CYBER DEFENSE NEWS

In Cyber Defense and Security, You are at the Center

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

16 March 2018 **Issue No. 2018-010**

Fitness app Strava overhauls map that revealed military positions

Fitness-tracking app Strava said that starting 13 March 2018 it will restrict access to an online map that shows where people run, cycle and swim and remove some data after researchers found it inadvertently revealed military posts and other sensitive sites. Strava Chief Executive James Quarles said the company is launching a new version of the heat map, a tool that displays data in map form, that bar access to street-level details to anyone but Strava users. Roads and trails with little activity will not show up on the revised map until several different users upload workouts in that area. The map will also be refreshed monthly to remove data people have made private. Notably, the map drew worldwide attention in January when academics, journalists and private security experts used it to deduce where military personnel were deployed by looking on the app for workout locations in war zones. **(Reuters.com, 13 March 2018)**

"OceanLotus" spies use new backdoor in recent attacks

OceanLotus, a cyber-espionage group believed to be operating in Vietnam, has been using a new backdoor in recently observed attacks but also using previously established tactics, according to IT security company ESET. Also known as APT32 and APT-C-00, the advanced persistent threat (APT) has been targeting high-profile corporate and government organization in South East Asia, particularly in Vietnam, the Philippines, Laos, and Cambodia. The group is well-sourced and determined and is known to be using custom-built malware in combination with techniques long known to be successful. One of the latest malware families used by the group is a fully-fledged backdoor that provides operators with remote access to compromised machines, along with the ability to manipulate files, registries, and processes, as well as the option to load additional components if needed. **(SecurityWeek.com, 13 March 2018)**

Researchers find 'critical' security flaws in AMD chips

Security researchers from Israeli-based security firm CTS Labs published a study showing "multiple critical security vulnerabilities and exploitable manufacturer backdoors" in AMD chips. CTS itemized 13 flaws, saying they "have potential to put organizations at significantly increased risk of cyberattacks." CTS added that the newly discovered flaws could compromise AMD's new chips that handle applications in the enterprise, industrial and aerospace sectors, as well as consumer products. AMD, one of the largest semiconductor firms specializing in processors for PCs and servers, said it was studying the latest report. Meantime, analysts at the security firm enSilo said the AMD flaws could be worse that those affecting Intel chips. **(Inquirer.net, 14 March 2018)**

CredSSP flaw in Remote Desktop Protocol affects all versions of Windows

A critical vulnerability has been discovered in Credential Security Support Provider protocol (CredSSP) that affects all versions of Windows to date and could allow remote attackers to exploit Remote Desktop Protocol (RDP) and Windows Remote Management (WinRM) to steal data and run malicious code. CredSSP protocol has been designated to be used by RDP and WinRM that takes care of securely forwarding credentials encrypted from the Windows client to the target servers for remote authentication. Discovered by researchers at Cybersecurity firm Preempt Security, the issue (CVE-2018-0886) is a logical cryptographic flaw in CredSSP that can be exploited by a man-in-the-middle attacker with Wi-Fi or physical access to the network to steal session authentication data and perform a Remote Procedure Call attack. As a defense against the CreSSP exploit, users are recommended to patch their workstations and servers using available updates from the Microsoft. **(TheHackerNews.com, 13 March 2018)**

Microsoft patches 15 critical bugs in March patch Tuesday update

Microsoft patched 15 critical vulnerabilities this month as part of its March Patch Tuesday roundup of fixes. The company has issued a total of 75 fixes, with 61 rated as important. Products receiving the most urgent patches includes Microsoft browsers and browser-related technologies such as the company's JavaScript engine Chakra. Of the 21 browser-related fixes that were rolled by Microsoft, 14 are rated as critical while the remaining seven (7) were ranked as important. Of the bugs, "scripting engine memory corruption vulnerabilities" represented 14 of the flaws. Part of this month's round of patches also included an additional update for the Meltdown vulnerabilities. Windows 32-bit versions of Windows 7 and 8.1, as well as Server 2008 and 2012 now have mitigations for Meltdown and Spectre. **(Threatpost.com, 13 march 2018)**

'Kill Switch' to mitigate Memcached DDoS attacks discovered

Researchers from Corero Network Security discovered a "kill switch" that could help companies protect their websites under massive Distributed Denial of Service (DDoS) attack launched using vulnerable Memcached servers. Through the technique that the researchers found, the DDoS victims can send back a simple command, i.e. "shutdown\r\n", or "flush_\r\n", in a loop to the attacking Memcached servers in order to prevent amplification. The flush_all command simply flush the content (all keys and their values) stored in the cache, without restarting the Memcached server. The company said its kill-switch has efficiently been tested on live attacking Memcached servers and found to be 100% effective, and has already been disclosed to national security agencies. **(TheHackerNews.com, 07 March 2018)**

Chrome 65 update ready, contains 45 security fixes

The Google Chrome team reported that it moved Chrome 65 to the stable channel for Windows, Mac, and Linux with the latest update containing 45 security fixes, with at least nine (9) rated as "high." Google said that Chrome 65.0.3325.146 containing patches will be rolled out in the next few weeks. Meantime, while it gave a high-level description of the issue being fixed, details will not be made available until the majority of users have updated their version

of Chrome. The Chrome team also did not list all the issues fixed, just those discovered by outside sources. **(SCMagazine.com, 07 March 2018)**

FBI Chief: Corporate hack victims can trust we won't share info

Federal Bureau of Investigation (FBI) director Christopher Wray said that the agency views companies hit by cyberattacks as victims and will not rush to share their information with other agencies investigating whether they failed to protect customer data. Wray encouraged companies to promptly report when they are hacked to help the FBI investigate and prevent future data breaches. He also contrasted FBI's approach to that of other regulators and state authorities. Without naming other agencies, Wray referred to "less-enlightened enforcement agencies," some of which ha said take a more adversarial approach. **(Reuters.com, 08 March 2018)**

Cyber espionage campaign 'Slingshot' targets victims via routers

Researchers have uncovered a new cyber-espionage threat, dubbed Slingshot that targets routers and uses them as a springboard to attack computers within a network. Kaspersky Lab, which released details of its discovery during its Security Analyst Summit (SAS) last 09 March 2018, said that the campaign has successfully targeted at least 100 victims in the Middle East and Africa from at least 2012 until February 2018.

Slingshot stands out for its unusual attack vector – the malicious actors infected victims through compromised MikroTik routers and placed a malicious dynamic link library inside it that acts as a downloader for other malicious components. After infecting the router, Slingshot downloads an array of additional malware modules onto the device – including two particularly sophisticated ones called Cahnadr and GollumApp – that are linked and can support each other in gathering information.

Researchers said that the complexity of Slingshot could mean that the group behind it is highly organized and potentially state sponsored. To avoid falling victim to Slingshot, Kaspersky recommends that MikroTik users upgrade to the latest firmware version as soon as possible. **(Threatpost.com, 10 March 2018)**

US Senator Mark Warner: The country is 'woefully unprepared' for cyber threats

Speaking at the South for South West (SXSW) festival last 10 March 2018, U.S. senator Mark Warner said that the United States is "woefully unprepared" to combat cyberattacks and disinformation campaigns. He added that it's time to consider the liability of tech platforms and software makes. Warner, the top Democrat on the Senate Select Intelligence Committee, outlined four-part "cyberdoctrine," actions the government could take to address the cybersecurity threats.

He suggested the establishment of basic rules for cyber aggressions, like those in place of nuclear weapons. Warner also called for using the government's purchasing power to force tech product makers to adopt security standards and said that the United States should reallocate some defense resources into the cyber domain. He also added that he wants to bring together parliamentarians of all Western nations that have been attacked to get some commonality around cybersecurity efforts. **(CNN.com, 10 March 2018)**