August 12 – 18, 2024

CHECK POINT RESEARCH

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- The campaign of United States presidential nominee Donald Trump has had its internal communications hacked and leaked, allegedly by an Iranian threat actor. This aligns with Microsoft's previous identification of a related spear phishing attack by an Iranian group, raising concerns about foreign interference in the US elections.

- Luxembourg-based Orion SA reported a significant financial loss due to a business email compromise (BEC) scam, resulting in fraudulent wire transfers of approximately $60 million. This scam involved deceiving an Orion employee through sophisticated phishing methods to authorize transfers to accounts controlled by criminals.

- The city of Flint, Michigan, is dealing with disruptions to its municipal services following a ransomware attack that compromised its internal networks. The FBI and state attorney general are investigating the incident, which has affected payment systems and led to outages of digital services.

- Unicoin, a cryptocurrency company, reported that a hacker compromised their Google G-Suite accounts, altering user passwords and blocking access for nearly four days. The firm is investigating the breach's full impact, including potential discrepancies in employee data.

- Beregini, a self-described Ukrainian hacktivist group with pro-Russian narrative, is suspected of being supported by a hostile state in a cyberattack on Poland's anti-doping agency POLADA. The attack resulted in the leak of over 50,000 confidential files, including medical records and testing histories of Polish athletes. POLADA has notified affected athletes and is working with law enforcement and cybersecurity agencies to secure its systems and investigate the breach.

- Evolution Mining, an Australian gold mining company, shared that a ransomware attack is impacting its IT systems. The company has contained the attack and is collaborating with external cyber forensic experts to investigate the incident. No specific ransomware group or details on any extortion payment were provided.

- Schlatter Group, the Switzerland-based manufacturer, disclosed a significant disruption to its IT systems due to a cyber-attack. The incident, which involved unauthorized access, did not specify the details of data potentially compromised nor the attackers.

- RansomHub ransomware gang has breached Hudson Civil Engineering, a Tasmanian firm, claiming the theft of 112GB of data. This joins a list of other Australian engineering and construction companies attacked by the group, including McDowall Affleck and Kempe Engineering.

  Check Point Threat Emulation and Harmony Endpoint provide protection against this threat
  (Ransomware.Win.RansomHub; Ransomware.Wins.RansomHub.ta.)*

VULNERABILITIES AND PATCHES

- Check Point Research has identified an increase in Server-Side Template Injection (SSTI) vulnerabilities, which allow attackers to execute arbitrary commands and access sensitive data. Recent examples include high-profile platforms like Atlassian Confluence and CrushFTP. The vulnerabilities, which pose risks like data theft and reputation damage, have seen a rise in critical CVEs, underlining their potential for severe impact on organizations.

  Check Point IPS provides protection against this threat (Python Server-Side Template Injection, Java Server-Side Template Injection, PHP Server-Side Template Injection, Ruby Server-Side Template Injection, Node.js Server-Side Template Injection, Expression Language Server-Side Template Injection)

- Microsoft's August Patch Tuesday has addressed 90 vulnerabilities in its products. Among those are 6 zero-day vulnerabilities that are being actively exploited in the wild (including high severity CVE-2024-38178 and CVE-2024-38193). The patch contains fixes to 8 critical vulnerabilities in Windows TCP/IP, Azure Stack, Azure Health Bot, Reliable Multicast Transport Driver, Windows Network Virtualization and Line Printer Daemon Service.

  Check Point IPS provides protection against this threat (Microsoft Scripting Engine Memory Corruption (CVE-2024-38178), Microsoft Windows Ancillary Function Driver for WinSock Elevation of Privilege (CVE-2024-38193))

- SolarWinds has issued a patch for a critical Java deserialization RCE vulnerability (CVE-2024-28986) in its Web Help Desk software. This flaw could allow unauthenticated command execution, posing security risks although the vulnerability has not been reproduced without authentication in tests.

THREAT INTELLIGENCE REPORTS

- Check Point Research have analyzed the Styx Stealer, a new malware already used in attack campaigns, capable of stealing browser data, instant messenger sessions from Telegram and Discord, and cryptocurrency. During the research, CPR found that the developers of Styx Stealer are linked to one of Agent Tesla threat actors. Additionally, due to a developer error that led to data leakage from their computer, large amount of intelligence about the operation was obtained.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat (InfoStealer.Wins.PhemedroneStealer.)*

- Check Point Research has found that following the contested presidential elections in Venezuela on July 28th, 2024, hacktivist groups including Anonymous Venezuela and Cyber Hunters have executed attacks against Venezuela government. The #OpVenezuela campaign involves DDoS attacks and alleged hacking attempts, driven by accusations of election fraud by Nicolás Maduro's government.

- Check Point Research warns that schools and universities, with their treasure troves of sensitive data and often insufficient cyber security measures, have become prime targets for cybercriminals. The blog elaborates on attack trends targeting the education and research sector and highlights that in 2024 this sector has been the most targeted one globally, with an average of 3,086 attacks per organization, per week.