CYBER SECURITY

Newsletter

June 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.

June 2, 2014

'OPERATION TOVAR' TARGETS 'GAMEOVER' ZEUS BOTNET, CRYPTOLOCKER SCOURGE:

The U.S. Justice Department is expected to announce today an international law enforcement operation to seize control over the Gameover ZeuS botnet, a sprawling network of hacked Microsoft Windows computers that currently infects an estimated 500,000 to 1 million compromised systems globally. Experts say PCs infected with Gameover are being harvested for sensitive financial and personal data, and rented out to an elite cadre of hackers for use in online extortion attacks, spam and other illicit moneymaking schemes. KrebsOnSecurity, June 2, 2014

http://krebsonsecurity.com/2014/06/operation-tovar-targets-gameover-zeus-botnet-cryptolocker-scourge/

June 2, 2014

CYBERSECURITY EXPERT RICHARD A. CLARKE AND LA COUNTY DISTRICT ATTORNEY JACKIE LACEY SPOKE AT ISSA-LA 6TH ANNUAL INFORMATION SECURITY SUMMIT ON CYBERCRIME SOLUTIONS:

Nearly 800 of the country's leading cybercrime experts, information security professionals, company CEOs and other C-suite business executives recently attended the 6th Annual Information Security Summit, The Growing Cyber Threat: Protect Your Business, that was held by the Los Angeles Chapter of the Information Systems Security Association (ISSA-LA). The diverse group of attendees reflected the new reality that cybercrime impacts the financial stability of all organizations and industries such as business, nonprofits, government agencies, schools, healthcare and financial services. The Summit advances ISSA-LA's core belief that 'It takes the village to secure the village' SM. PRWeb, June 2, 2014

http://www.prweb.com/releases/2014/05/prweb11894507.htm

June 4, 2014

UK PROPOSES HARSHER SENTENCES FOR HACKERS:

The UK government believes hackers who cause "catastrophic" damage should be imprisoned for life, Queen Elizabeth II said in a speech today, proposing a crime bill that would update the 1990 Computer Misuse Act. The Verge, June 4, 2014

http://www.theverge.com/2014/6/4/5780268/the-queen-of-england-wants-harsher-sentences-for-hackers

June 5, 2014

THEY HACK BECAUSE THEY CAN:

The Internet of Things is coming….to a highway sign near you? In the latest reminder that much of our nation's "critical infrastructure" is held together with the Internet equivalent of spit and glue, authorities in several U.S. states are reporting that a hacker has once again broken into and defaced electronic road signs over highways in several U.S. states. Earlier this week, news media in North Carolina reported that at least three highway signs

there had apparently been compromised and re-worded to read “Hack by Sun Hacker.” KrebsOnSecurity, June 5, 2014

http://krebsonsecurity.com/2014/06/they-hack-because-they-can/

June 9, 2014

UPSURGE IN HACKING MAKES CUSTOMER DATA A CORPORATE TIME BOMB:

With hackers stealing tens of millions of customer details in recent months, firms across the globe are ratcheting up IT security and nervously wondering which of them is next. Reuters, June 9, 2014

http://www.reuters.com/article/2014/06/09/technology-cybersecurity-idUSL6N0ON0RF20140609

June 12, 2014

P.F. CHANG’S CONFIRMS CREDIT CARD BREACH:

Nationwide restaurant chain P.F. Chang’s Chinese Bistro on Thursday confirmed news first reported on this blog: That customer credit and debit card data had been stolen in a cybercrime attack on its stores. The company had few additional details to share about the breach, other than to say that it would temporarily be switching to a manual credit card imprinting system for all P.F. Chang’s restaurants in the United States. KrebsOnSecurity, June 12, 2014

http://krebsonsecurity.com/2014/06/p-f-changs-confirms-credit-card-breach/

June 13, 2014

HEARTBLEED & THE LONG TAIL OF VULNERABILITIES:

To this day there are still unpatched systems, still hackers scanning for vulnerable systems, and still cyber criminals using Heartbleed every day to break into companies. DarkReading, June 13, 2014

http://www.darkreading.com/vulnerabilities---threats/heartbleed-and-the-long-tail-of-vulnerabilities/a/d-id/1269653?_mc=RSS_DR_EDT

June 16, 2014

BRITISH SPY AGENCIES ASSERT POWER TO INTERCEPT WEB TRAFFIC:

In a broad legal rationale for collecting information from Internet use by its citizens, the British government has asserted the right to intercept communications that go through services like Facebook, Google and Twitter that are based in the United States or other foreign nations, even if they are between people in Britain. The New York Times, June 16, 2014

http://www.nytimes.com/2014/06/17/business/international/british-spy-agencies-said-to-assert-broad-power-to-intercept-web-traffic.html?src=rechp

June 17, 2014

IF IT SOUNDS TOO GOOD TO BE TRUE…:

The old adage “If it sounds too good to be true, it probably is” no doubt is doubly so when it comes to steeply discounted brand-name stuff for sale on random Web sites, especially sports jerseys, designer shoes and handbags. A great many stores selling these goods appear to be tied to an elaborate network of phony storefronts and credit card processing sites based out of China that will happily charge your card but deliver nothing (or at best flimsy knockoffs). KrebsOnSecurity, June 17, 2014

http://krebsonsecurity.com/2014/06/if-it-sounds-too-good-to-be-true/

June 20, 2014

OIL CO. WINS $350,000 CYBERHEIST SETTLEMENT:

A California oil company that sued its bank after being robbed of $350,000 in a 2011 cyberheist has won a settlement that effectively reimbursed the firm for the stolen funds. TRC Operating Co. Inc., an oil production firm based in Taft, Calif., had its online accounts hijacked after an account takeover that started late in the day on Friday, November 10, 2011. KrebsOnSecurity, June 20, 2014

http://krebsonsecurity.com/2014/06/oil-co-wins-350000-cyberheist-settlement/

June, 2014

WHY SENIOR LEADERS ARE THE FRONT LINE AGAINST CYBERATTACKS:

All companies are aware of the growing risk of cyberattacks, yet few are taking the steps necessary to protect critical information. The key? Senior managers need to lead. McKinsey&Company, June, 2014

http://www.mckinsey.com//insights/business_technology/why_senior_leaders_are_the_front_line_against_cyberattacks

June 23, 2014

ANONYMOUS HACKERS FOUND ACCESSING VIETNAM MINISTRY COMPUTERS:

Unidentified hackers have launched targeted attacks against computers used by officials of the Vietnamese Ministry of Natural Resources and Environment, an Internet security company said in a report on Friday. tuoitrenews.vn, June 23, 2014

http://tuoitrenews.vn/business/20532/anonymous-hackers-found-accessing-vietnam-ministry-computers

June 25, 2014

COPS NEED A WARRANT TO SEARCH YOUR PHONE, RULES SUPREME COURT:

This term, the Supreme Court sank its teeth into yet another technology privacy issue that divided the country: whether the police can snoop in the smartphone of an arrested person without getting a warrant first. Looking at two cases in California and Massachusetts where photos and call logs from phones helped police bust a gang member for a shooting and a drug dealer, the country's highest court ruled that law enforcement should have gotten warrants before trawling through the contents of their phones. Forbes, June 25, 2014

http://www.forbes.com/sites/kashmirhill/2014/06/25/cops-cant-search-phones-without-a-warrant-rules-supreme-court/

June 26, 2014

DECADES-OLD VULNERABILITY THREATENS 'INTERNET OF THINGS':

A newly discovered bug in the pervasive LZO algorithm has generated a wave of patching of open-source tools such as the Linux kernel this week. A 20-year-old bug has been discovered in a version of a popular compression algorithm used in the Linux kernel, several open-source libraries, and some Samsung Android mobile devices. Dark Reading, June 26, 2014

http://www.darkreading.com/decades-old-vulnerability-threatens-internet-of-things/d/d-id/1278903?_mc=RSS_DR_EDT

June 26, 2014

CHINA CYBER CRIME COOPERATION STALLS AFTER U.S. HACKING CHARGES:

Fledging cooperation between the United States and China on fighting cyber crime has ground to a halt since the recent U.S. indictment of Chinese military officials on hacking charges, a senior U.S. security official said on Thursday. Yahoo News, June 26, 2014

https://news.yahoo.com/china-cyber-crime-cooperation-stalls-u-hacking-charges-205230325--finance.html

June 26, 2014

ANDROID MALWARE TARGETS SOUTH KOREAN ONLINE BANKING CUSTOMERS:

Malicious software that swaps itself for legitimate online banking applications is striking users in South Korea, with thousands of devices infected in the last week, according to a Chinese mobile security company. PCWorld, June 26, 2014

http://www.pcworld.com/article/2401480/android-malware-targets-south-korean-online-banking-customers.html

CENAA

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