February 15-21, 2021

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Russian APT group Sandworm has been targeting IT providers using Centreon servers in a three-years-long campaign. French company Centreon provides solutions for IT monitoring, and claims that only users of its open-source version, rather than the paid one, were affected.
- Threat actors associated with Clop ransomware gang and the FIN11 group have combined multiple zero-day vulnerabilities and a new web shell to breach up to 100 companies using Accellion's legacy File Transfer Appliance and steal sensitive files. Recent victims include supermarket giant Kroger and law firm Jones Day, among others.
- Underwriters Laboratories has suffered a ransomware attack that encrypted the certification giant's servers and caused a complete shutdown of its systems.
- Regional Internet registry RIPE NCC is warning of an ongoing credential-stuffing attack against its single sign-on service, RIPE NCC Access, and is encouraging users to implement two-factor authentication (2FA).
- Kia Motors America has been hit with a double-extortion ransomware attack executed by the "DoppelPaymer" group. The group is demanding $20 million for a decryptor and a guarantee to not publish sensitive data.

  Check Point SandBlast Agent provides protection against this threat

- A new variant of the credential stealer Trojan MassLogger has resurfaced in a recent phishing campaign targeting instant messenger apps, Outlook, and Google Chrome. The new variant uses a Microsoft compiled HTML help file format to start the infecting chain.
- Sequoia Capital, one of Silicon Valley's oldest Venture Capital firms, has suffered a data breach as a result of a successful phishing attack allowing an unauthorized third-party actor to access personal and financial information.

VULNERABILITIES AND PATCHES

- Two vulnerabilities have been found in Advantech WebAccess/SCADA software package. An adversary could exploit each of the vulnerabilities to disclose sensitive information and elevate their privileges on a targeted system.
- Brave browser has fixed a privacy bug that leaks the Tor onion URL addresses users visit to a locally configured DNS server, exposing the dark-web website browsing history.
- Researches have disclosed a vulnerability in Agora video SDK used by a variety of applications and sites that allows an attacker to obtain access and spy on ongoing audio and video calls (CVE-2020-25605).

THREAT INTELLIGENCE REPORTS

- Check Point Research has determined that Chinese hackers cloned and actively used a cyber offensive tool of a US-based hacking unit called Equation Group. The clone was placed into operation by Chinese hacking group, APT31, between 2014 and 2017 – three years before the tools were publically exposed.
- Check Point researchers have detected a new Office malware builder called APOMacroSploit, which was implemented in multiple malicious emails to more than 80 organizations worldwide. The analysis also led to the real identity of one of the threat actors behind the campaign.

  Check Point SandBlast provides protection against this threat
- A new malware infecting Apple Silicon had been found nesting on over 30,000 macOS endpoints. Named "Silver Sparrow", the malware currently lacks a malicious payload.
- The United States Federal Bureau of Investigation (FBI) has issued a stark warning about the consequences that telephony denial-of-service (TDoS) attacks on call centers could have.
- Researchers have spotted a new technique that abuses Google's App Script business application development platform to steal payment card information provided by customers of e-commerce websites.
- "WatchDog" botnet is now targeting Windows and Linux servers in a crypto mining campaign. The malware has flown under the radar for two years in what researchers call one of the largest monero cryptojacking attacks.

  Check Point SandBlast and Anti-Bot provide protection against this threat
- A cybercrime group that specializes in showing malicious ads has exploited an unpatched zero-day vulnerability in WebKit-based browsers in a campaign targeting iOS & macOS users, aimed to populate online gift card scams.