Global Cyber Bi-Weekly Report by INSS January 15 2019

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

Contributors: Simon Tsipis, Anna Danilova, Gal Sapir, Michal Beit Halachmi, Stefan Weenk

ISRAEL

Netanyahu says Israel's ready for any election cyber-meddling scenario, but it is not

Concerns about misinformation, malicious rumor-mongering, and cyberattacks in elections began since allegations were made of Russia's meddling in the 2016 US presidential elections, which saw the hacking of the Democratic Party's emails and the use of Facebook to manipulate information. Former Mossad chief Tamir Pardo emphasized at a digital conference, organized by the business daily, The Marker, that Israel has to be prepared to handle the use of bots and fake information since it is a global issue. About a month later, the head of the Shin Bet security services, Nadav Argaman, said that a foreign state "intended to intervene" through cyberattacks in Israel's national elections set for April 9. In August, Prof. Karine Nahon, president of the Israel Internet Association, wrote to Justice Hanan Melcer, the current chairman of the Central Elections Committee, to warn that "these attempts will increase and become more sophisticated in the run-up to Israeli elections."

https://bit.ly/2CjDsUf

Tel Aviv-based ForceNock's technology will be integrated into Check Point's Infinity total protection architecture

Check Point Software Technologies Ltd., an Israeli cyber security solutions company providing software products for IT security, has announced the acquisition of ForceNock Security Ltd. In an interview by Globes, ForceNock CEO and co-founder Dotan Bar-Noy told that the advantage of its technology lay in its ability to identify malicious hacking attempts with great accuracy, while being easy for the customer to deploy, with no need for continuing. The acquisition price of ForceNock was not disclosed, but a source at the company said the price was "below $10 million." "Check Point is committed to

providing the most comprehensive security architecture to prevent current and future generations of cyberattacks," said Check Point VP Products Dr. Dorit Dor and "incorporating ForceNock's technology into our Infinity Architecture will enable us to continue to provide the highest level of security for our customers worldwide."

https://bit.ly/2FDKJSb

Israeli high school cyber grads not promised army intel spots

High school students in the cybersecurity program of the Education Ministry were promised that they would get preference for assignments in army intelligence units and bonus points that enhance their chances for university admission, but both promises have not been realized. Information on the website of the Education Ministry states that "graduates of this major with high achievements will get preference for acceptance to positions in Israel Defense Forces intelligence units." The IDF does not give a preference to students of the cybersecurity program according to Haaretz. The Education Ministry said the information on its website is indeed inaccurate and would be corrected. In a statement, it added the IDF alone is responsible for intake of conscripts. "As to the bonuses in acceptance to higher studies, this issue is determined by universities themselves according to their respective policy."

https://bit.ly/2MczIbx

UNITED STATES

Navy reservists power a new cyber development unit

At the turn of the month, in Fort Meade, Maryland, the Navy Cyber Warfare Development Group (NCWDG) was activated, with its new commanding officer, Capt. James Lee. The reserve unit demonstrates the navy's efforts in "cyber warfare innovation," focusing on refining capabilities and processes, resulting in a cumulative increase in its competitive advantages. The NCWDG will support the "navy cyberwarriors" in its general mission, with technical research and development to produce, test, and provide superior "cyber, cryptologic, and electronic warfare capabilities." The unit structurally operates as a directorate within the Navy Fleet Cyber Command. The demonstration of harnessing the valuable skill set of the national guard and reservists—many

who work in the cyber and IT private sector—to amplify active duty elements is a larger effort initiated and applauded across the Department of Defense.

https://bit.ly/2FrGREh

Oreo lawsuit could set precedent for cyber insurance industry

Mondelez, US food distributer, owner of major brands Oreo and Cadbury, is suing its insurance company Zurich for $100 million in damages incurred in 2017 from the NotPetya cyberattack, causing over $10 billion in reparations. Although generally, insurance policies include acts of war, this case challenges the questions of scale and authority. It asks who decides whether a cyberattack originating from a nation-state is an act of war or not, subsequently determining coverage. It also asks what is the threshold of malicious cyber activity that would be considered an act of war as in exposed emails or malware that erased most servers, as exhibited in the 2014 Sony case; Sony, however, received $100 million in damages from its insurance company and did not go to court. In response to the proliferation of cyberattacks, experts observe the increase in cyber policies offered by insurance carriers, as most large ones offer such policies to public sector entities, such as governments, schools, and utility companies. According to RAND expert Sasha Romanosky, the cyber insurance market is expected to grow from about $2 billion as of late 2018, to $10 to $15 billion in the next decade.

https://bit.ly/2AOAeYW

Ryuk ransomware shows Russian criminal group is going big or going home

Since August 2018, $3.7 million has been collected in bitcoin by criminal hacking group referred to as Grim Spider, a subdivision of the entity Wizard Spider, in a series of cyberattacks ranging from wire fraud to ransomware and allegedly linked to Russia, although previously suspected to be North Korea. In the last year, large businesses have been targeted by the extortion tactic, paying "substantial fees to unlock data," including Onslow Water and Sewer Authority based in North Carolina, cloud hosting provider Dataresolution.net, and the Tribune Publishing umbrella. The ransomware has also affected newspaper production and delivery operations for the Los Angeles Times, San Diego Union-Tribune, Chicago Tribune, Baltimore Sun, and South Florida Sun

Sentinel to name the least. According to the cybersecurity company CrowdStrike, Ryuk source code and ransom note resemble Hermes ransomware and BitPaymer, respectively, despite modifications and constant development as in their effective TrickBot trojan. Additionally, the ransomware is only available for the Ryuk gang, unlike the Hermes "commodity" ransomware available on forums.

https://bit.ly/2VTAaA4

RUSSIA

US cyber security company Crowdstrike is on Russians' tail

The cybersecurity firm CrowdStrike that helped Democrats expel the Russians from their computer systems in 2016, and later shared information with the FBI as it investigated the election-season hacks, recently revealed that emails from top officials at the National Republican Congressional Committee were hacked during the 2018 midterm elections. According to the CrowdStrike source, the attackers could only have signed into those officials' accounts as if they were the officials themselves, and to do this, the source said, the attackers obtained the passwords belonging to the officials. However, Crowdstrikes' source did not say how the attackers obtained the passwords.

https://cnn.it/2RR3BUg

What will deter Russia?

According to John P. Carlin, a chair of the Aspen Institute's Cyber & Technology, a series of criminal charges indicate that Russia is a rogue state in cyberspace. He listed Russia's most severe cyberattacks, as well as the less known criminal complaint against Elena Alekseevna Khusyaynova, who is alleged to have participated in "Project Lakhta," a Russian-oligarch-funded effort to deploy online memes and postings to stoke political controversy. In addition, he noted similar coordinated charges filed by UK, Dutch, and US officials against Russia and its intelligence officers of a scheme to target anti-doping agencies, officials, and even clean athletes around the world in retaliation for Russia's doping scandal, in addition to new evidence that Russia has interfered in other foreign issues, such as a recent referendum in Macedonia aimed at easing that country's acceptance into Europe. Carlin argues that it is an obligation to respond with sanctions, as it will convince

Putin that additional attacks will trigger automatic, severe responses. According to the specialist, only this would be the best path to deter Russia.

http://bit.ly/2VONw0h

The Senate Committee: Social networks do not provide enough information on Russian activities

The report, commissioned by the Senate Intelligence Committee, about the Russian campaign to influence the 2016 US presidential election, are based on troves of data that Facebook, Twitter, and Google handed over to the committee. According to a source familiar with the report, the social media companies could have provided more valuable data to the committee and also could have presented it in a more accessible format. According to the source, social networks provided the "bare minimum" amount of data to aid the panel's investigation into Russian meddling in the 2016 presidential election.

https://cnn.it/2FpkVK0

MIDDLE EAST

Iran behind "unprecedented" cyberattacks on Middle Eastern governments, says US security firm

A study by Californian-based FireEye Intelligence found that Iranian hackers are suspected of orchestrating an "unprecedented scale" of cyberattacks targeting Middle Eastern governments in the last two years. Multiple government servers, telecommunications, and internet companies were affected by a wave of DNS hijacking across the Middle East and North Africa, Europe, and North America. The hackers use malicious software to access sensitive information and data, aimed at harvesting usernames and passwords. FireEye said it had "moderate confidence" of Iranian involvement following two years of studying malicious cyberattacks between January 2017 and January 2019. However, the firm said it could not be certain as to whether hackers were state-funded or private individuals.

https://bit.ly/2AIoxTh

Kaspersky Lab uncovers new exploited vulnerability in Microsoft Windows OS kernel

Kaspersky Lab has automatically detected a new exploited vulnerability in the Microsoft Windows OS kernel. The latest exploited vulnerability (CVE-2018-8611) was found in malware targeted a number of victims in the Middle East and Asia. The FruityArmor group is seen as the actor behind the attack as a PowerShell backdoor has exclusively been used by this threat actor in the past. Zero-day vulnerabilities were previously unknown and are therefore unpatched, software bugs that attackers can exploit to gain access to victim systems and devices. Upon discovery, Kaspersky Lab's experts immediately reported the vulnerability to Microsoft.

https://bit.ly/2VS9QpL

APAC

Vietnam claims Facebook has breached its new cybersecurity law

The new law, which entered into force on January 1, 2019, has caused concern among tech giants such as Facebook, Google, and Twitter to name a few, as it requires the companies to operate local branches and store user information in Vietnam. It forbids users from spreading anti-government information or post negative content against government officials or agencies.

Vietnam claims that content deemed forbidden under the new law was flagged, but Facebook had delayed removing it. Facebook claims that they follow their internal process of reviewing materials flagged by government and will react according to findings. However, the government claims that Facebook already disclosed that it did not find the posts, comments, or other materials flagged in breach of its own policy. Vietnam is considered a growing market for startups, but the new cybersecurity act raises concerns, as the government seeks control of content, as well as access to user's information.

https://goo.gl/9VQjVK

India to set up a defense cyber agency

India intends to set up a defense cyber agency, which will operate under Integrated Defense Staff (IDS). Combined of air force, navy, and army officers, it will serve as an inter-service agency, with the purpose of tracking and handling cyber threats. The IDS is responsible for coordination among the army branches. The unit will not be based in a main headquarter, but rather will be located at various points around the country, composed of officers who will deal exclusively with cyber threats. The agency will be headed under a two star rank officer, according to LT General Naravane of Eastern Command. Currently, the final stages are being formulated.

https://goo.gl/LuKzwk

India court examines petition against the government's latest breach of privacy, according to activists and right groups

India's top court has requested that the government respond to petitions filed by activists and internet rights group, after its latest directive of giving ten intelligence and investigative agencies the power to intercept, decrypt, and monitor any information stored on any computer. The government claimed in its defense that it was a continuation of a policy established by the previous government. The Supreme Court just recently curbed the government's use of a digital identity program, as well as programs to monitor social media posts and email. The Internet Freedom Foundation, one of the petitioning groups, claims this is a breach of the right of privacy, which was upheld as a fundamental right by the top court back in 2017. The petition also mentions provisions of India's technology law, which allows the government to intercept online content.

https://goo.gl/suzWB6

200 million resumes of Chinese jobseekers leaked

In one of the biggest known leaks to date, a mega base of resumes of 200 million people, including their personal information, was leaked and made available online for nearly a week, according to European bug bounty company HackenProof. One of the company's security researchers, Bob Diachenko, found the unprotected database on December 28, and claims it was open to the public between December 23–28, but taken offline shortly

after he published his findings. At least a dozen IP addresses have downloaded the data. An online scrapping tool was likely used to extract the data from Chinese job portals, including the leading site 58.com, which denied that the data was leaked from its server but acknowledged that it was likely from a third-party scrapper. Chinese laws ban illegal sales or publication of personal information, but there is no clear liability as lawmakers are calling for a specific bill regarding protection of data. Data scraping can be illegal if information is used against the individual's best interests, even if the person gave permission. It can also be used to steal identity and make fraudulent financial transactions.

https://goo.gl/f5bqjf