Check Point
SOFTWARE TECHNOLOGIES LTD.

February 25 – March 3, 2019

YOUR CHECK POINT
THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- The International Civil Aviation Organization (ICAO) has tried to hide a 2016 cyber-attack allegedly conducted by the China-linked APT-27 group which took control of two of its servers and exposed mail accounts and details of ICAO employees and website visitors.

- Following Check Point's last week's disclosure of WinRAR's "Absolute Path Traversal" vulnerability (CVE-2018-20250) a new email campaign distributing a malicious RAR archive file exploiting it to install a backdoor malware has been detected.

  Check Point IPS and SandBlast Agent provide protection against this threat *(RARLAB WinRAR ACE Format Input Validation Remote Code Execution (CVE-2018-20250))*

- Just three days after the Drupal developers announced they had patched a new vulnerability in their popular Content Management Software (CMS), a new series of attacks emerged, exploiting the same vulnerability, and targeting websites which have not yet updated their CMS to the patched version.

  Check Point IPS provides protection against this threat *(Drupal Core Remote Code Execution (CVE-2019-6340))*

- A new cyber-criminal group named "Pacha" that is believed to operate out of China has been hacking into Linux servers since last fall and installing a new strain of malware that mines cryptocurrency.

  Check Point Anti-Bot and Anti-Virus blade provide protection against this threat *(Trojan.WIN32.StratumMiner; Cryptominer.Linux.PachaAntd)*

- New evidence connects North Korean's "Lazarus" APT group to the global cyber-espionage campaign dubbed "Sharpshooter". Researchers gained access to a C2 server used in a campaign targeting at least 87 global defense and critical infrastructure players — including nuclear, defense, energy and financial companies.

VULNERABILITIES AND PATCHES

- Researchers have exposed vulnerabilities in the "Thunderbolt" interface, a common hardware interface created by Apple and Intel to connect peripheral devices, which affects all major operating systems, granting attackers direct access to content on system memory.
- Cisco has released a patch to a critical Remote Code Execution (RCE) vulnerability (CVE-2019-1663) rated as 9.8 Common Vulnerability Scoring System (CVSS) affecting its RV110W, RV130W, and RV215W Routers.

  Check Point IPS blade will provide protection against this threat in its next online package
- Adobe has released an emergency patch to fix a critical zero-day bug (CVE-2019-7816) exploited in the wild to its commercial web application development platform ColdFusion. All ColdFusion versions that do not have the current update are affected.

THREAT INTELLIGENCE REPORTS

- Cloud providers offering Infrastructure-as-a-Service (IaaS) are vulnerable to a new type of attack vector dubbed "Cloudborne". POC has demonstrated that hardware re-provisioned to new customers could retain backdoors installed on Baseboard Management Controllers (BMC) by previous users and be used to attack future users of the system.
- At least six different threat actors are exploiting known vulnerabilities (CVE-2014-3120 and CVE-2015-1427) on older versions of Elasticsearch clusters (versions 1.4.2 and lower) to drop cryptocurrency miners in a current spike of attacks.

  Check Point IPS provides protection against this threat *(Elasticsearch Sandbox Escape Command Execution (CVE-2015-1427); (ElasticSearch search Remote Code Execution (CVE-2014-3120))*
- Coinhive, a notorious in-browser cryptocurrency mining service popular among cybercriminals, has announced that it will discontinue its services due to the drop in mining rate and the 'crash' of the cryptocurrency market.
- In an offensive act prior to the US 2018 midterm elections, US Cyber Command had cut off internet access and formatted hard drives of the Russian Internet Research Agency (IRA), a company used by the Russian Government in propaganda and psyops operations.

  In light of increasing reports of malicious activity targeting the DNS infrastructure in attempts to perform traffic hijacking, the Internet Corporation for Assigned Names and Numbers (ICANN) has warned of a significant risk to key components of the Internet infrastructure and urged implementation of Domain Name System Security Extensions (DNSSEC) technology.