NYS Office of Cyber Security

Monthly Security Tips NEWSLETTER

January 2013

Volume 8, Issue 1

Emerging Trends and Threats for 2013

From the Desk of Thomas D. Smith, Director

During 2012, cyber security incidents ranged from theft of public and private intellectual property to hacktivism ransomware, malware targeting mobile devices, to a surge of other malware such as Black Hole Rootkit and Zero Access Trojan.

What Emerging Trends and Threats will we see in 2013? Below are a listing of several trends and threats that are expected in the next 12 months:

Mobile Devices in the Enterprise

As the use of mobile devices grew in 2012, so too has the volume of attacks targeting them. Each new smart phone, tablet or other mobile device provides an avenue of opportunity for potential cyber attacks. Many organizations have incorporated these devices into their networks. In some cases, organizations are allowing employees to "Bring Your Own Device" (BYOD) to their place of employment. This increases the cyber security risks for an organization particularly if it does not have control over the employee's personal mobile device. Risks include access to organization's e-mail and files, as well as the ability for mobile device applications to download malware, such as keyloggers or programs that eavesdrop on phone calls and text messages.

New capabilities, such as Near Field Communication (NFC*)*, will be on the rise in 2013 and will increase the opportunities for cyber criminals to exploit weaknesses. NFC allows NFS capable smartphones, or other NFS devices, to communicate with each other by simply touching or being in close proximity to one another. This technology is being used for credit card purchases and advertisements in airports and magazines and will most likely be incorporated into other uses in 2013. Risks with using NFC include eavesdropping—through which the cyber criminal can intercept data transmission, such as credit card numbers—and transferring viruses or other malware from one NFC-enabled device to another**.**

Ransomware

Ransomware is a type of malware that is used for extortion. The attacker distributes malware that takes over a system by encrypting the contents or locking the system. The attacker then demands money from the victim in exchange for releasing the data and/or unlocking the system. Once payment is made, the attacker may or may not provide the data or access to the system. Even if access is restored, the integrity of the data is still in question. This type of malware and delivery mechanism will become more sophisticated in 2013.

Social Media

Use of social media sites has grown beyond just sharing vacation photos and messaging. These sites are increasingly being used for advertising, purchasing and gaming which can include the sharing of Personally Identifiable Information (PII). Examples of PII include, but are not limited to: full name, maiden name, mother's maiden name, birth date, social security number, driver's license number, credit card number and bank account number. For 2013, attackers will look to exploit these sites and the variety of PII being shared.

Hactivism

Attacks carried out as cyber protests for politically or socially motivated purposes, or "just because they can" have increased, and are expected to continue in 2013. Common strategies used by hactivist groups include denial of service attacks and web-based attacks, such as SQL Injections. Once a system is compromised, the attacker will harvest data, such as user credentials, to gain access to additional data, e-mails, other credentials, credit card data and other sensitive information.

Advanced Persistent Threat

Advanced Persistent Threat (APT) refers to a long-term pattern of targeted hacking attacks using subversive and stealthy means to gain continual, persistent exfiltration of data. The entry point for these types of espionage activities is often the unsuspecting end-user or weak perimeter security. APT will remain a consistent threat to networks in 2013.

Spear Phishing Attacks

Spear phishing is a deceptive communication, often in the form of e-mail, text or tweet, targeting a specific individual, seeking to obtain unauthorized access to personal or sensitive data. Spear phishing attempts are not typically initiated by "random hackers" but are more likely to be conducted by perpetrators seeking financial gain, trade secrets or sensitive information. Spear phishing is often the nexus to cyber espionage/APT and will continue to increase in 2013.

What Can You Do?

By using sound cyber security practices as listed below, users and organizations can help defend against the myriad of challenges and mitigate potential impacts of incidents:

- Enable encryption and password features on your smart phones and other mobile devices.
- Use strong passwords that combine upper and lower case letters, numbers, and special characters, and do not share them with anyone. Use a separate password for every account. In particular, do not use the same password for your work account on any other system.
- Disable wireless, Bluetooth, and NFC when not in use.
- Properly configure and patch operating systems, browsers, and other software programs. This should be done not only on workstations and servers, but mobile devices as well.
- Use and regularly update firewalls, anti-virus, and anti-spyware programs.
- Do not use your work e-mail address as a "User Name" on non-work related sites or systems.
- Be cautious regarding all communications; think before you click. Use common sense when communicating with users you DO and DO NOT know. Do not open e-mail or related attachments from un-trusted sources.
- Don't reveal too much information about yourself online. Depending on the information you post, you could become the target of identity or property theft.
- Be careful with whom you communicate or provide information on social media sites. Allow access to systems and data only to those who need it and protect those access credentials.
- If a device is used for work purposes, do not share that device with friends or family.
- Follow your organization's cyber security policies and report violations and issues immediately.

For More Information:

- NYS Office of Cyber Security's Newsletters: www.dhses.ny.gov/ocs/awareness-training-events/news/
- National Institute of Standards and Technology – Guide to Protecting the Confidentiality of Personally Identifiable Information (PII): csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf
- FCC Smartphone Security Checker - www.fcc.gov/smartphone-security
- Mobile Device and Health Information Privacy and Security - www.healthit.gov/providers-professionals/your-mobile-device-and-health-information-privacy-and-security
- Symantec: www.symantec.com/connect/blogs/top-5-security-predictions-2013-symantec-0
- Security Predictions 2013-2014 – Emerging Trends in IT and Security: www.sans.edu/research/security-laboratory/article/2140
- Georgia Tech -- Emerging Cyber Threats Report: www.gtcybersecuritysummit.com/pdf/2013ThreatsReport.pdf

The information provided in the Monthly Security Tips Newsletters is intended to increase the security awareness of an organization's end users and to help them behave in a more secure manner within their work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the organization's overall cyber security posture. This is especially critical if employees access their work network from their home computer. Organizations have permission and are encouraged to brand and redistribute this newsletter in whole for educational, non-commercial purposes.

Brought to you by:

MS-ISAC
MULTI-STATE
Information Sharing
& Analysis Center™

A DIVISION OF CENTER FOR INTERNET SECURITY