Homeland Security | OPEN SOURCE ENTERPRISE

This document was prepared by the Office of Intelligence and Analysis to facilitate a greater understanding of the nature and scope of threats and hazards to the homeland. It is provided to Federal, State, Local, Tribal, Territorial and private sector officials to aid in the identification and development of appropriate actions, priorities and follow-on measures. This product may contain U.S. person information that has been deemed necessary for the intended recipient to understand, assess, or act on the information provided. It should be handled in accordance with the recipient's intelligence oversight and/or information handling procedures. Some content may be copyrighted. These materials, including copyrighted materials, are intended for "fair use" as permitted under Title 17, Section 107 of the United States Code ("The Copyright Law"). Use of copyrighted material for unauthorized purposes requires permission from the copyright owner. Any feedback regarding this report or requests for changes to the distribution list should be directed to the Open Source Enterprise via unclassified e-mail at: OSINTBranchMailbox@hq.dhs.gov.

DHS Open Source Enterprise Daily Cyber Report
3 October 2011

CRITICAL INFRASTRUCTURE PROTECTION:

- Nothing significant to report

INFORMATION SYSTEMS BREACHES:

- **Betfair Hides Credit Card Data Hack From Customers:** Sports betting exchange Betfair failed to notify customers of a massive credit card data theft 18 months ago…. According to the Daily Telegraph, the company disclosed in an internal report that between 28 March 2010 and 9 April 2010, cyber criminals stole 3.15 million account usernames with encrypted security questions, 2.9 million usernames with one or more addresses and 89,744 account usernames with bank account details. Customer accounts that existed at 1 February 2010 were affected, yet Betfair made no move to inform customers of the breach because it decided that there was "no risk to customers." "Eighteen months ago we were subject to an attempted data theft. Because of our security measures the data was unusable for fraudulent activity and we were able to recover the data intact." [HSEC-1.10; Date: 1 October 2011; Source: http://computerworld.co.nz/news.nsf/security/betfair-hides-credit-card-data-hack-from-customers]

- **Hackers Post Data On JP Morgan Chase CEO:** Hackers have posted personal information about the chief executive of J.P. Morgan Chase in solidarity with the Occupy Wall Street protests. The document released on Pastebin by "CabinCr3w" includes information about CEO James Dimon's addresses, family, business connections, political contributions and legal information. A spokeswoman for J.P. Morgan Chase said the company is declining to comment. The same hackers posted personal data of Goldman Sachs CEO Lloyd Blankfein and of New York Police Deputy Inspector Anthony Bologna earlier this week after Bologna was seen in videos pepper-spraying peaceful demonstrators in the face last weekend. [HSEC-1.10; Date: 30 September 2011; Source: http://news.cnet.com/8301-1009_3-20113943-83/]

CYBERTERRORISM & CYBERWARFARE

- **Iran Warns US And UK Cyber Attacks Will Result In Retaliation:** Iran has been flexing its muscles on the world stage again, warning the US and its allies that any cyber attack against the country will result in retaliation from Tehran. Muslim news organisation the Ahlul Bayt News Agency reported Brigadier General Ali Shadmani, head of the Operations Department of the Iranian Armed Forces, as saying that any cyber attack on Iran would be "risky" and met with swift reprisals. ... [O]f course there are acts of cyber espionage and nation state-related attacks occurring all the time, so Shadmani perhaps took this opportunity to remind the West that he knows what the US and its allies are up to. Or perhaps it was another reference to the infamous Stuxnet worm.... Iran itself, of course, has been implicated in several cyber attacks, most recently in the Comodo and DigiNotar breaches which yielded a treasure trove of fake SSL certificates which could have been used to build phishing sites. [HSEC-1.10; Date: 30 September 2011; Source: http://www.v3.co.uk/v3-uk/security-watchdog-blog/2113580/iran-warns-uk-cyber-attacks-result-retaliation]

VULNERABILITIES:

- **Security Hole In HTC Phones Gives Up E-Mail Addresses, Location:** A security hole found in some HTC Android phones could give apps with Internet permissions access to information like a user's location and their text messages…. The vulnerability is part of HTC's Sense UI and affects a subset of the brand's most popular phones, including the HTC Thunderbolt and the EVO 4G. … Apps with Internet permissions can access HTCLoggers.apk, which provides access to information like GPS data, WiFi network data, memory info, running processes, SMS data (including phone numbers and encoded text), and system logs that can include information like e-mail addresses and phone numbers. … Apps can send the data off to a remote server for safekeeping, as shown by a proof-of-concept app that Android Police researchers developed. The authors note that the flaw can't be fixed in the stock Sense UI without an update or patch from HTC. [HSEC-1.6; Date: 2 October 2011; Source: http://arstechnica.com/gadgets/news/2011/10/security-hole-in-htc-phones-gives-up-e-mail-addresses-location.ars]

- **Symantec IM Manager Multiple Vulnerabilities:** Multiple vulnerabilities have been reported in Symantec IM Manager, which can be exploited by malicious users to compromise a vulnerable system and by malicious people to conduct cross-site scripting attacks, according to Secunia. Input passed to the "refreshRateSetting" parameter in IMManager/Admin/IMAdminSystemDashboard.asp, "nav" and "menuitem" parameters in IMManager/Admin/IMAdminTOC_simple.asp, and "action" parameter in IMManager/Admin/IMAdminEdituser.asp is not properly sanitised before being returned to the user. This can be exploited to execute arbitrary HTML and script code in a user's browser session in context of an affected site. An input validation error exists within the Administrator Console. ... Successful exploitation of this vulnerability may allow execution of arbitrary code. [HSEC-1.6; Date: 3 October 2011; Source: http://www.net-security.org/secworld.php?id=11716]

GENERAL CYBER/ELECTRONIC CRIME:

- **Anonymous Launches Analytics Research Branch:** [A]nonymous has branched out with a spin-off research unit dedicated to producing investigative reports designed to expose corrupt companies. Anonymous Analytics has its own web site which includes a contact form and a drop box secured with AES-256 bit encryption designed to encourage tip-offs. "Anonymous Analytics, a faction of Anonymous, has moved the issue of transparency from the political level to the corporate level," said a statement on the site. "To this end, we use our unique skill sets to expose companies that practise poor corporate governance and are involved in large-scale fraudulent activities." [HSEC-1.2; Date: 30 September 2011; Source: http://www.v3.co.uk/v3-uk/security-watchdog-blog/2113507/anonymous-launches-analytics-research-faction]

- **Australia's NetRegistry Suffers A Major DDoS Attack:** Reports are coming in that the NetRegistry, one of Australia's key internet registries, has suffered a major distributed denial of service (DDoS) attack this week. According to the ITwire, the attack has left many customers unable to access their websites or virtual private servers (VPS) for one or more days earlier this week. … NetRegistry says its engineers have confirmed a DDoS attack has been in progress, with multiple connections swamping a server and eventually taking it offline. Although most clients had some access restored by 5pm Monday AEST, users on the Telstra network were still experiencing problems, and an ETA on their services being restored is still not available. [HSEC-1.10; Date: 30 September 2011; Source: http://www.infosecurity-magazine.com/view/21065]

- **NICE's Acelera Internet Service Hacked:** A hacker attacked the Instituto Costarricense de Elecetricidad's (ICE) Acelera internet network on Saturday. ICE reports damage in San José and Heredia [Costa Rica]. Early reports by the state telecom say that the hacked directly affected equipment installed in the homes or offices of clients. ICE said it does not yet know the extent of the hack and how many customers were affected and is working on restoring passwords and user information from backup data. [HSEC-1.10; Date: 2 October 2011; Source: http://www.insidecostarica.com/dailynews/2011/october/02/costarica11100201.htm

- **Thailand's Prime Minister's Twitter Account Hacked:** Yingluck Shinawatra, the prime minister of Thailand, had her personal Twitter account hacked in an attempt to stain the politician's image. According to the Bangkok Post, authorities are committed to discover those responsible for the hit, the first clues indicating that the attack was launched from a prepaid SIM card installed in an iPhone. The main suspects are the people who work with the prime minister as Mr Prinya, who is advising Ms Yingluck's IT team, revealed "This case is more about vulnerabilities in people and processes, not hacking. It's about a political agenda." [HSEC-1.10; Date: 3 October 2011; Source: http://news.softpedia.com/news/Thailand-s-Prime-Minister-s-Twitter-Account-Hacked-224925.shtml]

- **Google And Yahoo Services Become Spammers' Heaven:** Because any email arriving from Yahoo or Google services is considered to be legitimate and useful, spammers take advantage of this bug to spread their malevolent messages. Chester Wisniewski from Sophos revealed that he has been receiving a lot of spam email from Google Picasa and Yahoo! Groups, all being attempts of hackers to cast "spammy" alerts. In the case of Google's Picasa ... anything coming from the popular picture manager is considered to be harmless, it never ends up in the spam folder of the mail box.... With Yahoo! Groups the principle is more complicated but spammers can just as easily take advantage of the policy slip. The rules allow anyone who owns a group to add members without asking for their permission. Instead, after you are unwillingly made part of a group, you have to unsubscribe in order to stop receiving alerts. [HSEC-1.8; Date: 1 October 2011; Source: http://news.softpedia.com/news/Google-and-Yahoo-Services-Become-Spammer-s-Heaven-224879.shtml]