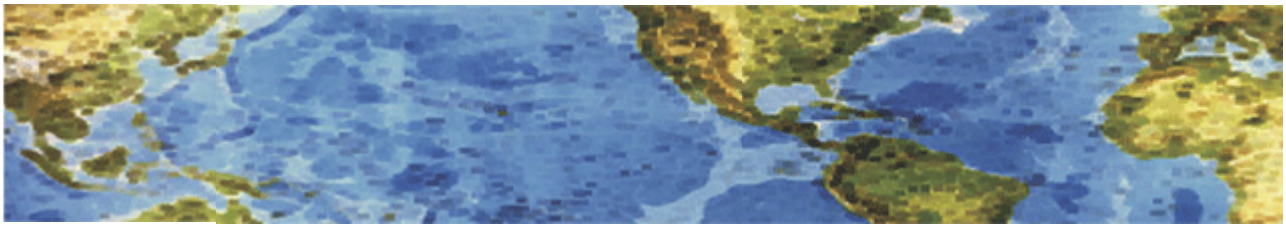
HALL ASSOCIATES



Risk-Based Decision Making Commentary
17 February 2014 Newsletter

Cryptolocker scrambles US law firm's entire cache of legal files
Trojan looked like voicemail attachment

A small US law firm has bravely admitted losing its entire cache of legal documents to the Cryptolocker Trojan despite attempting to pay the $300 (£180) ransom in a bid to have them unscrambled. According to TV reports, Goodson's law firm in the North Carolina's largest city Charlotte became the latest victim of a malware menace that was custom-written to lever ransom money from precisely this type of relatively cash-rich but time-poor firm.

The email infected a company server holding thousands of important documents after an email with a malicious attachment was mistaken for a message sent from the firm's phone answering service. That error left every single document used by firm on its main server in an encrypted state, including Word, WordPerfect and PDF files, said Goodson's owner, Paul M. Goodson.

"The virus also warned if you tried to tamper or decrypt anything, it was going to be permanently locked and you could never open it," Goodson said. After IT staff were unable to make any headway against the malware's encryption, Goodson tried to pay the ransom but discovered that the grace period - another nasty aspect of Cryptolocker - had expired. The only blessing was that the malware had scrambled files and not stolen them, Goodson added.

According to the WSOC TV channel, local police were aware of at least 30 cases where paying the ransom had resulted in an unlock key being delivered. Balancing this, we should point out that not everyone has reported having this success. The best general advice is to avoid needing an unlock key at all by backing and archiving up files on a regular basis. Cryptolocker starts encrypting files quickly so anything backed up even hours before should be recoverable if a backup is available.

Goodson's Law Firm is only the latest in a very long line of SMEs that has found itself on the receiving end of Cryptolocker's nastiness but there are some encouraging elements to the incident. The fact that an SME is willing to speak of its troubles to a local TV station suggests that the traditional taboo over owning up to malware incidents could be waning.

A less positive way of looking at it is to say that such attacks are now so normal many SMEs are being forced to view malware as just another hazard to be endured as a straightforward cost of business. Other recent Cryptolocker attacks in the US have included a town hall that lost eight years of documents and even a police department that brazenly admitted to having paid $750 for two Bitcoins to buy back sensitive files locked by the Trojan. Small-town America is only slowly waking up to this remarkably effective malware's potent threat.

http://www.computerworlduk.com/news/security/3501150/cryptolocker-scambles-us-law-firms-entire-cache-of-legal-files/

HALL ASSOCIATES

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

US CERT Alert (TA13-309A) CryptoLocker Ransomware Infections

Systems Affected: Microsoft Windows systems running Windows 8, Windows 7, Vista, and XP operating systems

Overview: US-CERT is aware of a malware campaign that surfaced in 2013 and is associated with an increasing number of ransomware infections. CryptoLocker is a new variant of ransomware that restricts access to infected computers and demands the victim provide a payment to the attackers in order to decrypt and recover their files. As of this time, the primary means of infection appears to be phishing emails containing malicious attachments.

Description: CryptoLocker appears to have been spreading through fake emails designed to mimic the look of legitimate businesses and through phony FedEx and UPS tracking notices. In addition, there have been reports that some victims saw the malware appear following after a previous infection from one of several botnets frequently leveraged in the cyber-criminal underground.

Impact: The malware has the ability to find and encrypt files located within shared network drives, USB drives, external hard drives, network file shares and even some cloud storage drives. If one computer on a network becomes infected, mapped network drives could also become infected. CryptoLocker then connects to the attackers' command and control (C2) server to deposit the asymmetric private encryption key out of the victim's reach. While victims are told they have three days to pay the attacker through a third-party payment method (MoneyPak, Bitcoin), some victims have claimed online that they paid the attackers and did not receive the promised decryption key. US-CERT and DHS encourage users and administrators experiencing a ransomware infection to report the incident to the FBI at the Internet Crime Complaint Center (IC3).

Prevention: US-CERT recommends users and administrators take the following preventative measures to protect their computer networks from a CryptoLocker infection:

- **Conduct routine backups of important files, keeping the backups stored offline**.
- Maintain up-to-date anti-virus software.
- Keep your operating system and software up-to-date with the latest patches.
- **Do not follow unsolicited web links in email.**
- Use caution when opening email attachments.
- Follow safe practices when browsing the web.

Mitigation: US-CERT suggests the following possible mitigation steps that users and administrators can implement, if you believe your computer has been infected with CryptoLocker malware:

- Immediately disconnect the infected system from wireless or wired networks. This may prevent the malware from further encrypting any more files on the network.
- Users who are infected with the malware should consult with a reputable security expert to assist in removing the malware.
- If possible, change all online account passwords and network passwords after removing the system from the network. Change all system passwords once the malware is removed from the system.

https://www.us-cert.gov/ncas/alerts/TA13-309A