CYBER DEFENSE NEWS

In Cyber Defense and Security, You are at the Center

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

04 May 2018 **Issue No. 2018-017**

Cyber-attack website Webstresser taken down

The United Kingdom's National Crime Agency, blocked Webstresser.org, a website blamed for launching more than four million cyber-attacks around the world, including attempts to crash banks in the UK. Six suspended members of the gang behind the site have been arrested, with computers seized in the UK, Holland and elsewhere.

The site was one of many operating openly on the web as a "stresser" business, offering to test a company's cyber-defenses. Investigators say that the gang offered a form of cyber attack known as Distributed Denial of Service (DDoS), in which a target website is overwhelmed by requests for access. This means that the target, either an online bank or a secondary school's portal for students, can seize up and crash, unless the attack is blocked. **(BBC.com, 25 April 2018)**

Portugal joins NATO Cyber-Defense Centre

Portugal on 24 April 2018 became the 21st country to join the North Atlantic Treaty Organization's (NATO) cyber defense center. The said center was founded in 2008 in Tallinn, the capital of Estonia, ranked as having one of the world's highest internet user rates, which itself had come under attack the previous year. Estonia accused Russia, NATO's old Cold War foe, of being behind the attacks on its official sites and information networks. At the center, data experts from across Europe and the United States work to protect the information networks of the Western defense alliance's 29 countries. **(SecurityWeek.com, 25 April 2018)**

IS web media targeted in EU-led attack

The European Union (EU) police agency Europol said an international operation struck a major blow against the internet propaganda of the Islamic State (IS) group. Europol coordinated a "simultaneous multinational takedown" of IS media, seizing digital evidence and servers. IS jihadists may now be identified. The EU members involved in Europol's operations on 25 to 26 April were Belgium, Bulgaria, France, the Netherlands, Romania and the UK. Europol said the data retrieved is expected to help police identify the administrators behind IS media outlets and "potentially radicalized individuals". Rob Wainright, head of Europol said the latest operations had "punched a big hole" in IS's capability to spread propaganda and radicalize young people. **(BBC.com, 27 April 2018)**

Uber updates bug bounty program

Uber updated the legal terms of its bug bounty program and provided guidance for good faith vulnerability research. The changes come just months after the company admitted paying a couple of individuals as part of an effort to cover up a massive security incident. The new terms provide more specific guidance on what is and what is not acceptable conduct in terms of vulnerability research. Bug bounty hunters are now also provided clearer instructions on what to do if they come across user data during their investigations.

Researchers acting in good faith are informed that Uber will not initiate or recommend legal action against them. Furthermore, if a third party files a lawsuit, the company has promised to let them know that the activities were conducted in compliance with its program. **(SecurityWeek.com, 30 April 2018)**

Massive phishing campaign targets half a billion users in the first quarter 2018

Security researchers from cybersecurity company Vade Secure revealed that a massive phishing campaign has targeted more than 550 million email users globally since the first quarter of 2018. They spotted the campaign in early January with a high concentration of impacted email users in the US, UK, France, Germany, and the Netherlands. The attacks were not detected by many existing email security solutions since the phishing emails use IP addresses, servers, and domain names that appear to be leased and therefore legitimate. In order to prevent falling for the attacks, researchers recommend that users remain vigilant even if the email message appears to be coming from a familiar brand and never click the link within the suspicious emails. **(SCMagazine.com, 26 April 2018)**

Microsoft issues more Sprectre updates

Microsoft released additional Windows 10 mitigations for the Spectre side-channel flaw revealed in January, with an expanded lineup of firmware (microcode) updates for Intel CPUs that include the Broadwell and Haswell chipsets. The company released two Windows Update packages addressing Spectre, KB4091666 and KB4078407, both available as manual downloads from the Microsoft Update Catalog portal. The former contains the Intel microcode updates. Microsoft’s decision to help distribute available Intel firmware through Windows updates adds another layer of security for Intel-based processors on top of Intel’s reliance on motherboard and system vendors to package the microcode into BIOS updates for products. **(ThreatPost.com, 26 April 2018)**

ASEAN leaders issue statement on cybersecurity cooperation

On the occasion of the 32nd Association of Southeast Asian Nation (ASEAN) Summit last 27 April 2018, leaders of the member states of the ASEAN issued a statement on cybersecurity cooperation, in recognition of the growing urgency and sophistication of transboundary cyber threats. According to the statement, ASEAN leaders share the vision of a peaceful, secure and resilient regional cyberspace that serves as an enabler of economic progress, enhanced regional connectivity and betterment of living standards for all. They are also cognizant of the pervasiveness of cyber threats as an international problem, and of the urgency and increasing sophistication of the ever-evolving and transboundary cyber threats facing the region. They also recognizes cybersecurity as an issue that requires coordinated expertise from multiple stakeholders from across different domain to address effectively. **(OpenGovAsia.com, 30 April.com)**

A new cryptocurrency mining virus is spreading through Facebook

Cybersecurity researchers from Trend Micro are warning users of a malicious Chrome extension which is spreading through Facebook Messenger and targeting users of cryptocurrency trading platforms to steal their accounts' credentials. Dubbed as FacexWorm, the attack technique used by the malicious extension first emerged in August last year, but researchers noticed the malware re-packed a few new malicious capabilities earlier this month. These include stealing account credentials from websites, like Google and cryptocurrency sites, redirecting victims to cryptocurrency scams, injecting miners on the web page for mining cryptocurrency, and redirecting victims to the attacker's referral link for cryptocurrency-related referral programs. Thus, Facebook users are warned not to just click a link they receive on Facebook even if it looks exciting or sent by a friend. **(TheHackerNews.com, 01 May 2018)**

Facebook to allow users to opt out of browser history tracking

In a major policy change, Facebook said on 01 May that it will soon allow users to wipe their browsing histories from the platform and prevent the company from scooping up some of the data it uses to sell targeted ads. The new privacy initiative allows users to avoid some of the platform's abilities to track people on websites across the internet – including data collection through its "Like" button and its "Pixel" program. It would be called Clear History, a common name for the web browser function that lets users delete their cookies and browsing records. If used, identifying information will be removed so that a history of websites and apps used will not be associated with the account. **(NBCNews.com, 02 May 2018)**

Skilful software engineers will be hired as Captains in the U.S. Navy

The U.S. Navy is one step closer to recruiting officers with much-needed skills into the service and immediately promoting them to a pay grade up to captain (O-6) without any prior military experience. It's a move the Navy has been asking Congress to allow for the past couple years, specifically in the hope of adding high-powered cyber experts to expand the service's uniformed information warfare capabilities.

Though it's not a done deal, the move has passed its first hurdle in the approval process and was announced by the House Armed Services Subcommittee as one of its personnel proposals included in the latest mark-up of the FY19 National Defense Authorization Act. Despite being rocketed up the ranks, these officers won't be commanding ships. Instead, the skillful software engineers will serve the critical role of ensuring the military's ability to fight and wage cyber war, both on offense and defense. The new wording would allow lateral entry up to the O-6 pay grade to "any scientific or technical field designated by the Secretary of Defense" that "requires a high level of skill and that an insufficient number of officers possess in the military department concerned." **(FifthDomain.com, 01 May 2018)**

Drupal sites can be hacked by any visitor because of the code-execution bug

Drupal, a free and open source content management framework, written in PHP, has been hacked for the third time within 30 days. At the end of March, many sites running Drupal 8, Drupal 7, and Drupal 6 have been hacked after hackers exploited a bug called Drupalgeddon2. According to cyber researchers, about a million of sites were running the affected versions.

The hack has been marked as "highly critical" scoring 21 out of 25 under the National Institute for Standard and Technology (NIST) Common Misuse Scoring System. The Drupal's team released a patch for a quick fix immediately, though it was either poorly developed or people failed to install it. Said vulnerability could have allowed hackers to take over vulnerable websites, as well as create malware backdoors to inject crypto-miners. It is a remote code execution vulnerability. No more technical details beyond that are available. **(brica.de, 01 May 2018)**

Privilege Escalation Bug Lurked in Linux Kernel for 8 Years

A security vulnerability in a driver in Linux leads to local privilege escalation in the latest Linux Kernel version which was introduced 8 years ago, cyber security firm Check Point reveals. The security flaw provides a local user with access to a vulnerable privileged driver with the possibility to read from and write to sensitive kernel memory.

Because drivers commonly implement their own version of file operation functions, they are prone to implementation errors, and the discovery of this vulnerability is proof of that. The vulnerability was disclosed to the Linux Kernel on March 18 and a patch was issued the same day. After the patch was verified, the official Linux patch was issued for CVE 2018-8781 on March 21 and was integrated to the Linux Kernel the same day. **(SecurityWeek.com, 01 May 2018)**

Spam Botnet operators adopt a new technique to avoid detection

Necurs botnet was not active for a long period at the beginning of 2017 and resumed its activity in April 2017. It was used in the past months to push some malware, including Locky, Jaff, GlobeImposter, Dridex, Scarab, and the Trickbot. Now, the author implemented a new evasion technique. Crooks are sending out an email to a potential victim containing an archive file that once unzipped will present a file with the extension of *'.URL'*. The said extension is associated with Windows shortcut file that opens an URL into a browser. In the campaign observed by the experts, it points to a remote script file that downloads and executes a final payload.

Malware researchers added that crooks are using the standard folder icon to hide *'.URL'* files to deceive victims on their malicious nature. Once the victim has clicked on the archive it extracts a file that appears to the victims as a new folder on their PC. When the victims click on the folder to explore its content they will start the infection chain. Since this technique is revealed, internet users are advised to be vigilant. **(CyberDefenseMagazine.com, 01 May 2018)**