Emergency Management and Response Information Sharing and Analysis Center

CIP BULLETIN 1-10 January 26, 2010

NOTE: *CIP Bulletins will be distributed as necessary to provide members of the Emergency Services Sector with timely, important, unclassified information potentially affecting the protection of their critical infrastructures. They are prepared by the Emergency Management and Response- Information Sharing and Analysis Center (EMR-ISAC) at (301) 447-1325 or by e-mail at emr-isac@dhs.gov.*

Cyber Security Trends for 2010

This New Year is an opportune time to assess the cyber security landscape of Emergency Services Sector departments and agencies, and prepare for new challenges that may lie ahead, as well as the current threats which may continue.

- **Malware, worms, and Trojan horses:** These will continue to spread by email, instant messaging, malicious websites, and infected non-malicious websites. Some websites will automatically download the malware without the user's knowledge or intervention. This is known as a "drive-by download." Other methods will require the users to click on a link or button.

- **Botnets and zombies:** These threats will continue to proliferate as the attack techniques evolve and become available to a broader audience, with less technical knowledge required to launch successful attacks. Botnets designed to steal data are improving their encryption capabilities and thus becoming more difficult to detect.

- **Scareware – fake/rogue security software:** There are millions of different versions of malware, with hundreds more being created and used every day. This type of scam can be particularly profitable for cyber criminals, as many users believe the pop-up warnings telling them their system is infected and are lured into downloading and paying for the special software to "protect" their system.

- **Attacks on client-side software:** With users keeping their operating systems patched, client-side software vulnerabilities are now an increasingly popular means of attacking systems. Client-side software includes things like Internet browsers, media players, PDF readers, etc. This software will continue to have vulnerabilities and subsequently be targeted by various malwares.

- **Ransom attacks:** These occur when a user or company is hit by malware that encrypts their hard drives or they are hit with a Distributed Denial of Service Attack (DDOS) attack. The cyber criminals then notify the user or company that if they pay a small fee, the DDOS attack will stop or the hard drive will be unencrypted. This type of attack has existed for a number of years and is now gaining in popularity.

- **Social Network Attacks:** Social network attacks will be one of the major sources of attacks in 2010 because of the volume of users and the amount of personal information that is posted. Users' inherent trust in their online friends is what makes these networks a prime target. For example, users may be prompted to follow a link on someone's page, which could bring users to a malicious website.

- **Cloud Computing:** Cloud computing is a growing trend due to its considerable cost savings opportunities for organizations. Cloud computing refers to a type of computing that relies on sharing computing resources rather than maintaining and supporting local servers. The growing use of cloud computing will make it a prime target for attack.

- **Web Applications:** There continues to be a large number of websites and online applications developed with inadequate security controls. These security gaps can lead to the compromise of the site and potentially to the site's visitors.

- **Budget cuts:** These will be a problem for security personnel and a boon to cyber criminals. With less money to update software, hire personnel, and implement security controls, enterprises will be trying to do more with less. By not having up-to-date software, appropriate security controls or enough personnel to secure and monitor the networks, organizations will be more vulnerable.

What Can I Do?

The following are helpful tips to assist in minimizing risk:

- Properly configure and patch operating systems, browsers, and other software programs.
- Use and regularly update firewalls, anti-virus, and anti-spyware programs.
- Be cautious about 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.

Additional Information:

- IBM's Top Security Trends for 2010
- Symantec's Top Security Trends for 2010
- SANS Top Cyber Security Risks
- Bankinfosecurity.com article
- PC World
- Panda Labs 2009 Annual Malware Report

The information provided in this newsletter 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. Organizations have permission--and in fact are encouraged--to brand and redistribute this newsletter in whole for educational, non-commercial purposes.

Original Prepared by:

MS-ISAC

www.msisac.org