January 22 - 28, 2024

Check Point Research
WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Following the reports on Russia-affiliated APT29 (AKA Cozy Bear, Midnight Blizzard) attack against Microsoft, also [Hewlett-Packard Enterprise]acknowledged it was attacked by the same threat actor. While Microsoft detected the breach on January 12 and the password-spray attack began in November 2023; HPE's investigation points to evidence that APT29 was able to maintain persistence on the company's systems since May 2023. Security experts estimate more companies are expected to confirm their email system has also been compromised by the group in this cyber-espionage attack.

- Ransomware gang LockBit claimed responsibility for a recent attack on EquiLend, a Wall Street stock-lending firm. The attack rendered the EquiLend platform and other automation solutions offline, and a representative said it could take days to recover. The attack on the company, owned by BlackRock, JP Morgan and other major firms, is said to have 'limited' affect on financial market players that were forced to switch to manual processes as the platform crashed.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat
  (Ransomware.Wins.LockBit.ta; Ransomware.Win.Lockbit; Gen.Win.Crypter.Lockbit.AI, Ransomware_Linux_Lockbit)*

- Largest Ukrainian online bank Monobank was hit by a three-day long DDoS attack. Some of the mobile-only bank operations were disrupted due to the attack. While the attacker hasn't officially been identified, it is presumed the attack was executed by Russian hacktivists.

- Multiple Ukrainian state-owned entities, including Naftogaz, the Postal Service, Railway Services, and transportation agency DSBT, experienced cyberattacks, leading to service disruptions. The attacks targeted data infrastructures, causing operational issues such as postal delays, offline websites, and disruptions in border-crossing systems for cargo delivery. Russian hacktivist group, National Cyber Army, claimed responsibility for the DSBT attack but did not mention other affected entities.

- Genetic tests provider 23andMe, confirmed a credential stuffing attack that went unnoticed for five months. The cyberattack, which started in April and went unnoticed until September, compromised health reports and raw genotype data of 1 million Ashkenazi Jews and 4 million UK residents, and is currently being leaked on cyber-crime forums.

- Pro-Ukraine hacktivist group 'BO Team' claimed responsibility for an attack on a Russian research center known as 'Planeta'. According to Ukraine's defense intelligence directorate (GUR), the breach led to the destruction of state-owned Planeta's database and valuable equipment, compromising data from Earth-observing satellites.

VULNERABILITIES AND PATCHES

- Apple released security updates to address a zero-day vulnerability, tracked as CVE-2024-23222, in Apple's WebKit. This flaw could impact iPhones, Macs, and Apple TVs, and could lead to arbitrary code execution on affected devices. The vulnerability is actively exploited in the wild. In addition, Apple have also released security updates for multiple products (including iOS, iPadOS, macOS, Safari, watchOS, and tvOS) to address vulnerabilities that could allow cyber threat actors to take control of affected systems.

- A critical vulnerability, CVE-2024-21591 (CVSS score: 9.8), was discovered in Junos SRX and EX series devices, allowing unauthenticated Remote Code Execution (RCE) with root privileges or a denial-of-service attack. While no active exploitation is observed, due to past attacks on Junos OS and the severity of this threat, immediate patching is strongly advised for impacted devices.

- Researchers identified critical and high severity vulnerabilities in Jenkins - a widely used open-source Continuous Integration and Continuous Deployment software. The Critical vulnerability (tracked as CVE-2024-23897) allows unauthenticated attackers to read arbitrary data from Jenkins' server. The High severity vulnerability (CVE-2024-23898) is a cross-site WebSocket hijacking issue, enabling attackers to execute commands by tricking victims into clicking a link.

  Check Point IPS blade provides protection against this threat *(Jenkins Information Disclosure (CVE-2024-23897))*

THREAT INTELLIGENCE REPORTS

- Check Point reports on a rise in QR-code-based phishing attacks. These attacks are usually successful, as many email security solution do not include QR code protections, and cyber-criminals are adapting to bypass existing protections. For example, attackers are using different redirections for various operating systems, and use multiple obfuscation and anti-reverse engineering techniques.

- Researchers observed a recent campaign by North Korea-linked APT group ScarCruft. The group has recently been targeting South Korean media and research organizations with RokRAT, delivered via malicious documents. The research also brought to light evidence of potential targeting of the cybersecurity sector.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat *(Technique.Win.EmbedExeLnk; Trojan.Wins.SusLNK; Injector.Win.RemoteThread; Technique.Win.MalOfficeVBA; Exploit.Win.MalChildren)*

- Researchers reported on a new and sophisticated malware used by China affiliated APT group, dubbed 'Blackwood'. The malware was distributed via update mechanisms of legitimate popular software such as Tencent QQ, WPS Office, and Sogou Pinyin. The targets included Chinese and Japanese companies, as well as individuals located in China, Japan, and the United Kingdom.