Check Point
SOFTWARE TECHNOLOGIES LTD.

October 19-25, 2020

YOUR CHECK POINT THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Voter database in Hall Country, Georgia, used to verify voter signatures, has been breached by ransomware, alongside other government systems. This might be the first official election resource to be hit by ransomware. The ‘DoppelPaymer’ gang has claimed responsibility for the attack.
- US officials warn against a Russian attack wave targeting the networks of dozens of state governments and municipalities across the US in light of the approaching presidential election. Additionally, FBI seniors state that Iranian actors have been distributing pro-Trump threat emails allegedly sent from the Proud Boys group, as part of a disinformation campaign.
- Sopra Steria, a France-based system and software consultancy with massive financial and healthcare sector customers, has suffered an attack by the Ryuk ransomware affecting its IT network.

  Check Point SandBlast provides protection against this threat

- The multinational pharmaceutical company Dr. Reddy's Laboratories is currently investigating a cyber-attack that required it to take its databases offline. Based in India, the company has recently announced it is starting clinical trials of a Russian-developed COVID-19 vaccine.
- The public transport system of Montreal (STM) has been attacked by the RansomExx ransomware, resulting in the shut-down of multiple services including the official website and the door-to-door paratransit service.

  Check Point SandBlast and Anti-Virus provide protection against this threat (Ransomware.Win32.Ransomexx)

- The systems of the US chain Boyne Resorts, which owns multiple attractions, lakeside and ski resorts, has been hit by the WastedLocker ransomware, affecting its IT and reservation systems.

  Check Point SandBlast and Anti-Virus provide protection against this threat (Ransomware.Win32.Wastedlocker)

- Cisco has been warning users of an attack wave targeting routers, leveraging the high severity vulnerability assigned CVE-2020-3118. The flaw affects routers running the Cisco IOS XR Software, deployed in several Cisco router platforms.

VULNERABILITIES AND PATCHES

- Google has released a new version of the Google Chrome browser to address the vulnerability assigned CVE-2020-15999, an actively exploited zero-day flaw that resides in the FreeType font rendering library and could be leveraged to execute arbitrary code by using specially crafted fonts.

  Check Point IPS provides protection against this threat (Google Chrome Memory Corruption (CVE-2020-15999))

- Oracle has published a critical patch addressing over 400 vulnerabilities across multiple products. Among these is a flaw in Oracle MySQL assigned CVE-2020-14888; the vulnerability allows a privileged attacker to easily compromise a MySQL Server and cause a Denial of Service (DoS) situation.
- VMware has fixed vulnerabilities in ESXi, Workstation, Fusion and NSX-T products, including a critical remote code execution flaw assigned CVE-2020-3992 and ranked 9.8, which impacts the OpenSLP service in ESXi.
- Adobe has released a security update to fix 16 critical vulnerabilities across 10 software packages including Adobe Illustrator, Photoshop, After Effects and more. All flaws could lead to arbitrary code execution.

THREAT INTELLIGENCE REPORTS

- Check Point Research has released its Phishing report for Q3 2020, revealing that Microsoft was the most heavily targeted brand, with 19% of all themed phishing attempts related to the company. WhatsApp is ranked first in the field of phishing attacks sent via mobile.
- Security researcher has managed to gain access to the Twitter account of President Trump, by guessing his password correctly. This is the second time the researcher has been involved in accessing the account, which is not protected by a 2FA mechanism.
- The NSA has published a detailed list of the top 25 vulnerabilities exploited by Chinese state-sponsored threat actors, and recommended mitigations. The most exploited among them is a Pulse Secure VPN flaw that allows a remote attacker to send a crafted URI to perform an arbitrary file reading.

  Check Point IPS provides protection against these threats (e.g., Pulse Connect Secure File Disclosure (CVE-2019-11510); Microsoft Windows DNS Server Remote Code Execution (CVE-2020-1350); Microsoft Exchange Server Remote Code Execution (CVE-2020-0688))

- Researchers have investigated GravityRAT, an espionage group affiliated with Pakistan that targets the Indian armed forces. While they previously targeted PC users, recently it has shifted to Android devices, infecting Indian defense sector users through modified versions of open-source applications.

  Check Point Anti-Bot provides protection against this threat (Backdoor.MSIL.GravityRat)

- Joint investigation of UK and US security agencies has revealed that Russian cyber-attackers affiliated with the GRU military intelligence were planning to execute cyber-attacks against the organizers of the Tokyo 2020 Olympics and Paralympics, and has already begun the reconnaissance stage.