CYBER DEFENSE NEWS

In Cyber Defense and Security, You are at the Center

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

02 March 2018 **Issue No. 2018-008**

Russia and China Racing to Get Satellite Jammers

Weapons capable of jamming or destroying U.S. military and commercial satellites will reach initial operational capability in the next few years, according to a new intelligence report. Said report, which is titled "Worldwide Threat Assessment" and authored by National Intelligence Director Daniel Coats, state that the space domain will become ever more congested as hostile actors launch weapons into orbit.

The report added that Russia and China aim to have nondestructive and destructive counter space weapons available for use during a potential future conflict. It also assessed that, if a future conflict were to occur involving Russia or China, either country would justify attacks against U.S. and allied satellites as necessary to offset any perceived U.S. military advantage derived from military, civil, or commercial space systems. However, the U.S. military is already budgeting to shore up defenses against such attacks. **(Military.com, 16 February 2018)**

New North Korean hacking threat to worry about

Cybersecurity research firm FireEye reported on 20 February 2018 that another group of North Korean hackers dubbed as Reaper stepped up efforts to spy on big South Korean conglomerates. Most of the global cyberattacks previously tied to North Korea have been attributed to a group known as Lazarus. FireEye said Reaper is now another threat that governments and companies need to keep an eye on. John Hultquist, FireEye's director for intelligence analysis declined to name the target firms but said that they are Fortune Global 500 companies that are "the crown jewels" of the South Korean economy.

FireEye said Reaper has been active since at least 2012. It drew little attention as it discreetly spied on South Korea's government, military, defense, and media sectors. But last year, the hackers became more ambitious, targeting South Korean conglomerates in industries like aerospace, electronics, automotive, and manufacturing. **(CNN.com, 20 February 2018)**

Year-old Coldroot RAT targets MacOS, still evades detection

Researchers are warning users about the Coldroot remote access Trojan (RAT) that is going undetected by Anti-Virus engines and targets MacOS computers. The RAT is cross-platform and capable to planting a keylogger on MacOS systems prior to the OS High Sierra and is designated to steal banking credentials. The malware appears to have been for sale on underground markets since 01 January 2017 and versions of the Coldroot code have also been available on GitHub for nearly two years. **(Threatpost.com, 20 February 2018)**

Senate OKs bill on "lifetime" cellphone numbers

The Senate approved on 20 February a bill allowing cellphone users to keep their numbers for life, even if they change service providers of subscription plans. Senate Bill No.1636, the proposed "The Lifetime Cellphone Number Act," was sponsored and authored by Senator

Sherwin Gatchalian and was passed with 20 yes votes. **(CNNPhilippines.com, 20 February 2018)**

A.I. ripe for exploitation, experts warn

A report titled The Malicious Use of Artificial Intelligence (AI) warns that AI is ripe for exploitation by rogue states, criminals, and terrorists. The authors of the report said that those designing AI systems need to do more to mitigate possible misuses of their technology and that the governments must consider new laws. The report calls for the following:

- Policy-makers and technical researchers to work together to understand and prepare for the malicious use of AI.

- A realization that, while AI has many positive applications, it is a dual-use technology and AI researchers and engineers should be mindful of and proactive about the potential for its misuse.

- Best practices that can and should be learned from disciplines with a longer history of handling dual use risks, such as computer security.

- An active expansion of the range of stakeholders engaging with, preventing and mitigating the risks of malicious use of AI.

Significantly, the 100-page report identified three areas in which the malicious use of AI is most likely to be exploited: digital, physical, and political. **(BBC.com, 21 February 2018)**

uTorrent users warned of remote code execution vulnerability

Google Project Zero researchers are warning against two critical remote code execution vulnerabilities in popular versions of BitTorrent's web-based uTorrent Web client and its uTorrent Classic desktop client. According to researchers, the flaws allow a hacker to either plant malware on a user's computer or view the user's past download activity. The developer of the uTorrent apps, BitTorrent said the flaw has been fixed in the most recent beta version of the uTorrent Windows desktop app. A patch for the existing clients will be pushed out to users in the coming days. **(Threatpost.com, 21 February 2018)**

U.S. Transportation Security Administration (TSA) wants your face to be your passport

With current technology, travelers could find biometric identification to be much slower and prone to error. But as of this week, the U.S. Transportation Security Administration (TSA) is trying to streamline the experience, with an opt-in pilot program using biometric facial recognition technology, which is aimed at verifying and matching a passenger's identity to their travel documents. It is projected to automate the often repetitive and human error-prone process of verifying a passenger's boarding pass and passport several times over before boarding. The pilot project is being run at the boarding gate but documents will also be manually checked during the test program to ensure no security lapses would take palace. According to aviation industry intelligence company CAPA Centre for Aviation, the plan is in keeping with President Donald Trump's wider aims to tighten border security measures. **(DefenseOne, 21 February 2018)**

PNP data breach: Sensitive details of 10,000 credit, debit card holders leaked

India's Punjab National Bank (PNB) is reeling under great stress due to the banking fraud issue that happened recently. To add to the problems, a new data breach has been reported by The Asia Times, which has allegedly compromised sensitive data of some 10,000 credit and debit card holders. The data includes names, expiry dates, personal identification numbers and even card verification values of around 10,000 bank account holders. The leaked data has two sets of packages one with Card Verification Value (CCV) and the other without.

The Asia Times reported that this information has been available on the internet for three months. The breach was discovered by CloudSek Information Security, a Singapore based company that keeps a close eye on data transactions, even on sites that are unlisted on Google Search or any other major search engine. **(Businesstoday.in, 23 February 2018)**

Email inboxes still the weakest link in security perimeters

According to Finnish cyber security and privacy company F-Secure, over one-third of all security incidents start with phishing emails or malicious attachments sent to company employees. The single most common source of breaches analyzed in the report was attackers exploiting vulnerabilities in an organization's Internet facing services, which accounted for about 21 percent of security incidents investigated by F-Secure's incident responders. Phishing and emails with malicious attachments together accounted for about 34 percent of breaches which F-Secure says make attacks arriving via email a much bigger pain point for organizations. **(Helpnetsecurity.com, 23 February 2018)**

Intel did not tell U.S. cyber officials about chip flaws until made public

Intel Corporation did not inform U.S. cyber security officials, particularly those from the United States Computer Emergency Readiness Team (US-CERT), regarding the so-called Meltdown and Spectre chip security flaws until they are leaked in public six months after Alphabet Inc notified Intel of the problems. Current and former U.S. government officials have raised concerns that the government was not informed of the flaws before they became public because the flaws potentially held national security implications. Intel said it did not think the flaws needed to be share with U.S. authorities as hackers had not exploited the vulnerabilities. **(Reuters.com, 23 February 2018)**

Developer gets prison after admitting backdoor was made for malice

An Arkansas man has been sentenced to serve almost three years in federal prison for developing advanced malware that he knew would be used to steal passwords, surreptitiously turn on webcams, and conduct other unlawful actions on infected computers. Taylor Huddleston, 27, of Hot Springs, Arkansas, admitted that he developed a malware called "NanoCore" which is a remote-access Trojan (RAT). Said Trojan is capable of recording all keystrokes typed, extract passwords saved and send them over the Internet, remotely turn on webcams, view, delete, and download files, lock infected computers until users paid customers a ransom, and make infected computers to participate in distributed denial-of-service attacks. He marketed the malware on forums from 2012 to 2016. **(ArsTechnica, 25 February 2018)**

Russia hacked Winter Olympics and framed N.Korea in false-flag attack: US

During the opening ceremony of the PyeongChang 2018 Winter Olympics last 09 February its official website suffered a massive cyber-attack causing service disruption. Before that, IT security researchers at McAfee reported a new malware campaign aimed at the Winter Olympics. The prime suspect was North Korea due to the ongoing tensions with South Korea. However, Russian hackers were also under the radar due to the fact that the International Olympic Committee (IOC) had banned Russia from 2018 Olympics and told the athletes to compete under the Olympic flag. Washington Post (WP) reported that U.S. intelligence officials are convinced that the hackers behind the aforementioned cyber-attacks were Russians who targeted the cyber infrastructure of the Olympics and framed North Korea as the culprit. Accordingly, Russia carried out "false-flag" cyber attacks by making it looks like North Korea was behind these attacks. **(HackRead, 25 February 2018)**

DICT readies revival of Gov.PH as portal for government services

The Department of Information and Communications Technology (DICT) revealed that it developed productivity tools to automate and simplify the operations of agencies that will implement Gov.PH, which is being built as a single website for government data, information, and online services. Among the tools that are now available for use by government agencies are applications for portal management, data cleaning, collaboration, creation of forms, process management, and business analytics. These will be introduced to government agencies and stakeholders in a series of training, workshops and seminars throughout the year. **(Newsbytes.ph, 26 February 2018)**