CYBER DEFENSE NEWS

In Cyber Defense and Security, You are at the Center

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

06 April 2018 **Issue No. 2018-013**

U.S. Department of Defense to stamp out threats with bug bounty program

The U.S. Department of Defense (DoD) announced on 02 April 2018 that it is expanding its bug bounty program to include the agency's massive Defense Travel System. The "Hack the DTS" program was launched in partnership with bug bounty firm HackerOne. It targets potential threats found in a DoD enterprise system called Defense Travel System (DTS). Up to 600 eligible white-hackers will be invited to participate in the challenge according to HackerOne. The program is part of a push by the DoD explore new approaches to its security, and to adopt the best practices used by the most successful and secure software companies in the world. **(ThreatPost.com, 02 April 2018)**

Facebook finds hundreds more accounts run by Kremlin-linked troll group

Facebook said on 05 April 2018 that it removed almost 300 more pages and accounts run by the group, the vast majority targeted at Russian speakers. This came months after it removed hundreds of fake pages and accounts run by Kremlin-linked troll group that were targeted at Americans. The pages and accounts removed include 138 Facebook pages, 70 Facebook profiles, and 65 Instagram accounts determined to be linked to the Internet Research Agency (IRA). The pages, which were followed by more than one million users, were mainly aimed at Russian speakers around the world, including in Russia itself and neighboring countries Azerbaijan, Uzbekistan, and Ukraine. It must be noted that the pages and accounts that were previously removed by the company were ran by IRA and were designed to look like they were run by real American activists. **(CNN.com, 03 April 2018)**

Apple plans to replace Intel Chips in Macs with its custom designed CPUs

Apple is reportedly planning to use its custom-designed ARM chips in Mac computers starting as early as 2020, ultimately replacing the Intel processors running on its desktop and laptop hardware. The report by Bloomberg said that Apple executives have a project codenamed "Kalamata" that designs desktop-grade Arm-compatible processors, along with a macOS, allowing the company to craft a uniform architecture across all of its product lines. The changeover is likely to be in the wake of recent high-profile security issues around Intel chip architecture and chips from other manufacturers. Moreover, Apple would not have to share 5% of its annual revenue with Intel and pay for exclusive deals to offer high-end processors first to its customers, and competitors would not be able to copy innovations so easily. **(TheHackerNews, 02 April 2018)**

New Android Malware secretly records phone calls and steals private data

Security researchers at Cisco Talos have uncovered variants of a new Android Trojan that are being distributed disguising as a fake anti-virus application dubbed "Never Defender." The malware which is dubbed as KevDroid is a remote administration tool (RAT) designed to steal sensitive information from compromised Android devices, as well as capable of recording phone calls. Talos researchers published on 02 April the technical details of the two recent variants of KevDroid following the initial discovery of the Trojan by South Korean cybersecurity firm ESTsecurity two weeks ago.

Though researchers have not attributed the malware to any hacking or state-sponsored group, South Korean media have linked KevDroid with North Korean state-sponsored cyber espionage hacking group “Group123” primarily known for targeting South Korean targets. **(TheHackerNews.com, 03 April 2018)**

Investors view cyber attacks as the biggest threat to business

According to PwC Global Investor Survey 2018, forty-one percent of investor and analysts are now extremely concerned about cyber threats, ranking it as the largest threat to business. Forty percent of business leaders see cyber as a top-three threat, but business leaders rank over-regulation and terrorism higher. To improve trust with customers, 64 percent of investors believe that businesses should prioritize investment in cybersecurity protection, compared to 47 percent of CEOs. **(SecurityMagazine.com, 01 April 2018)**

Fauxspersky spyware impersonates Kaspersky Anti-Virus software, abuses AutoHotKey Tools

Researchers have discovered a Windows-based keylogger and information stealer that falsely poses as Kaspersky antivirus software and spreads via infected USB devices. The malware, named Fauxpersky, is also written using AutoHotKey (AHK) tools that under normal circumstances would be used to create keyboard shortcuts. Accordingly, Fauxpersky takes advantage of AHK’s abilities to read texts from Windows and send keystrokes to other applications. It is made up of four executables placed inside a directory labeled “Kaspersky Internet Security 2017.” This directory also contains a Readme.txt file and a PNG image that displays a Kaspersky logo as a splash screen when an infected machine logs into Windows. This image is meant to fool users into thinking that Kaspersky antivirus is actively running.

Google’s security team took down the malicious Google form almost immediately after it was disclosed to them. It is unknown however how many machines have been infected by the threat. **(SCMagazine.com, 02 April 2018)**

Facebook CEO says no plans to extend all of European privacy law globally

Facebook Chief Executive Mark Zuckerberg said on 03 April 2018 that the company had no immediate plans to apply strict new European Union law on data privacy in its entirety to the rest of the world. Zuckerberg said in a phone interview with Reuters that Facebook already complies with many parts of the law ahead of its implementation in May. He said Facebook wanted to extend privacy guarantees worldwide in spirit, but would make exceptions, which he declined to describe.

To note, the European law called the General Data Protection regulation (GDPR) is the biggest overhaul of online privacy since the birth of the internet, giving Europeans the right to know what data is stored on them and the right to have it deleted. **(Reuters.com, 04 April 2018)**

Malware attacks leveraging MS Word documents grew by 33% in Q4 2017

Amidst a major rise in zero-day malware attacks in the fourth quarter of 2017, researchers have observed how hackers are increasingly using Microsoft Office documents as carriers to deliver malicious payloads in enterprise systems while using phising techniques to trick employees into downloading and opening malicious attachments in emails. The latest Internet Security Report released by WatchGuard Technologies revealed how hackers are increasingly exploiting issues within Microsoft Office standard to execute code and to inject powerful malware into enterprise system. **(SCMagazine.com, 30 March 2018)**

Google's April Android security bulletin warns of 9 critical bugs

Nine (9) vulnerabilities rated critical were patched as part of Google's Android Security Bulletin for April. Critical vulnerabilities ranged from two remote code execution vulnerabilities tied to the Android media framework, to a Qualcomm W-Fi component flaw that allowed a nearby attacker to use "a specially crafted file to execute arbitrary code within the context of a privileged process." Google said firmware updates are available and will be delivered via over-the-air (OTA) updates to Google Pixel and Nexus devices. Update to other Android devices will be sent via respective OEM device makes and wireless carriers, were applicable. **(ThreatPost.com, 03 April 2018)**