Global Cyber Bi-Weekly Report by INSS April 15 2018

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

Contributors: Simon Tsipis, Ido Sivan, Anna Danilova, Sneha Mukherjee, Bryan McCarthy

ISRAEL

Palo Alto Networks buys Israeli cybersecurity firm Secdo

Palo Alto Networks Inc. is buying Israel-based cyber security firm Secdo. The deal is estimated at around $100 million. Secdo develops software meant to help security teams reduce the incident response time to minutes, through automation, and respond to attacks without affecting business continuity. Large companies get thousands or tens of thousands of security alerts every day, most of which are false positives. Investigating these alerts involves collecting evidence after the fact, which is slow and leaves security teams overextended. Secdo addresses this gap in incident response by continuously and automatically collecting data from all endpoints in the system, e.g., if someone has connected to a specific IP through Microsoft Word on their laptop. Secdo's system investigates alerts automatically using the collected data, and provides users with a full analysis.

https://goo.gl/HFWmY5

Red Team role in IDF cybersecurity – exclusive interview with Sergeant Major M.

It is commonly assumed that the task of cyber attackers will always be easier than the mission of the cyber security teams, because the assailants need only one breach in order to succeed, while the defenders must supply complete security for any breach. A new IDF team dubbed the Red Team operates in order to prevent any cyberattack on the IDF's systems. The mission of the field headed by Sergeant Major M., who recently won the Chief-of-Staff excellence honor, is to defend all the communication and teleprocessing systems operated by the soldiers in the battlefield, supplied by the IDF technological unit. Red Team is a cyber term referring to the enemy color or an internal

attack. Its role is to check the vulnerability of all the military systems — communications, programming, and so on—and create reports regarding their security level. In addition to this role, which is similar to what is done in the civilian cyber sector, the Red Team also fulfills a task unique to the military sector of operating cyber exercises that simulate an internal threat in order to expose situations whereas the unit is not prepared and to reveal the security gaps.

https://goo.gl/RxiLFA

The Israeli army's war on consciousness

"The IDF Spokesperson's Office has come to the understanding that we are actually conducting media operations," said IDF Spokesperson Brig.-Gen. Ronen Manelis. "The IDF's digital platforms are operational tools in the operational arm of the IDF." In the words of the chief spokesperson, the military is engaged in "a war over consciousness" changing what and how people think of Israel, its army — and if you're an Arab—what you think of your own leaders, government, and society. By effectively taunting Arabic-speaking audiences, including Hamas leaders, with pointed and controversial messages and posts on social media, the IDF is able to game social media algorithms so that audiences who would otherwise have no interest in interacting with Israel, let alone its army, are exposed to its propaganda, Manelis explained, giving the example of a recent Twitter face-off with senior Hamas official Moussa Abu Marzouk.

https://goo.gl/Kshsg4

UNITED STATES

Why a Chicago-Based cybersecurity firm just released its prized IP

Halock Security Labs recently gave away its "highly valuable" intellectual property. Halock Security's risk analysis procedure was unique to its firm and something not offered by its peers. It meant they could be selective in choosing clients and creating an air of exclusivity and quality. Guarding the crown jewels of the company no longer seemed ethically or socially worth the monetary rewards. Following a bitter lawsuit in which Halock had to provide testimony damning one of its loyal clients for not following best practices,

practices that the client was not completely aware of how to implement nor of their importance, a change in tact occurred. The partners of Halock decided to make their risk assessment procedures freely open after pairing up with CIS (Center for Internet Security). The new "Duty of Care Risk Analysis" method previously owned by Halock will be paired with CIS's new procedures, now called CIS RAM and released to the public April 30, 2018.

https://trib.in/2HnPujT

The Israel-Massachusetts cybersecurity ecosystem is thriving

Currently over thirty Israel-based cybersecurity firms have offices in Massachusetts and employ over 3,300 workers. A recent report by the Brandeis University International Business School showed that the growth in employment at Israel-founded cybersecurity firms from 2015–2018 is three times higher than the state average. One firm, Empow, is used as an example of the growth in Israel-based cyber firms in Massachusetts. The *Forbes* article highlights what Empow specializes in and the fact it is going through a second round of raising capital as well as bringing on a new CEO who is a veteran of cybersecurity.

https://bit.ly/2veGp85

NSA calls for cybersecurity community collaboration

Unsurprisingly with the massive amounts of terabytes that the National Security Agency (NSA) has to sort through daily, a call has gone out for the community as a whole to work together more efficiently. According to *Computer Weekly*, the ultimate goal of this collaboration is to better attack an adversary and inflict "pain" on aggressors. Dave Hogue, the technical director of the NSA's Cybersecurity Threat Operations Center, believes collaboration can have an effect on adversaries and cause them to be reactive instead of proactive. He stated this during the CyberUK 2018 conference in Manchester on April 10–12. The article goes on to cover structural issues both within the NSA and US Cyber Command, leading into a recently published document by the NSA's Cybersecurity Threat Operations Center, outlining five principles for security operations centers. First, establish a defendable perimeter. Second, ensure visibility across the network. Third, harden computer software for best practices. Fourth, use comprehensive threat intelligence and machine learning. Fifth, create a culture of curiosity. The fifth is pointed out as being the newest

and probably most important principle as it is seen as a way of retaining talented young NSA employees as well as attracting new ones.

https://bit.ly/2HtieW9

EUROPE

Survey: cyber, regulation biggest risks for Europe's businesses

Cyber and regulatory risk have become the biggest concerns for European business executives, overtaking political and economic risk, after several large cyberattacks and ahead of a major shake-up in data regulation, a survey showed. Devastating events such as last year's WannaCry and NotPetya attacks have focused attention on cyber risks, Dave Brosnan, chief executive of insurer CNA Hardy, which compiled the six-monthly survey, told Reuters. The survey of 450 executives from UK multinational firms and fifty executives from European multinationals showed that 25 percent of executives rate cyber risk as their highest concern, followed by 23 percent for regulatory risk, compared with 14 percent and 8 percent six months ago.

https://reut.rs/2JGIexL

UK reveals major cyberattack against ISIS

Britain's leading spy chief revealed that the United Kingdom's first major cyberattack was against the dreaded Islamic State, which hindered the terrorist group's ability to coordinate attacks and suppressed their propaganda. Jeremy Fleming, director-general of the Government Communications Headquarters (GCHQ), told a conference in Manchester that the surveillance agency had conducted a "major offensive cyber-campaign" last year against ISIS. "In 2017, there were times when (ISIS) found it almost impossible to spread their hate online, to use their normal channels to spread their rhetoric, or trust their publications," Fleming said during the CyberUK event organized by the National Cyber Security Center. "This is the first time the UK has systematically and persistently degraded an adversary's online efforts as part of a wider military campaign. Did it work? I think it did This campaign shows how targeted and effective offensive cyber can be," he said.

https://bit.ly/2IWA1nR

Denmark: A leader in cybersecurity

Denmark is among the countries that suffer from lowest number of cyberattacks, according to a report from Microsoft's Security Intelligence, based on data from 400 billion emails and 18 million websites. But despite the positive outlook of the report, consumers, businesses, and public institutions in the Scandinavian country must continue to focus heavily on cybersecurity, given the country's status as a highly digitalized society, Microsoft Denmark said.

https://bit.ly/2qvVNYd

First quarter cyberattacks on UK firms jump 27 percent

Online attacks on UK businesses jumped by over a quarter (27 percent) in the first three months of the year, according to Beaming, a business internet server provider. It claimed that each UK firm experienced on average 600 attempts per day to breach its firewall between January and March 2018, compared to 474 attempts in the same period last year. As per previous months, Internet of Things (IoT) endpoints were targeted the most, accounting for 54 percent of attacks, followed by attempts to compromise corporate databases (11 percent).

https://bit.ly/2EIWrqb

Dark web targeted in crime crackdown by government

Criminals are emboldened by the anonymity of the dark web, which has become a platform for horrific abuse, the Home Secretary said. New funding to crack down on the "dangerous" dark web will be launched by Amber Rudd in a speech at the Government's flagship event for cybersecurity. The National Cyber Security Center's CyberUK conference in Manchester was the backdrop for the launch of a £9 million fund to increase cyber capabilities and tackle organized crime online, focusing on those who use anonymous and hidden online services for illegal activities such as hacking, people trafficking, selling weapons, and drug dealing.

https://bit.ly/2ILvm8a

RUSSIA

Russian authorities continue tightening of internet usage

The Russian State Duma adopted the law on the blocking of information discrediting the honor, dignity, and business reputation of a citizen or legal entity. According to the document, in case of such offenses, a person is given time to voluntarily remove information from the network. Such measures might be considered to further the tightening by the Russian authorities of the free usage of the internet in Russia.

http://bit.ly/2vdTFKq

Russian authorities press to block Telegram messenger in Russia

The Russian Federal Service for Supervision of Communications, Information Technology and Mass Media (Roskomnadzor) has demanded that the court immediately block the Telegram messenger if the agency wins the case against the company. Earlier, Roskomnadzor filed a lawsuit in the Russian court demanding that Telegram be blocked due to the refusal of the instant messenger service to provide the Federal Security Services (FSB) with encryption keys.

http://bit.ly/2GUJdgf

US military review its troops' manuals, adding Russian cyber warfare

Due to a high risk of US troops engaged in Syria to encounter Russian forces, the US Army has crafted a handbook, detailing changes in the Russian military highlighting "anti-access/area denial" weaponry, small drones, electronic and cyber warfare topics, which are believed to be widely used by Russia in the battlefield.

http://bit.ly/2qrR7lW

MIDDLE EAST

Iranian data centers were attacked by hackers leaving the American flag as a message

Several data centers in Iran were attacked as hackers left behind them a message with the American flag saying: "Don't mess with our elections." Some routers were also changed to factory default settings as well. Mr Azari-Jahromi, the Iranian IT minister, tweeted that the country held an emergency meeting as a result of the attack, even though Twitter is not generally accessible to the Iranian public. He said that the core of Iran's National Information Network was not affected. He added that the attack revealed weaknesses in the country's cybersecurity defenses.

https://bit.ly/2H4cEwf

Social media campaign against cyber bullying launched in Egypt

The Greek campus technological park at the American university in Cairo has hosted the launch of a joint social media campaign by the National Council for Childhood and Motherhood under the hashtag #ImAgainstBullying. Cyberbullying made headlines in Egypt on a large scale recently after the infamous Blue Whale game was allegedly linked to the suicide of the son of former parliament member Hamdy El-Fakharany in the Gharbiya governorate.

https://bit.ly/2EOGBdN

UAE, FBI to cooperate in countering cyberattacks

Shaykh Mohammad Bin Rashid Al Maktoum, vice-president and prime minister of the UAE and ruler of Dubai received Christopher Wray, director of the US Federal Bureau of Investigation (FBI). Shaikh Mohammad and Wray exchanged views on a number of issues about the strengthening of cooperation between the authorities in the UAE and the FBI, especially with regard to exchanging information on combating extremism and terrorism at the regional and international levels. The meeting focused on the importance of constructive cooperation between the two sides in order to effectively respond to cyberattacks and electronic piracy. The FBI director referred to the

positive cooperation between the two sides in this regard to protect the interests, security, and stability of the two friendly countries.

https://bit.ly/2vfBCDB

CHINA and APAC

China's strategy to dominate in cyberspace

Each day China is sharpening its strategies and defense in cyber warfare. One of the recent one is the INEW (Integrated Network Electronic warfare) doctrine, combining network attack with electronic warfare. Its IW (Information warfare) militia unit provides each Chinese regional commander with unique network attack, exploitation, and defense capabilities. This unit focuses on improving network attack skills during military exercises. IW units gather intelligence on an adversary's networks, identifying critical nodes and security weaknesses. These units are capable of conducting network attacks that disrupt or destroy the identified critical nodes of an enemy's C4ISR (command, control, communications, computers, intelligence, surveillance, and reconnaissance) assets.

https://goo.gl/WVqbqU

Indian government sets up cyber coordination center to address cybersecurity threats

The Indian government has taken a decision to set up the National Cyber Coordination Center (NCCC) to address various kinds of cybersecurity threats, including threats arising from the misuse of social media. The Minister of State for Home Affairs Hansraj Gangaram Ahir said under the Information Technology Act, content that affects the interests of the sovereignty and integrity of India, India's defense and its security, friendly relations with foreign states or public order or for preventing incitement to the commission of any cognizable offense relating to the above will be blocked or removed.

https://goo.gl/P64N8f

UK government launches cybersecurity export strategy with focus on United States, Japan, India

The Department for International Trade is placing the UK cyber security market at the center of a new export opportunity, with the launch of a new strategy that identifies the United States, Japan, India, the Gulf, and Singapore as potential markets to tap. This new cyber security export strategy supports the ongoing work of the 2016 National Cyber Security Strategy, which provided £1.9 billion of investment in cybersecurity. The launch is backed by ADS, the UK trade association for the security sector, which say the export strategy is an important step to help the leading cyber security companies in the United Kingdom reach new markets and continue to grow.

https://goo.gl/LmcRzo