DHS Open Source Enterprise Daily Cyber Report
19 January 2011

CRITICAL INFRASTRUCTURE PROTECTION:

- Nothing significant to report

INFORMATION SYSTEMS BREACHES:

- **Carbon Trading Exchange Suspends Ops Following Hack Attack:** A carbon emissions trading registry in Austria has suspended operations until at least 21 January following a hacking attack earlier this month. The registry has been disconnected from the EU and UN carbon trading registries in response to the 10 January attack, details on which are unclear. A statement on the trading registry website explains that the disconnection from other registries and suspension of operations is a security precaution taken to safeguard the operation of wider EU systems while problems on the Austrian site are identified and resolved. ... The Austrian site is one of a network of sites across Europe that apply a market-based approach to tackling carbon emissions. ... [C]ybercrooks look at carbon exchanges as a left-field source of illicit income, so sites are subject to hacking attacks or scams from multiple sources. [Date: 19 January 2011; Source: http://www.theregister.co.uk/2011/01/19/carbon_trading_site_shuts_after_hack_attack/]

CYBERTERRORISM & CYBERWARFARE:

- Nothing significant to report

VULNERABILITIES:

- **ICQ's Critical Flaw Allows Attackers To Serve Malicious Software Update:** ICQ - the popular instant messaging application - has a gaping security hole that can allow attackers to execute malicious code on the targeted system, says researcher Daniel Seither. The flaw affects the application's automatic update mechanism, and affects all versions of ICQ 7 for Windows up to the latest one. The problem lays in the fact that the application doesn't verify the identity of the update server or the origin of updates through digital signatures or similar means. "By impersonating the update server (think DNS spoofing), an attacker can act as an update server of its own and deliver arbitrary files that are executed on the next launch of the ICQ client," explained Seither in a BugTraq post. "Since ICQ is automatically launched right after booting Windows by default and it checks for updates on every start, it can be attacked very reliably." ... Since there is no way to switch off the automatic updating mechanism, Seither advises users to stop using the application until a fix is issued. [Date: 18 January 2011; Source: http://www.net-security.org/malware_news.php?id=1594]

- **Keyless Systems On Cars Easily Hacked, Researchers Say:** The passive keyless entry and start (PKES) systems supported by many modern cars are susceptible to attacks that allow thieves to relatively easily steal the vehicles, say security researchers at Switzerland's ETH Zurich University. In demonstrations using 10 cars from eight makers, the researchers showed how they were able to unlock, start and drive away the cars in each case, by outsmarting the smart key system. The break-ins were carried out using commercial, off-the-shelf electronic equipment available for as little as $100, the researchers said in a paper describing their exploits. ... Details of the hacking are scheduled to be presented at a security conference in San Diego later this month.... [Date: 19 January 2011; Source: http://www.computerworld.com/s/article/9205478/]

- **Gaping Security Flaw Exposed On Anti-Tamper Devices:** Security devices used in transportation, packaging and even in accounting for nuclear materials are very vulnerable to attack, two security

researchers warned on Tuesday at the Black Hat security conference. The physical security devices, known as "tamper-evident devices," aren't intended to prevent theft but to alert inspectors that something has been broken into. The devices are wide-ranging in design and application, and are used to seal everything from evidence bags, large shipping containers and even things like the warranty seal on an Xbox gaming console. Jamie Schwettmann and Eric Michaud of i11 Industries went through a long list of tamper evident devices at the conference here and explained, step-by-step, how each seal can be circumvented with common items, such as various solvents, hypodermic needles, razors, blow driers, and in more difficult cases with the help of tools such as drills. [Date: 18 January 2011; Source: http://www.computerworld.com/s/article/9205461/]

GENERAL CYBER/ELECTRONIC CRIME:

- **Chinese Trojan Targets Cloud-Based AV Technologies:** A Trojan that tries to obstruct cloud-based antivirus technology present in major AV solutions offered by Chinese security firms is targeting users by posing as a video player and other popular software. According to Microsoft's researchers, the attackers use social engineering techniques to get the victims to install the Trojan - called Bohu - on their system. Once inside, the malware tries its best to not get noticed by the AV solution by modifying its payload components in such a way as to bypass hash-based detection. Having achieved that goal, it tries to install a Windows Sockets service provider interface (SPI) filter in order to block network traffic between the cloud security client and server and, for good measure, a Network Driver Interface Specification (NDIS) filter to impede the antivirus client to send any data to the server for further analysis. [Date: 19 January 2011; Source: http://www.net-security.org/malware_news.php?id=1598]

- **Pill Pushers Pop Military, Government, Education Sites:** A software vulnerability at a U.S. based Web hosting provider let hackers secretly add dozens of Web pages to military, educational, financial and government sites in a bid to promote rogue online pharmacies. For four months in 2010, a customer of Hostmonster.com, a Provo, Utah based hosting provider, exploited a bug in CPanel — a Web site administration tool used by Hostmonster and a majority of other hosting providers. The customer used the vulnerability to create nearly four dozen subdomains on a number of other Web sites at the hosting facility, said Danny Ashworth, co-founder of Bluehost.com, the parent company of Hostmonster. The subdomains were linked to dozens of pages created to hijack the sites' search engine rankings, and to redirect visitors to fly-by-night online stores selling prescription drugs without a prescription. [Date: 14 January 2011; Source: http://krebsonsecurity.com/2011/01/pill-pushers-pop-military-government-education-sites/]

- **Attack Tool Kits To Blame For 60 Per Cent Of Web Threats:** Nearly two-thirds of web-based threats last year were caused by attack toolkits, bundles of malicious software which have significantly lowered the bar to entry for new cyber criminals, according to the latest research from Symantec. ... Symantec senior manager Orla Cox explained that there are two main types of attack toolkit. The most popular is the sort that allows cyber criminals to set up a web site hosting any number of exploits which will drop onto a user's machine if they visit that site. "The goal here is pay-per-install schemes, using the toolkits to drop malware like fake anti-virus onto the machines so they get paid every time," she said. The second type of kit allows criminals to create their own malware, such as ZeuS, but requires a hosting site or another way to get it onto users' computers. ... Another sign of their growing sophistication and danger to global internet security is that most kits are easily updated, meaning that they can be targeted to exploit the latest zero-day vulnerabilities. [Date: 18 January 2011; Source: http://www.v3.co.uk/v3/news/2274285/symantec-tool-kits-zeus]

- **Hackers Eyed Sale Of Celebrity iPad Data:** Two hackers accused of stealing personal data belonging to 120,000 early adopters of Apple's iPad tablet last year discussed the possibility of selling it to spammers.... According to a criminal complaint filed Tuesday, Andrew Auernheimer and Daniel Spitler also used the information to contact board members for Reuters, The San Francisco Chronicle, and Rupert Murdoch's News Corp., telling them that their personal data had been leaked by unsecured servers belonging to AT&T. Release of the list of elite iPadders, which included then White House Chief of Staff Rahm Emanuel and New York Mayor Michael Bloomberg, was obtained using a PHP script that matched email addresses and names to the corresponding ICC-IDs, or integrated circuit card identifiers, of the must-have Apple tablets. ... The 14-page complaint charges both men with one felony count each of conspiracy to access a protected computer without authorization and stealing the identification information of thousands of people. [Date: 18 January 2011; Source: http://www.theregister.co.uk/2011/01/18/ipad_data_breach_charges_brought/]