Check Point
SOFTWARE TECHNOLOGIES LTD.

January 20 - 26, 2020

YOUR CHECK POINT
THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- UN calls for an investigation on Saudi Arabia's role in amazon CEO Jeff Bezos's phone hack. The alleged attack was carried via WhatsApp. Bezos was sent a video in 2018 by Saudi Arabia's crown prince, Mohammed bin Salman, and apparently was infected at that time. Speculations point to NSO as the possible provider of the spyware (PEGASUS 3). More than 6GB of his personal data were stolen in over a year.
- The UPS store has suffered a data breach during a phishing campaign exposing information contained within documents that costumers emailed to stores for printing and related services. The information stolen includes names, emails, government-issued identifications, and financials.
- Microsoft has suffered a data breach affecting 250 million users. Between 05 December and 31 December 2019, five servers storing customer support analytics containing information such as email addresses, IP addresses, and support case details were accidentally exposed online without authentication protection.
- US government agency has been hit with new malware dropper "Carrotball" spread via a phishing campaign. The malware is used as a second-stage payload in targeted attacks and is linked to the Russian attacking group KONNI.
- Greek government website has suffered a DDOS attack twice this week. The Turkish group named Anka Neferler claimed to hijack the official websites of the parliament, the foreign affairs and economy ministries, as well as the country's stock exchange for 90 minutes.
- A zero-day exploit in Trend Micro's OfficeScan AV has been used to breach Mitsubishi Electric. Chinese hackers have used the vulnerability (CVE-2019-18187) to plant a bot in Mitsubishi's servers, stealing employee and corporate information.
- Euro Cup and Olympics Ticket reseller has been hit by MageCart. A reseller of these two major sports events happening later this year, has been infected with JavaScript that steals payment card details.

VULNERABILITIES AND PATCHES

- Citrix has released a new round of security updates to resolve a critical vulnerability exposing thousands of servers to code execution attacks, including a patch for Citrix application delivery controller (ADC) and Citrix gateway (CVE-2019-19781).

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

- Samba has released security updates for vulnerabilities that could have resulted in an attacker taking control of an affected system (CVE-2019-14902, CVE-2019-14907 and CVE-2019-19344).

- Cisco has released patches for a vulnerability in the web-based management interface of Cisco Firepower Management Center (FMC) that could allow an unauthenticated, remote attacker to bypass authentication and execute arbitrary actions with administrative privileges on an affected device (CVE-2019-16028).

- Researchers have found security flaws in Apple's private-browsing technology. The flaws were found in Safari's intelligent tracking prevention that is designed to protect users from cross-site tracking. The vulnerabilities can potentially reveal user's browsing behavior to third parties.

- Netgear, a computer networking company has released firmware hotfixes for a vulnerabilities in its wireless routers exposing TLS certificates to the public. The keys could be used to intercept and tamper with secure connections decrypting any traffic passing through that device.

THREAT INTELLIGENCE REPORTS

- Researchers have discovered a new wave of FTCODE ransomware campaign that steals browser's login credentials and Encrypts files in Windows systems. FTCODE is a PowerShell-based ransomware strain first spotted in 2013, which resurfaced in October 2019 as the final payload in a spam email campaign.

  Check Point SandBlast Anti-Ransomware provides protection against this threat *(Ransomware.Win32.Ftcode)*

- Internet routers running "Tomato", an alternative firmware, are under attack targeting default credentials for remote administration. Attackers utilize Muhstik botnet to infect the targets with malicious payloads.

  Check Point Anti-Virus and Anti-Bot blades protect against this threat *(Botnet.Win32.Muhstik; Trojan.Linux.Muhstik)*

- sLoad 2.0, A PowerShell-based malware infecting Windows Systems has been updated, and now includes advanced anti-analysis techniques and uploads screenshots from the infected machines to the C2 server.

  Check Point Anti-Virus blade provides protection against this threat *(Sload.RS)*