

Global Cyber Bi-Weekly Report by INSS December 1, 2016

Editor-in-chief: Gabi Siboni, Editor: Hadas Klein; Contributors: Jeremy Makowski, Simon Tsipis, Gal Perl Finkel, Ido Sivan, Paola Aurucci

ISRAEL

Channel 2 and 10 newscasts temporarily disrupted by images of Muslim holy sites and the words “Allah is great”

Newscasts on Israeli Channels 2 and 10 were temporarily disrupted on the evening of November 29, 2016 by hackers suspected to be pro-Palestinian Arab activists. The disruption only affected the broadcasts streamed from an open satellite link, and subscribers to Israel's YES satellite television were not affected. Israel's broadcasting authority said in response that “this is a hostile takeover of the satellite carrying the broadcast. We view this with the utmost severity and consider an act of sabotage.” It added it was working with law enforcement officials and the defense establishment to investigate the incident.

<http://bit.ly/2gHtosX>

Ben-Gurion University of the Negev cyber researchers demonstrate malware that covertly turns PCs into eavesdropping devices

Researchers at Ben-Gurion University of the Negev have demonstrated malware that can turn computers into perpetual eavesdropping devices, even without a microphone. In the article, “SPEAKE(a)R: Turn Speakers to Microphones for Fun and Profit,” the researchers explain and demonstrate how most PCs and laptops today are susceptible to this type of attack. Using SPEAKE(a)R, malware that can covertly transform headphones into a pair of microphones, they show how commonly used technology can be exploited. “The fact that headphones, earphones, and speakers are physically built like microphones and that an audio port's role in the PC can be reprogrammed from output to input creates a vulnerability that can be abused by hackers,” said Professor Yuval Elovici, director of the BGU Cyber Security Research

Center (CSRC) and a member of BGU's Department of Software and Information Systems Engineering.

<http://bit.ly/2gwjee9>

UNITED STATES

Trump cyber security team, policy slow to take shape

President-elect Donald Trump's transition team has not yet announced a point person dedicated to cyber security policy or staffing in his administration. This omission could make the United States more vulnerable to threats and worsen the government's cyber security shortfall, said current and former national security officials.

<http://reut.rs/2fxaBze>

US statement on reliability of election results

The US federal government did not observe any increased level of malicious cyber activity aimed at disrupting electoral process on election day, claimed a senior administration official, to the New York Times in response to questions about the federal government's investigation into the integrity of the November 8 elections.

<http://nyti.ms/2fUZrEy>

EUROPE

The EU and NATO to discuss closer cooperation on cyber defense

A week ago, the European Union and NATO met to discuss the next practical steps in NATO-EU cooperation on cyber defense. Indeed, both organizations are trying to see how they can strengthen their cooperation to counter the growing cyber threats. According to NATO's Assistant Secretary General for Emerging Security Challenges, Ambassador Sorin Ducaru, "NATO and the EU are working more closely in this area than ever – sharing information between cyber crisis response teams, exchanging best practices, policy updates and working together on training, education, and

exercises.” Additionally, they discussed the progression of the developments of different programs such as NATO’s Cyber Defense Pledge and the implementation of the EU’s Network and Information Security (NIS) Directive. The aim is to increase the exchange of information as well as to organize more common exercises. This cooperation strengthening is one of the key points to counter cyber threats that nations currently face. As they become more sophisticated and persistent, states need to be extra careful regarding their cyber defense.

<http://bit.ly/2fBY1CQ>

Spain is mainly targeted by cyberattacks from foreign governments

A report of the National Cryptology Center (CCN), which is a branch of the Spanish intelligence services, asserts that foreign governments, such as China, Russia, the United States, and Eastern European countries were behind up to 90 percent of the large cyberattacks against Spanish government agencies or strategic companies. The report has shown that Spain faced 19,000 incidents this year, which is a 5 percent rise from 2015. In addition, 3 percent of these incidents were considered by the CCN as highly dangerous or critical. The CCN added that cyberespionage continues to pose a serious threat to its national infrastructure and industry. The CNN claimed that “this threat is particularly aimed at information systems of industrial corporations, defense businesses, high-tech firms, the auto industry, transportation, research institutes, and government agencies.” Spain is also facing cyber propaganda from jihadist who are proffering in Spain. The government needs to increase its cyber defense measures and to strengthen its cooperation with the European Union Agency for Network and Information Security.

<http://bit.ly/2fC0qNX>

RUSSIA

Russian military to connect new Armata Tank to drones with flexible cable

Izvestia newspaper reported that combat vehicle based on the Armata tank platform will be equipped with surveillance drones (UAVs), which will be connected by a

flexible cable. Quoting Vitaly Polanski, a senior researcher at the Moscow Aviation Institute, the new Russian UAV “Pterodactyl” will scan the battle field to provide essential intelligence to the Armata tanks’ team and will be connected by special cable to avoid cyber hacking and system penetration.

<https://ria.ru/arms/20161118/1481622668.html>

FSB to get access to internet traffic for implementing word recognition analysis system

Russian Federal Security Service (FSB), the Ministry of Communications, and the Ministry of Industry are discussing the technical implementation of decrypting all users’ internet traffic to implement a word recognition analysis system. This system would get access to all personal data and trafficking of internet users, critics say. This action comes in light of the Anti-Terrorism Law bill adopted by the Russian assembly

<https://ria.ru/society/20160921/1477533965.html>

Russian government to limit foreign providers’ online video services in Russian Territory

A new bill of regulation of OTT-services operation (video services) has been prepared by the Russian Media and Communications Union (ISS) and was submitted to the Russian assembly for voting. The project prohibits foreigners from providing online movie services in Russia, which exceeds 100,000 viewers daily.

<https://ria.ru/economy/20161126/1482222023.html>

All Russian federal agencies to be connected by unified electronic system

The Russian Prosecutor General’s Office plans to launch by 2022 a unified electronic document management system for law enforcement agencies, which will monitor the movement of all running open cases and affairs. This system will engage nine agencies: The Interior Ministry, the Federal Security Service (FSB), the Investigative Committee, Ministry of Emergency Situations (MChS), Customs, Prosecutor

General's Office, the Judicial Department at the Supreme Court, the Federal Bailiff Service (FSSP), and the Federal Penitentiary Service (FSIN).

<http://bit.ly/2fC3b1m>

MIDDLE EAST

The Middle East is on the verge of massive digital disruption

A recent report published by Digital McKinsey said that in the past decade, the cross-border data flow connecting the Middle East to the world has increased by more than 150 times. Cybersecurity, however, remains the main challenge and has become the top priority of 67 percent of the companies (as opposed to just 47 percent last year).

<http://bit.ly/2gUychn>

ISIS propaganda in cyberspace is one of the biggest threats to the West

According to an expert from the Carnegie Middle East Center, we need a cyber army around the clock to tackle ISIS' cyber propaganda.

<http://bit.ly/2gi6vhf>

CHINA and ASIA PACIFIC

Almost 1,000 percent increase in cyberattacks in China

Cyberattacks against Chinese companies have soared in the past two years. The average number of cyberattacks detected by companies in mainland China and Hong Kong grew 969 percent between 2014 and 2016. The number of attacks averaged more than seven per day for each of the 440 China-based respondents surveyed – around half of the global average of thirteen. According to the survey, the new technologies that connect household items to the internet and allow them to receive and send data are perceived as particularly vulnerable. China's rapid adoption of new consumer and industrial technology of the Internet of Things (IoT) era may be part of the reason for this rise in attacks, even though the average number of attacks fell globally by 30 percent since 2015. The Chinese companies surveyed had cut their

cybersecurity budget by 7.6 percent in 2016, and 34 percent had identified competitors as a source of attack, a rate higher than anywhere else in the world.

<http://nbcnews.to/2g5vlhP>

KISA shares cybersecurity expertise with Gabon

Korea Internet and Security Agency (KISA), announced a joint information security expert training program for Gabon's information security-related policymakers and technical experts, such as the National Agency for Digital Infrastructure and Frequencies (ANINF), the armed forces, military police, national police agency, and immigration service, together with the Ministry of Science, ICT, and Future Planning in Korea. The training program came followed a memorandum of understanding (MOU) on information security between KISA and Gabon's ANINF in November 2015 to share its experience and expertise in operating a cybersecurity response center and responding to cybersecurity incidents.

<http://bit.ly/2gHSSpR>

Pentagon Links Chinese Cyber Security Firm to Beijing Spy Service

Intelligence officials at the Pentagon claim a Chinese cyber security firm is covertly working with Beijing's Ministry of State Security intelligence service in conducting cyber espionage operations. The company, known as Boyusec and officially as the Bo Yu Guangzhou Information Technology Co., is also working with Huawei Technologies, China's global telecommunications company, which has been identified by US intelligence agencies as linked to the Chinese military. An internal report by the Pentagon's Joint Staff J-2 Intelligence Directorate asserts that Boyusec and Huawei are working together to produce security products that will be loaded into Chinese-manufactured computer and telephone equipment, which will allow Chinese intelligence to capture data and control computer and telecommunications equipment. No other details of Boyusec's activities could be learned. The employment of a cyber security firm as cover for intelligence gathering has been used in the past by Russian intelligence, and China appears to be following the same pattern.

<http://bit.ly/2gihW8N>

China's new cybersecurity law raises concerns, but foreign businesses likely will comply

Starting June 2017, China will enact new cybersecurity legislation governing internet use, especially with foreign operators in mind. The new law raises concern among foreign entities, as well as human rights groups, due to the vagueness surrounding some key articles such as what constitutes “technical support” or how security reviews will be carried out. Foreign businesses operation in China are concerned that the new legislation will require them to disclose proprietary data about how their systems work in order to pass inspections. It is not clear if or how this would be accomplished based on the current legislation. Chinese officials have denied that there are any ulterior motives to gain access to the architecture of these databases. The government now says it will be illegal to store or share information elsewhere without going through a review process, and failure to do so would result in service suspensions, among other penalties. As part of a wider crackdown on social media anonymity, the legislation further advances the government's determination to have all accounts registered with real, verifiable biographical data. The government's goal is that telecommunications service providers are required to verify all phone users' identities by the end of 2016.

<http://bit.ly/2gUW6tp>

India faces around 40,000 cybersecurity incidents each year

Information reported to and tracked by the Indian Computer Emergency Response Team (CERT-In), 41,319, 44,679, 49,455. and 39,730 cybersecurity incidents were observed during the years 2013, 2014, 2015. and 2016 respectively. The types of cybersecurity incidents include phishing, scanning/probing, website intrusions and defacements, virus/malicious code, and denial of service attacks. The National Crime Records Bureau (NCRB) data show that a total of 5,693, 9,622, and 11,592 incidents have been registered during 2013, 2014 and 2015 respectively for various cybercrimes under the Information Technology (IT) Act, 2000 and related Indian

Penal Code (IPC) sections. The Ministry of Electronics and Information Technology has also allocated Rs 500 crore in the twelfth five-year-plan (2012-2017) for a cyber security program, including cyber safety, security and surveillance, cybercrime Investigations, and cyber forensics.

<http://bit.ly/2gkdugc>

AFRICA

Kenyan companies lost KES 17.5 Billion to cybercrime in 2016

Kenyan companies have lost KES 17.5 Billion (\$175 Million) to cybercrime in the past year, according to the fourth annual Kenya National Cyber Security Study conducted by Serianu Ltd., the United States International University (USIU) Kenya, and Paladin Networks. This loss signifies an increase of 14 percent, compared to the KES 15 Billion lost in 2015. Organizations, however, have begun to acknowledge the sensitivity of the issue, with 93 percent of Kenyan companies viewing cybersecurity as a problem. The report states that insider threats are the largest contributor to the growth of these cases, and include fraud using information or employee abuse of IT systems and information. It also states that incidents of malware targeting critical mobile and internet banking infrastructure are on the rise. In addition, the number of cases related to mobile money has dramatically increased over the last year, mostly involving social engineering, malware, and account personifications.

E-commerce platforms on the other hand have seen a rise in the number of online fraud, ATM card skimming, and identity theft incidents. Another factor cited as the main cause for these cases is the low level of security awareness within companies and among their employees, where technical training of employees is insufficient. Most Kenyan organizations spend \$5,000 or less on cybersecurity issues while they allow Bring Your Own Device (BYOD) policies at work, which further aggravates the situation.

<http://bit.ly/2fKNVdY>

