Global Cyber Bi-Weekly Report by INSS November 15 2018

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

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

ISRAEL

Iran accuses Israel of launching new cyber attack

Iran's telecommunications minister accused Israel of a new cyberattack on its telecommunications infrastructure, after Iran neutralized a virus similar to the Stuxnet virus. The Islamic Republic is preparing to respond with legal action against Israel for the cyberattack through international bodies, Telecommunications Minister Mohammed Javad Azari-Jahromi said. The cyberattack took place at the same day that US sanctions were reimposed, after the sanctions had been lifted by the 2015 nuclear deal. "Recently we discovered a new generation of Stuxnet, which consisted of several parts . . . and was trying to enter our systems," said head of the military unit in charge of combating sabotage, General Gholam Reza Jalali. Stuxnet, which is widely believed to have been developed by the United States and Israel, was discovered in 2010 after it was used to attack a uranium enrichment facility at Iran's Natanz underground nuclear site .

https://bit.ly/2FmsBOa

Israeli cybersecurity startup Coronet enters partnership with DropBox

A California-based provider of products and solutions for the broadcast markets has acquired Israeli chip company Amimon for $55 million. Amimon is based in Silicon Valley and produces chipsets for real-time wireless video transmission. Amimon's main investors are Walden, Evergreen, and Cedar funds. The company will become part of Vitec's Creative Solutions Division and its Israel office will be turned into a research and development center. Amimon has been a supplier to Vitec since 2012 and bought the company to drive growth by taking wireless technology into adjacent markets.

https://bit.ly/2DCXI6a

Snowden: Saudis used Israeli spyware to track Khashoggi

Former US National Security Agency contractor and whistleblower, Edward Snowden, has claimed that software made by an Israeli cybersecurity firm was used to track murdered journalist Jamal Khashoggi. The software used to track Khashoggi, who was killed last month at the Saudi consulate in Istanbul, was created by NSO Group Technologies. NSO's Pegasus spyware had been installed on the phone of Omar Abdulaziz, another dissident and a friend of Khashoggi, according to a report by Canadian research institute Citizen Lab. The spyware is considered the world's most powerful mobile spyware application that allows unrestricted surveillance of mobile phones. The infected cell phone was used to discuss Saudi politics and plan joint projects with Khashoggi in the months before Khashoggi was killed in the consulate .

https://bit.ly/2DC6K3g

UNITED STATES

Internet traffic hijack disrupts Google services

Network monitoring company ThousandEyes detected office-wide connection problems with G Suite, Google Search, Google Analytics, its cloud-hosting services, and other business tools. Traffic passing through the platform was rerouted, suspiciously ceasing at internet service providers Transtelecom in Russia, China Telecom, and MainOne in Nigeria; the former two countries frequently linked to internet surveillance. The engaged circulation, referred as border gateway protocol hijacking, caused a significant denial of service to G Suit and Google Search; the outage—the window of exposed data—lasted about an hour and a half. The undertaking posed the threatening possibility of malicious action in both development and facilitation. None the less, 94 percent of traffic traversing to Google services are encrypted for the purpose of such events transpiring. Google responded with "access to some [of its] services were impacted," suspecting that the source is external to Google, with no impression the incident was malicious. A ThousandEyes executive noted the likelihood of state involvement, with China Telecom, a state-run company as the destination. This has been echoed by the work of scholars from the US Naval War College and Tel Aviv University who have discussed China's thorough efforts in appropriating US online traffic.

https://bit.ly/2PraJ9l

What happens when the US-China cyber agreement is not working

The Trump administration and a number of defense contractors have accused China of violating the 2015 Cyber Agreement, signed by then-President Barack Obama and President Xi Jinping, in which the two countries, among other provisions, committed not to hack each other's businesses for the purpose of economic espionage. Experts suggest the emerging attacks by China on US firms and supply chains correlate to the growing trade war between the two countries. As part of a broader initiation in attribution to cybercrime and China's unchecked trade practices, in the last year, the department of justice has charged three individuals for espionage on behalf of China and is currently prosecuting five other cases, which could provoke more cyberattacks and legal proceedings in the near future.

https://bit.ly/2qLql8T

Pentagon task force not a "quick-fix" to protect critical technology

Amid high profile cyber operations on US defense contractors and other firms led by China, Department of Defense Secretary James Mattis is forming a new cross-functional task force, with the purpose of protecting the Pentagon's classified data, controlled unclassified information, critical technology, and intellectual property of defense-industrial base partners from appropriation and theft. In addition, the task force will refine the prevalent gaps of cybersecurity measures in manufacturing supply chains. The Protecting Critical Technology Task Force will comprise an estimated twenty-five members from at least seven agencies, including the Defense Intelligence Agency, the Defense Cyber Crime Center, and the Army Counter Intelligence, led by Air Force Maj. Gen. Thomas Murphy. The task force will report to Deputy Secretary of Defense Patrick M. Shanahan and Vice Chairman of the Joint Chief of Staff Gen. Paul Selva. The recent increased activities in the department of defense are shadowed by the growing threat of foreign cyber capabilities to US national security, military superiority, and monetary cost to the economy. The latter particularly is representative of the multi-billion dollar losses suffered by companies, caused by intellectual property theft linked to China.

https://bit.ly/2K56vOy

EUROPE

Europol: Internet Organized Crime Threat Assessment 2018

The 2018 Internet Organized Crime Threat Assessment (IOCTA) fifth anniversary edition of the report has been issued. The IOCTA has been and continues to be a flagship strategic product for Europol. It provides a unique law enforcement-focused assessment of the emerging threats and key developments in the field of cybercrime over the last year. Each year the report highlights cyberattacks of an unprecedented scope and scale. This year is no different, demonstrating the continuing need for greater cooperation and collaboration within the law enforcement community, an ethos at the very heart of Europol's mission. The report also brings to attention previously underestimated threats, such as telecommunication frauds, demonstrating the necessity for law enforcement to constantly adapt and develop and the need for continued training in all aspects of cybercrime.

https://bit.ly/2D5vba8

Boundaries between the nation-state and criminal actors more blurred than ever

An analysis of threat activity and behavior across 4,400 companies by the Secureworks Counter Threat Unit (CTU) has concluded that any assumption that nation-state-sponsored Advanced Persistent Threats are "dimensionally different" from advanced cybercrime threats is now fundamentally flawed. In other words, the boundary between the nation-state and cyber-criminal actors is increasingly becoming blurred to the point of being almost irrelevant. Or is it? Researchers compiling the "State of Cybercrime Report 2018" (www.secureworks.com) found that a relatively small subset of professional criminal actors is actually "responsible for the bulk of cyber-crime-related damage" and does so by "employing tools and techniques as sophisticated, targeted and insidious as most nation-state actors".

https://bit.ly/2RWkdWK

Inception hackers target European organizations with old Office flaw

Security researchers have warned that the Inception group of hackers is active again and is using a year-old Microsoft Office vulnerability to attack organizations in Europe. According to a blog post by researchers at Palo Alto Networks, attacks against European targets were observed in October using CVE-2017-11882 and a new PowerShell backdoor, which researchers dubbed Powershower. The attack uses a feature of Microsoft Office called remote templates.

https://bit.ly/2zWgVeY

Spyware disguised as Spanish banking apps removed from Google Play

A spyware program fraudulently disguised as a Spanish-language banking app was found to be collecting users' device data and messages, which were later leveraged in phishing schemes. Advertised as "Movil Secure," the fake app pretended to be associated with the multinational, Spanish banking group Banco Bilbao Vizcaya Argentaria (BBVA). Published on October 19, the app was discovered by Trend Micro researchers three days later and had been available for download on Google Play.

https://bit.ly/2Q21gol

ICO report reaction: UK data security incidents rocket 224 percent

Following the recent release of the data security incident trends report by the Information Commissioner's Office, Egress Software CEO Tony Pepper had some thoughts on the topic and what the startling numbers mean for the industry as a whole. "This increase is likely due to the new data breach notification requirements under the General Data Protection Regulation, which require organizations to report incidents within 72 hours of becoming aware of them," Pepper said.

https://bit.ly/2z9Nk28

Zero-day vulnerabilities found in iPhone X, Samsung Galaxy S9, Xiaomi Mi6 Phones

At the Pwn2Own 2018 mobile hacking competition held in Tokyo on November 13–14, white hat hackers once again demonstrated that even the fully patched smartphones running the latest version of software from popular smartphone manufacturers can be hacked. Three major flagship smartphones—iPhone X, Samsung Galaxy S9, and Xiaomi Mi6—were among the devices that successfully got hacked at the annual mobile hacking contest organized by Trend Micro's Zero Day Initiative, earning white hat hackers a total of $325,000 in reward.

Teams of hackers participating from different countries or representing different cybersecurity companies disclosed a total of 18 zero-day vulnerabilities in mobile devices made by Apple, Samsung, and Xiaomi, as well as crafted exploits that allowed them to completely take over the targeted devices.

https://bit.ly/2FmqUzW

EU cybersecurity organizations agree on 2019 roadmap

Europol, the European Union Agency for Network and Information Security (ENISA), the European Defense Agency (EDA), and the Computer Emergency Response Team for the EU Institutions, Agencies, and Bodies (CERT-EU), have agreed to a roadmap on November 6 for what they describe as concrete activities and deliverables throughout 2019. Prepared by a Memorandum of Understanding (MoU) working group, the four principle bodies met at CERT-EU's premises to update each other on relevant developments and assess the progress made under the MoU, which provides a cooperation framework aiming at leveraging synergies between the four organizations to achieve a safe and open cyberspace.

https://bit.ly/2PXaDpo

RUSSIA

Russia used social media warfare long before the US elections' interference

According to the Washington Post, Ukrainian president Petro Poroshenko appealed to Mark Zuckerberg, the head of Facebook, asking him to open an office in Ukraine and help Ukraine to counter Russian social network warfare, which, according to Ukrainian authorities, was used by Russia long before its interference in US elections in 2016. According to Ukraine, Russia used these same methods already in 2014 during the Maidan revolution in Ukraine, and keeps using it, spreading propaganda, during the Ukrainian conflict in Donbass area.

https://wapo.st/2qMqglu

Pentagon had "finger on the trigger" in case of Russian cyber interference during midterm elections

Pentagon and the CIA had a plan of offensive cyberattack that the United States was prepared to unleash if Russia had electronically interfered with the 2018 midterm election held on November 6. In preparation for its potential use, US military hackers had been given the green light to penetrate Russian cybersystems in order to let the plan unfold quickly.

https://thebea.st/2DEoSd6

Russian reaction on its intelligence agent's massive information leak

The ministry of defense of the Russian Federation has developed a new "Regulations on the processing of personal data in the Armed Forces," regulating the procedure for dealing with personal data of military personnel and envisaging their additional protection. According to the Izvestia news source, the new rules for working with personal data of the military are similar to the rules for working with secret documents. The right to process information will be exclusively given to military officials who have passed a special test. These means of data protection apparently come in response to the scandal involving the personal information of tens of Russian intelligence agents, which was openly accessible due to a leak and poor security measures.

http://bit.ly/2K4QPuO

New security tasks for Russian State Secret Protection Service

The head of the State Secret Protection Service of the Armed Forces of the Russian Federation (ZGT) service, Lieutenant-General Yuri Kuznetsov, told reporters of the Krasnaya Zvezda newspaper that in connection to the rise of the possibilities of information and technical impact and penetration of military and state secret information infrastructures by foreign states and services for offensive and data collecting purposes, the ZGT Service has received new tasks. From now on, it will be also responsible for ensuring the information security of automated systems of the Russian Defense Ministry; that is, detecting, preventing, and eliminating the consequences of cyberattacks on critical military infrastructure and providing technical protection of sites that process information of restricted access.

http://bit.ly/2B5jHAb

MIDDLE EAST

Cyber drills maintain state's digital assets

Qatar started to run cyber drills in 2013, and the first event was joined by 120 participants and 20 entities. Qatar's ministry of transport and communications said that Qatar is one of the leading and first regional nations to run these drills in order to transfer knowledge and experience to other states and companies within their country. The Assistant Undersecretary for Cyber Security Khalid Sadiq al-Hashmi highlighted the importance of digital assets and the role of national cyber drills in protecting the state. The national strategy of Qatar is based on three important elements: the human element, the procedural element, and the technical element. A perfect balance of these elements is necessary to achieve the best results in protecting the information systems in Qatar.

https://bit.ly/2DAYLUg

Middle East cybersecurity market size is projected to reach $20 billion by 2022

According to a market research report published by MarketResearchEngine, the cybersecurity market in the Middle East is expected to grow at an annual growth rate of 22 percent during the period 2016–2022. The growth is driven by the increase in cyber threats, digitalization initiatives, and investment in

homeland security. Middle East cybersecurity reports provides key insights of the cybersecurity industry and projected the Middle East cybersecurity market size to reach $20 billion by 2022. There is a huge demand for better security products since the region of the Gulf Cooperation Council has become the center point for cyberattacks due to its strategic and economic significance .

https://on.mktw.net/2DBuZyL

Oman collaborates with Microsoft to harness 4IR technologies for digital transformation

In efforts to digitally transform the nation, Oman's Information Technologies Authority (ITA) has joined forces with Microsoft. The ITA is responsible for the national infrastructure projects and the supervision of all programs related to the implementation of the Digital Oman Strategy scheduled for 2040. The ITA's responsibility includes providing guidance to other government entities regarding digital transformation projects. The collaboration between Microsoft and the ITA will focus on 4IR. It links physical networks to cyber networks in one system, to capture big date through the Internet of Things. 4IR will work in areas of artificial intelligence, predictive analytics, machine-learning, and blockchain, which will accelerate digital transformation across the public and private sectors of the sultanate .

https://bit.ly/2z7hq67