September 07 – 13, 2020

Check Point
SOFTWARE TECHNOLOGIES LTD.

YOUR CHECK POINT THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- US data center giant Equinix has been hit by the Netwalker ransomware. The threat actor demanded $4.5 million worth of bitcoin in exchange for decryption keys and to prevent release of stolen data. Also hit by Netwalker were Argentina's immigration agency, and the largest power supplier in Pakistan, K-Electric.

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

- The REvil ransomware operators have hit the Chilean bank BancoEstado which has been forced to remain closed since September 7.

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

- US district court in Louisiana has been hit by ransomware, and court data was published online as proof. The attack is attributed to Conti, the group behind the Ryuk ransomware.

  Check Point SandBlast and Anti-Bot blades provide protection against this threat (Ransomware.Win32.conti)

- Fairfax county public schools, one of the largest in the US, with a budget of $3.2 billion has been hit by ransomware. The Maze ransomware operators assumed responsibility and published an archive of 100MB of student info and administrative data.

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

- European cryptocurrency exchange Eterbase has disclosed a major breach of its networks leading to the loss of $5.4 million worth of cryptocurrencies, stolen by the attackers. The platform operators, based in Slovakia, tracked the majority of transactions and contacted related exchanges in hope for assistance.

- CDRThief, a newly reported malware, targets Linux VoIP systems from the Chinese company Linknat and steals call-records and database information including credentials and IP addresses. Initial attack vector is still unknown, nor are the attackers' ultimate goals.

- A Misconfigured Elasticsearch cluster has exposed details of 100,000 gamers, clients of Razer gaming hardware manufacturer. Exposed info included names, emails, phone numbers, billing and shipping data.

VULNERABILITIES AND PATCHES

- Palo Alto Networks has released security updates to patch critical and high-severity vulnerabilities in its PAN-OS firewall. The critical vulnerability, tracked as CVE-2020-2040, could be exploited by sending requests to the MFA interface, resulting in buffer overflow ultimately allowing a remote unauthenticated attacker to execute arbitrary code as root.
- In September's Patch-Tuesday, Microsoft has addressed 129 fixes relating to Microsoft Windows, Edge, Internet Explorer, SQL Server, Office, Azure and more. 23 of the vulnerabilities were listed as critical and 105 as important.

  Check Point IPS provides protection against these threats (CVE-2020-1152; CVE-2020-0856; CVE-2020-0664; CVE-2020-1115; CVE-2020-1308; CVE-2020-1245; CVE-2020-0941)
- Adobe has released fixes to 18 vulnerabilities in InDesign, Framemaker, and Adobe Experience Manager.
- A newly reported vulnerability in the Bluetooth protocol, tracked as CVE-2020-15802, allows attackers to connect to nearby devices without user consent. The bug, dubbed BLURtooth, which could lead to MITM attacks (Man In The Middle) affects hundreds of millions of devices worldwide.
- Researchers have reported ten vulnerabilities in MoFi network routers, some could be exploited by unauthenticated remote attackers to take over targeted routers.
- A researcher has reported a cross-site scripting flaw in Google Map's export function, and then bypassed Google's released patch. The discoveries and reports were rewarded twice by the company's bug-bounty program.

THREAT INTELLIGENCE REPORTS

- Microsoft reports that Russian, Iranian and Chinese APT groups have stepped up their efforts to target the 2020 US elections, attacking political campaigns, parties and political figures associated with both the Joe Biden and Donald Trump Presidential campaigns.
- Researchers have examined the website-defacing market and uncovered 89 zero-day vulnerabilities in popular content management systems and plugins, exploited by different hacking bots.
- Cyber security agencies from multiple countries are warning of a surge in Emotet attacks. Recent attacks utilized .doc and password protected .zip files as malicious payloads sent in reply emails to hijacked conversations. The French Ministry of Interior decided to block all Office documents delivered via email.

  Check Point SandBlast and Anti-Bot provide protection against this threat (Trojan.WIN32.Emotet)