Global Cyber Bi-Weekly Report by INSS 01 August 2019

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

Contributors: Simon Tsipis, Robin Veldwijk, Thomas Abma, Donal Byrne

ISRAEL

Cross-border collaboration: Israel and Romania sign cybersecurity partnership

Israel and Romania agreed on a memorandum of understanding earlier this year, vowing to work together to strengthen security across both nations. In June, during the third annual Romania–Israel Cyber Security Forum, the nations signed an agreement to cooperate in cybersecurity research, technology, and industrial development in cybersecurity. The agreement is an information exchange agreement.

Romania has made waves recently with its cyber start-up industry. Israel, on the other hand, is successful in the cyber security business, and known as "the start-up nation" with the highest number of new businesses per capita in the world—around one for every 1,400 people.

https://bit.ly/2yqyq6U

Bipartisan Senate bill to inquire about creation of US-Israel cybersecurity center

US Senators Jacky Rosen (D-NV) and Mike Rounds (R-SD) introduced a bill to require the US State Department to investigate the potential benefits of establishing a joint US-Israel cybersecurity center. The legislation would help to take steps toward establishing a joint cybersecurity research center, since Israel is the United States' closest ally in the Middle East and a world leader in cybersecurity. A US-Israel cybersecurity center would leverage the expertise of institutions of higher education, the private sector, and government entities in

both countries in the areas of cybersecurity and protecting critical infrastructure.
https://bit.ly/330l2nZ

Israel launches cybersecurity program for students with special needs

Instructed and funded by the National Cyber Security Authority and the Ministry of Labor and Social Affairs, Israel has launched the first cohort of a new cybersecurity training program for students with special needs. Sixteen students have joined, all of which have varying degrees of autism and are aged twenty-one and older. They will receive mentorship from employees at companies, including IBM and Facebook, in the field of information security operations center (SOC).
https://bit.ly/2YbAgro

UNITED STATES

Capital One announces massive data breach; lone suspect arrested in Seattle

Software engineer Paige A. Thompson was recently arrested for allegedly hacking Capital One's cloud storage—Amazon Web Services. Thompson was employed at Amazon Web Services from 2015–2016. Enabled through a "misconfigured firewall," Thompson had access to over 700 folders of data, affecting the personal information of about 100 million people in the US and 6 million in Canada. The data extended from 2005 to the beginning of 2019, and "included names, addresses, zip codes/postal codes, phone numbers, email addresses, dates of birth… self-reported income [social security numbers, credit card numbers, and bank account numbers.]" Thompson "bragged" about her achievement on GitHub, though it is unclear if the personal information was published as well. Capital One expects the damage will cost them about $100 to $150 million, further disclosing they have an

insurance package with a coverage limit of $400 million. Thompson could face a five-year prison sentence and a significant monetary fine.

https://tiny.cc/futiaz

https://tiny.cc/331iaz

State election offices made for an easy target for Russian hackers

Against the backdrop of the 2016 election meddling and on the horizon of the 2020 elections, security remains a high priority and challenge. Recently, the Senate Select Committee on Intelligence released the first in a series of reports regarding "Russian interference," illustrating "how Russian actors targeted state networks and election infrastructure in 20 anonymous states and Illinois." More so, that the associated aggressors "scanned networks, attempted SQL injections, relied on phishing and sent malicious emails." Synonymous with official reports after the 2016 occurrence, most states were unaware to the extent of the breach, let alone did they have the technology to alert them, and in most incidences, they did not comply with federal warnings and advice. The Senate Committee concluded that "it was likely every state had been targeted." Tom Kellermann, who was a former commissioner on President Obama's commission on cybersecurity stated that "states view security through a very old-fashioned, a very antiquated lens of network security…" Although the report is in large redacted, some facts revealed the malicious campaign began in 2014, active "well into 2017, at the state and local level." Other uncensored facts revealed a more detailed scope and nature of the breaches conducted on some of the impacted states.

https://bit.ly/2YqLYtz

"This isn't IAD 2.0": NSA's new cybersecurity directorate plots its mission

During the cyber state-related reorganization, the National Security Agency (NSA), has announced the new Cybersecurity Directorate, to be operational on

October 1, with Anne Neuberger as the director, Dave Frederick as the deputy director, and Neal Ziring as the technical director. According to NSA director, Gen. Paul Nakasone, the new directorate, strategized as a "merger and acquisition," will focus on the permutation of signals intelligence and cybersecurity; the latter, in the scope of "intel information sharing." A decision "that unifies our foreign intelligence and our cyberdefense mission... charged with preventing and eradicating threats to national security systems and the defense industrial base," said an NSA spokesperson said. With the additional aim to streamline information and improve coordination among state agencies, the directorate will publish "research, open-source tools for malware, and threat warnings" on its upgraded website. The new directorate complements the efforts of the civilian arm, as in the cybersecurity division under the Department of Homeland Security, which similarly provides resources, as in "malware samples to information-sharing platform VirusTotal."

https://bit.ly/2YutOam

https://bit.ly/2JTcMP5

New York updates its breach notification law in response to Equifax, GDPR

Governor Cuomo signed two consumer-friendly legislation: "Stop Hacks and Improve Electronic Data Security," known as the SHIELD act, to take effect in March 2020, and A.2374/S.3582. In the event of a security breach, the former legislation requires businesses to notify (seemingly within thirty days) victims of the associated exposed data, including biometric and online credentials, while the latter legislation requires "consumer credit reporting agencies to offer identity theft prevention and mitigation services [to affected victims]." A response correlated to the Equifax data breach in 2017, which affected 147 million people, and was settled for $19.2 million regarding New York only. Additionally, if the number of victims exceeds 500 (NY residents), the company is "required to provide written determination to the state attorney general." Furthermore, similar to the EU GDPR, SHIELD requires the same

notification procedures from any individual or entity that holds information of NY residents, even if physically located outside New York.
https://bit.ly/330D3SX
https://on.ny.gov/32XPa37

FBI investigators describe Methbot investigation as "beautiful concert of things shutting down"

The four-year fraudulent advertisement scheme known as Methbot/3ve garnered more than $30 million, although, according to the US Department of Justice, ad fraud has already cost the industry a billion dollars and is set to reach $44 billion by 2022. "Malicious software, botnets, and falsified web traffic" were among some of the technical tools used. At one point "1.8 million infected computers were used to artificially inflate the number of visitors to web pages set up… [to scam] marketing firms." The operation also consisted of exhausting "3 billion ad requests… 10,000 spoofed web domains…[more than] 60,000 accounts selling advertising inventory." It was recently disclosed that the FBI, assisted by the bot detection firm White Ops, other companies, and international agencies, coordinated an operation that took nearly two years to investigate and plan. Ultimately, Russian nationals Aleksander Zhukov and Yevgeniy Timchenko were arrested in Bulgaria and Estonia respectively, and Sergey Ovysannikov, identified as being from Kazakhstan, was arrested in Malaysia; others are still at large, in part, due to a "phone tree" alert system and other methods to convey the status of the authorities' operation.
https://bit.ly/2Gxc9sk

Symantec suspends takeover talks with Broadcom over price clash

In efforts to expand into software, the chipmaker Broadcom acquired the software company CA Technologies for $18.9 billion last year. However, the last year and a half has proven to be unsuccessful for the company. This was demonstrated by the Qualcomm deal, which was valued at $117 billion and

was canceled after President Trump blocked the development. As of recently, the advanced negotiations between Broadcom and Symantec have halted. Allegedly Broadcom was willing to pay $28.25 per share in cash, valuing Symantec at $17.5 billion, although what has transpired seems to be that Broadcom lowered their bid to $1 per share.

https://bit.ly/2MpqECq

EUROPE

United Kingdom barred from key EU cyber security meeting

British officials have been disinvited from an EU cyber security meeting addressing the risks posed by the Chinese equipment maker Huawei. This has resulted in a complaint made by the UK ambassador to the European Union. As the United Kingdom prepares to leave the European Union in October, Tim Barrow wrote a letter to the European Council raising "questions and concerns in London with regards to the treatment and process around meetings." The United Kingdom remains a full Member State until it leaves with the right to attend meetings that do not involve Brexit. On the agenda of this important cyber security meeting were discussions surrounding standards and the protection of 5G networks in the context of potential security risks from Huawei's presence in Europe. The ambassador argued that the UK participation in such meetings did not endanger EU security interests. The United Kingdom has yet to decide whether to place restrictions on Huawei equipment. The British parliament's science and technology committee advised the government to ban Huawei in core parts of telecom networks however, keeping the rest of the market open to Chinese telecom equipment makers. The European Union has urged the new prime minister to make a swift decision.

https://politi.co/2YbBSS0

Teenage hackers are offered a second chance under European experiment

EU Authorities are testing out the idea that not every cybercrime investigation has to end with a hacker going to prison. Both UK and Dutch police have created a legal intervention campaign for first-time offenders' accused of committing cybercrimes. The effort, called "Hack Right," is aimed at young people who may be in danger of breaking the law from behind their keyboard but may not be aware of it. The experiment, which began last year, has already involved incidents with more than 400 young people across the United Kingdom. Many of these offenders are committing crimes, such as stealing a password with harmless intent, while not having the social context to understand that what they are doing is illegal. Upon determining a first-time offender, police representatives visit with the suspect and explain the crime that they have committed. However, instead of threatening legal action, the police encourage the teenage hacker into doing community service, which consists of ethical computer training and are then put in touch with professionals who can explain possible career paths to them and suggest different educational paths based on their interests. In order to qualify for the program, suspects must confess to their actions, not have a criminal record, and be willing to change their behavior.

https://bit.ly/3128Gty

Next European Commission president takes aim at artificial intelligence

Former German defense minister and the next European Commission president, Ursula von der Leyen, has joined national governments and EU digital policymakers in calling for hard rules to govern artificial intelligence, sooner rather than later. Addressing the European Parliament, von der Leyen pledged that "In my first 100 days in office, I will put forward legislation for a coordinated European approach on the human and ethical implications of artificial intelligence." The European Commission has promised to draw up

rules on issues relating to artificial intelligence over the next five years building on its legacy as the world's premier of online privacy building on the recent GDPR regulation. Despite many large companies claiming it would slow down innovation, Europe is currently trying to catch up with China and the United States in developing their artificial intelligence capabilities.
https://politi.co/2MmDrp6

No prison for British cyber expert in malware case

The British computer expert who helped shut down the WannaCry cyberattack on the NHS said he is "incredibly thankful" after being spared jail in the United States for creating malware. Marcus Hutchins was hailed as a hero in May 2017 when he found a "kill-switch" that slowed the effects of the WannaCry virus affecting more than 300,000 computers in 150 countries. However, FBI agents arrested the 25-year-old, in a Las Vegas airport months later after attending a hacking convention. On the day of the verdict, the US district judge said the virus that Hutchins helped stop was much more damaging than the malware he had created and sentenced him to time served with a year of supervised release. He had pleaded guilty to two charges relating to writing malware, which court documents have described as "malicious computer code" known as Kronos. The documents said that "the malware was designed to target banking information and to work on many types of web browsers, including Internet Explorer, Firefox, and Chrome."
https://bit.ly/2YrdGKJ

RUSSIA

Russia's Federal Security Service hacked

Apparently, hackers have successfully targeted Russia's Federal Security Service, the FSB, the successive agency to the infamous KGB, which reports directly to Russia's president. The hackers managed to steal 7.5 terabytes of data from Sytech, a major FSB contractor, exposing secret FSB projects. These projects are targeted to de-anonymize "Tor" browsing, scrape social media

(including Facebook and LinkedIn), and help the state sever its internet from the rest of the world. The data was passed to mainstream media outlets for publishing. The BBC described the breach as possibly "the largest data leak in the history of Russian intelligence services." The BBC claims that Sytech's projects were mostly contracted with Military Unit 71330, part of the FSB's 16th Directorate that handles signals intelligence. The same group was accused of emailing spyware to Ukrainian intelligence officers in 2015.
http://bit.ly/2YuRKhN

Senate's conclusions on Russian 2016 US elections hacking revealed

A report by the Senate Intelligence Committee recently released provided new details about what happened in 21 US states that were said to have been cyber-targeted by Russia. According to the report, Russian actors used a variety of techniques, including spearfishing, scans, and SQL attempts. Much of the activity were so-called "scans," which have been equated to a thief looking for open doors and windows but not actually breaking in. In one state, according to the report, cyber actors scanned the state's entire IT infrastructure, include its website for election results. The main conclusions are that "Russian intentions regarding US election remain unclear. Russia might have intended to exploit vulnerabilities in elections' infrastructure during the 2016 elections," yet according to the report, "decided not to execute these options." Moreover, "Russia might have sought to gather information in the conduct of traditional espionage, or to catalog options for clandestine actions, to execute them at a later stage." Overall, the report said that the intelligence community believes that the activity was in line with Russia's larger goal of "undermining the integrity of elections and American confidence in democracy."
http://bit.ly/2ZiLaIi

Private site, investigating Russian military crimes, endlessly hacked

Bellingcat—the online investigations site that has become synonymous with investigations into crimes committed by Russia's military, including the downing of Malaysia's MH17, the Skripal poisonings, the bombing of civilian targets in Syria, and the linking of the Russian hacker team Fancy Bear to the Russian GRU agency—has again been targeted by cyberattacks almost certainly linked to agents of the Russian security agencies. According to the Financial Times, Russian hackers were likely behind a cyberattack on the secure email platform used by Bellingcat's team. The email platform in question is the Swiss-based ProtonMail, which enjoys the protection of Switzerland's strict privacy laws as well as end-to-end encryption and anonymized accounts. Bellingcat's team is heavily involved in linking the downing of MH17 to Russia's 53rd Anti-Aircraft Missile brigade. The Boeing 777 was downed by a missile strike, killing all 298 people on board. Bellingcat then made the link all the way to "senior officers of the Russian Ministry of Defense and its military intelligence agency, the GRU." The same team identified the GRU officers allegedly responsible for the Skripal poisoning and also for the Russian missile strikes on civilian targets in Syria.
http://bit.ly/2YqgYhb

FaceApp's Russian connection

Shortly after FaceApp went viral as the most downloaded smartphone App in the United States, it was revealed that a Russian tech firm is behind the application's development. US cyber experts started shortly to wonder to where millions of people's photos been sent. Apparently, millions of photos of faces of American citizens have been sent to a Russian-based tech company; however, US cyber experts announced that the servers hosting the information are under US control and are being run by American companies. Nonetheless, there is no restriction on Russian individuals owning an American company. Experts warn that the free "old age filter," created in 2017 by developers at Wireless Lab in St. Petersburg, Russia, poses security

concerns that may give them access to people's personal information and identity.

https://wapo.st/2SJDsEM

https://nyp.st/2ZfZdhV

APAC

Google warns Hong Kong's Joshua Wong of government-backed hackers

Joshua Wong, a Hong Kong protest icon, was told by Google that "government-backed attackers" might have tried to steal his password and access his data. The 22-year-old man recently posted the notice on Twitter. Google said that it cannot reveal what tipped them off, but what happened to Wong's account happens to "less than 0.1% of all Gmail users." Wong, who is the face of Hong Kong's 2014 Umbrella Movement, was released from prison last month after serving one month for a contempt of court charge. Following his release, Wong went straight back to protesting, helping to organize a rally that saw the city's police headquarters surrounded by thousands of demonstrators. Google failed to add which government it believes is trying to get Wong's password, although it is not difficult to determine which government this may be. Last month, the founder of the Telegram messaging app explicitly accused China of attempting to flood its servers with a powerful DDoS attack to keep protesters from communicating with each other during one particular demonstration.

https://bloom.bg/2Yg1MEo

A top Japanese fund returns 37 percent betting on US stocks fighting cybercrime

One of the best-performing funds in Japan this year invests in upcoming US technology stocks in order to fight cybercrime. Mitsubishi UFJ Kokusai Asset Management cyber security fund has returned 37 percent in 2019, beating almost all peers, after shares of top picks surged. The fund invests in

everything from online identity-management firms to cloud-based security providers. The global cyber security market is forecast to grow 80 percent to $248.3 billion by 2023, from $137.6 billion in 2017. The fund holds 39 stocks, most of which specialize in cybersecurity. US firms accounted for more than 80 percent of investments at the end of May. It comes in two versions, one hedged against currency movements, and has increased its assets to about 111 billion yen ($1.03 billion) in total since its inception in July 2017. Okta Inc., its largest holding, allows users to access multiple websites and applications with a single, secure password. The stock, which accounts for 9 percent of the unhedged fund's assets, has more than doubled this year as investors bet on the prospects for growth of earnings.
https://bloom.bg/2Mp4LD1

MIDDLE EAST

Iranians manage to surf the web despite tide of censorship

Despite the Iranian authorities' attempts to limit the "Western cultural influence" since the 1979 Islamic Revolution, Iranian citizens have found a way around the blockade of websites like Twitter, Facebook, and YouTube. Virtual private networks (VPNs) and other services allow many young Iranians access to online platforms that the government claims "make the people pessimistic about the government."
http://bit.ly/2KdVE5I

SoftBank sets up $108 billion investment fund, with no Saudi money

Japanese internet company SoftBank Group Corp. has set up a fund for technology investments such as artificial intelligence, funded with money from the company itself as well as from Apple, Microsoft, and other tech companies. SoftBank's earlier fund came under scrutiny after the killing of Saudi journalist Jamal Khashoggi. Most of the funding for that investment entity came from Saudi Arabia.

http://bit.ly/2YBmwG0

Saudis warned against using FaceApp

The National Cybersecurity Authority (NCA) has warned Saudi citizens against using the viral face-transforming mobile application FaceApp. The app allows users to upload photos of their faces and have them edited to look older, but cybersecurity concerns are arising over possible misuse, mainly pertaining to privacy.

http://bit.ly/2K8moo6

LATIN AMERICA

Justice Ministry: Brazil's President Bolsonaro's cellphones targeted by hackers

The Brazilian Justice Ministry announced in a recent statement that cellphones utilized by President Jair Bolsonaro were targets of a cyberattack. The suspected hackers are also suggested to be responsible for the earlier attacks targeting Justice Minister Sergio Moro and other state-legislative officials. The malicious campaign is thought to be associated with the arrest of four hackers a week earlier. The hacking exposed conversations on several online platforms and triggered "a political storm." The exposed information was related to the corruption prosecution of former president Luiz Inacio Lula da Silva.

https://reut.rs/338L2O6

https://tiny.cc/yx1iaz

Chinese hacking campaign targeted diplomats from Slovakia and South America

The Ke3chang group, suspected to consist of Chinese hackers, has been active since 2010. It is known for collecting information about "international government contractors, military organizations and breached computers used by foreign ministries before the 2012 G20 Summit, according to FireEye." It

has emerged that their targeting behavior has expanded to include diplomatic missions, with Belgium, Brazil, Chile, Guatemala, and Slovakia being among the states targeted. The group used updated software tools, as in the Ketrican malware, and "a technical backdoor, Okrum" to infiltrate and intercept information about employees and other actors, "including usernames, IP addresses, and operating systems among other data." Ke3chang tools have been utilized and linked to other hacking groups in China, such as APT15 and Playful Dragon. Thailand's CERT has designated the dynamics as a "state-sponsored operation."

https://tiny.cc/951iaz