Systems Affected

Microsoft Windows

Overview

Ransomware is a type of malicious software (malware) that infects a computer and restricts access to it until a ransom is paid to unlock it. This Alert is the result of Canadian Cyber Incident Response Centre (CCIRC) analysis in coordination with the United States Department of Homeland Security (DHS) to provide further information about crypto ransomware, specifically to:

- Present its main characteristics, explain the prevalence of ransomware, and the proliferation of crypto ransomware variants; and
- Provide prevention and mitigation information.

Description

WHAT IS RANSOMWARE?

Ransomware is a type of malware that infects a computer and restricts a user's access to the infected computer. This type of malware, which has now been observed for several years, attempts to extort money from victims by displaying an on-screen alert. These alerts often state that their computer has been locked or that all of their files have been encrypted, and demand that a ransom is paid to restore access. This ransom is typically in the range of $100–$300 dollars, and is sometimes demanded in virtual currency, such as Bitcoin.

Ransomware is typically spread through phishing emails that contain malicious attachments and drive-by downloading. Drive-by downloading occurs when a user unknowingly visits an infected website and malware is downloaded and installed without their knowledge. Crypto ransomware, a variant that encrypts files, is typically spread through similar methods, and has been spread through Web-based instant messaging applications.

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 inevitably become infected with additional malware, including 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 user's and organization's files, and render them useless until criminals receive a ransom.

Additional variants observed in 2014 included CryptoDefense and Cryptowall, which are also considered destructive. Reports indicate that CryptoDefense and Cryptowall share the same code, and that only the name of malware itself is different. Similar to CryptoLocker, these variants also encrypt files on the local computer, shared network files, and removable media.

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 doesn't only target home users; businesses can also become infected with ransomware, which can have 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.

CCIRC recommend users and administrators take the following preventive measures to protect their computer networks from ransomware infection:

- Perform regular backups of all critical information to limit the impact of data or system loss and to help expedite the recovery process. Ideally, this data should be kept on a separate device, and backups should be stored offline.
- Maintain up-to-date anti-virus software.
- Keep your operating system and software up-to-date with the latest patches.
- Do not follow unsolicited web links in email. Refer to the Security Tip Avoiding Social Engineering and Phishing Attacks for more information on social engineering attacks.
- Use caution when opening email attachments. 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.

Individuals or organizations are not encouraged to pay the ransom, as this does not guarantee files will be released. Report instances of fraud to the FBI at theInternet Crime Complaint Center or contact the CCIRC(link sends e-mail) .

References

- Kaspersky Lab, Kaspersky Lab detects mobile Trojan Svpeng: Financial malware with ransomware capabilities now targeting U.S.(link is external)
- Sophos / Naked Security, What's next for ransomware? CryptoWall picks up where CryptoLocker left off(link is external)
- Symantec, CryptoDefence, the CryptoLocker Imitator, Makes Over $34,000 in One Month(link is external)
- Symantec, Cryptolocker: A Thriving Menace(link is external)
- Symantec, Cryptolocker Q&A: Menace of the Year(link is external)
- Symantec, International Takedown Wounds Gameover Zeus Cybercrime Network(link is external)

Revisions

- October 22, 2014: Initial Release
- October 24, 2014: Minor edit to the reference section