CTS Enterprise Security Services

Monthly Security Tips NEWSLETTER

January 2013

Emerging Trends and Threats for 2013

During 2012, cyber security incidents included theft of public and private intellectual property, hacktivism, ransomware, malware targeting mobile devices, and a surge of other malware, Black Hole Rootkit and Zero Access Trojan. What will we see in 2013? Below is a brief roundup, listed in no particular order, of several threats and trends we can expect during 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 targeted to them. Every new smart phone, tablet or other mobile device provides another opportunity for a potential cyber attack. Many enterprises have incorporated these devices into their networks. In some cases, organizations are allowing employees to "Bring Your Own Device" (BYOD). 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 corporate email and files, as well as the ability for the mobile device apps to download malware, such as keyloggers or programs that eavesdrop on phone calls and text messages.

New capabilities, such as NFC (Near Field Communication), will be on the rise in 2013 and will increase the opportunities for cyber criminals to exploit weaknesses. NFC allows for smartphones to communicate with each other by simply touching another smart phone, or being in close proximity to another smart phone with NFC capabilities or an NFC device. 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 will take 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 delivered, 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 personal information, such as vacation photos and messaging. These sites are being increasingly used for advertising, purchasing and gaming. For 2013, attackers will look to exploit this volume and variety of data being shared to credentials or other Personally Identifiable Information (PII), such as social security numbers.

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, emails, 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 type of espionage activities is often the unsuspecting end-user or weak perimeter security. Whether focused on exploiting vulnerable networks or unsuspecting end-users, APT will remain a consistent threat to networks in 2013.

Spear Phishing Attacks
Spear phishing is a deceptive communication, such as 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 this year.

What Can You Do?
By using sound cyber security practices, users and organizations can strengthen readiness and response to 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 email 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 email or related attachments from un-trusted sources.
- Don't reveal too much information about yourself online. Depending on the information you reveal, you could become the target of identity or property theft.
- Be careful with whom you communicate or provide information on social media sites. Those 'friends' or games might be looking to steal your information.
- Allow access to systems and data only to those who need it and protect those access credentials.
- If the 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:

- **Symantec:** http://www.symantec.com/connect/blogs/top-5-security-predictions-2013-symantec-0
- **Security Predictions 2013-2014 – Emerging Trends in IT and Security**: http://www.sans.edu/research/security-laboratory/article/2140
- **Georgia Tech -- Emerging Cyber Threats Report:** http://www.gtcybersecuritysummit.com/pdf/2013ThreatsReport.pdf
- **Blackhole Rootkit – Zero Access Trojan:** http://www.mcafee.com/us/downloads/free-tools/rootkitremover.aspx

Brought to you by:

MS-ISAC MULTI-STATE Information Sharing & Analysis Center™
A DIVISION OF CENTER FOR INTERNET SECURITY

Consolidated Technology Services
Security Operations Center

The mission of the CTS Security Operations Center is to provide centralized information sharing, monitoring, and analysis of Washington State security posture. Contact us at: soc@cts.wa.gov