January 27 – February 2, 2020

YOUR CHECK POINT
THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Crooks are exploiting the global panic concerning the outbreak of the Coronavirus to infect Japanese users with Emotet through emails pretending to be a notice regarding infection prevention measures.

  Check Point SandBlast and Anti-Bot blades provide protection against this threat *(Trojan.Win32.Emotet)*

- The Japanese firm NEC, a contractor for Japan's defense industry, has suffered a data breach on December 2016. The breach, which was publicly disclosed by Japanese media, happened after an unauthorized actor hacked one of the company's servers, potentially accessing 28,000 files.

- The US government contractor Electronic Warfare Associates has fallen victim to a Ryuk ransomware attack, which compromised its web servers and other online sites. The attack occurs days after Ruyk's newest variant was enhanced to allow its operators to steal government-related data in large quantities.

  Check Point SandBlast and Anti-Bot blades provide protection against this threat *(Ransomware.Win32.Ryuk)*

- Despite the release of final security patches, attackers are continuing to actively exploit the critical Citrix vulnerability tracked as CVE-2019-19871, affecting Citrix NetScaler ADC and Gateways. It is estimated that around 80,000 companies from United States, United Kingdom, Germany and more are still at risk.

  Check Point IPS blade provides protection against this threat *(Citrix Multiple Products Directory Traversal (CVE-2019-19781))*

- Following the credit card breach affecting over 850 Wawa convenience stores, hackers have put up for sale more than 30 million payment details on a dark web marketplace.

- A leaked confidential United Nations report reveals that several UN servers of offices in Geneva and Vienna were compromised by an unknown actor. The report speculated that the attack was conducted by state actors, which were able to compromise an Active Directory server via SharePoint vulnerability.

- OurMine, a hacking group known to target celebrity social media accounts, hacked the official accounts of a number of NFL teams on various platforms, including Twitter, Facebook and Instagram.

VULNERABILITIES AND PATCHES

- Check Point Research has disclosed a flaw in Zoom video conference, which could allow attackers to brute-force Zoom for meeting IDs and hack into sessions that are not password-protected.
- Two vulnerabilities have been found in Microsoft Azure Cloud Infrastructure by Check Point Research - a server-side request forgery (SSRF) issue (CVE 2019-1234) and a remote code execution flaw (CVE-2019-1372). The first may allow an attacker to access sensitive information from virtual machines running on Azure cloud. The second may lead to a remote code execution and complete takeover of the affected server through the Azure App service. Both were addressed and patched by Microsoft.
- A critical security flaw in OpenSMTPD email servers has been discovered, and may potentially allow remote attackers to take complete control over OpenBSD-based and other Linux-based servers. The flaw resides in OpenSMTPD sender validation function, and can be exploited by sending a specially-crafted SMTP message to the server.
- A newly-discovered vulnerability in Intel's CPU, dubbed CacheOut, may allow sensitive information leakage from the secured SGX enclave, the OS kernel and virtual machines.

THREAT INTELLIGENCE REPORTS

- The newest variant of Predator the Thief has been examined by Check Point Research. The current version of the info-stealer was found to use various anti-debugging and anti-analysis techniques. Researchers traced the stealer back to its underground market sales and the potential authors.

  Check Point Anti-Virus and Anti-Bot blades provide protection against this threat (Trojan-PSW.Win32.Predator)
- After analyzing Phorpiex botnet's infrastructure and monetization methods, Check Point Research has published the first part of a thorough analysis of the malicious modules deployed onto victim machines.

  Check Point Anti-Bot and Anti-Virus blades provide protection against this threat (Worm.Win32.Phorpiex.)*
- Researchers have uncovered a highly-targeted campaign operated by the Winnti APT group targeting Hong-Kong universities using the ShadowPad backdoor and Winnti malware.

  Check Point Anti-Bot blade provides protection against these threats (Backdoor.Win32.Shadowpad; Backdoor.Win32.Winnti)
- A series of targeted attacks on the US government research contractor Westat has been observed by researchers, who attributed the campaign to the Iranian OilRig group (also known as APT34). The group used a phishing document masquerading as an employee satisfaction survey that installed the TONEDEAF backdoor as well as the VALUEVAULT password stealer.

  Check Point Anti-Bot blade provides protection against this threat (Backdoor.Win32.TONEDEAF; Infostealer.Win32.VALUEVAULT)