CYBER DEFENSE NEWS

In Cyber Defense and Security, You are at the Center

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

20 April 2018 **Issue No. 2018-015**

Facebook affirms commitment to protect users' information

Facebook assured on 13 April 2018 that they were committed to protect its users' information and that they were engaged with the Philippines' National Privacy Commission (NPC). This came after the NPC announced that it has launched an investigation on Facebook over a data breach involving British political consulting firm Cambridge Analytica. The NPC sent a letter to Facebook CEO Mark Zuckerberg informing him of the said investigation. According to Facebook, data of about 1.2 million Filipinos were among those 'improperly shared' by Cambridge Analytica. **(Inquirer.net, 13 April 2018)**

Government cyber defenses should look to Ai, behavior analytics, CISCO report

According to Cisco's 2018 Annual cybersecurity report, advances in malware, the increasing use of encrypted web traffic, email threats, and sandbox tactics are all adding to the threat landscape designed to undermine government efforts to protect critical infrastructure and public data. The increased use of cryptojacking, Internet of Things (IoT) attacks, and Distributed Denial of Service (DDoS) attacks were also among the emerging threats government agencies need a plan for.

Researchers said government agencies must secure data and infrastructure in a way that promotes resilience of governance and public services by leading in the securing of data of both the agency and private citizens, keeping key infrastructure and assets secure, and staying ahead of emerging technologies used by adversaries.

One of the proposed solutions is greater adoption behavior analytics tools with 88 percent of government security professionals feeling that they have a good understanding of the value that behavioral analytics can bring to the cybersecurity initiatives.

Another solution is for more agencies to adopt machine learning and artificial intelligence to help monitor encrypted network communications used by various malware samples. **(SCMagazine, 11 April 2018)**

Outlook bug allowed hackers to use .RTF files to steal Windows passwords

A vulnerability in Microsoft Outlook allowed hackers to steal a user's Windows password just by having the target preview an email with a Rich Text Format (RTF) attachment that contained a remotely hosted Object Linking and Embedding (OLE) object. A researcher from the Computer Emergency Response Team (CERT) Coordination Center who discovered the vulnerability explained that by convincing a user to preview an RTF email message with Microsoft Outlook, a remote, unauthenticated attacker may be able to obtain the victim's IP address, domain name, user name, host name, and password hash. Microsoft was notified of the vulnerability in November 2016 and launched a patch that prevents Outlook from automatically initiating Server Message Block (SMB) connections when an RTF email is

previewed. But researchers at CERT suggest the fix could be better. **(ThreatPost.com, 12 April 2018)**

Standards milestones could mark beginning of end for passwords

A Web standards milestone which was announced last 10 April could mark the end of pesky passwords. The new standard, WedAuthn, has won near-final approval from the World Wide Web Consortium, which establishes Web standards. WebAuthn defines a standard Application Program Interface that can be incorporated into a browser and Web infrastructure. It opens the door for new ways for users to authenticate themselves on the Internet that are more secure and convenient than passwords.

WebAuthn, which is based on a specification written by the FIDO alliance, can make the Internet more secure for consumers. FIDO, the world's largest ecosystem for standards-based, interoperable authentication, is resistant to phishing attacks and data breaches. Moreover, WebAuthn incorporates logic which allows for various sources of stronger authentication including biometrics, facial recognition system (FaceID), and external authenticators such as device to device. **(TechNewsWorld.com, 11 April 2018)**

Hackers found a new code injection technique to evade detection

Security researchers at cyber security company Cyberbit found a new code injection technique, dubbed as Early Bird, being used by at least three different sophisticated malware that helped attackers evade detection. As its name suggests, Early Bird is a "simple yet powerful" technique that loads a malicious code in a very early stage of thread initialization, before many security products place their hooks. This allows the malware to perform its malicious actions without being detected. According to researchers, the three malware that were found using Early Bird code injection are: "TurnedUp" backdoor developed by an Iranian hacking group (APT33), a variant of "Carberp" banking malware, and "Dorkbot" malware. **(TheHackersNews.com, 13 April 2018)**

Zuckerberg resists efforts by U.S. senators to commit him to regulation

Facebook Chief Executive Mark Zuckerberg went through the first of two U.S. congressional hearings last 10 April without making any further promises to support new legislation or change how the social network does business. During the nearly five hours of questioning by 44 U.S. senators, Zuckerberg repeated the apologies that he previously made for a range of problems that have beset Facebook, from lack of data protection to Russian agents using Facebook to influence U.S. elections. But he managed to deflect any specific promises to support any congressional regulation for Facebook and other U.S. internet companies. **(Reuters.com, 10 April 2018)**

SMASHINGCOCONUT malware looks a lot like malware used by North Korea in Sony attack

The U.S. Department of Homeland Security (DHS) said that a newly identified malware, SMASHINGCOCONUT, bears a striking resemblance to the malware used by North Korea in the November 2014 cyberattack against Sony. DHS described the malware as "32-bit Microsoft Windows-based wiper malware capable of rendering a Windows-based system inoperable if run using administrator privileges. **(SCMagazine, 12 April 2018)**

Tech firms, including Microsoft, Facebook, vow not to aid government cyber attacks

Global technology companies Microsoft, Facebook and 30 others announced on 17 April the Cybersecurity Tech Accord which is a pledge not to assist any government in offensive cyber attacks. The accord vows to protect all customers from attacks regardless of geopolitical or criminal motive. It also promised to establish new formal and informal partnerships within the industry and with security researchers to share threats and coordinate vulnerability. It builds on an idea for a so-called Digital Geneva Convention. Microsoft President Brad Smith said during a speech at the RSA cyber security conference in San Francisco said that countries should develop global rules for cyber attacks similar to those established for armed conflict at the 1949 Geneva Convention that followed Word War Two. **(Reuters.com, 17 April 2018)**

12-year-old "cyber ninja" shows how a hacker's poison can spread

As Facebook's Cambridge Analytica scandal is fueling the debate on how to protect digital information, Reuben Paul, a 12-year old hacker from Texas, U.S.A. is also raising awareness about the growing cyber threats. Paul, a self-proclaimed "Cyber Ninja" said he's on a mission to show how hacking is child's play. In an interview by CBS News, he hacked a CloudPet's Teddy Bear to demonstrate how they can be exploited to spy on or even harm people, such as turning "smart toys" into listening devices. He also said that Bluetooth and Wi-fi connections that people use almost every day are extremely vulnerable to hacking. As a demonstration, he was able to obtain a CBS reporter's Twitter name and password using a fake page he cloned after the said reporter connected to a public Wi-fi network. **(CBSNews.com, 16 April 2018)**

Intel Processors now allows antivirus to use built-in GPUs for malware scanning

Intel announced on 17 April 2018 two technologies – Threat Detection Technology (TDT) and Security Essentials – that not only offer hardware-based built-in security features across Intel processors but also improve threat detection without compromising system performance. The TDT offers a new set of features that leverage hardware-level telemetry to help security products detect new classes of threats and exploits. It includes two main capabilities – Accelerated Memory Scanning and Advanced Platform Telemetry.

Accelerated Memory Scanning allows antivirus programs to use Intel's integrated Graphics Processing Unit (GPU) to scan and detect memory-based malware attacks while reducing the impact on performance and power consumption. Meantime, Advance Platform Telemetry incorporates cloud-based machine learning and endpoint data collection to better identify potential security threats, "while reducing false positives and minimizing performance impact."

The second security solution is the Security Essentials which is a built-in toolkit which includes a bunch of different hardware-based security features available across Intel Core, Xeon, and Atom processors. Its properties offer a chain of trust to protect against a wide range of attacks. **(TheHackerNews.com, 17 April 2018)**