December 9 - 15, 2024

CHECK POINT RESEARCH

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- The Romanian National Cybersecurity Directorate (DNSC) has disclosed a ransomware attack conducted by Lynx ransomware gang on the country's energy provider Electrica Group, which provides services to more than 3.8M people across Muntenia and Transylvania. DNSC confirms that critical power supply systems were not impacted.

  Check Point Threat Emulation and Harmony Endpoint provide protection against this threat (Ransomware.Win.Lynx; Ransomware.Win.Lynx)

- SRP Federal Credit Union, one of South Carolina's largest credit unions, has suffered a cyberattack that has compromised the personal data of over 240,000 customers. Information accessed includes names, Social Security numbers, driver's license numbers, dates of birth, and financial data. Nitrogen ransomware gang took responsibility for the attack, claiming to have stolen 650GB of data.

- American non-profit Anna Jaques Hospital has concluded its investigation and confirmed a ransomware attack that resulted in the exposure of sensitive data of over 300,000 patients on the dark web. The attack, conducted by the Money Message group in late 2023, involved exfiltration and encryption of files containing Social Security numbers, driver licenses, as well as sensitive demographical, medical and financial information.

  Check Point Threat Emulation provides protection against this threat (Ransomware.Wins.MoneyMessage)

- Bitcoin ATM giant Byte Federal was hit by a cyber-attack in November that resulted in the compromise of the personal data of 58,000 clients. The threat actor gained access to Byte Federal systems by exploiting a GitLab vulnerability, exposing names, addresses, phone numbers, government-issued IDs, Social Security numbers, transaction activity, and user photos.

- Artivion, an American manufacturer of heart surgery medical devices, has been a victim of a ransomware attack that occurred in November and forced it to take some systems offline as a precaution. The attack disrupted its delivery and shipping systems by encrypting files, causing operational delays and an expected financial impact. No ransomware gang has taken credit yet.

- Auto parts giant LKQ Corporation has suffered a cyber-attack that resulted in unauthorized access to its Canadian business unit's IT systems, causing operational disruptions for several weeks. The incident may have compromised data of individuals associated with the affected unit. No ransomware gangs or other threat actors have claimed responsibility for the attack.

- Krispy Kreme Doughnut Corporation has experienced a cyber-attack that resulted in unauthorized access to its IT systems, causing disruptions to online ordering for customers. The incident is expected to have a material financial impact due to ש digital sales and restoration costs.

VULNERABILITIES AND PATCHES

- Microsoft's December 2024 Patch Tuesday addresses 71 vulnerabilities across 10 product families, including 16 critical issues and one zero-day vulnerability (CVE-2024-49138). This zero-day is a privilege escalation vulnerability within the Microsoft Windows Common Log File System (CLFS) driver. The most affected product is Microsoft Windows with 58 patches, followed by Extended Security Updates (ESU), and Microsoft Office.

  Check Point IPS blade provides protection against this threat (Microsoft Windows Common Log File System Driver Elevation of Privilege (CVE-2024-49138))

- Google has released a security update for Google Chrome, addressing two high severity vulnerabilities, CVE-2024-12381 and CVE-2024-12382. The first flaw is a type confusion vulnerability in the Chrome V8 JavaScript engine and the second is a use after free vulnerability in Chrome's Translate function. These vulnerabilities could allow unauthorized control over affected systems.

- Apple has published a security advisory addressing vulnerabilities in its products' operating systems iOS 18.2 and iPadOS 18.2. The security patch for iOS includes fixes more than 20 security vulnerabilities. One of the flaws, CVE-2024-54526, could result in access to private information.

THREAT INTELLIGENCE REPORTS

- Check Point Research has released November 2024's Most Wanted Malware report, highlighting the rise of Androxgh0st, a Mozi-integrated botnet exploiting vulnerabilities across multiple platforms, including IoT devices and web servers. Among top mobile malware threats, Joker remains most prevalent, followed by Anubis and Necro. Joker steals SMS messages, contacts, and device information while silently subscribing victims to premium services.

- Threat actors posed as IT support on Microsoft Teams, tricking employees into installing AnyDesk for remote access. The attackers leveraged registration bombing to flood victims' inboxes with legitimate spam emails, sowing confusion and prompting them to seek help. After gaining access, they deployed multiple malicious files, including the DARKGATE malware.

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

- Researchers have analyzed a new packer-as-a-service (PaaS) called HeartCrypt, used to protect malware. Developed since July 2023 and launched in February 2024, it serves malware families like LummaStealer, Remcos, and Rhadamanthys. HeartCrypt operators charge $20 per file, support Windows x86 and .NET payloads, and advertise it via underground forums and Telegram.

  Check Point Threat Emulation and Harmony Endpoint provide protection against this threat (InfoStealer.Win.Lumma; InfoStealer.Wins.Lumma.ta.; Trojan.Wins.Remcos; RAT.Win.Remcos.glmw.*; RAT.Win.Remcos; InfoStealer.Wins.Rhadamanthys; InfoStealer.Wins.Rhadamanthys.ta.*)*