The Cyber Shield

Cyber News for Counterintelligence / Information Technology / Security Professionals

2 May 2014

Purpose
Educate recipients of cyber events to aid in the protection of electronically stored corporate proprietary, DoD and/or Personally Identifiable Information from theft, compromise, espionage, and / or insider threat

Source
This publication incorporates open source news articles educate readers on security matters in compliance with USC Title 17, section 107, Para a. All articles are truncated to avoid the appearance of copyright infringement

Publisher
* SA Jeanette Greene
Albuquerque FBI

Editor
* CI SA Scott Daughtry
DTRA Counterintelligence

Subscription
To receive this newsletter please send an email to scott.daughtry@dtra.mil

NMCIWG Members
Our membership includes representatives from these agencies: 902nd MI, AFOSI, AUSA, DCIS, DOE, DSS, DTRA, FBI, HSI, Los Alamos Labs, NAG, NCIS, NGA, NRO, Sandia Labs

April 30, WANE 15 Fort Wayne – (Indiana) **Patient info breached after DeKalb hospital website hacked.** DeKalb Health notified 17 patients after a third party firm's server used to operate the hospital's Web site was hacked in February, allowing access to their personal information and credit card numbers. Investigators also stated that an additional database containing information on 24 patients, along with approximately 1,320 nursery babies may have been created by hackers, as well as a fake Web site which appeared as a donation page for the DeKalb Health Foundation in order to send fake phishing emails. Source: http://wane.com/news/health/patient-info-breached-after-dekalb-hospital-hacked/

April 28, Durango Herald – (Colorado) **Mercy records breach.** Centura Health notified about 1,000 individuals in Durango that their personal and medical information may have been compromised through a phishing email attack that targeted employees in February. Officials stopped the attack and began an investigation into the incident. Source: http://www.durangoherald.com/article/20140428/NEWS01/140429556/article/20140428/NEWS01/140429556/Mercy-patient-info-hacked-

May 1, The Register – (International) **Staunch your Heartbleed patching: FreeBSD has a nasty credentials leak.** The creators of FreeBSD advised users to apply a patch that was released after a TCP ordering issue was discovered which could allow attackers to perform denial-of-service (DoS) or data leakage attacks. Source: http://www.theregister.co.uk/2014/05/01/freebsd_next_to_leak_credentials/

April 30, SC Magazine – (International) **Possibly the first Android worm, spreading through SMS, found in wild.** ESET researchers reported that the Android/Samsapo.A malware may be the first Android worm seen in the wild. The malware spreads via SMS messages, can perform a variety of actions, and is currently seen targeting users in Russia. Source: http://www.scmagazine.com/possibly-the-first-android-worm-spreading-through-sms-found-in-wild/article/344873/

Internet Explorer bug fixed, even for XP
CNN Money, 1 May 2014: Microsoft has issued a patch for the Internet Explorer flaw that lets hackers take control of your computer -- even for users of Windows XP. Microsoft was racing to issue a fix for theInternet Explorer browser bug that security researchers discovered this past weekend. Starting Thursday, PC users will get an automatic update for Windows to keep hackers from hijacking machines. The bug, which affects many version of the browser, allows hackers to take total control of your computer if they manage to slip malware into your PC. That means you'd have to click on a bad link and visit an infected site with the Internet Explorer browser to get it. There were concerns that many PC users would be left exposed to hackers, because Microsoft no longer supports Windows XP. But the company on Thursday reconsidered and issued a fix for XP users too. To read more click **HERE**

Some Windows 7 Users Cannot Install Internet Explorer Zero-Day Patch

SoftPedia, 2 May 2014: Microsoft today issued a patch for the Internet Explorer zero-day flaw affecting all Windows versions on the market, but it turns out that a number of Windows 7 users cannot install it due to some errors. According to Microsoft itself, who has already confirmed the issue on Windows 7 computers, Internet Explorer might crash all of a sudden when trying to deploy the zero-day patch. This is happening because the security update 2929437 is not installed on these PCs, the company explained. Redmond recommends users to install security update 2964358 in order to address the issue, but in case you're coming across similar issues, there's always a second option. "Install security update 2964444 instead of security update 2964358. Security update 2964444 is intended for systems that do not have security update 2929437 installed," Microsoft added. At this point, the patch is being delivered to users via Windows Update, so you should basically have nothing to do if you're trying to deploy it automatically. On the other hand, if you're experiencing the issues mentioned here, make sure that you first install the required security update and only then proceed with the deployment of the zero-day patch aimed at Internet Explorer. Microsoft says that the issue is only happening on Windows 7 and no other versions of Windows are affected. To read more click **HERE**

University of North Carolina Wilmington Suffers Data Breach

SoftPedia, 2 May 2014: The University of North Carolina Wilmington (UNCW) has revealed that one of its application servers has been breached. The attackers could have accessed the personal details of employees and students. The server stores a database of names, addresses and social security numbers of UNCW employees, including part-time and temporary employees. It also contains the details of graduate students, adjunct instructors, and people who took a foreign language placement test at the university between 2002 and 2006. In a notice published on its website, the educational institution says that there's no evidence that the information has been accessed by the cybercriminals, or that it has been misused. It appears that the cybercriminals abused the server to host a phishing page. The attackers somehow gained access to the password for an administrator account. The file containing the sensitive information has been removed from the server in question. The organization has also updated all server operating systems and applications. It has restricted access to the application server, and has increased the frequency of security scans. Existing applications have been moved to separate, more secure servers, and special software has been deployed to find personally identifiable information stored on the university's computers. Impacted individuals are being notified via email or snail mail if an email address is not available. Regulators and law enforcement have also been notified of the incident. To read more click **HERE**

UK National Crime Agency Report Warns of Increase in Cyber Threats

SoftPedia, 1 May 2014: The United Kingdom's National Crime Agency (NCA) has published the National Strategic Assessment of Serious and Organised Crime for 2014. The report covers child exploitation and abuse, the criminal use of firearms, drugs, economic crime, immigration crime and human trafficking, and cybercrime. British authorities seem to be aware of the fact that cybercrime will be increasingly problematic in the upcoming period. The report highlights five main types of cyber threats:

1. large-scale harvesting of personal and business data for fraud against individuals and organizations;
2. attacks whose goal is to delete, modify or steal data to gain competitive advantage, gain control of infrastructure, damage reputations, or undermine user confidence;
3. disruption of access to systems with the aid of distributed denial-of-service (DDOS) attacks;
4. the increasing use of the services offered on the cybercrime marketplaces by traditional crime groups;

5. the increasing use of support services critical to the success of cyber-dependent crimes by other crime actors.

Of these five threats, only the first is likely to remain constant, the rest are either increasing or likely to increase in the next one to three years, according to the NCA's report. When it comes to cyber-dependent crimes carried out by traditional crime groups, the agency highlights the limited capacity and capability of law enforcement to respond. It also emphasizes the increasing gap between the capabilities of law enforcement and criminals. "Specialist service providers and bespoke toolkits are opening opportunities for those criminals who have limited technical competence. Different organised crime groups who share the use of key criminal technical and other infrastructures is a growing threat. Criminal online forums provide a market place for the trading of such services," the report reads. "Distributed Denial of Service (DDOS) protocols capable of launching powerful attacks against business critical systems are increasing in numbers. These tools, coupled with better understanding of the financial and reputational damage they can cause, are increasing the industry's perception of DDOS as a significant threat." The NCA says that it's currently difficult to estimate the costs of cybercrime, but the agency notes that it could "reasonably be assessed" at several billion pounds each year. Many recent studies conducted by third-party security companies have shown that the UK is among the most targeted countries in Europe. For instance, the Regional Advanced Threat Report published by FireEye earlier this week shows that the largest number of malware infections have been spotted in the UK. Furthermore, the country takes the second place when it comes to the highest advanced persistent threat (APT) activity. The National Strategic Assessment of Serious and Organised Crime 2014 report is available on the NCA's website (**link**). To read more click **HERE**