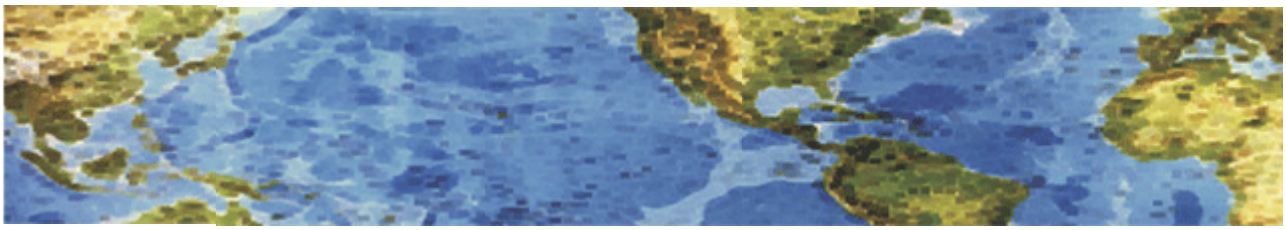
HALL ASSOCIATES



Risk-Based Decision Making Commentary
19 December 2013 Newsletter

LOCKER Malware - Yet another new variant of CryptoLocker Ransomware

Yet another new variant of CryptoLocker Ransomware, a current threat to internet users that continues to grow in popularity with cyber criminals due to its success and monetary potential, has been found in the wild. This is nothing new and to be expected. There have been many discussions on underground hacking forums about "How to create Ransomware like CryptoLocker malware" or "Malware - hacking tool-kit with ransomware features". Security intelligence provider, IntelCrawler has discovered a new ransomware variant called Locker that demands $150 (£92) to restore files that it has encrypted. Like CryptoLocker, this new ransomware is also nasty because infected users are in danger of losing their personal files forever. **Locker mainly spreads by drive-by downloads from compromised websites, disguised itself as MP3 files** and uses system software vulnerabilities to infect the end user. Once it has infected a system, the malware first checks whether the infected machine has an internet connection or not. Then it deletes any original files from the victim's computer after using AES-CTR for encrypting the files on infected devices and add ". perfect" extension to them. Locker's encryption is based on an open source tool called 'TurboPower LockBox' library. After encrypting all files, the malware places a "CONTACT.TXT" file in each directory, which provides contact details of the author to buy the decryption key and once the ransom is paid, each victim gets a key to unscramble files. The good news is that the researchers are working on the universal decryption software in order to help the victims. It appears that the hackers are simply comparing the list of infected IP addresses of users, along with their host names. **IntelCrawler had discovered 50 different builds of the malware, which are being sold in underground markets for pay-per install programs.** One build had just under 6,000 infected machines. This malware, like CryptoLocker, will encrypt all drives visible on an infected system, **so you must be sure that your backups are stored remotely or in a location that is not simply another drive partition or mapping to another location.** The malware infects users from the United States, Turkey, Russia, Germany and the Netherlands. Users should remain vigilant about their security. D**ouble check the legitimacy of links received in emails and ensure you have your antivirus/antimalware up to date to help protect against such threats. Backing up ALL data daily doesn't hurt, either. But remember, the backups should be separate from your computer or networks or they will be encrypted by the malware at the same time.**

Mohit Kumar, The Hacker News - Friday, December 13, 2013

HALL ASSOCIATES

Cyber Hygiene with Critical Security Controls

In this digital age, we rely on our computers and mobile devices for so many aspects of our lives that the **need to be proactive and vigilant to protect against cyber threats has never been greater**. However, in order to be as secure as possible, we need to use good cyber hygiene – that is, making sure we are protecting and maintaining systems and devices appropriately and using cyber security best practices. Many key best practices are outlined in the Top 20 Critical Security Controls, managed by the Council on CyberSecurity (see URL at the end of this article). These Controls assist in mitigating the most prevalent vulnerabilities that often result in many of today's cyber security intrusions and incidents. The Center for Internet Security (CIS) provides free, PDF-formatted configuration guides (Benchmarks) that can be used to implement the Controls and improve cyber security (URL also at the end of this article). **Below are several best practice strategies for strengthening defenses.**

Update Your Applications, Software and Operating Systems

Even though you may be diligent in keeping your software up-to-date, you are still at risk from malware infections. Malware can infect your computer from a variety of different vectors, including compromised websites, malicious attachments in email, and infected thumb drives. This is why strong malware defenses are crucial. Anti-virus and anti-spyware will scan your files to see if there's any malware in the files. It may even tell you if you're about to download a potentially malicious file. Update your anti-virus software regularly. Keeping applications, software, and operating systems patched will help keep you more secure by providing you with the most recent and secure version. Just remember that as new malware comes out, it requires days to months for the antivirus/antimalware companies to respond with changes.

Securely Configure Your Systems and Devices

The "out-of-the-box" configurations of many devices and system components are default settings that are often set for ease-of-use rather than security. This often results in vulnerabilities that offer easy targets for hackers to exploit, often using automated programs that scan for holes. To mitigate risk, systems and devices (especially individual computers and mobile devices) should be configured according to industry-accepted system hardening standards. Remember to encrypt your data – all your data.

Secure Your Browser and Browser Add-ons

Cyber attackers search for programming errors and other flaws in web browsers and associated plug-ins in order to exploit them. These vulnerabilities, if successfully exploited, can give cyber criminals access -- and sometimes control over -- your computer system. To minimize these risks, keep your browser(s) updated and patched, and set to auto update. In addition, keep any programs (known as plug-ins) updated and patched as well, particularly if they work with your browser (such as multi-media programs and plug-ins used to run videos, for example), block pop-up windows, as this may help prevent malicious software from being downloaded to your computer and consider disabling JavaScript, Java, and ActiveX controls when not being used. Activate these features only when necessary.

HALL ASSOCIATES

Back Up Your Data
Be sure to back up your important data so you can retrieve it if your computer fails or you get caught by malware like CryptoLocker. External hard drives and online backup services are two popular vehicles for backing up files. Remember to back up data (from your computer system and ALL mobile devices) at regular intervals (daily is recommended) and periodically review your backups to determine if all your data has been backed up accurately.

Secure Your Wireless Network
Before the days of wireless (Wi-Fi) home networks, it was rather easy to see who was linked into your home network; you could simply follow the wires. You wouldn't allow a stranger to connect to your network, so check to see who is connected to your wireless network. The first step is to lock down your wireless network with a strong password and encryption. This will prevent people who don't have the password from connecting to your network. While there are fewer wires to follow, you can still follow some digital breadcrumbs to see who is connected to your network. Connect to your router (for more information refer to the manufacturer's user guide) to see who the clients (the connected devices) are. Are there more devices connected to your network than you expect? If there are some devices you don't recognize, change your security settings and passwords. Don't forget about your printers, many of which can connect to your network and are Wi-Fi enabled.

Protect Your Administrative Accounts
Administrator or "admin" accounts give a user more control over programs and settings for a computer than a typical user account. If an intruder accesses an admin account, he could potentially take over your computer. Non-administrator accounts, or guest accounts, can limit the ability of someone gaining unauthorized access. It is important to change the default password on your admin accounts and to always log on to your computer as a non-administrator or non-admin account. Another aspect to protecting admin accounts is to **change default passwords on your devices**. Many of them are published on the Internet, so be sure to change them to something unique and strong. Default passwords are especially prevalent in routers, wireless access points and other networked devices.

Many computer defaults are set for ease of use, which is convenient not only for us, but also for cyber criminals. Cyber criminals can use weak or unnecessary services as a first step to compromising your computer. Many computers and routers already come with a firewall built in to prevent malicious access to these services. It is recommended that you set the firewall to the securest level you think is appropriate: if this is a laptop you'll use for traveling and connecting to public networks, it is recommended that you choose the strictest level of security and only allow exceptions for services you need. You can always relax the controls if necessary.

Create, Use and Regularly Change Strong Passwords And <u>Use Different Ones for Different Accounts!!!!</u>
A strong password is at least eight characters long, does not contain your user name, real name, or company name, does not contain a complete word, is significantly different from previous passwords and contains characters from each of the following four categories: Uppercase letters, Lowercase letters, Numbers and Symbols found on the keyboard (all keyboard characters not defined as letters or numerals) and spaces.

http://www.counciloncybersecurity.org/
http://benchmarks.cisecurity.org/downloads/benchmarks/
http://benchmarks.cisecurity.org/downloads/crosswalk/

Original Article from MS-ISAC , December 2013 Volume 8, Issue 12