July 20 - 26, 2020

Check Point
SOFTWARE TECHNOLOGIES LTD.

YOUR CHECK POINT THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Check Point Research has found a long-term evolving phishing campaign turning to Google Cloud Storage and Google Cloud Functions to host phishing pages and steal users' e-mail credentials.
- Telecom Argentina has suffered a major ransomware attack demanding $7.5 million in cryptocurrency to unlock encrypted files.

  Check Point SandBlast Anti-ransomware blade provides protection against this threat
- Researchers have discovered an attack affecting over 4,000 unsecured databases. The attackers are deleting ElasticSearch and MongoDB databases exposed to the internet, wiping their data and replacing it with the word “Meow”. The motivation behind the attack is unclear, as the attackers did not leave a ransom note.
- Digital banking app, Dave.com, has suffered a security breach, exposing over 7.5 million user details on a public forum. The breach originated on the network of a former third-party service provider, Waydev.
- A Chinese APT group has been targeting India and Hong Kong with a new variant of MgBot malware through a unique phishing campaign. The same group seems to also be using an Android RAT, capable of recording screen and audio, locating the device, and stealing data such as contacts and SMS.

  Check Point SandBlast Mobile, SandBlast and Anti-Bot blades provide protection against this threat (Trojan.Win32.Mgbot)
- University of York has suffered a data breach, in which student and staff data was stolen. The breach stems in a ransomware attack against the university's CRM provider Blackbaud.

VULNERABILITIES AND PATCHES

- D-Link has disclosed severe vulnerabilities affecting its router models. The flaws include reflected cross-site-scripting (XSS), buffer overflow, bypassing authentication issues, and arbitrary code execution bugs.
- Cisco has fixed a high severity vulnerability, actively exploited in the wild. The vulnerability may allow unauthenticated attackers to read sensitive files on unpatched systems through directory traversal attacks.

  Check Point IPS provides protection against this threat (Cisco Adaptive Security Appliance Directory Traversal (CVE-2020-3452))
- Citrix has released security updates to address a vulnerability in the workspace app for Windows. A remote attacker could exploit this vulnerability to take control of an affected system if SMB is enabled.
- A new hacking technique uses Shadow Attacks to manipulate and replace content in digitally signed PDF files. 15 out of the 28 desktop PDF readers that were tasted were found to be vulnerable.
- IBM has patched a vulnerability (CVE-2020-4400) in Verify Gateway (IVG) that allows attackers to brute-force their way into systems remotely.

THREAT INTELLIGENCE REPORTS

- Check Point Research has released its 2020 mid-year report addressing cyber-attack trends, milestones and more aspects of the threat landscape while providing examples and statistics of real-world events.
- Lazarus hacking group has unleashed a new multi-platform malware framework with an aim to infiltrate corporate entities around the world, steal database, and distribute ransomware. The MATA malware framework is capable of targeting Windows, Linux, and macOS operation systems.

  Check Point SandBlast and Anti-Bot blades provide protection against this threat (Trojan.Win32.MATA)
- The popular android app of DJI GO 4 drone has been found to be violating Google Play policies by collecting sensitive user information, and is able to download and execute additional code on the user's device.

  Check Point SandBlast Mobile provides protection against this threat
- Researchers have found a new Cryptojacking botnet called "Prometei" spreading across compromised networks via multiple methods including Windows Server Message Block (SMB) protocol. The botnet's goal is to mine for Monero cryptocurrency and infect as many systems as possible.

  Check Point SandBlast and Anti-Bot blades provide protection against this threat
- The US Cybersecurity and Infrastructure Security Agency (CISA) has issued an alert about active exploitation of the unauthenticated remote code execution vulnerability affecting F5 big-IP ADC devices.

  Check Point IPS blade provides protection against this threat (F5 BIG-IP Remote Code Execution (CVE-2020-5902)