CYBER DEFENSE NEWS

In Cyber Defense and Security, You are at the Center

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

27 July 2018 **Issue No. 2018-028**

White House cyber security strategy at a crossroads

Trump administration's initial lack of a unified front in the wake of Russian election-hacking indictments worries cybersecurity experts. Fallout from a rapid-fire series of developments surrounding the 2016 election hacking and meddling by Russia continues as U.S. President Donald Trump attempted to walk back his public dismissal of U.S. intelligence agencies' findings pointing to Russia. The chaos of his apparent disconnect with intelligence officials and others in the administration underscores concerns that the administration's cybersecurity strategy could be unraveling. **(DarkReading.com, 17 July 2018)**

Microsoft, Google, Facebook, Twitter launch data transfer project

Microsoft, Google, Facebook, and Twitter have teamed up to launch a new initiative dubbed as Data Transfer Project (DTP), which is intended to simplify data sharing across services. The open-source effort is dedicated to building tools that will enable users to directly transfer information from one service to another so they don't have to download and re-upload it. Instead, people can port data from one company to another from within an application. While it may seem weird to see four tech giants working together on a project like this, breaking down the barriers for data transfer would make things easier for users and companies in the wake of Europe's General Data Protection Regulation (GDPR), which requires platforms to provide all available information on a person. **(DarkReading.com 23 July 2018)**

Egypt targets social media with new law

On 16 July 2018 Egypt's parliament passed a law giving the state powers to block social media accounts and penalize journalists held to be publishing fake news. Under the law, social media accounts and blogs with more than 5,000 followers on sites such as Twitter and Facebook will be treated as media outlets, which makes them subject to prosecution for publishing false news or incitement to break the law. The Supreme Council for the Administration of the media will supervise the law and take action against violations. **(Reuters.com, 18 July 2018)**

Microsoft says Russia tried to hack three 2018 midterm election candidates

During the Aspen Security Forum on 18 July 2018, Microsoft said that it detected and helped the U.S. government to block hacking attempts against at least three congressional candidates this year. Although the company refused to name the targets, it said that the three candidates were "people who, because of their positions, might have been interesting targets from an espionage standpoint as well as election disruption standpoint." Accordingly, the Russian hackers targeted the candidates' staffers with phishing attacks, redirecting them to a fake Microsoft website, in an attempt to steal their credentials. Immediately after learning of this

incident, Microsoft took down the fake domain, which served as the landing page for said attacks, and worked with the government to avoid being infected by that particular attack. **(TheHackerNews.com, 19 July 2018)**

New concerns over user sharing leads Facebook to suspend analytics firm Crimson Hexagon

Facebook has suspended Crimson Hexagon, a company that generates consumer insights from public social media posts, while it evaluates whether Crimson Hexagon violated Facebook policies. According to a Wall Street Journal (WSJ) article, Facebook is specifically looking into contracts that the Boston-based Crimson Hexagon entered into with both the U.S. government and a Russian nonprofit associated with the Kremlim. Citing more than a dozen sources, the report noted that Facebook did not approve the government contracts in advance, and has historically had little oversight as to how Crimson Hexagon uses data once it's pulled from the social media platform. **(SCMagazine.com, 23 July 2018)**

Hackers hiding web shell logins in fake HTTP error pages

Malware distributors, hackers, and phishing scammers are continuing to use the practice of hiding login forms for their web shells in fake HTTP error documents. These pages pretend to be HTTP errors such as 404 Not Found or Forbidden, while in reality they are login pages that allow an attacker to access a web shell to issue commands on the server. While this practice is not new, a phishing expert and security researcher has noticed an increase in the use of these types of fake error pages to hide web shells. These web shells allow the hackers to upload malware, phishing scripts, or other software. Web shells hiding behind these fake error pages pose a particular danger to system administrators who may clean up a phishing install, but not realize another page on the site is hiding a web shell that could allow an attacker to easily re-infect the site. (**BleepingComputer.com, 24 July 2018**)

Attackers concealing malware in images uploaded to Google servers

Cybercriminals are putting a new spin on the old trick of hiding malware code in Exchangeable Image File Format (EXIF) data. Recently, attackers were observed using this technique in image files, rather than text files, and uploading them to googleuseraccount.com servers. One case that was cited by malware researchers was that an EXIF code from a Pacman.jpg image was used to mask a malicious script that steals PayPal security tokens, uploads web shells and arbitrary files, inserts defacement pages and communicates addresses of exploited websites back to the attacker. **(SCMagazine.com, 20 July 2018)**

Malware author builds 18,000-strong botnet in a day

A malware author has built a huge botnet comprised of over 18,000 routers in the span of only one day. This new botnet has been spotted by security researchers from NewSky Security and their findings have been confirmed by Qihoo 360 Netlab, Rapid7, and Greynoise. The botnet has been built by exploiting a vulnerability in Huawei HG532 routers. Scans for this vulnerability, which can be exploited via port 37215, started on 18 July 18 according to data collected by Netlab's NetScan system. (**Threatbrief.com, 20 July 2018**)

Cyberattack on Singapore health database steals details of 1.5 million including PM

A major cyberattack on Singapore's government health database stole the personal information of about 1.5 million people, including Prime Minister Lee Hsien Loong, the government said. The attack, which the government called "the most serious breach of personal data" that the country has ever experienced comes as the country has made cyber security a top priority for the ASEAN bloc and for itself. Accordingly, it was a deliberate, targeted and well-planned cyberattack and not the work of casual hackers or criminal gangs. The attackers specifically and repeatedly targeted Prime Minister Lee Hsein Loong's personal particulars and information on his outpatient dispensed medicines. Singapore's Ministry of Communications said that a Committee of Inquiry will be established and immediate action will be taken to strengthen government systems against cyberattacks. **(Reuters.com, 20 July 2018)**

Hackers launched multiple new campaigns leveraging Mirai and Gafgyt IoT botnets

Security researchers have uncovered three new campaigns that have been built on the publicly available source code of the Mirai and Gafgyt malware families. Malware samples used by these campaigns have incorporated multiple exploits. The campaign also support several new DDoS attack methods that have previously not been used by any Mirai variant. The first campaign leveraged the Omnibot, a Mirai variant, while the second campaign leveraged Okane.

According to security researchers at Palo Alto networks, who discovered the new campaigns, the Gafgyt botnet has been upgraded with new Layer-7 DDoS attacks targeting specific DDoS protection service vendors. **(Cyware.com, 23 July 2018)**

In cyber, Germany needs to counter-attack, minister says

Germany is considering laws that would let it respond actively to foreign cyberattacks, Interior Minister Horst Seehofer said as he presented a domestic intelligence agency report showing Iran was the latest power to ramp up hack attacks on German systems. The agency reported that volume of cyberattacks from China had seemingly dwindled as the number of acquisitions of German high-tech companies by Chinese firms had risen. Meatime, the number of cyberattacks with a likely origin in Iran had been rising since 2014. In response to the report, which highlighted cyberattacks by Iran, Russia and China, Seehofer said the agency needed to acquire the power not just to track and clean up cyberattacks but also to launch counter-measures. **(Reuters.com, 24 July 2018)**

Chrome browser flags Daily Mail and other sites as 'not secure'

Security warnings will pop up on the Daily Mail website starting 24 July if visitors are using the latest version of Google's Chrome browser. It is one of the many sites the browser will flag because they do not use HTTPS, the secure version of the web's underlying data transfer protocol. Websites without HTTPS are not safe because they do nothing to scramble the data passing between the users and that website.

The warnings are appearing because Google updated to Chrome 68 which has been changed to flag HTTP-only sites. It began the process of warning people about sites that use HTTP in early 2007. Initially Google's "Not secure" warnings were only used on sites that collected passwords or credit cards. Firefox and Safari added similar systems about the same time. **(BBC.com, 24 July 2018)**

SMPlayer 18.6.0 - memory corruption (DoS) vulnerability

A memory corruption vulnerability resulting in a denial of service has been discovered in the official SMPlayer v18.6.0 software. The vulnerability is caused by an invalid pointer corruption while processing a corrupted .m3u file through the SMPlayer reader, which could be exploited by attackers to crash a complete software process via denial of service. The vulnerability is located in the Qt5Core.dll when processing an .m3u file on import. SMPlayer is a 64-bit free media player for Windows and Linux with built-in codecs that can play virtually all video and audio formats. All users of SMPlayer are advised to update their software. (**Vulnerability-lab.com, 23 July 2018**)

New Malwarebytes Anti-Exploit

Malwarebytes Anti-Exploit, formerly ExploitShield by ZeroVulnerabilityLabs, protects users from zero-day exploits targeting browser and application vulnerabilities. Its proprietary technology shields a user's browser and applications in that critical period between the release of a new exploit and its subsequent security patch. Easy to install and lightweight, users can now download Malwarebytes Anti-Exploit and crush the most dangerous breed of malware attack. (**TechSpot.com, 23 July 2018**)