Global Cyber Bi-Weekly Report by INSS April 1 2018

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

Contributors: Simon Tsipis, Ido Sivan, Anna Danilova

ISRAEL

XM Cyber launches automated APT simulation platform

XM Cyber, an Israel-based company founded by top former cyber intelligence community officials, has unveiled HaXM, the first fully automated advanced persistent threat (APT) simulation platform to continuously expose all attack vectors, above and below the surface, from breach point to any critical organizational asset. HaXM operates as an automated purple team that fluidly combines red team and blue team processes to ensure that organizations are always one step ahead of the hacker. HaXM continuously leverages advanced offensive methods to expose the most critical blind spots. In the process, HaXM provides data-driven remediation that focuses on an organization's critical assets, reduces its IT risk, and enables it to optimize its cyber resources. "The best way to prevent a cyberattack is to identify in advance the attack vectors hackers will use to compromise an organization's critical assets," said CEO and Co-founder Noam Erez.

goo.gl/V7Zrra

Israel to probe Facebook over Cambridge Analytica data breach

Israel's Justice Ministry informed Facebook that it is opening an "administrative investigation" into the social media giant following reports of the transfer of personal information from Facebook to the data-mining firm Cambridge Analytics, "and the possibility of additional violations of Israelis' personal information." Cambridge Analytica been under fire since the *New York Times* and the *Guardian* newspaper reported that it had used data

inappropriately obtained from roughly fifty million Facebook users to try to influence elections, including the 2016 US presidential election. A report by the British Channel 4 revealed hidden camera footage in which Cambridge Analytica's Chief Executive Alexander Nix describes using Israeli private companies' "intelligence gathering" methods to get information about voters. "According to [Israeli] privacy laws, personal information may only be used for the purpose for which it was handed over and may be transferred to another party only if consent has been given," stated the Justice Ministry's Privacy Protection Authority (PPA). Under Israeli law, protected personal data includes any information relating to an individual, whether it relates to his or her private, professional, or public life. It includes names, photos, email addresses, bank details, posts on social network websites, medical information, and even computer IP addresses.
http://goo.gl/Pmvwyi

Bulgaria, Israel consider cybersecurity cooperation

As part of Israel's efforts to expand cooperation with countries in Central and Eastern Europe Bulgaria's President Rumen Radev visited Israel's national computer emergency response team (CERT) in Beersheba. He was accompanied by a delegation of ministers, officials, and businessmen and discussed possibilities of cooperation in the cyber security sphere with Israel. Israel's head of the National Cyber Directorate, Yigal Unna, described the CERT areas of responsibility and how it interacts with other cyber security entities in Israel and presented the lurking cyber security threats and the efforts made to cope with them.
goo.gl/zFWk7K

UNITED STATES

Institute to develop cybersecurity hub for manufacturing

The Digital Manufacturing Design and Innovation Institute (DMDII) announced the launch of a cyber hub for manufacturing with seed funding from the US

Department of Defense (DOD). The hub will serve as a testbed for the creation and adoption of cybersecurity technologies to secure manufacturing shop floors across the United States. DMDII is a public-private partnership as a Manufacturing USA institute sponsored by the DOD, with its goal being to advance digital manufacturing in the United States.
https://bit.ly/2IavQor

United States charges, sanctions Iranians for global cyberattacks on behalf of Tehran

The United States charged and sanctioned nine Iranians and an Iranian company for attempting to hack into hundreds of universities worldwide, dozens of firms and departments of the US government, including its main energy regulator, on behalf of the Iranian government. The cyberattacks, beginning in at least 2013, pilfered more than thirty-one terabytes of academic data and intellectual property from 144 US universities and 176 universities in twenty-one other countries, the US Department of Justice said, describing the campaign as one of the largest state-sponsored hacks ever prosecuted. The US Treasury Department said it was placing sanctions on the nine people and the Mabna Institute, a company that prosecutors characterized as designed to help Iranian research organizations steal information.
https://reut.rs/2G0mrD7

EUROPE

Mastermind behind EUR 1 billion cyber bank robbery arrested in Spain

The leader of the crime gang behind the Carbanak and Cobalt malware attacks targeting over one hundred financial institutions worldwide has been arrested in Alicante, Spain, after a complex investigation conducted by the Spanish national police, with the support of Europol, the US FBI, the Romanian, Moldovan, Belarussian, and Taiwanese authorities and private

cyber security companies. Since 2013, the cybercrime gang has attempted to attack banks, e-payment systems, and financial institutions using pieces of malware that they designed, known as Carbanak and Cobalt. The criminal operation has struck banks in more than forty countries and has resulted in cumulative losses of over EUR 1 billion for the financial industry. The magnitude of the losses is significant; the Cobalt malware alone allowed criminals to steal up to EUR 10 million per heist.
https://bit.ly/2uoWKqh

UK police spend over £ 1 million on cybersecurity training

UK police forces have spent more than £1.3 million in the last three years training its staff on cybersecurity issues. The figures, contained in a new report released by the Parliament Street Think Tank, show that almost 40,000 staff have taken part in the training. North Wales Police lead the way in the amount of training, spending more than £375,000 in the past three years. Most of the funds went into the "Main Stream Cyber Training," a five-day course that trained 147 staff and cost £160,000.
https://bit.ly/2Gat9FM

UK National Lottery: ten million players told to change passwords as attackers hit online accounts

Millions of National Lottery players have been urged to change their passwords following what parent company Camelot describes as "suspicious activity" involving lottery accounts. Camelot, which runs the National Lottery, insists there has not been any access to core systems or databases that would affect lottery draws or prizes, but has recommended that its 10.5 million registered users change their passwords following a number of unauthorized logins.
https://zd.net/2HP3Jej

Survey: One quarter of email attacks result in employee termination

Global market research from Proofpoint, a cybersecurity company, has revealed that nearly one in four email-based attacks (24 percent) resulted in employment termination. Proofpoint's 2018 "Understanding Email Fraud Survey" asked 2,250 senior IT decision makers across the United States, United Kingdom, France, Germany, and Australia for their email fraud experiences over the past two years. The study also showed that 82 percent of boards are concerned with email fraud and more than half (59 percent) consider it a top security risk and no longer just an IT issue. However, almost a third (30 percent) of respondents cited a lack of executive support as a key challenge to email fraud protection deployment.
https://bit.ly/2pFRb2c

New cybersecurity export strategy from UK government to bolster global defenses

The UK government announced the launch of a new strategy to support the export of the nation's cybersecurity technologies. With recent cyberattacks threatening NATO countries as well as large global and UK organizations, the government is hoping to help businesses from both the United Kingdom and allied countries strengthen their defenses and have the best cybersecurity possible. UK international trade secretary Dr Liam Fox says the strategy will help 800 cybersecurity companies to win contracts that provide security for high profile international buyers and protect networks across the world.
https://bit.ly/2GcUG6f

RUSSIA

US intelligence assumption: Russia has access to US critical energy infrastructure

US cyber intelligence authorities are warning that Russian hackers might have access to US critical infrastructure systems. According to the sources,

cybercriminals from Russia have regularly hacked nuclear power plants since 2015. US-CERT noted that a surge in hacker activity also occurred in the spring of 2017, following the inauguration of Donald Trump. The assumption of US intelligence is that Russian hackers have managed to break into the systems and may have access to electricity and other energy supplying stations and could cut them off at a crucial moment of crisis.
http://bit.ly/2pI0wpZ

Russian authorities threaten to block one of the biggest messenger platforms

Russian authorities, the Federal Service for Supervision of Communications, Information Technology, and Mass Media (Roskomnadzor) released a fifteen-day ultimatum to the Telegram social network messenger, demanding that the company deliver to the authorities the soft-keys to access its client's accounts, or else it will be blocked in Russia. Messenger's owner, Pavel Durov replied in his Twitter account that the company stands for protecting the privacy of its users.
http://bit.ly/2GbjqA2

Going further: Roskomnadzor to block fifteen million Amazon-hosted IP addresses used in Russia

The Federal Service for Supervision of Communications, Information Technology, and Mass Media (Roskomnadzor) released a letter addressed to Russian telecommunication companies advising them to block fifteen million IP addresses hosted by Amazon and belonging to users in Russia.
http://bit.ly/2ujW2L0

MIDDLE EAST

Iran rallies against US sanctions on ten citizens

Iran has railed against US sanctions imposed on ten citizens and a tech firm accused of cyberattacks on at least 320 universities worldwide, along with US

firms and government agencies. Tehran called the sanctions a gimmick that was provocative, illegal, and unjustified. By targeting the email accounts of more than 100,000 professors worldwide, the hackers compromised about 8,000 of them, according to the justice department.
https://bbc.in/2GAIr71

New scale of cyber activity from Iran raises concerns

Experts are sounding the alarm about new cyber activity from Iran, as hackers become more emboldened and skilled at carrying out surveillance operations and other attacks outside the Iran's borders. In recent years, Iranian-linked hacker groups have showed signs become more sophisticated, expanding their cyber toolkits and stepping up operations against new international targets, including in the Middle East and the United States. Cybersecurity professionals have detected Iranian hackers breaking into networks of defense contractors, aviation firms, oil and gas companies, technology companies, and telecommunications providers.
https://bit.ly/2pLlrb8

Cyberattack in Saudi Arabia failed to cause carnage, but the next one could be deadly

In August, a petrochemical company with a plant in Saudi Arabia was hit by a new kind of cyber assault. The attack was not designed to simply destroy data or shut down the plant, investigators believe; rather, it was meant to sabotage the firm's operations and trigger an explosion. The attackers were sophisticated and had plenty of time and resources, indicating that they were likely to have been supported by a government, according to more than a dozen people, including cybersecurity experts who investigated the attack and asked not to be identified because of the confidentiality of the continuing investigation.
https://ind.pn/2DW7o7G

CHINA and APAC

Chinese hackers ordered to report software holes to spy agency

Beijing seeks to tighten its control over technology and information. China's intelligence agency has ordered local hackers to abstain from global hacking contests and instead report any vulnerabilities to the security ministry or the affected company. Clearly this is about local control," said Christopher Ahlberg, co-founder and chief executive of the US-based cyber intelligence firm Recorded Future. "Vulnerabilities could be problems in software but are also an opportunity to get backdoors into them."

https://on.ft.com/2GksRJd

WTO envoy: China to respond to US tariffs, resist protectionism

Beijing's ambassador to the World Trade Organization (WTO), Xiangchen Zhang, said that China is preparing a range of responses to planned US tariffs and will stand up to protectionism but still hopes for dialogue. The WTO envoy said China was considering a complaint against the package of tariffs that President Trump was expected to announce later on. China is already under US pressure at the WTO for its industrial overcapacity and its cyber security law. As for the question if China would invoke national security to avoid a WTO dispute over cyber security, ambassador Zhang said China would exercise self-restraint.

https://reut.rs/2Ic0m19

US trade report lays bare Chinese government cyber espionage

According to a US government trade report made public last week, China's government is engaged in a systematic program of cyberattacks on American and foreign companies. American officials say that in response to China's unfair practices, the Trump administration will seek to narrow the trade deficit

between the countries by imposing tariffs on up to US$60 billion worth of still-to-be-identified Chinese goods. The report charges that Chinese cyberattacks service strategic objectives that are aligned with national industrial policies. As part of its overall strategy, the Chinese government has denied any role in the attacks. The report states that "the global economy has increased its dependence on information systems in recent years, cyber theft became one of China's preferred methods of collecting commercial information because of its logistical advantages and plausible deniability."
https://bit.ly/2uksOLV

Japan's Cyber Security Cloud is expanding cloud firewall solution into Southeast Asia

Tokyo-based Cyber Security Cloud (CSC), the Japanese startup behind a cloud-based web application firewall (WAF) called Shadankun, announced that it has partnered with Future Spirits to expand the solution into Malaysia, Thailand, and Vietnam. CSC has specialized in developing cloud-based WAF solutions to secure cloud-based web servers, launched Shadankun in December 2013. Future Spirits is a Japanese cloud-solution company serving Southeast Asian markets through their regional subsidiary Future Spirits Asia. CSC is planning to sell the Shadanukun WAF solution in a bundle with Future Spirit's dedicate server or virtual private server solutions.
https://bit.ly/2I9UipE

Korea's Samsung Heavy's cybersecurity solution for smart ships certified in United States

Korea's Samsung Heavy Industries announced that it has been certified as the world's first provider of cybersecurity technology for smart ships by the American Bureau of Shipping (ABS). Achieving ABS recognition means that the solution can now be used by smart ship operators to protect vessel data, data network, and storage from internal and external cyberattacks. Korea's Samsung Heavy Industries' Smart Ship Solution has demonstrated its ability to

help the next generation of ships to thoroughly respond to cyber risks, the ABS said. Cyber security is increasingly imperative for the shipping and shipbuilding sector amid growing chances that information can be exchanged between ships or between ship and ground facilities. Poor cybersecurity can interrupt business and inhibit productivity by allowing data to be wiped or stolen.

goo.gl/1u1m5H