CHECK POINT RESEARCH

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- The Superior Court of Los Angeles was forced to shut down its network following a ransomware attack. The court, the largest in the United States, has closed all of its 36 courthouse locations due to the attack for a few days. No ransomware group has publicly claimed responsibility for the attack.
- American cybersecurity firm KnowBe4 recently discovered that a newly hired Principal Software Engineer was a North Korean state actor attempting to install information-stealing malware. The company detected the malicious activity before any data breach occurred.
- Acadian Ambulance, a United States privately-owned ambulance company, has suffered a ransomware attack. The threat actors, Daixin Team, claim to have exfiltrated personal and medical data of 10 million patients, and demands $7M in ransom.

  Check Point Harmony Endpoint provides protection against this threat.
- Ukraine's Main Intelligence Directorate has announced a successful cyber-attack targeting Russia's banking system. According to the agency, it has gained access to major Russian banks' databases, blocked credit card transactions and stopped the withdrawal of cash from ATMs. Ukraine also claims to have disrupted several Russia mobile and internet providers.
- Belarusian state-sponsored hacker group GhostWriter (UAC-0057) targeted Ukrainian organizations and local government agencies with PicassoLoader malware in a recent campaign. Researchers reported that the hackers also used Cobalt Strike Beacon to infect their victims. The phishing emails were related to the USAID's Hoverla project, which aims to reform Ukraine's local governance. While the campaign's specific goal is unclear, GhostWriter is typically involved in cyber espionage.
- An ongoing crypto-mining campaign dubbed "SeleniumGreed" is exploiting exposed Selenium Grid services. Selenium is a widely used testing framework that can be found in 30% of cloud environments. The threat actors leverage the Selenium WebDriver API to run Python with a reverse shell, deploying scripts to download a modified XMRig miner.
- An unnamed Middle Eastern financial institution faced a six-day distributed denial-of-service (DDoS) attack launched by the pro-Palestinian hacktivist group SN_BLACKMETA, resulting in 100 hours of disruption. The attack was pre-announced on the group's Telegram channel. Despite the intensity, the attackers failed to impact the institution's services significantly.
- A German member of Europe's Parliament (MEP) revealed that his mobile phone was targeted with commercial spyware, likely from Candiru, in an attempted attack disguised as an email link. The MEP suspects Hungary's government, led by Viktor Orbán, due to his vocal criticism of Orbán and Hungary's known use of spyware.

VULNERABILITIES AND PATCHES

- Researchers have discovered several 0-day vulnerabilities (CVE-2024-32484, CVE-2024-29073, CVE-2024-32152, and CVE-2024-26020) in Anki, the widely-used flashcard application. These include arbitrary file reads and remote code executions through exploits in its web server, LaTeX content handling, and media hosting services.

- ServiceNow, a software company that provides cloud computing platform for operations management, disclosed two critical and one medium vulnerabilities (CVE-2024-4879; CVSS 9.3, CVE-2024-5217; CVSS 9.2, CVE-2024-5178; CVSS 4.0). The critical flaws allow remote code execution to unauthenticated attackers in the Now Platform, while the medium vulnerability allows administrative users to gain unauthorized access to sensitive files on the web application server.

THREAT INTELLIGENCE REPORTS

- Check Point Research uncovered a network of GitHub accounts, dubbed the Stargazers Ghost Network, that distributes malware and malicious links through phishing repositories. Operated by the threat group Stargazer Goblin since August 2022, this network functions as a sophisticated Distribution as a Service (DaaS) model. The group uses over 3,000 accounts to create an illusion of legitimacy by starring, forking, and subscribing to malicious repositories. The network has distributed various malware families, such as Atlantida Stealer and RedLine, and earned significant profits.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat
  (InfoStealer.Win.Atlantida., Trojan.WIN32.AtlantidaStealer*, InfoStealer.Wins.Lumma.ta*, InfoStealer.Win.Lumma*, Injector.Win.RunPE.C, Loader.Wins.GoBitLoader.A, Trojan.Wins.Imphash.taim.LV, InfoStealer.Wins.Redline.ta.BY)*

- Check Point Research released its latest Brand Phishing Ranking for the second quarter of 2024. For the second quarter this year, Microsoft remained the most imitated brand in phishing attacks, accounting for more than half of all attempts with 57%. Apple jumped to second spot with 10%, moving up from fourth position in the first quarter of 2024, and LinkedIn kept its previous third place ranking with 7% of such attempts. Meanwhile, there were new entries to the list with Adidas, WhatsApp, and Instagram moving into the top 10 for the first time since 2022.

- Check Point Research detailed a process injection method via atypical APIs that are not commonly used in well-established attack chains. The method uses relatively new Windows APIs and allows injection of a shellcode into a running process.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat
  (Behavioral.Win.ImageModification.C, Behavioral.Win.ImageModification.F)

- Check Point Research analyzes the trend of increasing sophistication of cryptocurrency scams. Threat actors target users of popular legitimate blockchain platforms Uniswap V3 and Safe.global by using aggregate functions, which allow them to mask malicious transactions within contracts that otherwise appear legitimate.