CYBER SECURITY

Newsletter

May 2014

Aim of the long-term CENAA program on cyber security (Global Netizenship in Cyberworld - GNC) is in-depth analysis of multi-spectral and cross-cutting issues of national and international security. In last years, cyber attacks have become powerful and fully-fledged tool in conventional war and industrial espionage. Through establishing network of national and international partnerships, CENAA strives to ensure that cyber security will get into focal point of political, corporate and expert elites. Goal of this Newsletter and GNC project is also de-tabuise issue of cyber security to all.

May 1, 2014

SUSAN TOMPOR: TIME TO GET A 'LITTLE PARANOID' AFTER CREDIT, DEBIT CARD BREACHES:

Mike Rosinski, 51, doesn't really know how a string of fraudulent charges ranging from as little as $3.19 for some odd outfit in Missouri to $434.10 at a Fry's Electronics in another state ended up hitting his Visa credit card in mid-April. Detroit Free Press, May 1, 2014

www.freep.com/article/20140501/COL07/305010031/Susan-Tompor-Time-to-get-a-little-paranoid-after-credit-debit-card-breaches

May 1, 2014

MICROSOFT ISSUES FIX FOR IE ZERO-DAY, INCLUDES XP USERS:

Microsoft has issued an emergency security update to fix a zer0-day vulnerability that is present in all versions of its Internet Explorer Web browser and that is actively being exploited. In an unexpected twist, the company says Windows XP users also will get the update, even though Microsoft officially ceased supporting XP last month. KrebsOnSecurity, May 1, 2014

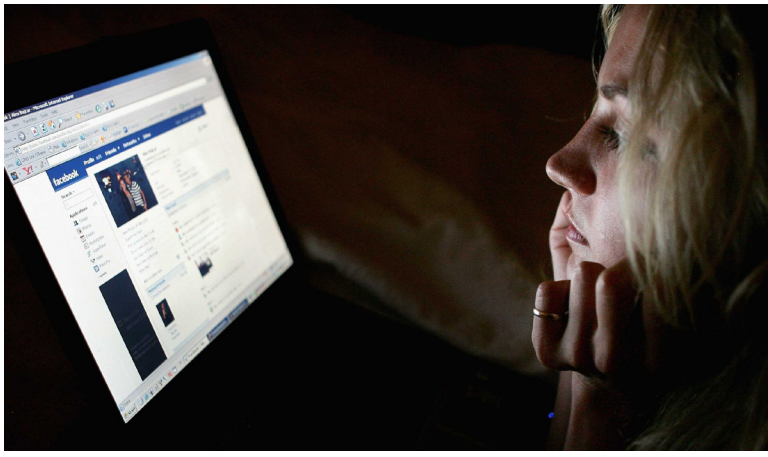
http://krebsonsecurity.com/2014/05/microsoft-issues-fix-for-ie-zero-day-includes-xp-users/

May 1, 2014

GOOD INFORMATION SECURITY LEADERSHIP DEMANDS FOCUS ON SHARED KNOWLEDGE:

One of information security's most venerable thought leaders believes the evolution of leadership in the industry has reached a turning point and without a disciplined, holistic approach emphasizing shared knowledge, enterprise security programs will never achieve their desired results. During a keynote Wednesday at the SANS Security Leadership Summit, SANS Innovation Center director Tony W. Sager drew from his 30-plus years at the National Security Agency's defense-focused Information Assurance Directorate (IAD) SearchSecurity, May 1, 2014

http://searchsecurity.techtarget.com/news/2240219965/Good-information-security-leadership-demands-focus-on-shared-knowledge



MY EXPERIMENT OPTING OUT OF BIG DATA MADE ME LOOK LIKE A CRIMINAL:

Here's what happened when I tried to hide my pregnancy from the Internet and marketing companies. Time, May 1, 2014

http://time.com/83200/privacy-internet-big-data-opt-out/

May 2014

THE RISING STRATEGIC RISKS OF CYBERATTACKS:

More and more business value and personal information worldwide are rapidly migrating into digital form on open and globally interconnected technology platforms. As that happens, the risks from cyberattacks become increasingly daunting. Criminals pursue financial gain through fraud and identity theft; competitors steal intellectual property or disrupt business to grab advantage;

"hacktivists" pierce online firewalls to make political statements. Research McKinsey conducted in partnership with the World Economic Forum suggests that companies are struggling with their capabilities in cyberrisk management. McKinsey&Company, May 2014

http://www.mckinsey.com/insights/business_technology/The_rising_strategic_risks_of_cyberattacks?cid=other-eml-alt-mkq-mck-oth-1405

May 7, 2014

ANTIVIRUS IS DEAD: LONG LIVE ANTIVIRUS!:

An article in The Wall Street Journal this week quoted executives from antivirus pioneer Symantec uttering words that would have been industry heresy a few years ago, declaring antivirus software "dead" and stating that the company is focusing on developing technologies that attack online threats from a different angle. KrebsOnSecurity, May 7, 2014

http://krebsonsecurity.com/2014/05/antivirus-is-dead-long-live-antivirus/

May 9, 2014

ACCIDENTAL HEARTBLEED VULNERABILITIES UNDERCUT RECOVERY EFFORT:

Scans find 300,000 affected servers, but a surprising number of newly vulnerable servers have surfaced since Heartbleed warning was first sounded. Dark Reading, May 9, 2014

http://www.darkreading.com/vulnerabilities---threats/accidental-heartbleed-vulnerabilities-undercut-recovery-effort/d/d-id/1251166?_mc=RSS_DR_EDT

May 9, 2014

GOOGLE BLOCKS FILESHARING WEBSITE DEMONOID OVER MALWARE DOWNLOADS:

Google is warning users of its search engine that if they visit filesharing website Demonoid, they could find malicious software being downloaded and installed on their computers. Anyone searching for the site, which relaunched earlier this year after a lengthy period offline, sees a message warning that "This site may harm your computer" The Guardian, May 9, 2014

http://www.theguardian.com/technology/2014/may/09/google-demonoid-filesharing-malicious-software

May 9, 2014

DOJ ASKS FOR NEW AUTHORITY TO HACK AND SEARCH REMOTE COMPUTERS:

The U.S. Department of Justice wants new authority to hack and search remote computers during investigations, saying the new rules are needed because of complex criminal schemes sometimes using millions of machines spread across the country. CIO, May 9, 2014

http://www.cio.com/article/752689/DOJ_Asks_for_New_Authority_to_Hack_and_Search_Remote_Computers?source=rss_all&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+cio%2Ffeed%2Farticles+%28CIO.com+Feed+-+Articles%29

May 13, 2014

IRANIAN HACKERS TARGETED DEFENSE WORKERS AND POLITICAL DISSIDENTS:

There's a new politically motivated hacker gang to keep track of, one that started out defacing websites but which has progressed more recently into conducting full-blown campaigns of cyber espionage abroad and political oppression at home. And it is based in Iran. Re/code, May 13, 2014

http://recode.net/2014/05/13/iranian-hackers-targeted-defense-workers-and-political-dissidents/

May 13, 2014

POSTAL SERVICE: BEWARE STAMP KIOSK SKIMMERS:

he United States Postal Inspection Service is investigating reports that fraudsters are installing skimming devices

on automated stamp vending machines at Post Office locations across the United States, KrebsOnSecurity has learned. KrebsOnSecurity, May 13, 2014

http://krebsonsecurity.com/2014/05/postal-service-beware-stamp-kiosk-skimmers/?utm_source=feedburner

May 16, 2014

PAYPAL FIXES SERIOUS ACCOUNT HIJACKING BUG IN MANAGER:

PayPal patched a hole in its Manager portal this week that could have made it easy for an attacker to hijack an admin's account, change their password and steal their personal information — not to mention their savings. ThreatPost, May 16, 2014

http://threatpost.com/paypal-fixes-serious-account-hijacking-bug-in-manager/106117

May 21, 2014

EBAY URGES PASSWORD CHANGES AFTER BREACH:

eBay is asking users to pick new passwords following a data breach earlier this year that exposed the personal information of an untold number of the auction giant's 145 million customers. KrebsOnSecurity, May 21, 2014

http://krebsonsecurity.com/2014/05/ebay-urges-password-changes-after-breach/

May 22, 2014

INDICTMENT OF PLA HACKERS IS PART OF BROAD U.S. STRATEGY TO CURB CHINESE CYBERSPYING:

Two years ago, a senior official from the State Department and one from the Pentagon held an extraordinary four-hour meeting with their counterparts in Beijing. For the first time, the U.S. government confronted the Chinese government with proof that American companies were being hacked by the People's Liberation Army to benefit Chinese firms. Washington Post, May 22, 2014

http://www.washingtonpost.com/world/national-security/indictment-of-pla-hackers-is-part-of-broad-us-strategy-to-curb-chinese-cyberspying/2014/05/22/a66cf26a-e1b4-11e3-9743-bb9b59cde7b9_story.html

May 23, 2014

SOME PRIVACY, PLEASE? FACEBOOK, UNDER PRESSURE, GETS THE MESSAGE:

Do you know who can see what you are posting on Facebook, including your photos, birthday and personal cellphone number? The New York Times, May 23, 2014

http://www.nytimes.com/2014/05/23/technology/facebook-offers-privacy-checkup-to-all-1-28-billion-users.html?hp&_r=1

May 23, 2014

U.S. INDICTMENTS SHED SOME LIGHT ON CHINA'S HACKER ARMY:

One man accused of being a hacker for the Chinese military, Wang Dong, better known as UglyGorilla, wrote in a social media profile that he did not "have much ambition" but wanted "to wander the world with a sword, an idiot," Edward Wong reports. The New York Times, May 23, 2014

http://bits.blogs.nytimes.com/2014/05/23/daily-report-u-s-indictments-shed-some-light-on-chinas-hacker-army/

May 26, 2014

BANKS CHALLENGED BY CYBERSECURITY THREATS, STATE REGULATORS ACTING:

A new report concludes that while financial institutions have taken significant steps to bolster cyber security efforts, they will continue to be challenged by the speed of technological change and the increasingly sophisticated nature of threats. Forbes, May 26, 2014

http://www.forbes.com/sites/gregorymcneal/2014/05/26/banks-challenged-by-cybersecurity-threats-state-regulators-acting/

May 30, 2014

HACKERS IN IRAN USE SOCIAL MEDIA TO TARGET SENIOR U.S., ISRAELI OFFICIALS:

Hackers based in Iran used social networks to spy on high-ranking U.S. and Israeli officials, a new report by a cybersecurity firm claims. CNN, May 30, 2014

http://edition.cnn.com/2014/05/30/world/meast/iran-hacking-report/

CENAA

Tolstého 9
811 06 Bratislava
E-mail: office@cenaa.org