Public Service Announcement
FEDERAL BUREAU OF INVESTIGATION

June 23, 2015

Alert Number
I-062315-PSA

CRIMINALS CONTINUE TO DEFRAUD AND EXTORT FUNDS FROM VICTIMS USING CRYPTOWALL RANSOMWARE SCHEMES

Data from the FBI's Internet Crime Complaint Center (IC3) shows ransomware continues to spread and is infecting devices around the globe. Recent IC3 reporting identifies CryptoWall as the most current and significant ransomware threat targeting U.S. individuals and businesses.[1] CryptoWall and its variants have been used actively to target U.S. victims since April 2014. The financial impact to victims goes beyond the ransom fee itself, which is typically between $200 and $10,000. Many victims incur additional costs associated with network mitigation, network countermeasures, loss of productivity, legal fees, IT services, and/or the purchase of credit monitoring services for employees or customers. Between April 2014 and June 2015, the IC3 received 992 CryptoWall-related complaints, with victims reporting losses totaling over $18 million.

These financial fraud schemes target both individuals and businesses, are usually very successful, and have a significant impact on victims. The problem begins when the victim clicks on an infected advertisement, email, or attachment, or visits an infected website. Once the victim's device is infected with the ransomware variant, the victim's files become encrypted. In most cases, once the victim pays a ransom fee, he or she regains access to the files that were encrypted. Most criminals involved in ransomware schemes demand payment in Bitcoin. Criminals prefer Bitcoin because it's easy to use, fast, publicly available, decentralized, and provides a sense of heightened security/anonymity.

If you believe you have been a victim of this type of scam, you should reach out to your local FBI field office. You may also file a complaint with the IC3 at www.IC3.gov. Please provide any relevant information in your complaint.

Tips to protect yourself:

- *Always use antivirus software and a firewall.* It's important to obtain and use antivirus software and firewalls from reputable companies. It's also important to continually maintain both of these through automatic updates.
- *Enable popup blockers.* Popups are regularly used by criminals to spread malicious software. To avoid accidental clicks on or within popups, it's best to prevent them from appearing in the first place.
- *Always back up the content on your computer.* If you back up, verify, and maintain offline copies of your personal and application data, ransomware scams will have limited impact on you. If you are targeted, instead of worrying about paying a ransom to get your data back, you can simply have your system wiped clean and then reload your files.
- *Be skeptical.* Don't click on any emails or attachments you don't recognize, and avoid suspicious websites altogether.

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. Alert your local law enforcement personnel and file a complaint at www.IC3.gov.

	[1]Ransomware is a type of malware (or malicious software) that blocks access to a computer system or files until a monetary amount is paid.