United States Coast Guard

Maritime Cyber Bulletin

Bulletin 001-16 **December 22, 2015**

RANSOMWARE

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 Bulletin is the result of recent ransomware activity in the maritime domain and is designed to provide further information about the malware and to:

- Provide an overview of ransomware characteristics, discuss the prevalence of this malware, and the proliferation of 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 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 be paid to restore access. This ransom typically ranges from $100 - $10,000 dollars, and is sometimes demanded in virtual currency, such as Bitcoin.

SCREENSHOT OF TYPICAL RANSOMWARE SPLASH SCREEN

Ransomware is typically spread through phishing emails that contain malicious attachments or links and by drive-by downloading. Drive-by downloading occurs when a user unknowingly visits an infected website and malware is downloaded and installed unbeknownst to the user. Crypto ransomware, a variant that encrypts files, is typically spread through similar methods, and has also 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 the $100 fine."
- "All files on your computer have been encrypted. You must pay this ransom within 96 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 that malicious actors profited $33,600 per day, or $394,400 per month from a single C2 server. These rough estimates illustrate how profitable ransomware can be for malicious cyber actors.

This financial success has likely led to the proliferation of ransomware variants. In 2013, more destructive and lucrative ransomware variants were introduced including Xorist, CryptoBit, 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 a user's and organization's files, and render them useless until the criminals receive the 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 the malware itself is different. Similar to CryptoLocker, these variants also encrypt files on the local computer, shared network files, and removable media.

The Federal Bureau of Investigation (FBI) Internet Crime Complaint Center (IC3) reported that between April 2014 and June 2015, the IC3 received 992 CryptoWall-related complaints, with victims reporting losses totaling over $18 million.

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.

Impact

Ransomware does not only target home users; businesses can also become infected with ransomware, which can have significant negative consequences including:

- Temporary or permanent loss of sensitive or proprietary information;
- Disruption to operations;
- Financial losses incurred to restore systems and files;
- 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.

The Department of Homeland Security's United States Computer Emergency Readiness Team (US-CERT), FBI, and CGCYBER recommend users and administrators take the following preventative 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.
- Be skeptical. Do not click on any emails or attachments you do not recognize, and avoid suspicious websites altogether.
- Enable popup blockers. Most internet browsers provide popup blockers. Popups are regularly used by criminals to spread malicious software. To avoid accidental clicks on or within popups, it is best to prevent them from appearing in the first place.
- If you receive a ransomware popup or message on your device alerting you to an infection, immediately disconnect from the internet to avoid any additional infections or data losses.
- Follow safe practices when browsing the web.

It is recommended that individuals and organizations DO NOT pay the ransom, as this does not guarantee files will be released. Report instances of fraud to the Federal Bureau of Investigation (FBI) via the Internet Crime Complaint Center (IC3).

Individuals or organizations who are the victim of ransomware are encouraged to work with their local IT support staff to remediate the issue and, if necessary, obtain the services of a reputable data recovery specialist to assist.

Questions

For maritime cyber safety and security questions or questions related to this report, contact the U.S. Coast Guard Liaison Officer to the Department of Homeland Security National Cybersecurity and Communications Integration Center (NCCIC) at:

Email: CGNCCICLNO@hq.dhs.gov

Phone: (703) 235-8850

Feedback

Your feedback is important to us. Please e-mail any comments and/or feedback on this product to CGNCCICLNO@hq.dhs.gov.