CYBER DEFENSE NEWS

In Cyber Defense and Security, You are at the Center

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

13 April 2018 **Issue No. 2018-014**

Palace denies Cambridge Analytica involved in Duterte campaign

Malacañang denied on 10 April 2018 that President Rodrigo Duterte has availed the services of the British political consulting firm Cambridge Analytica, which is currently at the center of a controversy involving improper sharing of data from millions of Facebook accounts. The issue came after the Duterte campaign team was seen in a May 2015 photograph with Alexander Nix, then board director of Cambridge Analytica parent company Strategic Communications Laboratories (SCL). Presidential Spokesperson Harry Roque said Finance Secretary Carlos Dominguez, treasurer of the Duterte campaign team, "assures that he did not pay anything to Cambridge Analytica nor did he transact with them." **(Abs-cbnnews.com, 10 April 2018)**

Facebook says data leaks hits 87 million users, widening privacy scandal

Facebook Inc. said on 04 April 2018 that personal information of up to 87 million users, mostly in the United States, may have been improperly shared with political consultancy firm Cambridge Analytica. The figure is more than the previous news media estimate of more than 50 million. Chief Executive Mark Zuckerberg said in a conference call with reporters that Facebook have not seen "any meaningful impact" on usage or ad sales since the scandal, although he added, "it's not good" if people are unhappy with the company. He also told reporters that he accepted blame for the data leak, which has angered users, advertisers and lawmakers, while also saying that he was still the right person to head the company he founded. **(Reuters.com, 05 April 2018)**

SecurityWeek's ICS Cyber Security Conference returns to Singapore with strong lineup

SecurityWeek's Industrial Control Systems (ICS) Cyber Security Conference returns to Singapore for a three-day event packed with talks from world-renowned experts, unfettered panel discussions, workshops, new research, new technologies, and international networking. This event will bring together top experts in the field of industrial cyber security to discuss the current landscape, pressing challenges, and ways to overcome them. The conference will address a wide range of topics, including protecting critical infrastructure from emerging cyber threats, assessing and understanding risks to ICS environments, and incident response. It will take place on 24 to 26 April at the Fairmont Singapore. **(SecurityWeek.com, 09 April 2018)**

Microsoft Office 365 gets built-in ransomware protection and enhanced security features

Ransomware has been targeting big businesses, hospitals, financial institutions, and individuals, and extorting millions of dollars. Last year, major ransomware outbreaks including WannaCry and NotPetya, wreaked havoc across the world, hitting hundreds of thousands of computers and business networks worldwide. Small to mid-range businesses mostly use Microsoft Office 365 and it has become a primary target for viruses, ransomware, and phishing schemes.

To combat such cyber attacks, Microsoft has announced some new security features for Office 365 that can help users mitigate the damage done by ransomware and other malware infections. According to Microsoft Office blog (https://blogs.office.com), the new features were initially introduced for OneDrive for businesses, but the company is now rolling them out to anyone who has signed out for an Office 365 Home or Personal subscription. **(TheHackerNews.com, 06 April 2018)**

Malware activity slows, but attacks more sophisticated

Figures from Malwarebytes's Cybercrime Tactics and Techniques report for first quarter 2018 revealed that malware activity declined in the first quarter of 2018, with both detections for ransomware and cryptominers lower than the last quarter of 2017. However, major reductions in consumer instances mask an increase in both activities against businesses. This is because businesses can afford to pay higher ransom and may be forced to pay for reasons outside of their own control (to ensure that service level and other contracts are met, or, for healthcare, to ensure continuous service to patients). At the same time, business computers will likely have greater processing capacity for illicit mining. **(SecurityWeek.com, 09 April 2018)**

Researchers link new Android backdoor to North Korean hackers

The recently discovered KevDroid Android backdoor is tied to the North Korean hacking group APT37, Palo Alto Networks researchers said. Also tracked or known as Reaper, Group 123, Red Eyes, and ScarCruft, the APT37 was observed earlier this year to be using a Flash Player zero-day vulnerability and has been expanding the scope and sophistication of its campaigns over the past months.

Recently, the group was said to have targeted victims with Android spyware via spear phishing emails. Cisco's Talos security researchers analyzed the malware, which they called KevDroid, but were not able to find a strong connection with the group. However, according to Palo Alto Networks, KevDroid is indeed a part of APT37's arsenal of mobile tools. Furthermore, the security researchers were able to find a more advanced version of the spyware, as well as Trojanized iterations of legitimate applications that are used as downloaders for the malware. The Android was initially found to be masquerading as an anti-virus app from Naver, a large search and web portal service provider in South Korea. **(SecurityWeek.com, 06 April 2018)**

Cisco protocol abused by nation state hackers

Russian government hackers flagged in March 2018 for targeting U.S. critical infrastructure (CNI) are abusing a Cisco protocol known to have been vulnerable for over a year. The "protocol misuse" issue in Cisco's Smart Install Client was first detailed in February 2017, when Cisco warned that it had detected parties scanning for unsecured versions of the legacy utility, which allows for speedy installation switches. Cisco said some of the attackers looking to abuse the protocol were nation-state Kremlin hackers linked to the attacks on the U.S. energy sector in March. According to Kaspersky Lab, however, the campaign is mostly targeting Russian-speaking segment of the internet, with attackers leaving a message that reads: "Do not mess with our elections" on affected machines with an image of a U.S. flag. **(InfoSecurity-Magazine.com, 09 April 2018)**

Iran hit by global attack that left U.S. flag on screens

The Iranian Communication and Information Technology Ministry said on 07 April 2018 that hackers have attacked networks in a number of countries including data centers in Iran where they left an image of a U.S. flag on screens along with a warning: "Don't mess with our elections." Accordingly, the attack affected 200,000 router switches across the world, including 3,500 switches in Iran alone. The attack, which hit internet service providers and cut off web access for subscribers, was made possible by a vulnerability in routers from Cisco which had earlier issued a warning and provided a patch that some firms had failed to install over the Iranian new year holiday. It was detected late Friday night, 06 April, in Iran and was neutralized within hours with no data lost. **(Reuters.com, 08 April 2018)**

Intel admits it won't be possible to fix Spectre (V2) flaw in some processors

As speculated by the researchers who disclosed Meltdown and Spectre flaws in Intel processors, some of the Intel processors will not receive patches for the Spectre (variant 2) side-channel analysis attack. In a recent microcode revision guidance, Intel admits that it would not be possible to address the Spectre design flaw in its specific old CPUs because it requires changes to the processor architecture to mitigate the issue fully. Intel has marked "stopped" to the production status for a total of nine (9) product families. These vulnerable chip families, which are mostly old that went on sale between 2007 and 2011, will no longer receive microcode updates. This leaves more than 230 Intel processor models vulnerable to hackers that powers millions of computers and mobile devices. **(TheHackerNews.com, 04 April 2018)**

Gamers make the best cyber security experts, McAfee survey says

A new report by California-based security software company McAfee suggested that gamers make the best candidates for cyber security jobs. According to its survey involving 300 senior security managers and 650 security professionals at major corporations, at least 92 percent of respondents say that gamers have the necessary skills for cyber security jobs, such as endurance and perseverance, the urge to look things at a new angle, different perspective and, logic and problem solving skills. The survey also noted that 78 percent of respondents believe that the current generation – which consist of a large population of gamers who began playing video games at a young age, is best suited to handle cyber security roles. **(StraitsTimes.com, 07 April 2018)**

U.S. senators urge Google, Twitter to be transparent about political ads

U.S. senators are urging Alphabet and Twitter to follow Facebook after the latter said it would support efforts to regulate political ads. Two U.S. senators, Sen. Amy Klobuchar, a Democrat from Minnesota, and Sen. Mark Warner, a democrat from Virginia, sponsored the Honest Ads Act, a bill that would require tech companies to disclose how political ads were targeted and how much they cost. The act was drafted in response to Russian trolls abusing Facebook and other online platforms to sow discord among Americans during the 2016 U.S. presidential election. **(Cnet.com, 09 April 2018)**