CYBER DEFENSE NEWS

In Cyber Defense and Security, You are at the Center

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

09 March 2018 **Issue No. 2018-009**

Artificial intelligence development course offered for free by Google

Google wants to help people understand AI and machine-learning development by offering a crash course for free. According to a statement, the Machine Learning Crash Course (MLCC) offers the same educational material previously provided to over 18,000 Googlers. The course covers machine-learning fundamentals and moves all the way up to classification models and neural networks. Programming background is not required. The course itself will be intuitive and media-driven, with hands-on tools to help learn machine-learning concepts. After finishing the course, "new graduates" can test out their skills and join the Kaggle competition to help DonorChoose.org to create a system for screening the thousands of project proposals the organization receives annually. **(Inquirer.net, 06 March 2018)**

New 4G LTE network attacks let hackers spy, track, spoof and spam

A new research paper recently published by security researchers at Purdue University and the University of Iowa discovered a set of severe vulnerabilities in 4G LTE protocol that could be exploited to spy on user phone calls and text messages, send fake emergency alerts, spoof location of the device and even knock devices entirely offline. The research paper details 10 new cyberattacks that exploit design weakness in three protocol procedures of the 4G LTE network known as attach, detach, and paging. The vulnerabilities are most worrying that once again raise concerns about the security of the cell standards in the real world, potentially having an industry-wide impact. **(Thehackernews.com, 05 March 2018)**

Swiss firm brings in cloud-based e-vehicle charging stations in the Philippines

The Local start-up QEV Philippines Electromobility Solutions and Consulting Group, Inc. (QEV Philippines) has partnered with Switzerland-based industrial technology firm ABB to supply 200 Terra 53 electric vehicle (EV) fast-charging stations in the Philippines for the next three years. Four EV charging stations are expected to be installed in selected gasoline stations in Metro Manila during the first quarter of 2018. ABB has installed more than 6,000 cloud-based charging solutions in over 55 countries. Fast-charging stations like Terra 53 should be able to charge batteries from 20% to up to 80% in 15 minutes. **(Newsbytes.ph, 28 February 2018)**

Biggest-ever DDoS attack (1.35 Tbps) hits Github website

GitHub's code hosting website was hit with the largest-ever distributed denial of service (DDoS) attack on 28 February 2018 that peaked at record 1.35 terabits per second (Tbps). Attackers did not use any botnet network. Instead, they utilized misconfigured servers to amplify the DDoS attack. Dubbed as "Memcrashed," the attack works by sending a forged request to the targeted Memcrashed server on port 11211 using a spoofed IP address that matches the

victim's IP. When exploited with “Memcrashed,” the result is a whopping 51,000 times powerful than its original strength.

Though amplification attacks are not new, this attack vector evolves thousands of misconfigured Memcached servers. To prevent Memcached servers from being abused, administrators should consider firewalling, blocking or rate-limiting User Datagram Protocol (UDP) on source port 11211 or completely disable UDP support if not in use. **(Thehackernews.com, 01 March 2018)**

Hackers breached German government’s secure computer networks

The Russia-linked Sofacy hacking group has breached the secure computer networks of a number of German federal agencies. The group – also known as APT28, Fancy Bear, and Pawn Storm – has been targeting government institutions, political organizations and military/defense companies around the world for over a decade. Johannes Dimroth, a spokesman for the German Interior Ministry, confirmed the breach but he did not comment on the possible perpetrator. The finger-pointing was apparently made by German security forces who are confident that hackers with links to the Russian state had originated the attacks. Dimroth further disclosed that among the compromised networks are those of the foreign and defense ministries, the German Chancellery, and the Federal Court of Auditors. **(Helpnetsecurity.com, 01 March 2018)**

An Iranian hacking group is expanding operations

An Iran-based hacking group called Chafer is expanding its spying operations in the Middle East according to a new report from cybersecurity firm Symantec. The cybersecurity firm said that last year the group attacked organizations in Israel, Jordan, Saudi Arabia, Turkey, and the United Arab Emirates. Some of the sectors the group has targeted include airlines, aircraft services, telecom firms, and technology companies serving the air and sea transport sectors. Chafer, according to Symantec, appears to be primarily engaged in surveillance and tracking of individuals and most of its attack is likely carried out to gather information on targets. Symantec previously wrote about the group's activities in a 2015 blog post where the firm said it mostly spied on individuals within Iran. But the report added that the group was already targeting telecom and airline companies in the region.

U.S. intelligence officials previously said that hackers believed to be linked to the Iranian government attacked Saudi state oil giant Aramco in 2012, successfully wiping thousands of computers and paralyzing operations. **(CNBC.com, 01 March 2018)**

The 'First' IPv6 denial-of-service attack puts IT bods on notice

Network guru Wesley George noticed the strange traffic earlier this week as part of a larger attack on a Domain Name System (DNS) server in an effort to overwhelm it. He was taking packet captures of the malicious traffic as part of his job at Neustar's SiteProtect DDoS protection service when he realized there were packets coming from IPv6 addresses to an IPv6 host. George claimed that it was the first IPv6-based distributed denial-of-service (DDoS) attack and consequently warn that it is only the beginning of what could become the next wave

of online disruption. Accordingly, anyone running an IPv6 network needs to, therefore, ensure they have the same level of network security and mitigation tools in place as their IPv4 networks. **(Theregister.co.uk, 03 March 2018)**

Windows Defender detects spyware used by law enforcement

Windows Defender Advanced Threat Protection (Windows Defender ATP) is capable of detecting behavior associated with the sophisticated “FinFisher” spyware, Microsoft says. FinFisher or FinSpy is a lawful interception solution built by Germany-based FinFisher GmbH, which sells it exclusively to governments. The said malware has been around for over half a decade and has been associated with various surveillance campaigns.

According to Microsoft, FinFisher is complex enough to require “special methods to crack it” but despite its sophistication, the malware cannot go unnoticed by its security tools. It was packed with various detection, evasion and anti-analysis capabilities, including junk instructions and “spaghetti code,” multi-layered virtual machine detection, and several anti-debug and defensive measures. Thus, FinFisher wasn’t easy to tear apart and analyze Microsoft says.

All personnel are advised to enable their built-in Windows Defender software and protect their computers from FinFisher or FinSpy. **(Securityweek.com, 04 March 2018)**

Java EE was renamed ‘Jakarta EE’ after Oracle spat

The open source version of Java Enterprise Edition (Java EE) has been renamed Jakarta EE to satisfy the desire of the computer technology company Oracle to control the "Java" brand. The renaming became necessary after Oracle moved Java EE to the Eclipse Foundation. Oracle would not grant the project the rights to use the Java brand. In February 2017 the Eclipse Foundation conducted a ballot to pick a new name. On offer were the names "Jakarta EE" and "Enterprise Profile". The vote went in favor of the former, 64.4% to 35.6%. **(Theregister.co.uk, 04 March 2018)**

Cisco Systems released its annual cybersecurity report

Cisco System released the 2018 edition of its Annual Cybersecurity Report (ACR) last week. The report, compiled from a survey of 3,600 chief security officers (CSOs) and security operations leaders from across the globe, seeks to highlight emerging threats in the rapidly evolving landscape of cybersecurity.

One of the big findings from the new report was that malware, particularly ransomware, is becoming increasingly more sophisticated and dangerous. Attackers are now building their malware to be self-propagating and “worm-like,” capable of spreading throughout a network to cause unprecedented damage.

Another key finding is that cybercriminals, too, are embracing encryption. The report found that 50 percent of global web traffic was encrypted as of last October and the number is rising.

However, more and more criminals are turning to the tool to help them hide command-and-control (C2) activity.

The growth of the Internet of Things (IoT) is also presenting many opportunities for attackers. More and more organizations are deploying IoT devices, without doing their due diligence in ensuring the security of these systems. As such, cybercriminals are easily able to gain access to networks via these unpatched and unmonitored IoT devises.

Meanwhile, the following are the recommendations of Cisco System based on the findings of the report:

- the implementation of scalable first-line-of-defense tools
- adherence to corporate policies for patching, network segmentation
- deployment of next-generation endpoint process monitoring tools
- increased analytics
- frequent backup of data
- annual review of security systems
- security response procedures (when hacked)
- explore the of use AI and machine learning in network security to give organizations better visibility, allowing them to identify and detect unusual patterns in large volumes of encrypted web traffic **(Forbes.com, 05 March 2018)**