

Ransomware continues to be a threat.

Don Cathey
Kansas Highway Patrol
KCJIS information Security Officer

This is a reprint of a Security Alert Received June 23, 2015.
View this article online to use the highlighted links.



IC3 Issues Alert on CryptoWall Ransomware

Original release date: June 23, 2015

The Internet Crime Complaint Center (IC3) has issued an alert warning that U.S. individuals and businesses are still at risk of CryptoWall ransomware fraud.

Scam operators use ransomware—a type of malicious software—to infect a device and restrict access until a ransom fee is paid. Individuals and organizations are discouraged from paying the ransom, as this does not guarantee files will be released.

US-CERT encourages users and administrators to review the [IC3 Alert](#) for details and refer to the US-CERT Alert [TA-295A](#) for information on crypto ransomware.

This product is provided subject to this [Notification](#) and this [Privacy & Use](#) policy.

As the link to US-CERT Alert TA-295A above states, this is now a known threat (CryptoLocker, an earlier variant of ransomware, was reported to KCJIS via a broadcast message in November 2013). Yet people and organizations continue to fall prey to it with resulting loss of important information. The alert lists the basic preventative measures *everyone should already* be taking on *any* device with access to the internet or email - particularly if it contains data or can access your criminal justice network and systems that contain data that is important to you or your agency.

Agencies should review the following policy areas in all 3 parts of the KCJIS Policy and Procedures manual when developing data protection and recovery plans that include off-site storage:

- 5.1.1.5 Private Contractor User Agreements and CJIS Security Addendum
- 5.3 Incident Response
- 5.8 Media Protection
- 5.10.1.2 Encryption
- 5.10.1.5 Cloud Computing

Also review policy area 5.2 for Security Awareness.

If you have questions or concerns, contact your Technical Security Auditor. [Their contact information can be found on the KHP CJIS Launch Pad.](#)