Data Privacy & Cybersecurity Alert

PULLMAN & COMLEY

A publication of Pullman & Comley, LLC

Attorneys:

- **Timothy G. Ronan**
  tronan@pullcom.com
  203.674.7933
- **Erick A. Russell**
  erussell@pullcom.com
  203.330.2154
- **James T. Shearin**
  jtshearin@pullcom.com
  203.330.2240

Measures to Avoid Being Held for Ransom by CryptoLocker

Posted by Erick Russell
December 12, 2013

As mentioned in last month's Cyber Law Tracker, US-CERT (the United States Computer Emergency Readiness Team) identified a malware campaign titled CryptoLocker, which is a new version of ransomware that has been spreading through phony e-mails designed to resemble legitimate businesses (https://www.us-cert.gov/ncas/alerts/TA13-309A). In addition to updating its alert to include information about the effects of CryptoLocker, US-CERT also included some recommendations about measures that users and administrators could take to protect their computer networks from this malware. We thought it might be helpful to list here some of the more common prevention and mitigation tips that you might want to consider:

Prevention

- Treat all unsolicited e-mails (especially those from unknown senders) with caution and never click on links in these e-mails.
- Carefully read the terms and conditions before agreeing to install third party programs or applications.
- Install a firewall to help protect against unauthorized users accessing your system.
- Perform regular backups of all systems to limit the impact of data and/or system loss.
- Maintain up-to-date anti-virus software and keep your operating system and software up-to-date with the latest patches.
- Participate in routine vulnerability scanning to identify where your system is vulnerable to malicious activity, and remedy those weaknesses.

PULLMAN & COMLEY

Measures to Avoid Being Held for Ransom by CryptoLocker

Mitigation

- Immediately disconnect the infected system from wireless or wired networks to prevent the malware from infecting any more files on the network.
- Block all outbound traffic to external networks.
- If possible, determine if any of the infected systems successfully connected to any site on the Internet and what information, if any, was exposed.
- If identifying personal information has been compromised, notify the relevant individuals.
- Consult with a reputable security expert to assist in removing the malware.
- Change all online account passwords and network passwords after removing the system from the network.