DHS Open Source Enterprise Daily Cyber Report
24 May 2011

CRITICAL INFRASTRUCTURE PROTECTION:

- Nothing significant to report

INFORMATION SYSTEMS BREACHES:

- Nothing significant to report

CYBERTERRORISM & CYBERWARFARE:

- Nothing significant to report

VULNERABILITIES:

- **LinkedIn Slashes Cookie Lifespan After Research Exposes Security Flaws:** LinkedIn said it would reduce the persistence of cookies it uses to identify users of the business-focused social networking site following the discovery of security issues with the site that create a possible means for fraudsters to hijack profiles. Security researcher Rishi Narang discovered that LinkedIn session cookies are transmitted over an unsecured HTTP connection even in cases where users follow the option of signing in over a secure (SSL) connection. These cookies remain active for up to a year. Hackers who captured these cookies...would be able to obtain unauthorized access to other users' accounts. ... In response to the research, LinkedIn reduced the persistence of the authentication cookie from a year to three months. In addition, the business-focused social network is extending plans to support SSL across its site – not just during logins. [HSEC-1.6; Date: 24 May 2011; Source: http://www.theregister.co.uk/2011/05/24/linkedin_cookie_vuln/]

- **Researchers Find Irreparable Flaw In Popular CAPTCHAs:** Computer scientists have developed software that easily defeats audio CAPTCHAs offered on account registration pages of a half-dozen popular websites by exploiting inherent weaknesses in the automated tests designed to prevent fraud. Decaptcha is a two-phase audio-CAPTCHA solver that correctly breaks the puzzles with a 41-percent to 89-percent success rate on sites including eBay, Yahoo, Digg, Authorize.net, and Microsoft's Live.com. The program works by removing background noise from the audio files, allowing only the spoken characters needed to complete the test to remain. ... Most audio-based CAPTHA systems are wide open to the attack with the notable exception of the Google-owned Recaptcha.net, which uses a different approach known as semantic noise. [HSEC-1.6; Date: 23 May 2011; Source: http://www.theregister.co.uk/2011/05/23/microsoft_yahoo_captchas_busted/]

- **Travel, Education Industries Most 'Phish Prone':** The top five industries most susceptible to cyber crime include travel, education, financial services, government services and IT services, according to a recent phishing experiment conducted among small and medium enterprises featured in the latest Inc. 500 and Inc. 5000 listings. Cybersecurity awareness training firm KnowBe4 sent out a simulated phishing email to about 29,000 employees at more than 3,500 companies found on the Inc.com website. Those who clicked the link were directed to a web page that informed them they had just participated in phishing research. Of all the companies, nearly 500 of those companies had one or more employees who clicked the link. ... The experiment revealed the industries most prone to fall prey to phishing attempts are travel (25 percent), education (22.92 percent), financial services (22.69 percent), government services (21.23 percent) and IT services (20.44 percent). ... A false sense of security could be one of the main reasons companies are vulnerable to cyber crime, with most assuming that antivirus software and an in-house IT team provide adequate cybersecurity. [HSEC-1.6; Date: 23 May 2011; Source: http://www.thenewnewinternet.com/2011/05/23/travel-education-industries-most-phish-prone/]

- **Kaspersky: Android Is The New Windows:** The security situation on Android looks more and more like the security situation in Windows. This is the opinion of the security experts at Kaspersky in their Malware report for the first quarter of 2011. They expand on that comparison, first noting that there is already a "plethora of Android devices" with outdated software and that this software can contain unpatched vulnerabilities. The update policy of negligent manufacturers is criticized because the manufacturers can sell vast amounts of Android devices into the market and leave them with old and vulnerable versions of Android having little interest in supporting rapidly obsolete models. ... The next similarity with Windows was that users tend to ignore security alerts when any application is installed or launched for the first time, giving them privileges such as SMS by merely rubber-stamping approval without the consequences being clear. The devices most at risk were, according to Kaspersky, those which had been jailbroken (or "rooted") to give the user full administrator level access to the system. [HSEC-1.6; Date: 24 May 2011; Source: http://www.h-online.com/security/news/item/Kaspersky-Android-is-the-new-Windows-1248329.html]

GENERAL CYBER/ELECTRONIC CRIME:

- **Osama Alive Scam Snowballs On Twitter:** Fraudsters wasted little time running scams based on the death of Osama bin Laden, so it's no big surprise that they are now running cons based on the conspiracy theory that the former head of al Qaida is alive. Tweets relaying the false news that the uber-terrorist is alive supposedly point to a non-existent news story on CNN. In reality, the links point to a phishing site that attempts to trick marks into handing over login credentials for the micro-blogging service. Those taken in by the scam are forwarded to a YouTube video of protestors in Pakistan who claim that Osama is alive. It's likely the attackers are attempting to use Twitter as a springboard to attack associated webmail accounts. [HSEC-1.10; Date: 24 May 2011; Source: http://www.theregister.co.uk/2011/05/24/osama_alive_twitter_scam/]

- **Exploited Hotmail Bug Stole Email Without Warning:** Microsoft has patched a bug in its Hotmail email service that attackers were exploiting to silently steal confidential correspondences and user contacts from unsuspecting victims. The vulnerability was actively being exploited using emails that contained malicious scripts, Trend Micro researcher Karl Dominguez said.... Successful attacks required only that a Hotmail user open the malicious email or view it in a preview window. The commands embedded in the emails uploaded users' correspondences and user contacts to servers under the control of attackers without requiring the victim to click on links or otherwise take any action. The scripts also had the capability of enabling email forwarding on the targeted Hotmail account, allowing attackers to view emails sent to the victim in the future. ... Monday's blog post said Microsoft has since plugged the hole, which resided in CSS, or cascading style sheet functionality, but didn't say when. [HSEC-1.10; Date: 24 May 2011; Source: http://www.theregister.co.uk/2011/05/24/microsoft_hotmail_email_theft_attack/]

- **Black Hole Exploit Kit Available For Free:** Just a couple of weeks after the source code for the Zeus crimeware kit turned up on the Web, the Black Hole exploit kit now appears to be available for download for free, as well. Black Hole normally sells for $1,500 for an annual license, and is one of the more powerful attack toolkits on the market right now. The Black Hole exploit kit is somewhat newer and less well-known than attack toolkits such as Zeus and Eleonore, but it has been used by attackers for major Web-based attacks for the last few months. [HSEC-1.10; Date: 23 May 2011; Source: http://threatpost.com/en_us/blogs/black-hole-exploit-kit-available-free-052311]

MISCELLANEOUS:

- **Bin Laden's Tech Habit Could Trip Up His Terrorist Group:** [A]lthough bin Laden went to great lengths to avoid leaving a detectable digital trail...the terrorist leader's desire for technology abstinence was far from complete. According to Pentagon officials, he relied heavily on laptop computers and portable storage devices for planning and issuing commands, and those devices are now in the hands of the U.S. government. ... [E]fforts to access the terrorist group's digital records likely started on site in Pakistan only minutes after the first U.S. special forces set foot inside bin Laden's walled compound, which could increase the chances of success, Greg Hoglund, CEO of HBGary, told InformationWeek's Mathew Schwartz. That's because it's easier to access information from an encrypted computer drive while it is still running, Hoglund and others have said. He added that it would take a computer specialist accompanying the assault team about 15 to 30 minutes to scan and record what's in the active computer's memory and make a copy of the hard drive. The raid lasted about 40 minutes. ... However, if the computers in bin Laden's home were powered off at the time of the raid and their owners had been using readily available encryption software and avoiding weak pass phrases, it might be impossible to access the data, experts said. [HSEC-1.9; Date: 23 May 2011; Source: http://fcw.com/articles/2011/05/23/buzz-bin-laden-tech-habit.aspx]