Global Cyber Bi-Weekly Report by INSS March 15 2018

Editor-in-chief: Gabi Siboni, **Editor:** Hadas Klein, Gal Perl Finkel

Contributors: Simon Tsipis, Ido Sivan, Sanjana Rathi, Anna Danilova

ISRAEL

How Israel is becoming the world's top cyber superpower

Israel has become a world leader in cybersecurity, and the nation's military is fueling its supremacy. Israel continues to revolutionize its military and lead the way in the field. To start, the Israeli Defense Force recruits the best and brightest coders and hackers as teens, to funnel them into their elite cyber warfare units. "Because going to the service is compulsory, you can look at the Israeli army as the largest HR organization in the world," said Roni Zehavi, the CEO of CyberSpark, a government initiative that serves as an innovation incubator. These elite units are some of the most impressive in the world. Unit 8200, for example, used to be a closely guarded secret because it is believed to be responsible for the STUXNET cyberattack that sabotaged the Iranian nuclear program. The skills these soldiers learn in units like 8200 are extremely profitable in the free market. Former Israeli soldiers have brought their military and technological know-how to the private sector and have created companies that specialize in cyber defense and offense.

http://bit.ly/2ImnnPA

Israeli researchers find cybersecurity flaws in baby monitors, web cameras

Cybersecurity researchers at the Ben-Gurion University of the Negev (BGU) have found serious security issues in devices, such as baby monitors, home security and web cameras, doorbells, and thermostats. The researchers easily hacked these devices as part of their ongoing study to detect the vulnerabilities of the Internet of Things, internet-connected home devices, and networks. By arming ourselves with smart doorbells, personal assistants, smartphones and ever-so-clever baby monitors, we are increasingly exposing

ourselves to the chances of our devices being taken over by criminal minded hackers. "It is truly frightening how easily a criminal, voyeur, or pedophile can take over these devices," said Dr. Yossi Oren, a senior lecturer in BGU's Department of Software and Information Systems Engineering and head of the Implementation Security and Side-Channel Attacks Lab at Cyber@BGU. "Using these devices in our lab, we were able to play loud music through a baby monitor, turn off a thermostat and turn on a camera remotely, much to the concern of our researchers who themselves use these products." "It only took 30 minutes to find passwords for most of the devices and some of them were found merely through a Google search of the brand," said Omer Shwartz, a PhD student and member of Oren's lab. "Once hackers can access an IoT device, like a camera, they can create an entire network of these camera models controlled remotely."
http://bit.ly/2piGFwR

Police Cybercrimes Unit issues warning after cameras hacked at women's apparel shop

A viral Peeping Tom who hacked into the closed-circuit TV surveillance camera at a women's bathing suit shop has led the Israel Police Cybercrimes Unit to warn that similar systems may be compromised, violating the privacy of unsuspecting persons. Israel Police Cybercrimes Unit stated that an unidentified forty-one-year-old man was arrested after he allegedly used his computer to hack into the CCTV system at a boutique in northern Tel Aviv and recorded customers as they undressed and tried on bathing suits. While details of the incident remain unclear due to a gag order, police said the suspect subsequently posted the videos to a social media page. Police Spokesman Micky Rosenfeld said that "When the footage became public earlier this week, the national Cybercrimes Unit opened an investigation and arrested the suspect on Wednesday."
goo.gl/Jr5LNP

UNITED STATES

United States not coordinating against Russian cyber threat

US officials have warned repeatedly that Russia is trying to interfere in the 2018 mid-term US elections by hacking or using social media to spread propaganda and misleading reports, much as it did during the 2016 presidential race. Lawmakers, particularly Democrats, have accused the Trump administration of doing too little to combat hacking. Some lawmakers have stressed the need for a "whole of government approach." "I don't believe there is an effective unification across the interagency, with the energy and the focus that we could attain," US Army General Curtis Scaparrotti, who is also NATO's Supreme Allied Commander, Europe, told a Senate Armed Services Committee hearing.

http://reut.rs/2DqiHo9

Tax software providers not protecting emails from phishing and spoofing

Only half of the top tax software providers are using the most basic of email protections to secure communications with customers, according to new research from the Global Cyber Alliance. Tens of millions of Americans will use tax software to prepare their federal and state taxes, yet some of the industry's biggest names, such as H&R Block, TaxAct, Turbo Tax, and Free Tax USA are not securing their email domains from hijackers who could trick consumers into sharing sensitive data, including social security numbers, bank account numbers, and dates of birth.

http://prn.to/2HAK9SQ

EUROPE

European firms lagging on Amazon Web Services CloudTrail adoption

European organizations view security as their number one priority when moving workloads to the cloud, but many are failing to take advantage of

native security and compliance tools, according to Sumo Logic. The log management and analytics firm gathered data from over 1,500 customers around the world and found that just 43% of European firms used Amazon Web Services CloudTrail tool, compared to over 51% in the United States and 58% in Australia.

This is a missed opportunity, especially when firms are increasingly using new technologies like containers which could be exposing them to greater risk, according to the vendor.

http://bit.ly/2DsVKAG

Cyberattack targets German ministries

The German Interior Ministry announced on February 28 that several federal agencies had been hacked in December 2017, allegedly by Russian APT28 hackers. The attack targeted the government computer network and has now been brought under control. APT28, which has been linked to Russian military intelligence, introduced a piece of malware in the Informationsverbund Berlin-Bonn (IVBB) network, a special communication platform designed to be highly secure, used by the German federal ministries or the Bundestag. It is rumored that the hackers managed to steal sensitive data from the Foreign and Defence Ministries, while officials asserted the Defence Ministry and the German military were not affected.

http://bit.ly/2pcCnqs

British at risk of fraud as UK banks "seriously lagging behind" in security

UK consumers are at risk of fraud because banks are "seriously lagging behind international competitors" when it comes to security. New research has revealed UK financial services organizations are failing to invest and to keep up with digital investment as seen in other sectors. While other countries are taking a lead in facial recognition, social media data, and automated electronic data capture to ID customers and improve the customer experience,

British-based banks are stuck in the dark age. A third of British banks and FinTechs say they are "seriously lagging behind international competitors" when it comes to fraud checks, while 84% of UK financial service firms are concerned about their ability to identify customers.
http://bit.ly/2phnMv5

UK political system is at risk of cyberattacks from terror groups

The UK political system could be targeted in cyberattacks by terror groups, a report warns. The report raised the prospect of parliamentary networks being hacked or fake information being planted on legitimate websites. The Intelligence and Security Committee, which has high-level access, assessed the threat in its annual report, saying that "the UK's political system is a potential target for cyberattacks by hostile foreign states and terrorist groups. Such attacks could include hacking into parliamentary or private computer networks and obtaining communications and data belonging to political figures, or obtaining sensitive data on the electorate, which is held by political parties.
http://bit.ly/2FQpJbh

RUSSIA

Russia is about to "leave" global internet for its own?

The presidential adviser on internet development issues, Herman Klimenko, stated that Russia is technically ready to disconnect from the global internet. Klimenko reminded that Russia is one of the three states having a "full internet cycle," meaning the existence of its own search engines, social networks, and advertising, along with China and the United States.
http://bit.ly/2DmfINy

Russia suspected behind German government hacker attack

At the end of February, it was reported that the government information network of Germany had been hacked. Hackers who attacked the governmental servers stole the protocol of consultations between the European Union and Great Britain about Brexit, as well as documents on the EU negotiations with Ukraine and Belarus. It was also reported that APT28 hacker group, also known as Fancy Bears, could be involved in the attack. In some countries, its activities are connected to Moscow.

http://bit.ly/2FyLgBM

Following Telegram's refusal, FSB will develop its own user data hacking software.

The Russian Federal Security Service (FSB) ordered a software product development for its own usage, with the ability to access and identify any Telegram user's personal data. The order was released under the Anti-terror and Anti-Extremism Federal Law Act.

http://bit.ly/2HmZN43

MIDDLE EAST

New Iranian cyberattacks concern the West

Experts have sounded the alarm about new Iranian cyber activity, as hackers become more emboldened and skilled at carrying out surveillance operations and other attacks outside the country's borders. Cybersecurity professionals have detected Iranian hackers breaking into networks of defense contractors, aviation firms, oil and gas companies, technology companies, and telecommunications providers. In many cases, Iran-linked cyber activity is limited to intelligence operations, but some groups have also shown signs of destructive capabilities.

http://bit.ly/2p8kE3L

Egypt's Cyber-operations against ISIS jams Israeli cellular networks

In recent weeks the Egyptian military has been waging a major campaign against the Islamic State fighters in Egypt's Sinai Peninsula, which has affected Israeli cellular networks. The Israeli military said that the cellular blackouts that have affected southern Israel in recent weeks have been caused by electronic warfare waged by the Egyptian military in its campaign against ISIS. The military said that it was aware of the disruptions in Israel, adding that it was working with the Egyptian army to solve the problem.

http://bit.ly/2Fztz8g

North Korea suspected in cyberattack on Turkey

Suspected North Korean hackers blitzed Turkish financial institutions and a government organization last week, seeking intelligence for a future heist, says a new report by McAfee. The Turkish attacks are unusual because the hackers quickly created software to exploit a recently revealed weakness in Adobe Flash, using the program to implant malware onto victims' computers. It was also unusual how swiftly McAfee researchers discovered the effort. To trick the Turkish targets into opening the attachment, the hackers sent the emails from an account with the domain name falcancoin.io, which is similar to that of a leading cryptocurrency lending platform, Falcon Coin. The Microsoft Word document had an embedded Adobe Flash file that exploited a problem for which a software patch had been distributed just weeks before. The attackers were assuming that users had not yet downloaded that update.

http://on.wsj.com/2FtOXc1

CHINA and APAC

Indian Home Minister: Cybercrime becoming industry, may occur "very often"

Home Minister Rajnath Singh said that cybercrime has become a global industry and that such offences occur "very often" due to the availability of resources in the wrong hands. Singh also said that penetration of the internet and self-radicalization have further added to the woes of law enforcement agencies and that continued availability of radicalized materials on the internet is likely to have drastic change in society and subsequently to humanity.

http://bit.ly/2HAYtLb

HenBox malware targets Chinese minority group

A new Android malware family dubbed HenBox is targeting a large online population in China who has been the subject of numerous cyberattacks in the past. The app's name is based on metadata found in most of the malicious apps, such as package names and signer detail. HenBox was spotted masquerading as a variety of legitimate Android apps, such as VPN and Android system apps and appears to primarily target the Uyghurs, a minority Muslim Turkish ethnic group in China.

http://bit.ly/2GrnQzr