CYBER SECURITY

Newsletter

November 2013

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.

November 4, 2013

HACKERS TAKE LIMO SERVICE FIRM FOR A RIDE:

A hacker break in at a U.S. company that brokers reservations for limousine and Town Car services nationwide has exposed the personal and financial information on more than 850,000 well-heeled customers, including Fortune 500 CEOs, lawmakers, and A-list celebrities. The high-value data cache was found on the same servers where hackers stashed information stolen from PR Newswire, as well as huge troves of source code data lifted from Adobe Systems Inc. — suggesting that the same attacker(s) may have been involved in all three compromises. KrebsOnSecurity, November 4, 2013

http://krebsonsecurity.com/2013/11/hackers-take-limo-service-firm-for-a-ride/

November 6, 2013

CRYPTOLOCKER CREW RATCHETS UP THE RANSOM:

Last week's article about how to prevent CryptoLocker ransomware attacks generated quite a bit of feedback and lots of questions from readers. For some answers — and since the malware itself has morphed significantly in just a few day's time — I turned to Lawrence Abrams and his online help forum BleepingComputer.com, which have been following and warning about this scourge for several months. KrebsOnSecurity, November 6, 2013

http://krebsonsecurity.com/2013/11/cryptolocker-crew-ratchets-up-the-ransom/

November 8, 2013

CYBERCRIME'S BOTTOM LINE: $500 BILLION:

No one knows the true cost of cybercrime. Annual loss estimates for U.S. corporations range from $70-140 billion in a recent report from the Center for Strategic and International Studies (CSIS) to $400 billion quoted by U.S. House of Representatives Intelligence Committee leaders who introduced the Rogers-Ruppersberger Cybersecurity Bill. USA TODAY, November 8, 2013

http://www.usatoday.com/story/cybertruth/2013/11/08/cybercrimes-bottom-line-500-billion/3478235/

November 11, 2013

RUSSIAN DRAFT UN RESOLUION ON INFORMATION SECURITY WINNING SUPPORT THANKS TO SNOWDEN:

A Russian-proposed draft UN resolution calling for an international code of conduct for information security is beginning to win support as Washington loses moral authority in the wake of Edward Snowden's revelations. The Voice of Russia, November 11, 2013

http://voiceofrussia.com/news/2013_11_11/Russian-draft-UN-resoluion-on-information-security-winning-support-thanks-to-Snowden-4469/

November 13, 2013

NOW, YOUR REWARD FOR BEING A LOYAL CUSTOMER:

Identity Theft: They signed up to receive discounts on vacation travel and other perks. Instead, more than 1.5 million Europeans who had enrolled in customer-loyalty programs learned this week that their personal data, including credit-card details in some instances, had been stolen in a cyber attack on an Irish company they'd never heard of. BusinessWeek, November 13, 2013.

http://www.businessweek.com/articles/2013-11-13/now-your-reward-for-being-a-loyal-customer-identity-theft

November 15, 2013

ANONYMOUS-LINKED HACKERS ACCESSED U.S. GOVERNMENT COMPUTERS, FBI REPORTEDLY WARNS:

Activist hackers linked to the collective known as Anonymous have secretly accessed U.S. government computers in multiple agencies and stolen sensitive information in a campaign that began almost a year ago, the FBI warned this week. Huffington Post, November 15, 2013

http://www.huffingtonpost.com/2013/11/16/anonymous-hackers_n_4284799.html

November 17, 2013

MASSIVE CYBERCRIME CASE UNFOLDING IN LAS VEGAS:

The Carder.su organization was about as big as any criminal syndicate could get until an undercover Las Vegas federal agent put a crimp in its worldwide operations. Las Vegas Review-Journal, November 17, 2013

http://www.reviewjournal.com/news/massive-cybercrime-case-unfolding-las-vegas

November 18, 2013

SIX ARRESTED IN $45 MILLION GLOBAL CYBERCRIME SCHEME:

Six people were arrested and charged on Monday for participating in a worldwide ATM heist that stole $45 million from two Middle East banks. Reuters, November 18, 2013

http://www.reuters.com/article/2013/11/18/us-usa-crime-cybercrime-idUSBRE9AH0YZ20131118

November 19, 2013

U.S.-FUNDED RADIO FREE EUROPE/RADIO LIBERTY SAYS ITS NEWS SERVICES HAVE BEEN DISRUPTED BY A CYBERATTACK.

The Prague-based broadcaster says the intermittent cyberwarfare began Thursday. It says the attackers have been using a distributed denial of service attack that floods the computer servers with fake traffic from numerous computers infected with malware. It did not elaborate.The network experienced a similar but more limited attack in 2008.It says other similar U.S. media, including the Voice of America, Middle East Broadcasting, and the Office of Cuban Broadcasting services have also been affected by the attack. ABC News, November 19, 2013

http://abcnews.go.com/International/wireStory/us-funded-radio-faces-cyber-attack-20932857

November 20, 2013

ISSA-LA NOVEMBER LUNCH MEETING:

Topic: In today's world of advanced cyber threats, security professionals need to implement new methods and strategies to gain the upper hand in protecting their business. Thinking like an attacker isn't really good enough. However, incorporating hacker methodologies & tools will give security teams the situational awareness and intelligence needed to respond quickly to new & previously unknown threats. The security industry is changing. For some, it's a good thing, and for others, they're watching their antiquated ways of failing to prevent exploits become irrelevant for smart security teams. ISSA-LA, Event Date: November 20, 2013

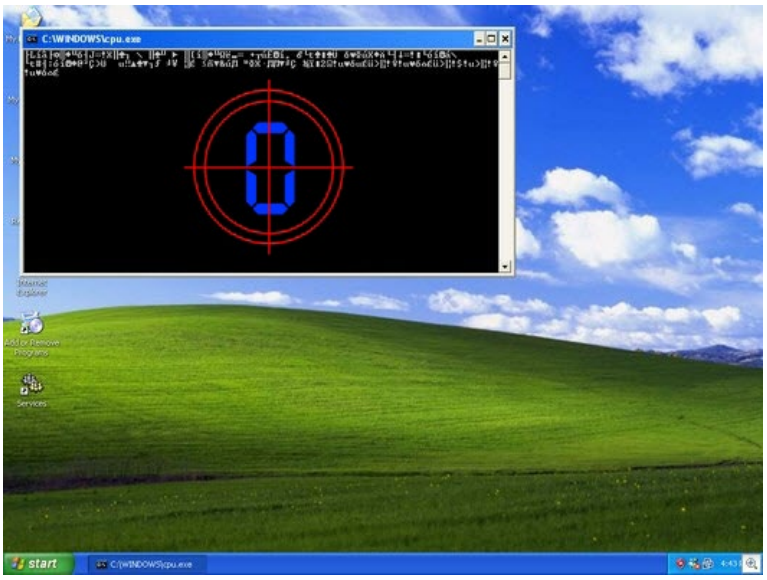
http://www.issala.org/event/issa-la-november-lunch-meeting/

November 26, 2013

POTENTIAL FOR ABUSE STALLS CELLPHONE KILL SWITCH DEBATE

Kill switches in cellphones might be a theft deterrent, but they might also invite other types of crime that could have grim consequences -- for example, disabling the phones of government officials. That's the argument carriers are making against installing the switches, at any rate, although cynics are inclined to think their objections are more about revenue loss. TechNewsWorld, November 26, 2013

http://www.technewsworld.com/story/79514.html



November 29, 2013

USERS WARNED OF WINDOWS XP ZERO-DAY EXPLOIT HACKERS COULD GAIN ACCESS TO DATA AND INSTALL MALWARE.

Microsoft has warned that a recently-discovered bug in Windows XP could allow hackers to run code in the system's kernel from a standard user account . The bug also appears to affect Windows Server 2003.

According to Trend Micro security researcher Gelo Abendan, such attacks have already been spotted in the wild. In a blog post, Abendan said Trend Micro researchers had managed to obtain samples of the flaw and that the exploit took advantage of "elevation of privilege vulnerability". This then allowed hackers to delete or view data, install programs, or create accounts with administrative privileges. IT PRO, November 29, 2013

http://www.itpro.co.uk/security/21130/users-warned-of-windows-xp-zero-day-exploit

CENAA

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