October 2014
Volume 9, Issue 10

Trick or Treat…or Should We Say Trick or Threat

ENTERPRISE INFORMATION SECURITY PROGRAM
Keeping our organization's data safe.

Enterprise Information Security Program

Tacoma

From the Desk of Paul Federighi, Chief Information Security Officer

October is not only National Cyber Security Awareness Month, it's also the time to celebrate Halloween, bringing to mind scary things that are merely figments of our imagination. In the digital world, however, there are many scary things that are *not* figments of our imagination, that we should in fact be worried about. The threats in cyber space are real. One of the most important concerns is malware, short for malicious software. The volume of malware continues to surge, with ransomware infections increasing, malware now targeting mobile devices, and new strands of malware attempting to exploit vulnerabilities in aging automated teller machines (ATMs).

Playing on the Halloween theme of scary things, below are some examples of malware you should be aware of, and some tips for minimizing your risks.

What are Some Examples of Malware?

Ransomware. Ransomware is designed to essentially hold your system hostage until you meet the hacker's demands. A popular version of ransomware currently circulating is known as CryptoWall, which infects a victim's machine and encrypts its data. The hacker alerts the victim that their files have been encrypted and directs the victim to pay a ransom by a certain date, otherwise the key necessary to decrypt the files will be destroyed.

Ghosts. No, we aren't talking about the ghosts you'll see on Halloween. In the cyber world we have Gh0st, an infamous piece of malware that is commonly used by threat actors to remotely access a target and assume complete control. Some versions of Gh0st have the ability to activate the camera and audio-recording functions of the infected machine if the machine has those features.

Zombies. Unlike the make-believe zombies you see in the movies, cyber zombies are real. In the online world, a zombie is a machine compromised with malware and controlled by a hacker. Zombies can send spam, launch denial-of-service attacks and infect other machines, becoming part of a large group of compromised computers being controlled remotely (known as botnets).

Mutations. This malware (known as polymorphic malware) morphs its code to constantly change its form. This mutating process keeps the malware from being detected by pattern-matching analysis tools.

Frankenstein. Continuing along the lines of the mutating software, the Frankenstein malware takes small pieces of software from trusted programs and stitches them together, making the resulting malware undetectable.

How Does Malware Get on Your Machine?

Tricks-n-Treats. Social engineering continues to be the path of least resistance to your data. These "tricks" often rely on establishing trust by purporting to be sourced from an individual or

company you know and trust. The cyber criminal then tries to entice you into viewing the "treat," whether it's a celebrity photo, the promise of a cash prize or some other lure. Phishing email messages have evolved from being full of easy-to-spot grammatical or spelling errors to appearing very credible, with a look and feel that closely matches a legitimate organization.

Poison. Hackers looking to target your machine know how to poison search results to get you to click on a site that hosts malware. Cyber criminals can sometimes deface legitimate websites by adding content that is designed to rank highly in search results, knowing the first returned sites are more likely to be clicked on directly.

How Can You Minimize Your Risk?

Avoid the tricks by being aware of the tactics:

- Do not respond to unsolicited emails or telephone calls from an unknown or untrusted source. Verify the identity of an individual claiming to represent an organization by contacting the organization directly.
- Be especially wary of emails that ask you to verify your information or provide sensitive information. Do not open attachments contained in a suspicious email.
- Keep the software on your computers and devices up to date through regular patching. Use automatic update settings on your security software, operating system, and web browser.
- Only install third-party applications from trusted sources.
- Discuss security awareness best practices with your family, friends, colleagues and community.

REMEMBER: While October is recognized as National Cyber Security Awareness Month, we need to be vigilant and proactive every day, not just during the month of October.

For More Information:

CIS Cryptowall Alert: http://www.cisecurity.org/cyber-alerts/2014/20141008.cfm
CIS Newsletter: Bots, Botnets and Zombies: http://msisac.cisecurity.org/newsletters/2014-06.cfm
CIS Awareness Month Toolkit: https://msisac.cisecurity.org/resources/toolkit/Oct14/index.cfm
AntiPhishing Work Group: http://www.antiphishing.org/
OnGuard Online: https://www.onguardonline.gov/
NetSmartz: http://www.netsmartz.org/Parents

Provided By:

CENTER FOR INTERNET SECURITY

STOP | THINK | CONNECT