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. 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.

Tips to protect yourself:

Antivirus- Verify that the antivirus on your computers (mobile and desktop) is active and up to date. The City of Albuquerque provides antivirus for each City owned machine. If you are uncertain of the status of antivirus on your computers, contact the DTI Service Desk at 768-2930.

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's best to prevent them from appearing in the first place.

Always back up the content on your computer. The City utilizes network directories to save staff documents. These directories are backed up on a regular basis and can be restored in a quick fashion in the event files are lost or corrupted. DTI can not restore files if they have been saved on the local computer and the computer has been corrupted with ransomware.

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 and alert the DTI Service Desk at 768-2930 immediately.

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