CYBER SECURITY

Newsletter

Summer 2013

Aim of the long-term CENAA program Global Netizenship in Cyber World (GNC) is in-depth analysis of multispectral and cross-cutting issues of national and international cybersecurity. In last years, cyberattacks 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 cybersecurity will get into focal point of political, corporate and expert elites. Goal of this Newsletter and GNC project is also de-tabuise issue of cybersecurity to all.

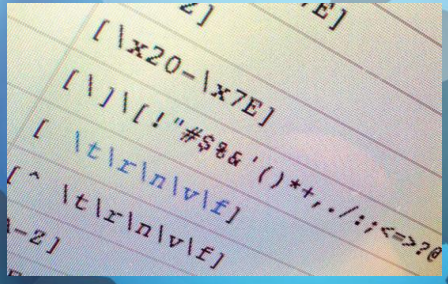
Tougher cybercrime and snooping sentences coming to EU: EU lawmakers agreed on tuffer criminal penalties across the EU for cyber attacks- especially those that include harming critical national infrastructure or hijacking computers to steal sensitive data. *NBCnews, July 4, 2013.*

More: http://www.nbcnews.com/technology/tougher-cybercrime-snooping-sentences-coming-eu-6C10543908

Financial Industry Is Serious About Cybersecurity: For the past few years the financial industry (private or state one) has been under a constant attack of hackers. So far the industry has managed to protect its client, however hackers are adapting more quicker than everyone has expected. "My trade group, the Securities Industry and Financial Markets Association, is organizing an industry wide exercise called "Quantum Dawn 2" on July 18. This exercise will simulate a cyber-attack on the U.S. financial system. It will force individual companies to test their response plans in order to maintain effective and orderly markets and protect client data." *Bloomberg, July 5, 2013.*

More: http://www.bloomberg.com/news/2013-07-04/financial-industry-is-serious-about-cybersecurity. html

One big threat to cybersecurity: IT geeks can't talk to management: A new report on the state of risk-based cybersecurity management helps explain why IT employees and their corporate bosses don't see eye to eye about hacking and other computer-based threats. *Quartz, July 15, 2013.*
More: http://qz.com/103907/one-big-threat-to-cybersecurity-it-guys-cant-talk-to-management/



Merkel Urges Europe to Tighten Internet Safeguards: Angela Merkel is requesting the EU to adopt a new legislation where Internet companies have to disclose what information about users they store and to whom they provide it. This is the response on the current case "E.J.Snowden". "That has to be part of such a data privacy agreement because we have great regulation for Germany, but if Facebook is registered in Ireland, then it falls under Irish jurisdiction," she said. "Consequently we need a common European agreement." *NY Times, July 15, 2013.*

More: http://www.nytimes.com/2013/07/16/world/europe/merkel-urges-europe-to-tighten-internet-safeguards.html?pagewanted=all&_r=0

South Korea Blames North for June Cyberattacks: 69 Web sites were paralyzed, probably by North Korea. South Korean investigators found similarities in the previous attack on broadcasters and banks earlier this year. In the June attacks was "Anonymous" blamed for the responsibility of the fallen systems and websites. However on Tuesday, "the South Korean ministry said the North probably used the "Anonymous" identity to create confusion about the source of the attacks." So far the June attacks are the latest in a series of cyber-attacks where South Korea blamed North. "The attacks on South Korean targets were actually the conclusion of a covert espionage campaign," said McAfee. Besides this, McAfee did not blame North Korea by name. It also added that the "overall tactics were not that sophisticated in comparison to what we have seen before." *NY Times, July 16, 2013.*

More: http://www.nytimes.com/2013/07/17/world/asia/south-korea-blames-north-for-june-cyberattacks.html

Cisco Research on Targeted Phishing Attacks: The research from Cisco points out, cybercriminal business models have shifted toward low-volume targeted attacks. The report, Email Attacks - This Time Its Personal, documents that email remains the primary attack vector, the annualized email attacks has declined by more than half. As the research points out, the volume of mass attacks has declined, but the the ability of cybercriminal to use targeted phishing campaigns has increased. Organizations have to bear the burden of not only the monetary loss but also the cost of re-mediating infected hosts and the negative impact on their brand reputation. Business cannot ignore the risk from this threat vector. *NetWorkedBlogs, July 23, 2013.*

More: http://networkedblogs.com/NqxZ2

Android Trojan Banking App Targets Master Key: Vulnerability: Security researchers have spotted a legitimate banking app for Android smartphones and tablets that has been "trojanized" using the so-called master key vulnerability. That flaw, which affects all versions of Android prior to version 4.2.2, can be used by attackers to inject malicious code into a digitally signed, legitimate Android app. The trojanized banking app isn't the first known attempt to exploit the master key vulnerability for malicious purposes. That accolade goes to a legitimate app used for making a doctor's appointments in China, for which Symantec reported finding trojanized versions two weeks ago. In that case, the attacker behind the revamped app had added code that allowed the device to be remotely controlled, and which could siphon the phone's international mobile equipment identity (IMEI) number and phone numbers stored on the device, as well as dial premium-rate numbers, thus draining the smartphone user's account and enriching attackers. *InformationWeekSecurity, August 6, 2013*.

More: http://www.informationweek.com/security/vulnerabilities/android-trojan-banking-app-targets-maste/240159509

A Travel-Hack Mystery: How Can You Redeem Stolen Airline Miles?: Hackers love credit card numbers, sure, but frequent flier miles? US Airways (LCC) is notifying some members of its Dividend Miles loyalty program that miles have been stolen from some 7,700 compromised accounts. The breach was discovered on July 12, the airline said in a regulatory filing mandated under a North Carolina identity-protection law. US Airways's largest hub is in Charlotte. *Bloomberg, August 9, 2013.*

More: http://mobile.businessweek.com/articles/2013-08-09/a-travel-hack-mystery-how-can-you-redeem-stolen-airline-miles

Cracking Crypto Just Got a Little Easier: Starting with the Black Hat conference, researchers, engineers and hackers have been unveiling new weaknesses and attacks in different cryptographic implementations that threaten the security of communication and commerce on the Web. Not only have holes been shot in SSL over and over for years, but recently experts tried to put a prognosis on the lifespan of the RSA algorithm, which was met with some skepticism. *ThreatPost, August 16, 2013.*

More: http://threatpost.com/cracking-crypto-just-got-a-little-easier

Washington Post Site Hacked After Successful Phishing Campaign: The Washington Post acknowledged today that a sophisticated phishing attack against its newsroom reporters led to the hacking of its Web site, which was seeded with code that redirected readers to the Web site of the Syrian Electronic Army hacker group. According to information obtained by KrebsOnSecurity, the hack began with a phishing campaign launched over the weekend that ultimately hooked one of the paper's lead sports writers. On Tuesday morning, KrebsOnSecurity obtained information indicating that a phishing campaign targeting the Post's newsroom had been successful, and that the attackers appear to have been seeking email access to Post reporters who had Twitter accounts. *KrebsOnSecurity, August 15, 2013.*

More: https://krebsonsecurity.com/2013/08/washington-post-site-hacked-after-successful-phishing-campaign/

Syrian Electronic Army hacks Washington Post Web site: The Washington Post's Web site was disrupted Thursday morning by a hacker group sympathetic to Syrian President Bashar al-Assad that apparently launched a coordinated wave of attacks on American news outlets. A group calling itself the Syrian Electronic Army briefly succeeded in redirecting readers of some articles on washingtonpost.com to the SEA's own site. The organization supports Assad, who has led a long, bloody campaign to crush a rebellion in Syria. The intrusion lasted about 30 minutes and affected a number of foreign-news articles. "We've taken defensive measures, and at this time there are no other issues affecting the site," said Emilio Garcia- Ruiz, The Post's managing editor for digital. *The Washington Post, August 25, 2013.*

More: http://articles.washingtonpost.com/2013-08-15/lifestyle/41412289_1_electronic-army-human-rights-watch-hackers

Spy Service Exposes Nigerian 'Yahoo Boys': A crude but effective online service that lets users deploy keystroke logging malware and then view the stolen data remotely was hacked recently. The information leaked from that service has revealed a network of several thousand Nigerian email scammers and offers a fascinating glimpse into an entire underground economy that is seldom explored. *KrebsOnSecurity, September 9, 2013.*

More: http://krebsonsecurity.com/2013/09/spy-service-exposes-nigerian-yahoo-boys/

Internet Census 2012 Data: Million of devices Vulnerable by Default: Embedded device manufacturers have, been warned for ages about the risks of making networking telecom and critical infrastructure reachable, worse yet, leaving default credentials in place for authenticating to those devices. *ThreatPost, September 13, 2013.*

More: http://threatpost.com/internet-census-2012-data-millions-of-devices-vulnerable-by-default

WHOIS Privacy Plan Draws Fire: Internet regulators are pushing a controversial plan to restrict public access to WHOIS Web site registration records. Proponents of the proposal say it would improve the accuracy of WHOIS data and better protect the privacy of people who register domain names. *KrebsOnSecurity, September 16, 2013.*

More: http://krebsonsecurity.com/2013/09/whois-privacy-plan-draws-fire/

CENAA

Tolstého 9

811 06 Bratislava