CYBER DEFENSE NEWS

In Cyber Defense and Security, You are at the Center

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

08 June 2018 **Issue No. 2018-021**

Philippine internet speed grew most among SEA countries in 5 years

Data from Yugatech showed that average internet speed in the Philippines for fixed broadband had the most growth in the last five years compared with neighboring Southeast Asian countries. Based on data from Ookla Speedtest Global Index April 2018, from 3.5 Megabits per second in 2014, the average speed has gone up to 17.62 Megabits per second as of April 2018 for fixed broadband. This amounts to a 403 percent increase. On mobile internet, the average speed clocked in at 14.01 Megabits per second. Malaysia came in second at a close 391 percent growth, with an average internet speed of 26.9 Megabits per second. **(Inquirer.net, 31 May 2018)**

Federal agencies respond to 2017 cybersecurity Executive Order

The U.S. Department of State, the Department of Homeland Security (DHS), the Department of Commerce, and the Office of Management and Budget (OMB) published reports last week in response to the cyber security executive order signed by U.S. President Donald Trump last year in an effort to improve the protection of federal networks and critical infrastructure against cyber attacks.

The Department of State, which published two reports believes that the U.S. can deter both state and non-state actors using two approaches: improving security of networks, and through "cost imposition." Meantime, the OMB published a Federal Cybersecurity Risk Determination Report and Action Plan which assessed that the 96 civilian agencies showed 71 of them had been assigned an "At Risk" or "High Risk" rating for their ability to identify, detect and respond to cyber incidents and recover from them.

Meantime, the DHS and the Commerce Department in their report stated that there had been nearly 300,000 cybersecurity-related job openings in the US as of August 2017. The agencies believe veterans represent an underutilized workforce supply, and women and minorities are underrepresented in the field. **(SecurityWeek.com, 04 June 2018)**

North Korea-linked group stops targeting U.S.

A threat actor linked to North Korea's Lazarus Group has stopped targeting organizations in the U.S. but remains active in Europe and East Asia. The group, tracked by industrial cybersecurity firm Dragos as Covellite, has been known to target civilian electric energy organizations in an effort to collect intellectual property and information on industrial operations. Unlike some other actors whose activities have been monitored by Dragos, Covellite does not currently have the capability to disrupt industrial control systems (ICS). However, the security firm does see it as a primary threat to the ICS industry. **(SecurityWeek.com, 07 June 2018)**

Researchers warn of Microsoft ZeroDay RCE bug

Researchers have discovered a medium-severity Windows vulnerability that enables remote attackers to execute arbitrary code. But Microsoft has not issued a patch yet. The flaw, which was first discovered by Dmitri Kaslov of Telspace Systems, exists within the handling of error objects in JScript, according to a Tuesday advisory by Trend Micro's Zero Day Initiative group. However, there is so far no indication that the vulnerability is being exploited in the wild and it's likely because the bug would only be one part of a successful attack. **(ThreatPost.com, 01 June 2018)**

Facebook defends against device-integrated APIS policy, but concerns remain

Facebook is hitting back against a New York Times article alleging that it struck deals enabling phone-makers to access users' personal information. The article, posted on 02 June 2018, said Facebook reached a data-sharing partnerships with at least 60 device-makers including Apple, Amazon, Microsoft and Samsung, over the last decade. While these deals enabled vendors to offer customers integrated features with Facebook, like messaging and address books, the New York Times said that it found that they could also access the data of users' friends without their consent.

Facebook published a blog on 03 June 2018 defending its device-integrated application program interface (API) policies saying that while they agree with many of past concerns about controls over Facebook information shared with third-party app developers, it disagrees with the issues raised on APIs. Facebook Vice President of Product Partnerships Ime Archibong stressed that Facebook's device API policy is very different from the public APIs used by developers by Kogan, as Facebook's device partnerships were built on common interest, which is the desire for people to be able to use Facebook whatever their device or operating system is, and not necessarily the intent of collecting data. **(ThreatPost, 04 June 2018)**

Google Groups are leaking your sensitive emails: here's how to fix it

Security firm Kenna Security found that nearly one-third of 9,600 public Google Groups leaked sensitive information in emails sent through the platform. The said security firm found such public groups held by many prominent websites, including Fortune 500 companies, hospitals, universities, newspapers, and even U.S. government agencies. The post says that a misconfiguration in settings results in leakage of emails containing invoices, passwords, and other credentials. Things that people would not want to be shared on the internet. Accordingly, Google Groups has "complex terminology" and conflict between "organization-wide vs. group-specific permissions" which causes list admins to "inadvertently expose e-mail list contents." Apparently, when a G-Suite admin creates a Groups mailing list for specific recipients, it also provides a web interface for the list at https://groups.google.com. The privacy settings for each Google Group should always be set to "Private" if the group is meant to be internal to the company. **(Fossbytes.com, June 4, 2018)**

Europol forms new Dark Web Team to combat online criminal marketplace

Europol announced last week the formation of a "Dark Web Team" specifically dedicated to investigating and shutting down underground internet marketplaces, with the assistance of law enforcement agencies and operational third-party partners throughout the European Union. The unit will be responsible for sharing information; providing operational support and expertise; developing investigatory tools, tactics and techniques; organizing training and

capacity-building initiatives; and instituting prevention and awareness campaigns. **(SCMagazine.com, 01 June 2018)**

Drastic changes required to protect mobile users against cyber-attacks

During a U.K Mobile Security Event called Level 2018, it was pointed out that organizational practices and end-user behavior must both change fast to deal with the rising mobile-focused cyber attacks such as phishing, that are now more pervasive than malware. Industry leaders agreed that enterprises need to evolve their thinking on mobile protection by improving end-user solutions that can provide robust protection against the broad range of mobile threats. Dr. Michael Covington, vice president of product at mobile security company Wandera said that a more data-driven approach is needed, where more data points are examined. He also said that imminent advances in machine learning will also be a key facilitator of this, enhancing ability to predict and track attack patterns so they are blocked in real-time as soon as possible. **(SC Magazine.com, 04 June 2018)**

Google explains 'weird' 1975 text message bug

Google has addressed an unusual glitch in its Search and Assistant apps that made SMS text messages appear when specific search items were entered including "the 1975..com" and "izela viagens." The said glitch was discovered by an Android user on Reddit. Google said that it was a "language detection bug" that was being fixed. The company said the app could only display text messages if it had been given permission to do so, and it had implemented a fix that would be distributed within a few days. **(BBC.com, 01 June 2018)**

Apple jams Facebook's web-tracking tools

Apple's software chief Craig Federighi said that Apple will attempt to frustrate tools used by Facebook to automatically track web users within the next version of its iOS and Mac operating systems. He added that the web browser Safari would ask owners' permission before allowing the social network to monitor their activity. Mr. Federighi said that Facebook keeps watch over people in ways they might not be aware of. Meantime, cyber security expert Kevin Beaumont applauded the move and said that Apple is making changes to the core of how the browser works, surprisingly strong changes that should enable greater privacy. **(BBC.com, 04 June 2018)**

Firefox and Chrome bug leaked Facebook profile details for almost a year; now fixed

A vulnerability existed in the implementation of the CSS3 feature called "mix-blend-mode." It allowed an attacker to de-anonymize a Facebook user running Google Chrome or Mozilla Firefox by making them visit a specially crafted website. The flaw, which is now fixed, was discovered last year by the researcher duo Dario Weißer and Ruslan Habalov, and separately by another researcher named Max May. The researchers enabled them to harvest data like the profile picture, username, and 'like' status of unsuspecting visitors when a user visits a malicious site.

The exploit didn't affect Internet Explorer (IE) and Edge as the web browsers don't support the required feature. Safari wasn't affected either for some reason. While the flaw has been patched for good, the researchers warn that the advanced graphics capabilities added to Hypertext Markup Language (HTML) and Cascading Style Sheets (CSS) could open doors for more attacks like these. **(Fossbytes.com, June 1, 2018)**

Over 92 million MyHeritage emails containing hashed passwords breached

Online genealogy platform MyHeritage revealed that a security breach occurred in October 2017 after receiving a file containing the email addresses and hashed passwords of all users who signed up. It announced they will expedite ongoing development of stricter security measures – such as two-factor authentication (2FA) – and strongly advised users to change their passwords.

Accordingly, the company's Chief Information Security Officer received an email from an undisclosed researcher containing a file named "myheritage" that was reportedly retrieved from a server outside the company. An investigation uncovered the file containing a list of 92,283,889 emails and hashed passwords of legitimate users up to October 26, 2017. The company is looking further into the incident to determine the depth of the intrusion. It urged that all users should change their passwords immediately "for maximum safety." **(Trendmicro.com, June 6, 2018)**

Amazon and EBay pull CloudPets smart toys from sale

Amazon and eBay are among retailers pulling Spiral Toys' cuddly smart toys from sale after warnings they pose a cybersecurity threat. Concerns were raised about CloudPets products in February 2017 after it was discovered that millions of owners' voice recordings were being stored online unprotected. The CloudPets range includes a number of soft animal toys that are fitted with a microphone and speaker. These allow children to record their own messages and play back the voice recordings of friends and family members, which are uploaded to the net via a Bluetooth-connected app. These data are exposed online and had been accessed multiple times by unauthorized parties. Moreover, anyone can connect to the toy as long as it is switched on and not currently connected to anyone else. Although the toys no longer appear on Amazon's U.S. store, they are listed on its U.K. site. Meantime, Walmart and Target are among the other U.S. companies reported to be halting sales. **(BBC.com, 06 June 2018)**