February 1-7, 2021

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Check Point Research have collaborated in a research investigating the renewed activity and toolset of 'Infy', an Iranian APT active since 2007. Infy's targets are found mostly in Sweden, the Netherlands and Turkey, and the group has recently integrated a new second-stage payload called 'Tonnerre'.

  Check Point Anti-Virus and Anti-Bot provide protection against this threat (Trojan.Win32.Tonnerre; Trojan.Win32.Foudre)

- Check Point Research have investigated the current attack operations and infrastructure of Domestic Kitten, an Iranian APT that targets Iranian expats and dissidents. The group's newest campaign features an application mimicking the portal of Teheran restaurant 'Mohsen' and distributes the group's signature malware 'FurBall' under multiple covers.

  Check Point SandBlast Agent provides protection against this threat

- Hackers suspected to be of Chinese origin have exploited a bug in Solarwinds to access the National Finance Center, a federal payroll agency inside the US Department of Agriculture, among other organizations. The flaw utilized by the actor is separate from the one exploited in the infamous Solarwinds supply-chain attack.

- Popular music streaming platform Spotify has been hit by a credential-stuffing attack, only three months after a similar incident. The attack used stolen credentials from some 100,000 user accounts and leveraged a malicious Spotify login database.

- Stormshield, a French cybersecurity firm, has suffered a data breach. The incident affected the firm's technical portal used for support ticket management, possibly enabling access to personal user data. The attackers managed to steal source code for Stormshield Network Security firewall software.

- A new botnet leveraging the Mirai framework has recently emerged. The botnet, dubbed Matryosh due to its multi-layered structure, targets Android devices in order to launch DDoS attacks ,and propagates through the Android Debug Bridge (ADB) interface.

VULNERABILITIES AND PATCHES

- SonicWall has released a patch to address a critical SQL injection vulnerability in SonicWall's Secure Mobile Access 100 (SMA 100), a remote access product line. The flaw, assigned CVE-2021-20016, could grant an attacker access to login credentials as well as session information.
- Google has patched a zero-day vulnerability in its Chrome browser, actively exploited in the wild. The bug, assigned CVE-2021-21148, is a heap buffer overflow memory corruption bug in the V8 JavaScript engine. The bug may have been exploited by the North Korean Lazarus group in a recent campaign.
- Four vulnerabilities have been discovered in popular smart home cameras and doorbells, sold on Amazon and Walmart. The flaws could allow a remote attacker to obtain privileged access to these devices and their stored content, including audio and video recordings, and thus spy on their owners.
- Six critical security flaws have been discovered in Realtek RTL8195A Wi-Fi module, a highly integrated single-chip ideal for IoT applications in multiple industries. The flaws could be exploited to gain root access to a vulnerable device and gain control of its wireless communications.
- Mozilla has released an update to its Firefox browser to address a Windows 10 NTFS corruption bug triggered by accessing a certain path via the browser's address bar that could lead to filesystem corruption.

THREAT INTELLIGENCE REPORTS

- New malware dubbed 'Hildegard' has been targeting Kubernetes clusters. The malware was developed by the TeamTNT group, focusing on cloud and container infrastructures for Monero cryptocurrency mining.
- Researchers have uncovered an espionage supply-chain campaign dubbed 'Operation NightScout' that targets online-gaming communities across Asia. The operation leverages the update mechanism of an Android emulator called 'NoxPlayer' that has more then 150 million users.
- For nine months, researchers have tracked a dynamic email-based attack infrastructure used to distribute over a million emails per month delivering at least seven malware families, including Trickbot and Dridex. The investigation allowed researchers to connect seemingly unrelated campaigns.

  Check Point SandBlast and Anti-Bot provide protection against this threat (Trojan-Banker.Win32.TrickBot; Banking.Win32.Dridex)
- Malicious extension to Google's Chrome browser leverages the browser's sync feature, used to automatically sync the user's data and preferences, to harvest information from compromised machines and function as a communication channel, to exfiltrate the collected data to an attacker's server.
- The number of flaws in discovered in Industrial Control Systems (ICS) in 2020 has increased by almost 25% compared to 2019, and almost 33% compared to 2018, according to a report. 72% of the disclosed flaws could be exploited remotely, and 76% of them do not require authentication for exploitation.