CYBER DEFENSE NEWS

In Cyber Defense and Security, You are at the Center

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

13 July 2018 **Issue No. 2018-026**

Old malware gives criminals tricky choice: ransomware or mining

The old malware Rakhni Trojan has been rejiggered with a sneaky new trick, allowing adversaries to either extort money from the victims via ransomware, or hijack a computer's CPU via a stealthy cryptominer. Also known as Trojan-Ransomware.Win32.Rakhni was first spotted in 2013. It has mostly been infecting victims in Russia according to Kaspersky Lab and was first distributed via email spam campaigns. The phishing emails that researchers inspected contained fake corporate financial documents, leading them to believe the main targets of the criminals are companies. **(Threatpost.com, 06 July 2018)**

Vietnam activists flock to 'safe' social media after cyber crackdown

Tens of thousands of Vietnamese social media users are flocking to a self-professed free speech platform to avoid tough internet controls in a new cybersecurity law. The said law requires internet companies to scrub critical content and hand over user data if the Vietnam's communist government demands it. Due to take effect on 01 January 2019, it sparked outcry from activists who say it is a chokehold on free speech in the country. Many activists are now turning to Minds, a U.S.-based open-source platform, fearing Facebook could be complying with the new rules. **(SecurityWeek.com, 06 July 2018)**

Keyboard attack "Thermanator" steals passwords using body heat

A new attack discovered by a group of researchers let hackers steal people's passwords by recording thermal residue left on the keyboard after they walk away from it. The researchers from the University of California, Irvine (UCI) concluded that entire password could be recovered within a time span of 30 seconds of the first key being entered using a thermal imagining camera. And partial keywords can be retrieved in under one minute. According to the published report "Thermanator," the researchers attached a FLIR thermal imagining camera 25 inches away from the four standard PC keyboards by Dell, HP, AZiO Prism KB507 and Logitech. The UCI team say that the Thermanator attack can be used to recover verification codes, ATM pins, and even long strings of text.

The "hunt and peck" typists (pressing each key individually while looking at the keyboard) are more vulnerable to password stealing since they take longer completion times, which leaves longer time for keycaps to cool off before recording begins. (**FossBytes.com, 06 July 2018**)

Putin pushes for global cybersecurity cooperation

At a Moscow-based security conference, Russian President Vladimir Putin called on countries to better cooperate in the fight against cyber attacks. He discussed how cyber threats have escalated around the world and said "some nations' egoism and "attempts to act squarely to their advantage" have damaged data stability around the world. He said that Russia has

recently joined efforts with European countries on an agreement to protect personal data. He also claims that Russia would develop a system to automate data exchange between the private sector and law enforcement to improve security. **(DarkReading.com, 06 July 2018)**

Year-old vulnerabilities patched in ISP broadband gear

Patches for three critical vulnerabilities impacting broadband gateways made by Siwtzerland-based Advanced Digital Broadcast (ADB) have been released to the public, nearly two years after the bugs were found. Issues range from a privilege escalation flaw, an authorization bypass vulnerability and a local jailbreak bug. **(Threatpost.com, 05 July 2018)**

China tried to spy on German parliament

German newspaper Süddeutsche Zeitung reported on 06 July 2018 that Chinese spies attempted to bribe members of Germany's Bundestag for information in the form of "analyses." Accordingly, Chinese agents were using fake social media profiles, already networked with several members of the German parliament, to contact German MPs and offer them money in exchange for expertise and insider knowledge. The agents would invite these MPs to China to try to pressure them for information.

Germany's domestic intelligence agency, the Federal Office for the Protection of the Constitution (BfV) flagged last year that Chinese agents were using fake profiles on social networking sites such as LinkedIn to gather personal information about German officials and politicians and called for vigilance. **(DW.com, 07 July 2018)**

Twitter suspends over 70 million accounts in two months: Washington Post

The Washington Post reported that Twitter suspended more than one million accounts a day in recent months to reduce the flow of misinformation. Accordingly, Twitter suspended more than 70 million accounts in May and June, and the pace has continues in July. Twitter and social media platform such as Facebook have been under scrutiny by U.S. law makers and international regulators for doing too little to prevent spread of false content. **(Reuters.com, 07 July 2018)**

Facebook slapped with "maximum" U.K. fine for Cambridge Analytica scandal

Social media giant Facebook recently dealt a blow when a prominent U.K. watchdog imposed a maximum fine on the company for two breaches of the Data Protection Act. The Information Commissioner's Office (ICO) has been investigating the harvesting of Facebook users' data by political consultancy Cambridge Analytica. It is now estimated that a third-party app used by Cambridge Analytica to collect data from Facebook affected a total of 87 million users around the world. Facebook's chief privacy officer Erin Egan said in response to the ICO's report that Facebook should have done more to investigate claims about Cambridge Analytica and taken action in 2015. He added that the company has been working closely with the ICO in their investigation of Cambridge Analytica, as well as with authorities in the U.S. and other countries. (**FossBytes.com, 11 July 2018**)

Intel pays $100,000 bounty for new Spectre variants

Researchers discovered new variations of Spectre Variant 1 (CVE-2017-5752 and they are tracked as SPectre 1.1 (CVE-2018-3693) and Spectre 1.2. Just as researchers published their whitepapers describing the new vulnerabilities, Intel made a $100,000 payment to Kiriansky via the company's HackerOne bug bounty paper. Notably, following the disclosure of the Spectre and Meltdown vulnerabilities in January, Intel announced a bug bounty program for side-channel exploits with rewards up to $250,000 for issues similar to Meltdown and Spectre. The rewards for flaws classified "high severity" can be as high as $100,000. **(SecurityWeek.com, 11 July 2018)**

Polar Flow Fitness app exposes soldiers, spies

Research published by Bellingcat and De Correspondent revealed that the popular fitness app Polar Flow publicized more data about its users in a more accessible way as compared with other comparable apps "with potentially disastrous results." Polar flaw provides functionality that combined all of a person's exercise sessions on a single map. Not only does it reveal heart rates, routed, dates, time, duration and pace of exercise carried out by individuals at military, it also reveals the same information from their homes as well.

In response to the findings, Polar Flow temporarily suspended an API at a website that exposed a rich vein of user information. It emphasized that it had not leaked any data and that there had been np breach of privacy. **(TechWorld.com, 10 July 2018)**

Microsoft releases patch updates for 53 vulnerabilities in its software

Microsoft released on 10 July 2018 security patch updates for 53 vulnerabilities, affecting Windows, Inter Explorer (IE), Edge, ChakraCore, .NET Framework, ASP.NET, PowerShell, Visual Studio, and Microsoft Office and Office Services, and Adobe Flash Player. Out 53 vulnerabilities, 17 are rated critical, 34 important, one moderate and one as low in severity. Users are strongly advised to apply security patches as soon as possible to keep hackers and cyber criminals from taking control of their computers. **(TheHackerNews.com, 10 July 2018)**

DHS aims to turn mobile devices into no phishing zones

The Homeland Security Department and 16 other agencies are upgrading their mobile device security. Phishing attacks remain the misery of information security specialists across government, and as they advance in sophistication. According to DHS officials, the phishing protection update offers security beyond the detection of attacks through SMS messages. The system monitors and prevents attacks that hide inside mobile applications, social media messages and in personal or work email messages. In addition, it inspects any outbound connections at the network level and alerts users and administrators in real-time if connections are harmful. The updated platform will be available for iOS and Android operating systems immediately to 150 million consumer devices worldwide, as well as those issued by federal customer agencies, including DHS. (**DefenseOne.com, 10 July 2018**)