Computer Crime Investigative Unit
U.S. Army Criminal Investigation Command

# Cyber Crime Alert Notice

**Contact Information:**
**Cyber Criminal Intelligence Program**
**27130 Telegraph Road**
**Quantico, Virginia 22134**

**Phone: 571.305.4482 [DSN 240]**
**Fax: 571.305.4189 [DSN 240]**

**E-mail**

**CCIU Web Page**

CID Cyber Lookout
On Point for the Army

**DISTRIBUTION:**
**This document is authorized for wide release with no restrictions.**

"DO WHAT HAS TO BE DONE"

**2CAN 0002-15-CID361-9H** **29 January 2015**

## Held for Ransom - Part II

### Overview:

The cybersecurity community has noted a recent uptick in ransomware incidents. As previously reported, ransomware is a type of malware that infects a computer and restricts access to it until a ransom is paid to unlock it. Newer versions of ransomware, such as CryptoWall and CryptoLocker, can encrypt the computer's hard drive and any external or shared drives connected to it. Victims of ransomware are given a set amount of time, often by way of a countdown clock, to pay the requested ransom or the ransom increases. Earlier ransomware scams required victims to pay using pre-paid cards; however, victims are now being asked to pay with Bitcoins, a form of digital currency.

CID elements are encouraged to brief supported installations and units on the contents of this 2CAN.

### Background:

Ransomware typically spreads through legitimate looking emails that contain a malicious attachment. Victims can also become compromised by visiting an infected website and downloading malware without the victim's knowledge. Victims are often lured to an infected website by a deceptive email, pop-up window, or through a compromised advertisement on a widely-viewed website.

If your system becomes infected, **do not pay the ransom**. Paying the ransom does not guarantee the locked computer or encrypted data will be released or the malware removed. Invisible to the user, it is possible the ransomware could continue operate in the background and capture personal information such as usernames, passwords, banking information, or other sensitive data.

The average user will not be able to easily remove the ransomware and should seek assistance from a computer expert or reputable data recovery specialist. Ransomware does not discriminate and has the potential to impact home, work, private and public computers, as well as mobile devices.

# Cyber Crime Alert Notice

## Recommended Protective Measures:

- Do not open attachments or click on links in unsolicited emails. Simply opening a malicious email message can cause an infection.
- Maintain up-to-date anti-virus software on your computer. The Defense Information Systems Agency offers free antivirus software for DoD personnel to use on home computers: http://www.disa.mil/cybersecurity/network-defense/antivirus/home-use
- Perform regular backups of critical information to limit data or system loss and help expedite recovery processes. Store data backups in a safe location offline, preferably off-site, and encrypted if the critical information contains Personally Identifiable Information.
- Keep operating system and software applications up-to-date with the latest patches.
- Enable automatic software updates.
- Download software from trusted sites only.
- Use a pop-up blocker and follow safe computing practices.
- Use the same precautions on your mobile device as you would on your computer when using the Internet.

For any incident involving a U.S. Army computer, immediately notify your information assurance and security officers. For any incident involving a home computer, consider seeking assistance from a reputable computer expert and file a complaint with the Internet Crime Complaint Center.

## Previous CCIU Advisories related to Ransomware:

Held for Ransom, 2CAN 0016-12-CID361-9H , 4 September 2012
Apple Mobile Device Ransom Scam, CPF 0016-14-CID361-9H, 30 June 2014

For more information about computer security and other computer related scams, we encourage readers to visit the CCIU website to review additional cyber crime alert notices and crime prevention flyers.

## Additional Information:

Ransomware on the Rise, Federal Bureau of Investigation
Crypto Ransomware, United States Computer Emergency Readiness Team
CryptoLocker Ransomware Infections, United States Computer Emergency Readiness Team



***CCIU uses the Interactive Customer Evaluation (ICE) system. Please click on the ICE logo and take a moment to provide us with feedback.***