CYBER DEFENSE NEWS

In Cyber Defense and Security, You are at the Center

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

01 June 2018 **Issue No. 2018-020**

Viber tells millions in Philippines: We don't store, share user data

Viber marketing and business development head for Asia Pacific Anubhav Nayyar said that the company does not store or share user data and conversations are secured. He said that unlike other internet platforms, typing the word "pizza," for example, will not flood the user's feed with advertisement for pizza. Viber makes money from paid stickers and a service that allows users to call from the Viber app to a phone without internet connection or a landline. Moreover, conversations on Viber are encrypted from "end-to-end" meaning only those involved in the exchange can read the messages. **(ABS-CBN.com, 30 May 2018)**

Europol signs cybersecurity agreement with EU agencies, WEF

Europol signed on 23 May 2018 two memorandums of understanding related to cybersecurity cooperation – one with the World Economic Forum (WEF) and one with the European Union Agency for Network and Information Security (ENISA), the European Defence Agency (EDA), and the EU's Computer Emergency Response Team (CERT-EU). The MoU between Europol, ENISA, EDA and CERT-EU establishes a cooperation framework on cyber security and cyber defense. The agreement focuses on cyber exercises, education and training, exchange of information, strategic and administrative matters, and technical cooperation. It also allows cooperation in other areas that may turn out to be important for all four organizations.

As for the MoU signed by Europol and the WEF, it focuses on establishing a cooperation framework whose goal is to make cyberspace safe for individuals, businesses and organizations. The WEF and Europol recently announced the launch of a Global Cyber Security Centre located in Geneva, Switzerland. **(SecurityWeek.com, 25 May 2018)**

Facebook and Google are already facing lawsuits under new data rules

Europe's sweeping data protection law came into force on 25 May 2018 and legal experts say big tech companies are already violating the new rules. Facebook and its subsidiaries Whatsapp and Instagram, as well as Google are facing lawsuits for failure to comply with the General Data Protection Regulation (GDPR). Said companies could face billions of dollars in fines if European regulators agree they failed to comply. According to legal experts, Facebook is breaking a GDPR rule intended to prevent companies from hoovering up sensitive information like political opinions, religious beliefs, ethnicity and sexuality without their users' consent. **(CNN.com, 25 May 2018)**

U.S. judge dismiss Kaspersky suits to overturn government ban

A U.S. federal judge dismissed on 30 May 2018 the two lawsuits by Kaspersky Lab that sought to overturn bans on the use of the security software maker's products in U.S. government networks. The company said it would seek to appeal the decision, which leaves in place prohibitions included in a funding bill passed by Congress and an order from the U.S. Department of Homeland Security. To note, the ban were issued last year in response to allegations by U.S. officials that the company's software could enable Russian espionage and threaten national security. **(Reuters.com, 31 May 2018)**

Afghan diplomats in Pakistan targeted by 'state-backed hackers'

Afghan diplomats in Pakistan have been warned that they are believed to be victims of "government-backed" digital attacks trying to steal their email passwords. Afghan embassy sources said they received alerts from Google this month. Last week Amnesty International detailed attempts to install malware on computers and phones of activists critical of Pakistan's military. The army did not comment on allegations that intelligence services were to blame. **(BBC.com, 26 May 2018)**

UK warns that aggressive cyber attack could trigger kinetic response

UK says it doesn't need to demonstrate attribution before engaging cyber retaliation. In his speech at the Royal United Services Institute (RUSI) last week, Air Marshall Phil Collins, Chief of Defence Intelligence, UK Ministry of Defence, he talked about the growing use of non-kinetic (primarily cyber) warfare. He cited several examples like the unprecedented espionage activity against the UK and allies, private security contractors being used in high-end expeditionary warfare in Syria, cyber-attacks against national infrastructure and reputation across Europe, information operations that attempts to pervert political process and frustrate the rule of law, and attempted assassinations.

He warned that the nature of modern warfare is becoming broader, more strategic, and features "continuous full spectrum competition and confrontation." He said that the UK requires the ability to both respond to cyber-attacks and if necessary launch preemptive cyber-attacks effectively in self-defense. **(SecurityWeek.com, 25 May 2018)**

Phishers target Facebook to harvest user data

According to Kaspersky Lab's Spam and phising in Q1 in 2018 report, Facebook dominated attempts to phish unsuspecting netizens, accounting for 60% of all social network. Following Facebook, Russian social platform VK (21%), and LinkedIn (13%) were most commonly targeted, with victims tricked into handing over names, log-ins, and even credit card numbers. The reasons are that cyber-criminals follow the money, and with over two billion active monthly users, there is more opportunity to generate revenue in Facebook. Overall, the main targets for phisers remain internet portals, banks, online stores and payment services, with financial phishing the most popular (44%) type. **(InfoSecurity-Magazine.com, 24 May 2018)**

Singapore ISP leaves 1,000 router open to attack

According to IT security company NewSky Security, Southeast Asian telcom giant Singapore Telecommunications Limited (SingTel) left approximately 1,000 customer routers wide open to potential attack via an unprotected port. The flub occurred after the region's largest internet service provider (ISP) conducted remote maintenance on affected routers and failed to secure equipment when the work was complete. NewSky alerted the region's Singapore Computer Emergency Response Team (SingCERT) that worked with SingTel to resolve the issue. **(ThreatPost.Com, 28 May 2018)**

Sonic tone attacks damage hard disk drives, crashes OS

Using sonic and ultrasonic soundwaves as a weapon, researchers can disrupt the read, write and storage functions of a hard disk drive (HDD). The method can also be used to crash the host operating system, and in some cases damage targeted drives. Researchers said the attacks can be performed by “nearby emitters” that target a computer’s HDD; so attacks could be performed by an adversary using inexpensive off-the-shelf speakers or could also be carried out via laptop or desktop speakers. The attack scenarios were outlined by researchers from the University of Michigan and Zhejian University in China. The group presented their research last week in San Francisco at the IEEE Symposium on Security and Privacy. **(ThreatPost.com, 29 May 2018)**

Google patches reCAPTCHA bypass

Google has fixed a bypass for its reCAPTCHA authentication mechanism – the Turing test-based methodology for proving that website users are not robot, commonly spotted on log-in pages online. The news comes as Google releases a new version of reCAPTCHA in beta. Google has been working on refining and strengthening reCAPTCHA for years, and last year extended it to mobile websites for Android users.

There has been a reported problem. Accordingly, once a user solves the challenge and clicks verify, the reCAPTCHA function sends an HTTP request to the web application. That in turn sends its own request to the Google reCAPTCHA API, which both verifies itself as a trusted application and requests verification that the visitor solved the reCAPTCHA correctly.

An exploit for the bypass vulnerability required an HTTP parameter pollution in the web application, according to independent app security expert Andres Riancho, who reported the bypass. In other words, the web application would need to send verification requests to the reCAPTCHA API in an insecure way. This reduces the severity of the flaw, but also leads to a 100-percent success rate. Google has fixed the security issue upstream in the reCAPTCHA REST API, which fortunately means no modifications are required to the affected web applications. **(ThreatPost.com, 29 May 2018)**

Hackers infect 500,000 consumer routers all over the world with malware

Hackers possibly working for an advanced nation have infected more than 500,000 home and small-office routers around the world with malware that can be used to collect communications, launch attacks on others, and permanently destroy the devices with a single command, researchers at Cisco warned. Cisco reported about the malware called VPNFilter which is assumed to have targeted around 500,000 routers to create a massive botnet. It is believed that the malware, having a resemblance to BlackEnergy malware, could have its roots originating in Russia. It works on consumer-grade routers made by Linksys, MikroTik, Netgear, TP-Link, and on network-attached storage devices from QNAP. It’s one of the few pieces of Internet-of-things malware that can survive a reboot. Infections in at least 54 countries have been slowly building since at least 2016. **(Arstechnica.com, 24 May 2018)**

Real-time location data of nearly all U.S. smartphone users exposed

A cell phone tracking service called LocationSmart has been leaking real-time location data on millions of mobile phone customers across North America. Exploiting a bug in its website, anyone could track the location of U.S. cell phone users without obtaining their consent. This bug was spotted by Robert Xiao, a Carnegie Mellon University researcher, in a free trial feature of the website. LocationSmart provided a free of cost demo service which allowed anyone to see the approximate location of a mobile phone. The site was designed to ask for users' consent through their cellphone before passing on location data. A flaw in an API that powers the website made it possible to bypass the consent process and just about anyone could obtain real-time location data of any user. **(Fossbytes.com, 18 May 2018)**

Android devices found preinstalled with Adware Cosiloon

Thousands of Android devices owned by users in over 100 countries have been found preinstalled with the adware Cosiloon. Over a hundred varying models are affected, most of which are equipped with MediaTek chips, and a majority are tablets not certified by Google. Google is aware of the issue and is working on mitigation steps for the app variants and for several device models. Device manufacturers and firmware developers have also been notified as new device models were found still carrying the adware. Cosiloon pushes ads on webpages or apps users are accessing. The researchers who looked into the adware reported that it cannot be easily removed because it is installed at the firmware level and uses heavy and complex obfuscation.

To make sure that mobile devices are protected, the following must be followed: avoid clicking on pop-up ads while using your browser or app; regularly download patches to ensure that your operating system or application is updated; and, flag suspicious application behavior so developers can analyze and address issues. **(Trendmicro.com, 29 May 2018)**

Symantec ProxySG Security Restriction Bypass Vulnerability

A vulnerability has been identified in Symantec ProxySG wherein a remote user can exploit this vulnerability to trigger Security Restriction Bypass on the targeted system. When configured to authenticate network users with a Security Assertion Markup Language (SAML) authentication realm, ProxySG incorrectly handle responses. A remote attacker can modify a valid response without invalidating its cryptographic signature to bypass authentication security controls. No patch is currently available. **(Hkcert.org, 31 May 2018)**