CENAA CYBER SECURITY

Newsletter

February 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.

February 1, 2014

MALICIOUS JAVA APP INFECTS MAC, LINUX SYSTEMS WITH DDOS BOT:

Criminals are once again using Java's cross-platform design to add Linux and Mac users to their usual Windows target list, Kaspersky Labs researchers have discovered. The malicious Java application recently unearthed by the firm, HEUR:Backdoor.Java.Agent.a, is only the latest example of the opportunistic trend to use the huge potential of Java to get a malware three-for-one in the cause of turning systems into Distribued Denial of Service bots. PC World, February 1, 2014

http://www.pcworld.com/article/2092414/malicious-java-app-infects-mac-linux-systems-with-ddos-bot.html

February 6, 2014

SUSAN TOMPOR: DID YOUR CELL PHONE RING JUST ONCE? DO NOT CALL BACK:

If you see a missed cell phone call from an unknown number and call them back, hold on to your wallet before you get taken by yet another scam. Detroit Free Press, February 6, 2014

http://www.freep.com/apps/pbcs.dll/article?AID=2014302060028

February 6, 2014

MICROSOFT TAKES TO THE FRONT LINES IN THE WAR ON CYBERCRIME:

The global cost of cybercrime in 2013 was estimated by McAfee to be upwards of $300 billion. One in five small businesses have now been on the receiving end of an attack and every day one million more individuals become victims of cyber-criminal activity. The internet is under attack, and we are the targets. Stepping up to fight the cyber war, Microsoft unveiled a new state of the art Cybercrime Center specifically designed to battle botnets, malware and other various forms of internet crime. Inside its new headquarters, Microsoft's Digital Crimes Unit (DCU) is actively disrupting some of the most serious cybercrime threats currently facing modern society. This crack team of international technical and legal experts are working around the clock with the express aim of making the internet a safer place, and not without some success. Entrepreneur, February 6, 2014

http://www.entrepreneur.com/article/231298

February 7, 2014

N.S.A. PROGRAM GATHERS DATA ON A THIRD OF NATION'S CALLS, OFFICIALS SAY:

The National Security Agency's once-secret program that is collecting bulk records of Americans' domestic phone calls is taking in a relatively small portion of the total volume of such calls each day, officials familiar with the program said on Friday. The New York Times, February 7, 2014

http://www.nytimes.com/2014/02/08/us/politics/nsa-program-gathers-data-on-a-third-of-nations-calls-officials-say.html?hp

February 9, 2014

EXPERTS WARN OF COMING WAVE OF SERIOUS CYBERCRIME:

The rash of attacks against Target and other top retailers is likely to be the leading edge of a wave of serious cybercrime, as hackers become increasingly skilled at breaching the nation's antiquated payment systems, experts say. Washington Post, February 9, 2014

http://www.washingtonpost.com/business/economy/target-breach-could-represent-leading-edge-of-wave-of-serious-cybercrime/2014/02/09/dc8ea02c-8daa-11e3-833c-33098f9e5267_story.html

February 11, 2014

UNVEILING 'THE MASK': SOPHISTICATED MALWARE RAN RAMPANT FOR 7 YEARS:

A cyberespionage operation that used highly sophisticated multi-platform malware went undetected for more than five years and compromised computers belonging to hundreds of government and private organizations in more than 30 countries. PC World, February 11, 2014

http://www.pcworld.com/article/2096460/cyberespionage-operation-the-mask-compromised-organizations-in-30plus-countries.html

February 13, 2014

HACKERS CIRCULATE THOUSANDS OF FTP CREDENTIALS, NEW YORK TIMES AMONG THOSE HIT:

Hackers are circulating credentials for thousands of FTP sites and appear to have compromised file transfer servers at The New York Times and other organizations, according to a security expert. PC World, February 13, 2014

http://www.pcworld.com/article/2098020/hackers-circulate-thousands-of-ftp-credentials-new-york-times-among-those-hit.html

February 13, 2014

BIZARRE ATTACK INFECTS LINKSYS ROUTERS WITH SELF-REPLICATING MALWARE:

Researchers say they have uncovered an ongoing attack that infects home and small-office wireless routers from Linksys with self-replicating malware, most likely by exploiting a code-execution vulnerability in the device firmware. Johannes B. Ullrich, CTO of the Sans Institute, told Ars he has been able to confirm that the malicious worm has infected around 1,000 Linksys E1000, E1200, and E2400 routers, although the actual number of hijacked devices worldwide could be much higher. ars technica, February 13, 2014

http://arstechnica.com/security/2014/02/bizarre-attack-infects-linksys-routers-with-self-replicating-malware/

February 13, 2014

CERTIFICATES SPOOFING GOOGLE, FACEBOOK, GODADDY COULD TRICK MOBILE USERS:

Dozens of phony SSL certificates were discovered this week mocking legitimate certs from banks, e-commerce sites, ISPs and social networks. If a user stumbled over one of the bogus certificates on a mobile device it could put them at risk for a man-in-the-middle attack. ThreatPost, February 13, 2014

http://threatpost.com/certificates-spoofing-google-facebook-godaddy-could-trick-mobile-users/104259

February 13, 2014

FACEBOOK DEAL ON PRIVACY IS UNDER ATTACK:

Despite a class-action settlement in August that was supposed to ensure that Facebook users clearly consent to their comments, images and "likes" being used in ads, it has been business as usual on the service. The New York Times, February 13, 2014

http://www.nytimes.com/2014/02/13/technology/facebook-deal-on-privacy-is-under-attack.html?src=rechp

February 15, 2014

KICKSTARTER HACKED, USER DATA STOLEN:

The crowd-funding site says hackers broke into its systems and made off with data. Apparently credit card numbers escaped the attack. Cnet, February 15, 2014

http://news.cnet.com/8301-1009_3-57618976-83/kickstarter-hacked-user-data-stolen/

February 18, 2014

70 PERCENT OF ANDROID DEVICES EXPOSED FOR 93 WEEKS TO SIMPLE ATTACK:

Android devices prior to version 4.2.1 of the operating system—70 percent of the phones and tablets in circulation—have been vulnerable to a serious and simple remote code execution vulnerability in the Android browser for more than 93 weeks. ThreatPost, February 18, 2014

http://threatpost.com/70-percent-of-android-devices-exposed-for-93-weeks-to-simple-attack/104359

February 19, 2014

FIRE SALE ON CARDS STOLEN IN TARGET BREACH:

Last year's breach at Target Corp. flooded underground markets with millions of stolen credit and debit cards. In the days surrounding the breach disclosure, the cards carried unusually high price tags — in large part because few banks had gotten around to canceling any of them yet. Today, two months after the breach, the number of unsold stolen cards that haven't been cancelled by issuing banks is rapidly shrinking, forcing the miscreants behind this historic heist to unload huge volumes of cards onto underground markets and at cut-rate prices. KrebsOnSecurity, February 19, 2014

http://krebsonsecurity.com/2014/02/fire-sale-on-cards-stolen-in-target-breach/

February 20, 2014

ADOBE, MICROSOFT PUSH FIXES FOR 0-DAY THREATS:

For the second time this month, Adobe has issued an emergency software update to fix a critical security flaw in its Flash Player software that attackers are already exploiting. Separately, Microsoft released a stopgap fix to address a critical bug in Internet Explorer versions 9 and 10 that is actively being exploited in the wild. KrebsOnSecurity, February 20, 2014

http://krebsonsecurity.com/2014/02/adobe-microsoft-push-fixes-for-0-day-threats/

February 25, 2014

NEW YORK CITY MAKES ROOM FOR BREATHER:

a startup offering a mobile app that lets users rent private rooms on demand, is looking to break ground in New York City.The Canadian company said Tuesday that it had launched in the Big Apple, after going live in Montreal last year. Breather's service operates almost like Airbnb, but with a short-term twist focused around work. CIO, February 25, 2014

http://www.cio.com/article/748761/New_York_City_Makes_Room_for_Breather

January 27, 2014

THE YEAR AHEAD IN PRIVACY AND DATA SECURITY:

2014 promises to be another eventful year in the privacy and data security fields. Although predictions are necessarily risky, there is little sign that the revelations regarding government surveillance will cease, that cyber criminals and insiders will stop hacking into personal and proprietary data and that the FTC and other regulatory authorities will stop focusing on companies' privacy and security policies and practices. [Author Tim Toohey is a member of ISSA-LA Community Outreach Advisory Board.] Morris, Pollich & Purdy, February 27, 2014

http://www.mpplaw.com//files//upload/The-Year-Ahead-in-Privacy-and-Data-Security-2014-TJT.pdf

February 27, 2014

CLOUD SECURITY CONCERNS ARE OVERBLOWN, EXPERTS SAY:

Security concerns should not deter enterprises from using public cloud technologies when it makes business sense.

http://www.cio.com/article/748863/Cloud_Security_Concerns_Are_Overblown_Experts_Say

CENAA

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