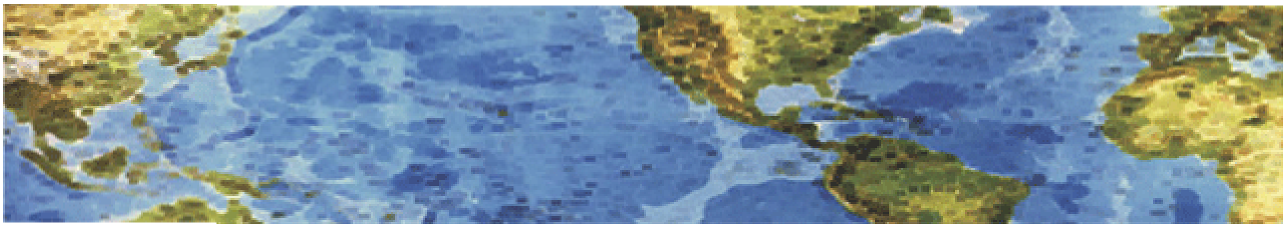
HALL ASSOCIATES

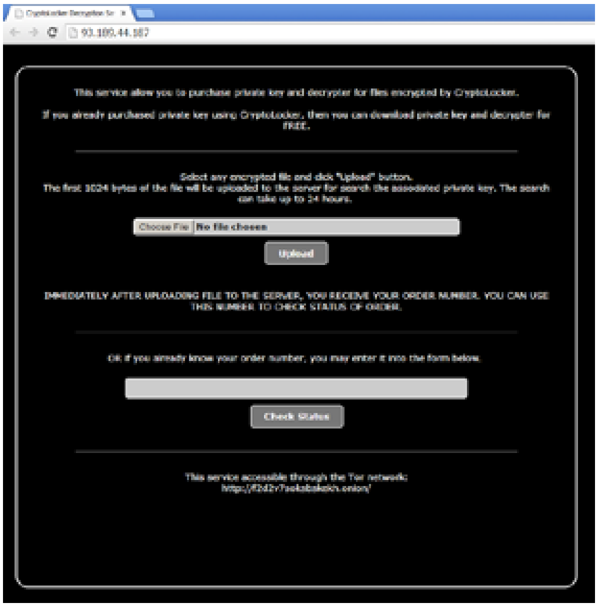


Risk-Based Decision Making Commentary
3 November 2013 Newsletter

CryptoLocker Ransomware – A Global Threat

CryptoLocker infections have been found across most regions, including North America, Europe, the Middle East, and Asia Pacific. **Almost 64% of the victims are in the US.** There are several different ways an organization or an individual can handle the CryptoLocker threat, but there is no known tool to decrypt any files encrypted by CryptoLocker. So you need to always have good backups of ALL your data and files. Some antivirus products now address some of the various CryptoLocker versions, so also be sure your antivirus and system software is up-to-date.

Yesterday there was an article in the Hacker News (see article URL below) about how the criminals behind CryptoLocker have launched a dedicated CryptoLocker Decryption Service website (using a Russian-based hosting server) that allows victims to purchase the decryption key for their encrypted files.



This service allow you to purchase private key and decrypter for files encrypted by CryptoLocker.

If you already purchased private key using CryptoLocker, then you can download private key and decrypter for FREE.

Select any encrypted file and click "Upload" button.
The first 1024 bytes of the file will be uploaded to the server for search the associated private key. The search can take up to 24 hours.

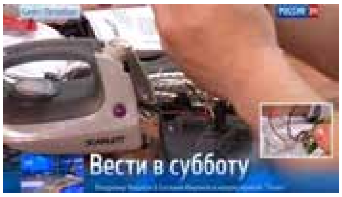
IMMEDIATELY AFTER UPLOADING FILE TO THE SERVER, YOU RECEIVE YOUR ORDER NUMBER. YOU CAN USE THIS NUMBER TO CHECK STATUS OF ORDER.

OR if you already know your order number, you may enter it into the form below.

This service accessible through the Tor network:
http://f2d2v7nokabakdch.onion/

Currently almost all antivirus companies are on Red Alert about CryptoLocker and they are releasing updates that can detect and remove the malware or the registry keys from your system. These are needed to actually pay the ransom and get the decryption key. So when this happens, the victim cannot get the decryption key **nor will the criminals get paid**. So, to get their ransom, the criminals have launched a site that looks like a customer support site for CryptoLocker victims. Using this site requires the victim to upload one of their encrypted files to generate an order number. You can then purchase your private key by paying 10 Bitcoins or $2,200. Once the payment is made, the victim can download the private key and a decrypter tool. If you have already paid the ransom, they will provide the key free of additional cost.

http://thehackernews.com/2013/11/CryptoLocker-Ransomware-Decryption-service-malware-keys.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+TheHackersNews+%28The+Hackers+News+-+Security+Blog%29&utm_content=Yahoo!+Mail&_m=3n.009a.389.wb0ao05fi9.8cr



“Intelligent Devices” Being Used to Spy

There has been lots of discussion about the rise (and increasing use) of intelligent devices – the Internet of Things. Now hidden chips have actually been found in some devices that enable them to be exploited for illegal activities. Currently only state-sponsored groups are using these, but the threat will expand in the future to criminals and thieves. It turns out that China is planting microchips in numerous manufactured electrical devices. These microchips are equipped with a little microphone and can connect to any unprotected Wi-Fi network within 200 to 600 feet. Mostly these chips are being used to spread malware and spam as well as spying on the surrounding environment but they can be turned to other things. Currently these chips have been found in electric irons, electric kettles, gaming consoles, chargers, network devices, mobile phones and car dashboard cameras.

http://thehackernews.com/2013/11/russia-finds-spying-microchips-planted_1.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+TheHackersNews+%28The+Hackers+News+-+Security+Blog%29&utm_content=Yahoo!+Mail&_m=3n.009a.389.wb0ao05fi9.8db

Insurance: Irresistible to Cyber Criminals ?

As insurers aggressively move into new online territory through agency portals, online policy applications, Web-based claims-management systems and mobile apps, they introduce new vectors of Cyberfraud risk. Cyber threats against financial institutions have increased exponentially in the last year and are expected to grow relatively unchecked. The world's biggest data breaches involve millions of records and subject consumers to identity theft risk for years to come. More and more, insurance consumers expect carriers to interact through online channels.

Insurers house a remarkable amount of personal information that identity thieves find irresistible. In October 2012, the insurance industry saw firsthand how intent hackers were on accessing this information when Nationwide suffered a major data breach. Hackers stole names, Social Security numbers, driver's license numbers and dates of birth for more than 1 million individuals – including policyholders as well as individuals seeking quotes.

Technologies and threats are rapidly evolving. In order to keep pace, response strategies also need to evolve. Many cyber threat mitigation programs are reactive – involving forensic analysis after a breach has occurred. More frequently, organizations are doing proactive penetration testing to look for vulnerabilities. But even this methodology is an increasingly outdated approach as it fails to keep pace with the scale and complexity of the cyber threats they are meant to prevent. **In the industry, there is a growing realization that cybersecurity must involve a broader, risk-based approach and move away from being seen as purely a technical problem.**

There are only two types of insurers: those that have been targeted and those that will be. As insurance companies continue to acquire vast amounts of sensitive information, they should reprioritize cybersecurity and data protection as mission-critical business objectives.

http://www.insurancetech.com/security/insurance-irresistible-to-cyber-criminal/240163420?goback=.gde_4387290_member_5803152437833392131#!