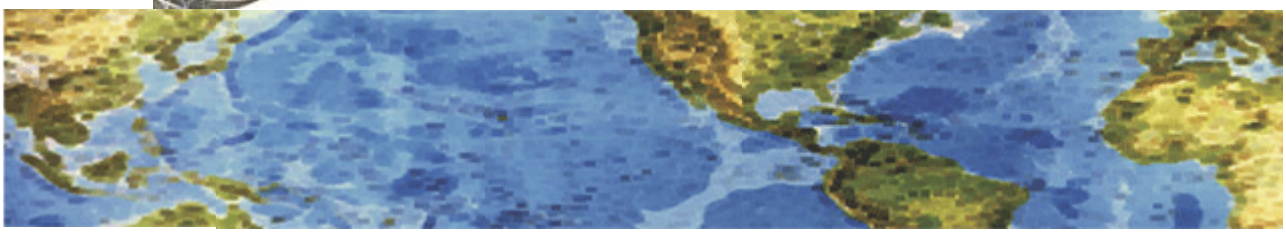
HALL ASSOCIATES



Risk-Based Decision Making Commentary
12 March 2014 Newsletter

Who's Spying on You?

You may be aware of the threats of malware to your business but are you aware of the ever-changing ground rules? **Cybercriminals now are launching attacks against businesses by copying sophisticated malware and techniques used to target governments and high-profile organizations and using automated applications.** Don't get caught in the crossfire. In future Newsletters we will discuss the techniques cybercriminals are now using; common exploited vulnerabilities; collateral damage from cyberespionage; and protecting your business from these types of threats.

Facebook 'Watch naked video of friends' malware scam infects 2 million people

There have been a lot of Facebook malware and virus infections spreading through the friends list, and this time a new clickjacking scam campaign is going viral on Facebook. Hackers spam Facebook timeline with a friend's picture and "See (Friend's) naked video," or "(Friend's Name) Private Video. "The Picture appears to be uploaded by a friend and you (or your employees) might want to see exactly what this is, **But beware!** If you get curious and click, you will be redirected to a malicious website that reports that your Flash Player is not working properly and **needs to be re-installed. Click this link!**

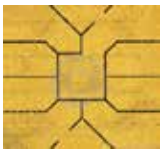
When the link on the website is clicked, users are sent to a very realistic-looking mockup of a YouTube page, where the hackers will try to immediately install a malware Trojan. That Trojan installs a malicious browser extension to spread the scam and steal users' photos. This particular Trojan doesn't yet steal other personal information, but it is constantly evolving.

So, Don't click on the link! According to several reports, over 2 million Facebook users are already infected by this malware campaign and unknowingly flood all of their friends Facebook timelines with this clickjacking scam. Clicking on the message will also automatically publish the same malware link on your Facebook wall, which then allows your friends to click on it.

This type of malware takes advantage of the fact that you trust your friends. So, keep an eye on the links and messages from your friends and customers, and if in doubt, ask them they actually sent you something or not. These recent malware attacks are just a few examples of the dangers of using social networks. **Stay safe by keeping your browser up-to-date and installing operating system and application updates when they are released and don't click on unknown links**.

http://thehackernews.com/2014/03/facebook-watch-naked-video-of-friends.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+TheHackersNews+%28The+Hackers+News+-+Security+Blog%29&_m=3n.009a.513.wb0ao05fi9.awd

HALL ASSOCIATES



Credit Card Chip Technology

Ending weeks of relative silence by the two major payment card brands in the wake of payments breaches at Target Corp., Neiman Marcus and others retailers, MasterCard and Visa have announced the formation of a cross-industry group to work on improving U.S. payment security. The collaborative effort aims to advance the migration to chip cards as well as point-to-point encryption. In addition to the card brands, the coalition will include banks of all sizes, credit unions, acquirers, retailers, point-of-sale device manufacturers and industry trade groups, the card brands say in announcing the effort. The initial focus of the group will be **on the adoption of payments cards using chip technology** based on the EMV standard that's widely used in other nations. The cards offer greater security than magnetic-stripe cards that are now commonly used in the U.S. **However, most Point of Sale systems will have to be upgraded to use these new cards.**

Other areas of focus for the new group will include:

- Promoting additional security solutions, including tokenization and point-to-point encryption. "While EMV addresses the physical point of sale, the need to protect mobile and online transactions is critical," the card brands say in their announcement. "In tokenization, **the traditional account number will be replaced with a unique digital payment code,** providing an additional layer of security."
- Developing an actionable roadmap for security across all segments of the payments industry.

At two Congressional hearings this week, cybersecurity experts stressed that adoption of EMV chip cards is just one of many steps that need to be taken to secure the U.S. payments system. **They also called for more education of retailers about card data security and stronger enforcement of Payment Card Industry data security standards.**

http://www.govinfosecurity.com/card-brands-launch-security-initiative-a-6610/op-1

Cumulative Security Update for Internet Explorer CIS ADVISORY NUMBER: 2014-021

Multiple vulnerabilities have been discovered in Microsoft's web browser, Internet Explorer, which could allow an attacker to take complete control of an affected system. Successful exploitation of these vulnerabilities could result in an attacker gaining elevated privileges on the system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED: Internet Explorer 6, Internet Explorer 7, Internet Explorer 8, Internet Explorer 9, Internet Explorer 10, Internet Explorer 11

RISK:

Government: Large and medium government entities: High; Small government entities: High

Businesses: Large and medium business entities: High; Small business entities: High

Home users: High

We recommend the following actions be taken: Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing; run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack; **remind users not to click links from unknown sources, or to click links without verifying the intended destination**.