Check Point SOFTWARE TECHNOLOGIES LTD.

Aug 16 - 22, 2021

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- The Hive ransomware gang has encrypted computers of Memorial Health System, a chain that operates hospitals and clinics in the US, eventually forcing workers to operate with paper charts and cancel surgeries. Although Hive had previously used “double-extortion” techniques, according to MHS, patients’ data was not stolen.

  Check Point Harmony Endpoint provides protection against this threat

- The Iranian threat group SiameseKitten (AKA Lyceum/Hexane) has targeted several Israeli IT organizations using impersonation of companies’ HR staff and fake job offers on LinkedIn. The attack was potentially in an attempt to infiltrate their environment and initiate a supply chain attack to gain access to their clients.

  Check Point Threat Emulation provides protection against this threat

- The largest-ever distributed denial of service (DDoS) attack has been detected, with 17.2M requests-per-second. The attack was facilitated by the Mirai botnet, targeting an organization in the financial industry.

- T-Mobile has announced that personal data of 5 million customers has been breached, in addition to over 40 million records previously announced to have been breached in the same attack. Clients’ financial data is said to be safe.

- JP Morgan Chase Bank has warned customers of a data breach that was caused by a technical issue on the bank’s app and website. The flaw allowed customers to see other customers’ personal information including account balance and name.

- A subsidiary of Tokio Marine Group, the Tokio Marine Insurance Singapore Ltd., has announced it was the victim of a ransomware attack and is currently evaluating the scope of damages.

- The US State Department has discovered a possible serious breach as the result of a cyberattack.

- The Brazilian National Treasury has been hit with a ransomware attack. The consequences are currently being investigated but it did not seem to have caused damages to their structural systems.

VULNERABILITIES AND PATCHES

- A Citrix ADC vulnerability has been exploited to hack the US Census Bureau back in January 2020. The Bureau had not mitigated the vulnerability (CVE-2019-19781), leaving its servers vulnerable.

  Check Point IPS provides protection against this threat *(Citrix Multiple Products Directory Traversal (CVE-2019-19781))*

- CISA warns of active attempts to exploit the "ProxyShell" Microsoft Exchange vulnerabilities patched in May 2021 to launch the LockFile ransomware on compromised systems.

  Check Point IPS provides protection against this threat *(Microsoft Exchange Server Remote Code Execution (CVE-2021-34473))*

THREAT INTELLIGENCE REPORTS

- As the new school-year approaches, Check Point Research has found a 29% increase in the number of attacks against organizations in the education sector, making it the most targeted vertical in July 2021.
- Security experts warn of new malware campaign that bypasses browser warnings by deceiving users into complying with a fake CAPTCHA challenge. The URL takes the victim to a page embedded with a YouTube video. Once users click "play", a malicious executable called "console-play.exe" is downloaded, and completing the fake CAPTCH actually goes to the toolbar and runs the downloaded executable.
- Researchers have found that the Diavol Ransomware is possibly linked to the TrickBot Gang, as Diavol samples share behavioral similarities with other malware attributed to the Trickbot gang.

  Check Point Harmony Endpoint and Anti-Bot provide protection against these threats *(Trojan.WIN32.TrickBot)*

- Following the May ransomware attack, Colonial Pipeline informed 5,810 of its personnel that the DarkSide threat group was able to steal their personal information.

  Check Point Harmony Endpoint provides protection against this threat

- A new extortion campaign attempts to leverage the Pegasus iOS spyware to intimidate potential victims. The scammers sent out emails extorting recipients to pay ransom demands by claiming that they have private videos of them, taken by the Pegasus malware allegedly installed on their iPhone devices.
- An exposed Elasticsearch database containing 1.9 million terrorist watch list records has been discovered, including no-fly status and sensitive information. The list was available across several search engines for at least three weeks before being taken down by the US Department of Homeland Security.