CYBER DEFENSE NEWS

In Cyber Defense and Security, You are at the Center

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

11 May 2018 **Issue No. 2018-018**

Pentagon's Cyber Command gets upgraded status, new leader

The Pentagon's cyber warfare unit received an elevated status and a new commander on 05 May 2018, signaling the growing importance of digital combat as the United States grapples with sophisticated hacking by Russia, China and other actors. Cyber Command was elevated to an independent "unified command" and Army Lieutenant General Paul Nakasone took over the leadership. He also took over as director of the National Security Agency. Under a "dual-hatted" arrangement, the NSA director also oversees Cyber Command.

The Cyber Command has a new $500 million Integrated Cyber Center on the heavily fortified Fort Meade campus. When it becomes operational in August. U.S. and allied personnel at the center will monitor and coordinate responses to cyber threats. **(Reuters.com, 05 May 2018)**

US is waking up to the deadly threat of cyber war

The American military is recognizing that the cyber battlefield can be very lethal as the traditional one. It can target systems from the nuclear power plants to emergency responders as any device manufactured to kill soldiers, sailors, or marines, can bring down planes or sink ships. Pentagon has now funded a joint cyber command on the level of every other uniformed force.

Recently, that level was put on display when every North Atlantic Treaty Organization (NATO) nation had an opportunity to try out their capacities in a real live-fire exercise called Operation Locked Shield. It was staged by the NATO Cooperative Cyber Defense Centre of Excellence, with its command center in the Baltic nation of Estonia. It was the largest and most intricate exercise ever mounted and with the goal of testing and training the participants and to make them learn how to make cyber defense stronger. **(CNN.com, 06 May 2018)**

Facebook's "Suggested Friends" feature helps ISIS expand its terror network

Researchers have found that Facebook's "suggested friends" feature has been used to introduce thousands of ISIS members to each other. It's a well-known fact that Facebook does its best to keep you tracking all the time, even if you're not a Facebook user. Using that data, it serves you ads, news feed content, friend's suggestion, etc. It has been found that often ISIS members are introduced to each other via the suggestions features. In a statement, Facebook has defended the steps it is taking. It said that the company have removed any content that praises or supports terrorism. However, it maintains that there is no easy technical fix to fight online extremism with 100% accuracy. **(Fossbytes.com, 07 May 2018)**

SynAck Ransomware uses Process Doppelgänging for evasion

Kaspersky Lab reported that SynAck has become the first ransomware family to leverage the Process Doppelgänging technique in an attempt to bypass security products. Discovered in September 2017, SynAck is not a new malware, but started using the evasion method last month. The technique is not new either as it was first detailed in December 2017 by security company enSilo. Similar to process hollowing, Process Doppelgänging abuses Windows loader to execute code without writing it to disk, making detection more difficult. **(SecurityWeek.com, 07 May 2018)**

GrandCrab Ransomware breaks Windows 7 systems

The latest variant of the GandCrab ransomware breaks infected Windows 7 systems, IT security company Fortinet warns. Version 3 of the ransomware, which was discovered at the end of last month, forces a system reboot, attempting to change the PC's desktop wallpaper. Because of a coding bug, however, only Windows 10 and Windows 8 systems would fully load, while Windows 7 machines would hang at a point before the Windows Shell is completely loaded. GandCrab spreads via spam emails, and Fortinet observed an uptick in messages distributing the ransomware last week. The emails carried version 2.1 of the malware and most of them (75%) targeted users in the U.S., with those in the U.K., Canada, Romania, and South Africa also impacted. **(SecurityWeek.com, 04 May 2018)**

Glitch: New 'Rowhammer' attack can remotely hijack Android phones

For the first time, security researchers have discovered an effective way to exploit a four-year old hacking technique called Rowhammer to hijack an Android phone remotely. Dubbed as GLitch, the proof-of-concept technique is a new addition to the Rowhammer attack series which leverages embedded graphics processing units (GPUs) to carry out a Rowhammer attack against Android smartphones. Since it exploits a computer hardware weakness, no software patch can completely fix the issue. **(TheHackerNews.com, 03 May 2018)**

Eight new Spectre-class vulnerabilities (Spectre-NG) found in Intel CPUs

A team of researchers discovered a total of eight (8) new "Spectre-class" vulnerabilities in Intel CPUs, which also affect at least a small number of ARM processors and may impact AMD processors architecture as well. Dubbed as Spectre-Next Generation or Spectre-NG, the partial details of the vulnerabilities were first leaked to journalists at German computer magazine Heise, which claims that Intel has classified four (4) of the new vulnerabilities as "high risk" and remaining four as "medium."

The new CPU flaws reportedly originate from the same design issue that caused the original Spectre flaw, but the report claims one of the newly discovered flaws allows attackers with access to a virtual machine (VM) to easily target the host system, making it potentially more threatening than the original Spectre vulnerability. **(TheHackerNews.com, 04 May 2018)**

Cryptojacking campaign exploits Drupal bug, over 400 websites attacked

Hundreds of websites running on the Drupal content management system have been targeted by a malicious cryptomining campaign taking advantage of unpatched and recently revealed vulnerabilities. The attacks, which impacted over 400 government and university websites worldwide, leverage the critical remote-code execution vulnerability (CVE-2018-7600) dubbed Drupalgeddon 2.0. The Drupal bug in question has been patched for over a month now. Meantime, the cryptominer in question was made by Coinhive, a company that offers a Monero JavaScript miner to websites as a nontraditional way to monetize website content. **(ThreatPost.com, 07 May 2018)**

US military bans Huawei, ZTE phones

Personnel on US military bases can no longer buy phones and other gear manufactured by Chinese firms Huawei and ZTE, after the Pentagon said the devices pose an "unacceptable" security risk. Concerns have heightened at the Pentagon about consumer electronics being used to snoop on or track service members. The Wall Street Journal said the Pentagon fears the Chinese government could track soldiers using Huawei or ZTE devices. Huawei spokesman Charles Zinkowski said the firm's devices meet the highest standards of security, privacy and engineering in every country it operates in, including the US.

In January, the Pentagon said it was reviewing its policy on fitness apps and wearable fitness trackers after exercise-logging company Strava published a map compiling its users' activity. In Iraq and Syria, viewers could easily spot beacons of activity in remote places where military bases are located, presumably indicating favorite jogging or walking routes. In February, Dan Coats, the Director of National Intelligence, along with several other top Intel officials, said Americans should not buy Huawei or ZTE products. (**Channelnewsasia.com, 05 May 2018)**

Crypto flaw in Oracle Access Manager can let attackers pass through

A padding oracle vulnerability in Oracle Access Manager (CVE-2018-2879) can be exploited by attackers to bypass authentication and impersonate any user account. The vulnerability arises from a flawed cryptographic format used by the OAM. SEC Consult researcher Wolfgang Ettlinger explained that the Oracle Access Manager is the component of the Oracle Fusion Middleware that handles authentication for all sorts of web applications. The vulnerability can be exploited to decrypt and encrypt messages used to communicate between the OAM and web servers. This allowed them to access protected resources as a user already known to the OAM. **(Wpengine.com, 04 May 2018)**

7-Zip RAR Archive Decoding error lets remote users execute Arbitrary Code

A remote user can create a specially crafted archive file that, when processed by the target application, will trigger a data structure initialization error in decoding RAR file data and execute arbitrary code on the target system. The code will run with the privileges of the target application. The vendor was notified on March 6, 2018. **(SecurityTracker.com, 03 May 2018)**

Javascript in Excel sparks security worries

Microsoft has added the ability for users to create custom Javascript functions in Excel spreadsheets, creating concern among security experts. Security experts have raised concerns around Javascript's potential to be abused by malicious actors to run arbitrary code on users' computers. In February this year, a compromised version of the Browse aloud Javascript accessibility library was found on thousands of Australian government websites. It attempted to utilize visitors' computers to illicitly mine for crypto currency. Microsoft said the functionality would continue to be expanded to enable developers to build powerful solutions within the spreadsheet. **(ITNews.com, 09 May 2018)**