United States Coast Guard

Maritime Cyber Bulletin

Bulletin 005-16 March 24, 2016

***DISCLAIMER**: This report is provided "as is" for informational purposes only. The U.S. Government (USG) does not provide any warranties of any kind regarding any information contained within. USG does not endorse any commercial provider or service referenced in this advisory or otherwise. This document was prepared by U.S. Coast Guard Cyber Command (CGCYBER) to facilitate a greater understanding of the nature and scope of threats and hazards impacting the Marine Transportation System (MTS). These materials, including copyrighted materials, are intended for "fair use" as permitted under Title, 17, Section 107 of the United States Code ("The Copyright Law"). Use of copyrighted material for unauthorized purposes requires permission from the copyright owner.*

SPIKE IN RANSOMWARE INFECTIONS IMPACTING MULTIPLE SECTORS

Overview

The U.S. Coast Guard and our interagency partners have observed a recent spike in ransomware infections impacting multiple organizations throughout; maritime, health care, law enforcement, and the emergency services sectors.

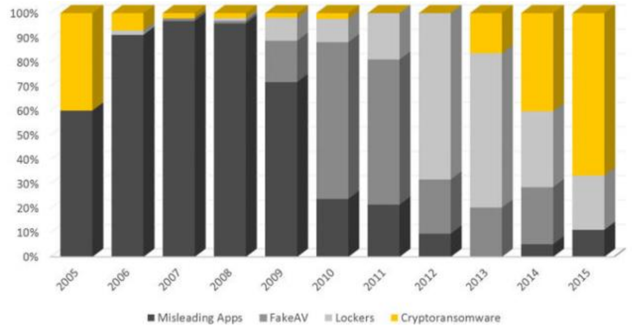
On December 22, 2015, the Coast Guard released Maritime Cyber Bulletin 001-16 which provided an in-depth overview of ransomware, its variants, best practices and remediation actions to assist victims of a ransomware infection.

This bulletin provides updates on recently observed ransomware variants, their prevalence and proliferation, and re-emphasizes best practices and mitigation strategies victims can take in the event of a ransomware infection.

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.

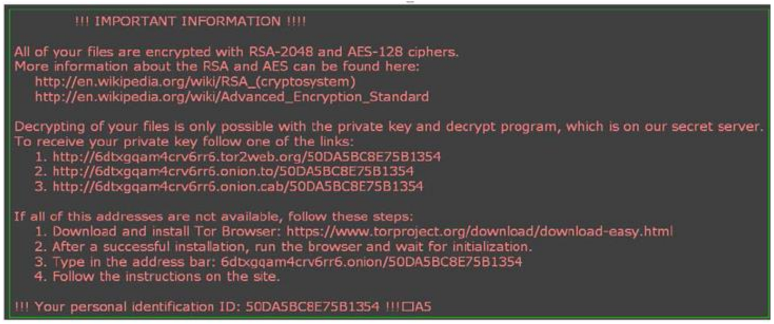


RANSOMWARE STATISTICS 2005-2015

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.

Recently Observed Ransomware

LOCKY: Locky is a ransomware that upon execution encrypts certain file types present in the user's system and is capable of spreading via network shares. The compromised user is asked to pay the attacker to get the files decrypted – typically 1 Bitcoin ($415 USD). Researchers indicate that they have observed over 400,000 cases of Locky ransomware proliferating through multiple sectors. The malware is typically propagated via emails which contain an attachment in the form of a malicious Microsoft Office document file which contain a macro to download Locky files. The malicious file is typically a Word document (.doc file and .docx file) or an Excel workbook (.xls file and .xlsx file). Macros can run in an Office application only if Macro Settings are set to "Enable All Macros" or if the user manually enables a macro.



```
        !!! IMPORTANT INFORMATION !!!!

All of your files are encrypted with RSA-2048 and AES-128 ciphers.
More information about the RSA and AES can be found here:
   http://en.wikipedia.org/wiki/RSA_(cryptosystem)
   http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server.
To receive your private key follow one of the links:
   1. http://6dtxgqam4crv6rr6.tor2web.org/50DA5BC8E75B1354
   2. http://6dtxgqam4crv6rr6.onion.to/50DA5BC8E75B1354
   3. http://6dtxgqam4crv6rr6.onion.cab/50DA5BC8E75B1354

If all of this addresses are not available, follow these steps:
   1. Download and install Tor Browser: https://www.torproject.org/download/download-easy.html
   2. After a successful installation, run the browser and wait for initialization.
   3. Type in the address bar: 6dtxgqam4crv6rr6.onion/50DA5BC8E75B1354
   4. Follow the instructions on the site.

!!! Your personal identification ID: 50DA5BC8E75B1354 !!!□A5
```

SCREENSHOT OF LOCKY INFECTION

Below are examples of email subjects used in the distribution of Locky ransomware:

- ATTN: Invoice J-12345678
- Per E-Mail senden: Rechnung-54-110090.xls

Below are examples of attachments used in the distribution of Locky ransomware:

- Invoice_j-12345678.doc
- Rechnung-54-110090.xls

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.