CENAA CYBER SECURITY

Newsletter

January 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.

January 1, 2014

SNAPCHAT, SKYPE HAVE SECURITY BREACH:

Several million Snapchat usernames and phone numbers were apparently leaked online late Tuesday night. Several outlets including The Verge reported that 4.6 million usernames and phone numbers were posted as a downloadable database by so-far anonymous hackers. The site where the database was posted appeared to be down on Wednesday morning. USA Today, January 1, 2014

http://www.usatoday.com/story/tech/2014/01/01/snapchat-usernames-leak/4277789/

January 2, 2014

WERE YOUR DETAILS LEAKED IN THE SNAPCHAT HACK?:

Security researchers have created a tool to help worried Snapchat users find out if their details were released online by hackers as part of an attack affecting 4.6 million people, as the temporary messaging company works with US law enforcement to find culprits. The Telegraph, January 2, 2014

http://www.telegraph.co.uk/technology/internet-security/10547145/Were-your-details-leaked-in-the-Snapchat-hack.html

January 6, 2014

MALWARE ATTACK HITS THOUSANDS OF YAHOO USERS PER HOUR:

A malware attack hit Yahoo's advertising server over the last few days, affecting thousands of users in various countries, an Internet security company said. In a blog post, Fox-IT said Yahoo's servers were releasing an "exploit kit" that exploited vulnerabilities in Java and installed malware. CNN, January 6, 2014

http://edition.cnn.com/2014/01/05/tech/yahoo-malware-attack/?hpt=hp_t2

January 7, 2014

USING PSYCHOLOGY TO CREATE A BETTER MALWARE WARNING:

It turns out the best way to get people to pay attention to those malware warnings that pop up in browsers may be to stop tweaking them, scrap them entirely and rebuild from scratch. According to a study on the subject published last week, efficient malware warnings shouldn't scare users away, they should give a clear and concise idea of what is happening and how much risk users are exposing themselves to. ThreatPost, January 7, 2014

http://threatpost.com/using-psychology-to-create-a-better-malware-warning/103459

January 8, 2014

LINKEDIN SUES UNKNOWN HACKERS IN AN ATTEMPT TO FIND OUT WHO THEY ARE:

LinkedIn (LNKD) is facing a common plague of social networking companies: thousands of fake accounts used for spam and other nefariousness. So the company is using an increasingly familiar tactic: It's suing those responsible for setting up the fake accounts, even though it doesn't know who they are. Bloomberg, January 8, 2014

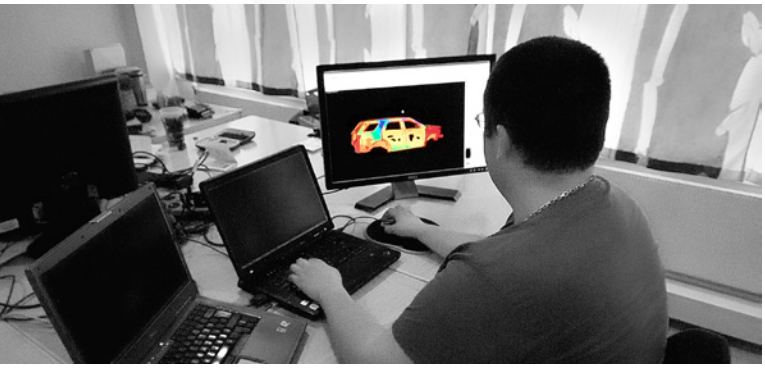
http://www.businessweek.com/articles/2014-01-08/linkedin-sues-unknown-hackers-in-an-attempt-to-find-out-who-they-are

January 10, 2014

THE NEXT DATA PRIVACY BATTLE MAY BE WAGED INSIDE YOUR CAR:

Cars are becoming smarter than ever, with global positioning systems, Internet connections, data recorders and high-definition cameras. Drivers can barely make a left turn, put on their seatbelts or push 80 miles an hour without their actions somehow, somewhere being tracked or recorded. The New York Times, January 10, 2014

http://www.nytimes.com/2014/01/11/business/the-next-privacy-battle-may-be-waged-inside-your-car.html?_r=2



January 11, 2014

YAHOO SAYS MALWARE ATTACK FARTHER REACHING THAN THOUGHT:

The company posts guidelines for Yahoo users worried about infection and says people outside Europe may have been hit. It also says the attacks went on longer than previously reported. CNet, January 11, 2014

http://news.cnet.com/8301-1009_3-57617082-83/yahoo-says-malware-attack-farther-reaching-than-thought/

January 14, 2014

RESEARCHERS FIND BEST TIME FOR HACKERS TO STRIKE:

For hackers, timing is key. At least that's according to a group of University of Michigan based researchers that authored a paper on hacking and how timing could factor into the decisions and decision making processes engaged in by cyber criminals. Digital Trends, January 14, 2014

http://www.digitaltrends.com/computing/researchers-find-best-time-hackers-strike-exploit-malware/

January 17, 2014

IS YOUR REFRIGERATOR REALLY PART OF A MASSIVE SPAM-SENDING BOTNET?:

Security researchers have published a report that Ars is having a tough time swallowing, despite considerable effort chewing—a botnet of more than 100,000 smart TVs, home networking routers, and other Internet-connected consumer devices that recently took part in sending 750,000 malicious e-mails over a two-week period. Ars-Technica, January 17, 2014

http://arstechnica.com/security/2014/01/is-your-refrigerator-really-part-of-a-massive-spam-sending-botnet/

January 17, 2014

A SNEAKY PATH INTO TARGET CUSTOMERS' WALLETS:

It was, in essence, a cybercriminal's dream. For months, an amorphous group of Eastern European hackers had been poking around the networks of major American retailers, searching for loose portals that would take them deep into corporate systems. The New York Times, January 17, 2014

http://www.nytimes.com/2014/01/18/business/a-sneaky-path-into-target-customers-wallets.html?hp

January 20, 2014

ANDROID VULNERABILITY ENABLES VPN BYPASS:

A vulnerability in the Android mobile operating system could allow hackers to write applications that would bypass a secure virtual private network connection and redirect traffic in clear text to an attacker. ThreatPost, January 20, 2014

http://threatpost.com/android-vulnerability-enables-vpn-bypass/103719

January 22, 2014

GANG RIGGED PUMPS WITH BLUETOOTH SKIMMERS:

Authorities in New York on Tuesday announced the indictment of thirteen men accused of running a multi-million dollar fraud ring that allegedly installed Bluetooth-enabled wireless gas pump skimmers at filling stations throughout the southern United States. KrebsOnSecurity, January 22, 2014

http://krebsonsecurity.com/2014/01/gang-rigged-pumps-with-bluetooth-skimmers/

January 2014

RISK AND RESPONSIBILITY IN A HYPERCONNECTED WORLD: IMPLICATIONS FOR ENTERPRISES:

For the world's economy to get full value from technological innovation, it must have a robust, coordinated approach to cybersecurity. A new report from the World Economic Forum and McKinsey & Company looks at how that could happen. Mckinsey&Company, January 2014

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

January 24, 2014

FEDS INFILTRATE, BUST COUNTERFEIT CARD SHOP:

Federal authorities in New Jersey announced a series of arrests and indictments of 14 individuals thought to be connected to an online one-stop shop selling embossed, counterfeit credit cards and holographic overlays. KrebsOnSecurity, January 24, 2014

http://krebsonsecurity.com/2014/01/feds-infiltrate-bust-counterfeit-card-shop/

January 27-28, 2014

JOIN OWASP LOS ANGELES, ORANGE COUNTY, SAN DIEGO, SANTA BARBARA, AND THE BAY AREA AS WE JOIN FORCES TO HOST APPSEC CALIFORNIA!:

AppSec California is the first of hopefully many annual conferences hosted by all of the California chapters. AppleSec California, Event Date: January 27-28, 2014

https://appseccalifornia.org/

January 28, 2014

FEDS TO CHARGE ALLEGED SPYEYE TROJAN AUTHOR:

Federal authorities in Atlanta today are expected to announce the arrest and charging of a 24-year-old Russian man who allegedly created and maintained the SpyEye Trojan, a sophisticated botnet creation kit that has been implicated in a number of costly online banking thefts against businesses and consumers. KrebsOnSecurity, January 28, 2014

http://krebsonsecurity.com/2014/01/feds-to-charge-alleged-spyeye-trojan-author/

January 30, 2014

RESEARCHER WARNS OF CRITICAL FLAWS IN ORACLE SERVERS:

There are two vulnerabilities in some of Oracle's older database packages that allow an attacker to access a remote server without a password and even view the server's filesystem and dump arbitrary files. Oracle has not released a patch for one of the flaws, even though it was reported by a researcher more than two years ago, and the researcher said the potential attack scenarios are frightening. TreathPost, January 30, 2014

http://threatpost.com/researcher-warns-of-critical-flaws-in-oracle-servers/103961

CENAA

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

prepared by Veronika Macková, designed by kracik.sk