The Growing Threat From Ran$omware

You are catching up on some Web surfing using your favorite mobile device, when all of a sudden everything freezes and you receive a message telling you...

YOU HAVE BEEN CAUGHT ACCESSING INAPPROPRIATE CONTENT AND YOUR DEVICE WILL REMAIN LOCKED UNLESS YOU PAY $$$$$

Welcome to the World of RANSOMWARE!

Ransomware was introduced almost 25 years ago. One of the first examples was called **Aids Info Disk** or **PC Cyborg Trojan**. This Trojan horse would encrypt all of the filenames on the "C" drive, making the PC unusable. Once the PC was infected, this Ransomware would demand a payment of $189 be sent to a post office box somewhere in Panama. Eventually the Aids Info Disk Trojan's author was arrested and charged with 11 counts of blackmail.

Typically, Ransomware keeps you from accessing your information by encrypting it (e.g. CryptoLocker) or by continuously displaying threatening messages on you PC until a ransom is paid.

What's Happening Now?

Antivirus software makers learned how to detect this category of malware and quickly block them for many years. However, the growing popularity of virtual currencies, such as Bitcoin, have made Ransomware a potentially lucrative opportunity for Cyber Criminals. Today, the victim is told to make a payment via Bitcoin to the hacker if they ever want to see their information again. The only sure thing is that the money will be taken.

New types of Ransomware are appearing faster than ever before and are taxing the abilities of the Antivirus Software providers to keep up with the latest exploits.

The latest threat is called **Ransom32**, ransomware-as-a-service. The potential cyber-criminal pays a fee to customize and uses this ready-made ransomware platform instead of developing his own. Ransomware-as-a-service providers charge a fee to use their product, or take a percentage of the profits. Expert skills are no longer required to hold a victims' information hostage.

It is Not Just PCs Anymore!

Ransomware branched out to beyond Windows PCs to infect Android mobile devices and even Network Attached Storage (NAS) devices. Over the past 6 month almost 300 new malware variants, impacting Android devices, have been detected.

A highly specialized Ransomware, designed to encrypt the information stored on a Synology Network Attached Storage device began to attack. This Ransomware, took advantage of a vulnerability in the device's software to take control of the stored information.

How Do You Protect Yourself from This Threat?

- Be Aware: Every employee at the organization should understand how Ransomware works and be conscious to malicious activity.
- Perform regular backups of all critical information to limit the impact of data or system loss.
  - Ideally, critical information should be kept on a separate device, and backups should be stored offline.
  - Your IT department can help you select the most effective back-up solution.
- Maintain updated anti-virus software.
- Make sure you have a strong anti-malware solution which is constantly updated with new signatures and new types of malware. It should be deployed on all workstations and laptops.
- Keep your operating system and software updated 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.

About Radware

Radware® (NASDAQ: RDWR), is a global leader of application delivery and cyber security solutions for virtual, cloud and software defined data centers. Its award-winning solutions portfolio delivers service level assurance for business-critical applications, while maximizing IT efficiency. Radware's solutions empower more than 10,000 enterprise and carrier customers worldwide to adapt to market challenges quickly, maintain business continuity and achieve maximum productivity while keeping costs down. For more information, please visit www.radware.com.

Radware encourages you to join our community and follow us on: Facebook, Google+, LinkedIn, Radware Blog, SlideShare, Twitter, YouTube, Radware Connect app for iPhone® and our security center DDoSWarriors.com that provides a comprehensive analysis on DDoS attack tools, trends and threats.