Security (DHS), in collaboration with Canadian Cyber Incident Response Centre (CCIRC), is releasing this Alert to provide further information on ransomware, specifically its main characteristics, its prevalence, variants that may be proliferating, and how users can prevent and mitigate against ransomware.

WHAT IS RANSOMWARE?

Ransomware is a type of malware that infects computer systems, restricting users' access to the infected systems. Ransomware variants have been observed for several years and often attempt to extort money from victims by displaying an on-screen alert. Typically, these alerts state that the user's systems have been locked or that the user's files have been encrypted. Users are told that unless a ransom is paid, access will not be restored. The ransom demanded from individuals varies greatly but is frequently $200–$400 dollars and must be paid in virtual currency, such as Bitcoin.

Ransomware is often spread through phishing emails that contain malicious attachments or through drive-by downloading. Drive-by downloading occurs when a user unknowingly visits an infected website and then malware is downloaded and installed without the user's knowledge.

Crypto ransomware, a malware variant that encrypts files, is spread through similar methods and has also been spread through social media, such as Web-based instant messaging applications. Additionally, newer methods of ransomware infection have been observed. For example, vulnerable Web servers have been exploited as an entry point to gain access into an organization's network.

WHY IS IT SO EFFECTIVE?

The authors of ransomware instill fear and panic into their victims, causing them to click on a link or pay a ransom, and users systems can become infected with additional malware. Ransomware displays intimidating messages similar to those below:

- “Your computer has been infected with a virus. Click here to resolve the issue.”
- “Your computer was used to visit websites with illegal content. To unlock your computer, you must pay a $100 fine.”
- “All files on your computer have been encrypted. You must pay this ransom within 72 hours to regain access to your data.”

PROLIFERATION OF VARIANTS

In 2012, Symantec, using data from a command and control (C2) server of 5,700 computers compromised in one day, estimated that approximately 2.9 percent of those compromised users paid the ransom. With an average ransom of $200, this meant malicious actors profited $33,600 per day, or $394,400 per month, from a single C2 server. These rough estimates demonstrate how profitable ransomware can be for malicious actors.

This financial success has likely led to a proliferation of ransomware variants. In 2013, more destructive and lucrative ransomware variants were introduced, including Xorist, CryptorBit, and CryptoLocker. Some variants encrypt not just the files on the infected device, but also the contents of shared or networked drives. These variants are considered destructive because they encrypt users’ and organizations’ files, and render them useless until criminals receive a ransom.

In early 2016, a destructive ransomware variant, Locky, was observed infecting computers belonging to healthcare facilities and hospitals in the United States, New Zealand, and Germany. It propagates through spam emails that include malicious Microsoft Office documents or compressed attachments (e.g., .rar, .zip). The malicious attachments contain macros or JavaScript files to download Ransomware-Locky files.

Samas, another variant of destructive ransomware, was used to compromise the networks of healthcare facilities in 2016. Unlike Locky, Samas propagates through vulnerable Web servers. After the Web server was compromised, uploaded Ransomware-Samas files were used to infect the organization’s networks.

LINKS TO OTHER TYPES OF MALWARE

Systems infected with ransomware are also often infected with other malware. In the case of CryptoLocker, a user typically becomes infected by opening a malicious attachment from an email. This malicious attachment contains Upatre, a downloader, which infects the user with GameOver Zeus. GameOver Zeus is a variant of the Zeus Trojan that steals banking information and is also used to steal other types of data. Once a system is infected with GameOver Zeus, Upatre will also download CryptoLocker. Finally, CryptoLocker encrypts files on the infected system, and requests that a ransom be paid.

The close ties between ransomware and other types of malware were demonstrated through the recent botnet disruption operation against GameOver Zeus, which also proved effective against CryptoLocker. In June 2014, an international law enforcement operation successfully weakened the infrastructure of both GameOver Zeus and CryptoLocker.

Impact

Ransomware not only targets home users; businesses can also become infected with ransomware, leading to negative consequences, including

- temporary or permanent loss of sensitive or proprietary information,
- disruption to regular operations,
- financial losses incurred to restore systems and files, and
- potential harm to an organization's reputation.

Paying the ransom does not guarantee the encrypted files will be released; it only guarantees that the malicious actors receive the victim's money, and in some cases, their banking information. In addition, decrypting files does not mean the malware infection itself has been removed.

Solution

Infections can be devastating to an individual or organization, and recovery can be a difficult process that may require the services of a reputable data recovery specialist.

US-CERT recommends that users and administrators take the following preventive measures to protect their computer networks from ransomware infection:

- Employ a data backup and recovery plan for all critical information. Perform and test regular backups to limit the impact of data or system loss and to expedite the recovery process. Note that network-connected backups can also be affected by ransomware; critical backups should be isolated from the network for optimum protection.
- Use application whitelisting to help prevent malicious software and unapproved programs from running. Application whitelisting is one of the best security strategies as it allows only specified programs to run, while blocking all others, including malicious software.
- Keep your operating system and software up-to-date with the latest patches. Vulnerable applications and operating systems are the target of most attacks. Ensuring these are patched with the latest updates greatly reduces the number of exploitable entry points available to an attacker.
- Maintain up-to-date anti-virus software, and scan all software downloaded from the internet prior to executing.
- Restrict users' ability (permissions) to install and run unwanted software applications, and apply the principle of "Least Privilege" to all systems and services. Restricting these privileges may prevent malware from running or limit its capability to spread through the network.
- Avoid enabling macros from email attachments. If a user opens the attachment and enables macros, embedded code will execute the malware on the machine. For enterprises or organizations, it may be best to block email messages with attachments from suspicious sources. For information on safely handling email attachments, see Recognizing and Avoiding Email Scams. Follow safe practices when browsing the Web. See Good Security Habits and Safeguarding Your Data for additional details.
- Do not follow unsolicited Web links in emails. Refer to the US-CERT Security Tip on Avoiding Social Engineering and Phishing Attacks or the Security Publication on Ransomware for more information.

Individuals or organizations are discouraged from paying the ransom, as this does not guarantee files will be released. Report instances of fraud to the FBI at the Internet Crime Complaint Center.

References

Kaspersky Lab, Kaspersky Lab detects mobile Trojan Svpeng: Financial malware with ransomware capabilities now targeting U.S.

Sophos / Naked Security, What's next for ransomware? CryptoWall picks up where CryptoLocker left off

Symantec, CryptoDefence, the CryptoLocker Imitator, Makes Over $34,000 in One Month

Symantec, Cryptolocker: A Thriving Menace

Symantec, Cryptolocker Q&A: Menace of the Year

Symantec, International Takedown Wounds Gameover Zeus Cybercrime Network

Sophos / Naked Security, "Locky" ransomware – what you need to know

McAfee Labs Threat Advisory: Ransomware-Locky. March 9, 2016

SamSam: The Doctor Will See You, After He Pays The Ransom

Revisions

March 31, 2016: Initial publication|May 6, 2016: Clarified guidance on offline backups|July 11, 2016: Added link to governmental interagency guidance on ransomware

---