Global Cyber Bi-Weekly Report by INSS 15 August 2019

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

Contributors: Simon Tsipis, Donal Byrne, Lea Abramski

ISRAEL

Amazon's AWS to set up Cloudfront infrastructure in Israel

The company's cloud service, Amazon Web Services (AWS) Content Delivery Network (CDN), referred to as CloudFront, was first established in Israel in 2014. It was followed by Amazon's establishment of a research and development center and its acquiring of a number of Israeli companies since 2015. AWS recently announced its infrastructure plans for CloudFront in Israel to enable a qualitative upgrade of services to Israeli companies, "including computation power integration, networking, and cybersecurity services."
https://bit.ly/2Z5pWgi

Israeli cyber experts identify serious security flaw in digital cameras

At the recent DEF CON hacking conference in Las Vegas, Nevada, the threat intelligence division of Check Point, the Israeli software company, disclosed the latest Information and Communication Technologies (ICT) at risk of ransomware and malware attacks includes "any 'smart' device, including the DSLR [digital, single lens reflex] camera." The company uncovered flaws in the Picture Transfer Protocol (PTP), which is the digital image transfer from camera to PC, and in other tools supported by the protocol commands, which include live photos and "upgrading the camera's firmware." The Canon EOS 80D DSLR camera was identified as having "multiple critical vulnerabilities in the PTP," along with other brands. The risk is further amplified due to latest camera models featuring the capability of connecting to the WiFi network, in addition to the USB component, making both camera and PC vulnerable

targets. Canon was informed of the findings before the presentation and worked with the company on patching the vulnerabilities. The company also released a statement noting that there have not been confirmed cases of such vulnerabilities exploited.
https://bit.ly/2TnK77Q

Senate to consider US-Israel cybersecurity center

At the turn of the month, the US-Israel Cybersecurity Center of Excellence Act, a bipartisan senate bill, was introduced. The legislation endorses the State Department to assess the advantages resulting from such cooperation, in addition to the establishment of such an institution with its closest ally and a center for emerging technologies in the Middle East. The center would utilize the expertise of actors across academia, as well as public and private sectors. Similar bipartisan legislation was introduced by the House of Representatives in the Spring. Current US-Israeli centers relate to water and energy.
https://bit.ly/2OEFesa

UNITED STATES

Apple upgrades Bug Bounty Program: Adds Macs, $1 million reward

Announced at the recent Black Hat conference, Apple decided it will open its once private Bug Bounty program to all researchers this Fall. The program will also extend to include MacOS, tvOS, watchOS, and iCloud. The rewards range between $250,000 to $1 million dollars for vulnerabilities found in its devices, "and for a network attack with no user interaction that could lead to zero-click kernel code execution with persistence." Rewards include a fifty percent bonus for "vulnerabilities found in pre-release software." The program was initiated in 2016, by invitation only, with rewards capping at $200,000 dollars, and a narrow scope of products to investigate. One factor, among many, correlated to the changes arises after Ian Beer, Google bounty hunter, critiqued Apple's iOS security during the 2018 Black Hat conference.

https://bit.ly/31GDaBY

Feds plan to use Securedrop as a vulnerability reporting portal

In an effort to increase partnership with "ethical hackers," the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (DHS CISA) announced the re-introduction of a portal for the purpose of publishing vulnerabilities. The hacking conference DEF CON will now host the servers and act as a middleman to the government. The amended process is intended to mitigate the fears of security specialists and white hat hackers, namely of "sharing directly with the government," the federal agencies' utility of such exploits, and potential legal repercussions. The open-source software is not yet active but is said to be secure and "runs through Tor, the anonymizing tool."

https://bit.ly/2Z3bbur

WhatsApp flaws could allow hackers to alter messages

Checkpoint, the Israeli software technologies company, uncovered security flaws that can enable hackers to augment both public and private messages of the 1.5 billion users using the application WhatsApp. The application, which was acquired by Facebook in 2014, is utilized for personal, business, and political communications to name the least, amplifying the suggestive proliferation of misinformation. Check Point identified three ways of modifying conversations: utilizing the "quote" feature to change the appearance of the sender's identity in a group chat, changing the text of someone's reply, and sending a private message to a group member concealed as a public message, resulting in the visibility of the response to the entire group conversation. Only the latter flaw has been fixed, since revealed a year ago to Facebook. The company has contested the former two capabilities as false designation but "merely the mobile equivalent of altering replies in an email thread to make it look like something a person didn't write."

https://bloom.bg/2KBf7yw

EUROPE

British Airways check-in flaw exposes personal data

British mobile security solutions company Wandera uncovered a security design flaw in British Airway's (BA) e-ticketing system—particularly the check-in link—resulting in potential exposure of passengers' personal data. Wandera disclosed the information to BA, as well as eight other major airlines impacted by this vulnerability in February of this year: Southwest, KLM, Air France, Jetstar, Thomas Cook, Vueling, Air Europa, and Transavia. Israel Barak, the chief information security officer at Cybereason, stated ten airlines were investigating a similar vulnerability earlier this year. One Wandera researcher found that the vulnerable check-in links sent via email to the passengers are unencrypted; furthermore, they can be intercepted when accessing the same public WiFi network. This incident emerges after BA was fined a record £183.39 million (about $230 million dollars) last month from the Information Commissioner's Office for the 2018 data breach that exposed personal and financial information of half a million customers.

https://bit.ly/2Z0XNXt

https://bit.ly/2H63nSl

https://bit.ly/2G3RDPE

Estonia debuts first ever cyber diplomacy training

EU and NATO diplomats who focus on cybersecurity issues have last week attended their first ever "summer school," which trains individuals on matters relating to cyber diplomacy. The sessions focused on lessons learned from previous international negotiations on cybersecurity issues, technological developments on the latest cyber threats, and international norms and laws in cyberspace. For five days, 80 diplomats participated with cybersecurity experts and academics, consulted one another, and more importantly, also participated in a simulation of a real-world international cybersecurity crisis. The objective was to help diplomats from EU and NATO countries get "a more in-depth understanding" of cybersecurity strategies and technological

developments and how those topics affect the implementation of norms and international law. Twenty-six countries were represented. The development of what is accepted nation-state behavior in cyberspace is still in its early stages. Estonia's Ambassador at Large for Cyber Diplomacy Heli Tiirmaa-Klaar said diplomats would continue to be prompted to negotiate on issues related to cyberattacks.

http://bit.ly/2Kvsq3l

How Brexit impacts the future of Europe's cybersecurity posture

The UK Parliament has been unable to reach a deal with the European Union. With the possibility of a "no deal" Brexit increasing, EU leaders are unsure about what the future UK-EU security relationship will look like. This uncertainty creates various opportunities, which cyber criminals could try to exploit. The United Kingdom incorporated the General Data Protection Regulation (GDPR) and NIS Directive into law, a political choice that shows that it desires to be aligned with the European Union in a security sense. However, while it will be possible for the United Kingdom to send data to the European Union, it is illegal for an EU Member State business or organization to export data to a non-EEA entity without specific legal safeguards in place. Therefore, given that the post-Brexit UK will be considered a "third country," EU countries may be hesitant in allowing them participate in future cyber collaboration projects. The number of UK data breaches reported to the Data Protection Commission rose by almost 70 percent last year, totaling 4,740 breaches during 2018. At the same time, UK organizations, such as universities, businesses, online stores, and social media (like Facebook), have been subject to breaches that affected millions of people. By limiting the right of free movement, Brexit could have a significant impact on the capability of the United Kingdom to fight against cyber criminals and nation-state threats. Additionally, UK-based universities will potentially lose access to huge amounts of EU research funding because of Brexit.

http://bit.ly/31xQxEn

Most EU cookie consent notices are meaningless or manipulative, study finds

New research into how European consumers interact with the cookie consent mechanisms which have proliferated since a major update to the EU online privacy rules last year casts an unflattering light on widespread manipulation of a system that is supposed to protect consumer rights. As Europe's General Data Protection Regulation (GDPR) came into force in May 2018, bringing in a tough new regime of fines for non-compliance, websites responded by adding pop-up legal disclaimers, which signpost visitor-tracking activities. Some of these cookie notices even ask for consent to track you, but many do not—even now—more than a year later. The study, which looked at how consumers interact with different designs of cookie pop-ups and how various design choices can nudge and influence people's privacy choices, also suggests consumers are suffering a degree of confusion about how cookies function, as well as being generally mistrustful of the term "cookie" itself. This is thought to be a growing problem as the EU has tried to implement the GDPR across member states.

https://tcrn.ch/2H4Ewyn

RUSSIA

The Russian submarine that caught fire and killed 14 may have been designed to cut undersea internet cables

On July 1, a Russian navy submarine caught fire, killing fourteen sailors on board. The vessel caught fire near the naval base of Severomorsk. Russia's Defense Ministry said in a statement that the sailors died of smoke inhalation. Two independent Russian news outlets reported that the vessel was the AS-12 Losharik, a nuclear-powered vessel that US officials have said is designed to cut undersea cables that keep the world's internet running, according to BBC Monitoring. Moscow officials have remained secretive, however, about the type of vessel and whether it was nuclear-powered, prompting accusations of a cover-up. American and other Western officials have long warned that

Russian ships have been active near major undersea fiber-optic cables that carry calls, emails, texts, and trillions of dollars' worth of daily financial transactions.
http://bit.ly/2yTOBJS

FSB will be able to remove sites from Runet without trial

One of the structures of the FSB dealing with cybersecurity—the National Coordination Center for Computer Incidents (NCCTC)—can now start the process of depriving sites of their domains that violate Russian law. Unlike blocking through the courts and Federal Service for Supervision of Communications, Information Technology and Mass Media (Roskomnadzor), this new obligation includes that everyone who registers a domain agrees to the possibility of domain blocking in the case of violations. The speed of the procedure is compensated by the limited scope. This is not the case for sites registered outside the Russian national domain zones of .ru and .rf.
http://bit.ly/2N4zJRx

Cyber Warfare: Army Deploys 'Social Media Warfare' Division to fight Russia

Lieutenant General Ivan Jones, the commander of Britain's field army, announced the formation of a cyber warfare unit. The new special cyber operations unit, 6 Division (6 Div), will move beyond the typical cyber capabilities within the military sphere into full-blown social media "information warfare." And here the primary adversary is Russia, which has turned the dark art of peddling fake news and political propaganda across major social media platforms into a national security strategy. Much of the work of the new unit will be relatively traditional signals activities—jamming and intercepting enemy communications, supporting the field world of allied intelligence agencies. Nonetheless, as a sign of the times, the new unit also has an offensive and defensive propaganda remits—taking the social media fight to Russia.
http://bit.ly/2H0Nj4a

APAC

Writers use AI to clone voices for audiobooks

Chinese search engine Sogou is creating artificial-intelligence (AI) lookalikes to read popular novels in authors' voices. It announced "lifelike" avatars of Chinese authors Yue Guan and Bu Xin Tian Shang Diao Xian Bing, both created from video recordings. Last year, Sogou launched two AI newsreaders, which are still used by the government Xinhua news agency. Furthermore, China has witnessed a surge in the number of people wishing to use audio books. It is expected that the market will more than double between 2016 and 2020, to 7.8 billion Chinese yuan (£900 million) a year. Using digitized synthetic voices, it is now a simple process to use text-to-speech technology to quickly generate an audio version of a book. At present, most people prefer audiobooks that are "professionally narrated" by authors, actors, or famous public figures. Today, advances in machine learning and speech-to-text technologies mean that digitized voices are becoming more lifelike and replicate these voices perfectly. For example, the company Lyrebird allows clients to create custom "vocal avatars" from just a one-minute recording of their voices. On its website, it showcases its services with two audio recordings of former US President Barack Obama and current US President Donald Trump, created by using machine learning.
https://bbc.in/33wbEsn

A phishing campaign with nation-state hallmarks is targeting Chinese government agencies

A group of hackers with possible links to a threat group are trying to steal usernames and passwords from Chinese government officials as part of an apparent cyber espionage effort. Malicious websites with registrations dating back to 2018 that impersonate email login pages from numerous ministries, including the Chinese Foreign Ministry, were discovered. However when conducting their attack the group mistakenly tied multiple subdomains to individual Let's Encrypt certificates, allowing anyone who investigated the

certificates to quickly determine all of the sites. One certificate with a validity period from April 23 through July 22 of this year was used for nine distinct subdomains, which then were disguised as login pages of the Chinese Foreign Ministry. Two independent experts suggested the attack appears to be nation-state activity because of the organizations targeted; the use of Let's Encrypt, which is known to be used by nation-state hackers and scammers alike; and most notably, the IP addresses involved, which two sources said they already have been tracking independently. However, it is not possible to definitively determine whether the attack was actually conducted by a state.
http://bit.ly/2YZGytT

China's cyber spies make money on the side by hacking video games

Members of a prolific state-sponsored Chinese cyber espionage operation are using their hacking skills to carry out financially motivated cyberattacks against targets around the world. Dubbed APT41, the group spies on organizations worldwide across fifteen sectors, including healthcare, high-tech, telecommunications and higher education. The attacks coincide with "Made in China 2025," Beijing's strategy to push China toward producing higher value products and services. However, analysis by researchers found members of APT41 are also employing their hacking skills on the side, using them to conduct attacks purely for financial gain, predominantly against the video game industry. It is believed that two attackers, who are Chinese espionage contractors, are working for APT41 and their activity has been traced as far back as 2012, where the main focus for individuals attacking video game companies and players is to make profit.
http://bit.ly/2MfP4iy

UN report: North Korea took $2 billion in cyberattacks to fund weapons program

Parts of a confidential UN report reveals the investigation of North Korea's (DPRK) cyberattacks targeting the financial sector to raise illegal capital for its weapons of mass destruction program, stating that there were "at least 35 reported instances of DPRK actors attacking financial institutions, cryptocurrency exchanges and mining activity... [in some 17 countries]." Some of the countries include South Korea, India, Bangladesh, Chile, Costa Rica, Gambia, Guatemala, Kuwait, Liberia, and Malaysia. The report was compiled by experts and the UN Security Council North Korea sanctions committee, focused on monitoring compliance over the last half year. The report identified the malicious actors as "operating under the direction of the Reconnaissance General Bureau [a top North Korean military intelligence agency]."Cyberspace was utilized to steal and launder the money. Such efforts by North Korea may correlate with sanctions imposed since 2006, which have the high possibility of increasing to include ships importing gasoline and diesel. The report was completed before the missile launched by North Korea in early August.

https://reut.rs/2YP1rUk

https://bit.ly/2KKPkmb

https://bit.ly/2Kw1r7J

MIDDLE EAST

Cybersecurity award launched in Abu Dhabi

Dark Matter Group, the region's first digital and cyber transformation firm, in partnership with the Khalifa University, announced the launch of a cybersecurity award. The joint project invites students and researchers from both local and international institutions to submit ideas that will help smart and digital cities to counter cybersecurity threats. The best applicants will be selected to present their proposals to the Cybersecurity Research Award (CRA) teams. The CRA committee will assess which contestants' ideas best ally technical dimensions and effective cybersecurity solutions to protect and secure smart cities. The first awards will be announced on May 2020.

https://bit.ly/31KzZJx

Emirates' Etihad partners with Swiss blockchain platform Winding Tree

A Swiss blockchain startup, Winding Tree, will give logistical support to the United Arab Emirates' national airline, Etihad, in the building of its internal information system. The open-source travel platform will help Etihad to exploit the distributed ledger technology of blockchain to allocate its products and services. Over the last few years, Etihad has been working along Winding Tree to avoid the use of global distribution systems (such as Amadeus or Sabre) that usually collect and provide data for travel agents. The Swiss platform enables companies (airlines and hotels) to share updated inventory directly with their customers through their platform, bypassing mediators, avoiding related fees, and disrupting the traditional market.

https://nyti.ms/2MXNCAQ

Iran announces new rules to regulate cryptocurrency market

The Iranian government has ratified new rules regarding the regulation of cryptocurrencies and the mining market. Even if the bill does not legalize either the trading of cryptocurrencies inside Iran or digital coins as legal tender whose value would be guaranteed by the Iranian Central Bank, there are some legal evolutions regarding activities related to the cryptocurrency market. Mining digital currencies will be allowed under certain conditions, such as receiving approval from the industry ministry, respecting defined geographical boundaries, paying special electricity charges, and so on. This bill comes soon after the media reported the multiplication of mining farms across the country. Iran is reportedly developing its crypto industry as it could be an alternative means of circumventing international sanctions and accessing foreign currency.

https://bit.ly/2N5DLbY

LATIN AMERICA

Mexico tech revolution may be sitting on cybersecurity bomb

Although Mexico is progressing with its "technological transformation," with projects pending, and defining a cybersecurity strategy, the country's financial payments infrastructure recently faced the consequences of cyber-related malfunctions. Prosa, "a regulated payment, clearing and settlement firm" experienced a system failure, which was said to have been caused by electrical issues. It resulted in the nationwide inoperability of the banking systems' debit and other card transactions for seven hours. The event took place shortly after the government issued details about a plan to ban cash transactions at gas stations and toll plazas. The director of the Software Alliance in Mexico stated at an event about the urgent need for the current administration to "create a national cybersecurity agency that consolidates regulatory power for the online security of citizens, governments, and businesses."

https://bit.ly/33sqZKu

UAVs secured major soccer tournament

The first utilization of drones (Unmanned Aerial Systems) for security efforts in a major sporting game took place in the recent Copa America soccer tournament, organized by CONMEBOL, South America's football authoritative body. The Military Police of Rio de Janeiro in Brazil partnered with Atlas, an autonomous UAS company that develops UAVs, of which one of its partners is the Israeli defense technologies company Rafael. The AtlasPRO drones flew along the Maracana Stadium, providing real time data and wide-range awareness of public safety and hazards, further decreasing emergency response obstacles. Some features of the AtlasPRO include 50 minute flight time, 10 km range, semi to fully autonomous capability, multi-node communication—enabling one operative to control a network of drones simultaneously, and "hot swap"—when a low-battery drone is replaced by a fully-charged one.

https://bit.ly/2KE4fOY