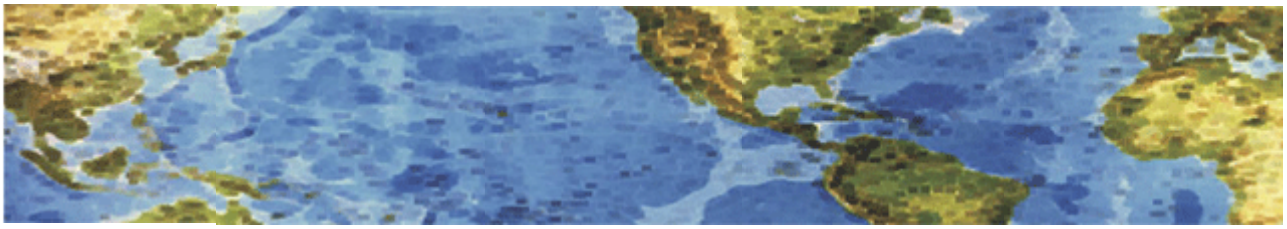
HALL ASSOCIATES



Risk-Based Decision Making Commentary
30 July 2013 Newsletter

US-CERT

Recent Reports of DHS-Themed Ransomware

This is a change in the type of Ransomware previously discussed. See page 2 for the original discussion.
US-CERT has received reports of increased activity concerning an apparently DHS-themed ransomware malware infection occurring in the wild. Users who are being targeted by the ransomware receive a message claiming that use of their computer has been suspended and that the user must pay a fine to unblock it. One iteration of this malware also takes a webcam (if available) photo or video of a recipient and posts it in a pop-up to add to the appearance of legitimacy. The ransomware falsely claims to be from the U.S. Department of Homeland Security and the National Cyber Security Division.
US-CERT and DHS encourage users and administrators not to pay the perpetrators and to report the incident to the FBI at the Internet Crime Complaint Center (http://www.ic3.gov/default.aspx).

Use caution when encountering these types of email messages and take the following preventive measures to protect yourself from phishing scams and malware campaigns that attempt to frighten and deceive a recipient for the purpose of illegal gain.

- Do not click on or submit any information to webpages.
- Do not follow unsolicited web links in email messages.
- Use caution when opening email attachments. Refer to the Security Tip Using Caution with Email Attachments (http://www.us-cert.gov/ncas/tips/st04-010) for more information on safely handling email attachments.
- Maintain up-to-date antivirus software.
- Users who are infected should change all passwords AFTER removing the malware from their system.
- Refer to the Recognizing and Avoiding Email Scams document (http://www.us-cert.gov/sites/default/files/publications/emailscams_0905.pdf) for more information ..
- Refer to the Security Tip Avoiding Social Engineering and Phishing Attacks (http://www.us-cert.gov/ncas/tips/st04-014) for more information on social engineering attacks.
- Users who are infected with the malware should consult with a reputable security expert to assist in removing the malware, or perform a clean reinstallation of their OS after formatting their computer's hard drive.

https://www.us-cert.gov/ncas/current-activity/2013/07/30/Recent-Reports-DHS-Themed-Ransomware-UPDATE

HALL ASSOCIATES

A new Citadel malware platform used to deliver ransomware is named Reveton. The ransomware lures the victim to a drive-by download website, at which time the ransomware is installed on the user's computer. Once installed, the computer freezes and a screen is displayed warning the user they have violated United States federal law. The message further declares the user's IP address has been identified by the Federal Bureau of Investigation as visiting websites that feature child pornography and other illegal content.

To unlock the computer, the user is instructed to pay a fine to the U.S. Department of Justice using a Prepaid money card service. The geographic location of the user's IP address determines what payment services are offered. In addition to the ransomware, the Citadel malware continues to operate in the background even tho your screen does not show it and can be used to commit online banking and credit card fraud.

This is an attempt to extort money with the additional possibility of the victim's computer being used to participate in online bank fraud. If you have received this or something similar, do not follow payment instructions. Turn off your computer and unhook from the internet immediately. Seek out a local computer expert to assist with removing the malware. You can file a complaint at **www.IC3.gov**.

Malware, scams, frauds and other cybercrimes continue to evolve and shift. Knowledge of these scams and frauds and of the fact that government organizations and legitimate companies will NEVER send out warnings like this is the main way to protect yourself.