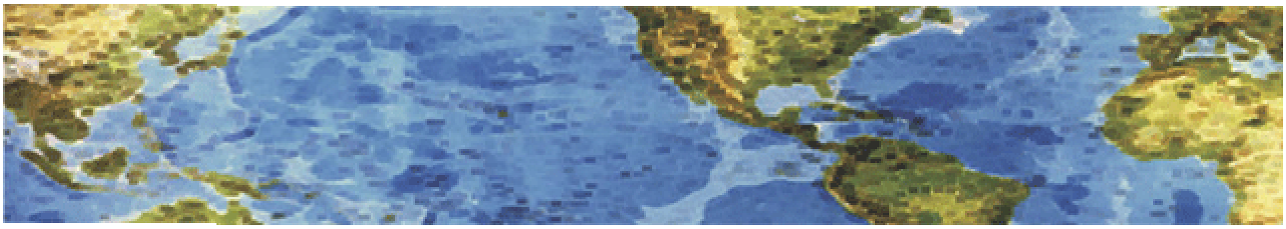
HALL ASSOCIATES



Risk-Based Decision Making Commentary
12 July 2014 Newsletter

Oracle Not Updating Java for Windows XP
Oracle's next quarterly patch update will be released on Tuesday, July 15, but the fixes will not include updates for Java running on Windows XP. Oracle stopped supporting Java for XP on April 8, the date Microsoft announced months earlier as the operating system's cut-off date. The current version of Java, Java 8, will not install on XP. Oracle says people running XP can continue using Java 7 at their own risk. This is one of the first of many software vendors who are not going to provide updates for the Windows XP platform. **If you have not changed to a supported operating system yet you need to review your vulnerability management program for how you will manage these vulnerabilities until you are migrated from Windows XP.**

The Internet of Things: Smart Light bulb Exposes Wi-Fi Password
In a proof-of-concept attack, Internet-connected LED light bulbs were used to gain access to the Wi-Fi network that controls them. LIFX smart light bulbs can be controlled with iOS and Android devices. LIFX was made aware of the problem and has issued a firmware update to address it. The attackers were able to trick the devices into revealing the network password; they had to be within 30 meters of the devices they were targeting. At the SANS 2013 "Securing the Internet of Things Summit" Nitesh Dhanjani demonstrated remote hacking of smart light bulbs and Wi-Fi enabled baby monitors. There has been more talk than action around IoT security since then. Most people aren’t really impacted by these types of vulnerabilities in IoT home user applications, but you should realize that **the lack of security at the integration-level in any of these devices becomes one more weak link in your smart home or building.**

DailyMotion users redirected to exploits in pay-per-click ruse
Popular video sharing service DailyMotion was compromised on June 28, and briefly redirected users to the Sweet Orange Exploit kit. Attackers “injected an iframe” onto the site, which rerouted users to a different website hosting the exploit kit. The exploit kit then attempted to leverage several vulnerabilities on a user's computer associated with Internet Explorer (CVE-2013-2551), Adobe Flash (CVE-201302551), and Java (CVE-2013-2460). Although these bugs have been patched, if a user does not have the latest version of the programs and Sweet Orange successfully exploits any of the vulnerabilities, the compromised machine will download pay-per-click malware and generate revenue for the miscreants by artificially producing traffic for their web advertisements. The site, which ranks 90 in Alexa's top 100, is no longer compromised.
This is just another in the numerous ways a web site can be compromised and malware injected into your computer/network. In this case no information was stolen, but the exploit kit could be used for that. And so it goes on and on.

Crooks Seek Revival of ‘Gameover Zeus’ Botnet

Cybercrooks today began taking steps to resurrect the Gameover ZeuS botnet, a complex crime machine that has been blamed for the theft of more than $100 million from banks, businesses and consumers worldwide. The revival attempt comes roughly five weeks after the FBI joined several nations, researchers and security firms in a global and thus far successful effort to eradicate it. Researchers at Malcovery began noticing spam being blasted out with phishing lures that included zip files booby-trapped with malware. Looking closer, the company found that the malware shares roughly 90 percent of its code base with Gameover Zeus. This new Gameover variant relies on an approach known as fast-flux hosting. Fast-flux is a kind of round-robin technique that lets botnets hide phishing and malware delivery sites behind an ever-changing network of compromised systems acting as proxies, in a bid to make the botnet more resilient to takedowns.

Gameover is based on code from the ZeuS Trojan, an infamous family of malware that has been used in countless online banking heists. Unlike ZeuS - **which was sold as a botnet creation kit to anyone who had a few thousand dollars in virtual currency to spend** - Gameover ZeuS has since October 2011 been controlled and maintained by a core group of hackers from Russia and Ukraine. Those individuals are believed to have used the botnet in high-dollar corporate account takeovers that frequently were punctuated by massive distributed-denial-of-service (DDoS) attacks intended to distract victims from immediately noticing the thefts.

This is another example of the extensive market for malware available on the internet. Anyone with virtual (or real) currency can buy just about any malware and use it in their own schemes. They don’t have to develop their own code or capability, just buy it from the marketplace and start their own enterprise.

http://krebsonsecurity.com/2014/07/crooks-seek-rivival-of-gameover-zeus-botnet/

Hackers Reveal Nasty New Car Attacks

The fact that a car is not a simple machine of glass and steel but a hackable network of computers is what several folks are trying to demonstrate. Two researchers have even received an $80,000-plus grant last fall from the Defense Advanced Research Projects Agency to root out security vulnerabilities in automobiles. The duo **plan to release their findings and the attack software they developed** at the hacker conference Defcon in Las Vegas next month - the better, they say, to help other researchers find and fix the auto industry’s security problems before malicious hackers get under the hoods of unsuspecting drivers. The need for scrutiny is growing as cars are increasingly automated and connected to the Internet. Practically every American carmaker now offers a cellular service or Wi-Fi network like General Motors’ OnStar, Toyota’s Safety Connect and Ford’s SYNC. The Mobile-industry trade group GSMA estimates revenue from wireless devices in cars at $2.5 billion today and projects that number will grow tenfold by 2025. Without better security it’s all potentially vulnerable, and automakers are remaining mum or downplaying the issue.

But we need to understand that as cars approach Google’s dream of being passenger-carrying robots, more of their capabilities also become potentially hackable. I can imagine multiple software controlled cars being taken over as they drive down an street/interstate and the pileup that would cause at rush hour anywhere.

http://www.forbes.com/sites/andygreenberg/2013/07/24/hackers-reveal-nasty-new-car-attacks-with-me-behind-the-wheel-video/