CYBER DEFENSE NEWS

In Cyber Defense and Security, You are at the Center

Defense Situation Monitoring Center (DSMC) ▪ Management Information System Service (MISS)

30 March 2018 **Issue No. 2018-012**

Google, Twitter Security Chiefs leaving companies

Michael Coates, chief information security officer (CISO) of Twitter, announced on 21 March 2018 that he has decided to leave the social media giant. Senior manager for information security and risk of Google also announced his departure from the company. Said announcements came days after reports that Facebook CISO Alex Stamos is leaving the social media giant in the wake of internal clashes over how to deal the platform being used to spread misinformation. **(SecurityWeek.com, 22 March 2018)**

AMD acknowledges newly disclosed flaws in its processors – patches coming soon

Computer company Advanced Micro Devices, Inc. (AMD), has finally acknowledged 13 critical vulnerabilities, and exploitable backdoors in its Ryzen and EPYC processors disclosed earlier this month by Israel-based CTS Labs. The company promised to roll out firmware patches for millions of affected devices 'in the coming weeks.' According the CTS Labs researchers, critical that affect AMD's Platform Security Processor (PSP) could allow attackers to access sensitive data, install persistent malware inside the chip, and gain full access to the compromised systems. **(TheHackerNews.com, 20 March 2018)**

Zuckerberg admits Facebook mistakes amid Cambridge Analytica fallout

Facebook founder Mark Zuckerberg finally commented publicly on 21 March on his Facebook page about the Cambridge Analytica controversy, in which he admitted "mistakes" were made, and acknowledged his company's "responsibility to protect your data," and that a "breach of trust" occurred regarding that role. He pointed to a "breach of trust" between Cambridge University researcher Aleksandr Kogan (who developed a Facebook quiz app in 2013), Cambridge Analytica and Facebook.

Zuckerberg also state that Facebook learned from reporters in 2015 that Kogan shared user data without people's consent, which was against the company's policies. Meanwhile, U.S. senators and representative of both political parties are demanding answers about Facebook's data practices and whether Cambridge Analytica, which had been doing voter research on behalf of President Trump's campaign usurped data from 50 million Facebook accounts. **(SCMagazine.com, 21 March 2018)**

Facebook scandal could push other tech companies to tighten data sharing

Big internet companies and small software developers alike are likely to face scrutiny over how they share customer information in the wake of the scandal involving Facebook Inc and the British election consulting firm Cambridge Analytica. Lawmakers in the U.S. and the European Union have called for probes into how Facebook allowed Cambridge Analytica to access data on 50 million users and use it to help the election campaign of President Donald Trump. The scrutiny and risk of regulatory action could affect Alphabet's Google, Twitter Inc, Uber

Technologies Inc, Microsoft Corp’s LinkedIn and the many other that make their user data available to outside developers. **(Reuters.com, 22 March 2018)**

No fan of Ninoy, hackers deface Caap website

Hackers known as Anonymous Philippines defaced the Civil Aviation Authority of the Philippines (CAAP) website on 19 March 2018, leaving a message demanding that Ninoy Aquino International Airport (NAIA) revert to its former name, Manila International Airport (MIA). They cited a Change.org petition asking Senators Richard Gordon, Miguel Zubiri and Manny Paquiao to repeal Republic Act 6639, which changed the airport’s name from MIA to NAIA in honor of the slain senator Benigno “Ninoy” Aquino Jr. The hackers however may have targeted the wrong agency as NAIA is under the Manila International Airport Authority under the Department of Transportation and not under CAAP’s management. Meantime, CAAP said that no sensitive information was compromised. **(Inquirer.net, 22 March 2018)**

Facebook uploads call logs, contact numbers, and SMS

Android cellphone users have noticed that Facebook has saved a virtual trove of their personal call data that extends back years, according to a report in Ars Technica. The publication reported that several Android users who pulled down archive data from Facebook found very detailed personal metadata. That information included call logs containing names, phone numbers, and the length of each call made.

In a statement given to Ars Technica, Facebook pointed out that the call log was "a widely used practice to begin by uploading your phone contacts." The person added that users give their consent by uploading their contacts, a function that's optional. People can also delete contact data from their profiles by using a tool available on Web browsers, Facebook stated. **(Cnbc.com, 26 March 2018)**

Hackers tried to cause a blast at a Saudi petrochemical plant

A new cyber-attack against a Saudi petrochemical plant made the headlines wherein hackers attempted to hit the infrastructure in August. According to the New York Times, hackers hit the petrochemical plant in Saudi Arabia with sabotage purposes, and fortunately, the attack failed only because of a code glitch. The said hit was a new kind of cyber assault. The attack was not designed to simply destroy data or shut down the plant, investigators believe. It was meant to sabotage the firm’s operations and trigger an explosion. **(Cyberdefensemagazine.com, 20 March 2018)**

Uber self-driving car struck and killed a woman

The sad page of the book of technology evolution happened when an Uber self-driving car has struck and killed a woman while she was crossing the pedestrian in Arizona. Tempe Police says the vehicle was in autonomous mode at the time of the crash and the vehicle operator, 44-year-old Rafaela Vasquez, was also behind the wheel. No passengers were in the vehicle at the time. The woman was transported to the hospital where she has died. The company immediately suspended its service and all the self-driving cars in the US will be halted according to the Uber CEO. **(Cyberdefensemagazine.com, 22 March 2018)**

Google to invest $300 million to fight fake news menace

Google is working hard to combat the proliferation of fake news. With the company's latest efforts to crack down on fake news and support quality journalism, Google, a unit of Alphabet recently announced new measures termed as Google News Initiative (GNI). The company plans to spend $300 million over three years on different projects to support its new initiatives. Its GNI is focused towards strengthening reliable and quality journalism, supporting new organizations, and empowering credible news through technological innovation. Mr. Philipp Schindler, Google's chief business officer and senior vice-president, said the GNI is aimed at curbing online misinformation and disinformation, detecting "synthetic media" – like digitally altered photographs - and supporting information literacy programs to "build a stronger future for journalism. **(Yahoo.com, 26 March 2018)**

U.S. sanctions Iranian hackers for 'stealing university data'

The United States has imposed sanctions on an Iranian company and 10 individuals for alleged cyber attacks, including on hundreds of universities. The Mabna Institute is accused of stealing 31 terabytes of "valuable intellectual property and data." The U.S. justice department said the firm, which was established in 2013, is accused of carrying out cyber attacks on 144 U.S. universities, and 174 universities in 21 foreign countries, including the U.K., Germany, Canada, Israel, and Japan. It also targeted dozens of companies and parts of the U.S. government.

Nine (9) of the 10 individuals were indicted separately for related crimes. Meanwhile, the two (2) founders of the Mabna Institutes are among those sanctioned and their assets are subject to U.S. seizure according to a statement by the U.S. Treasury Department. **(BBC.com, 23 March 2018)**