TOP ATTACKS AND BREACHES

- Acuity, a federal contractor, confirmed a cyber incident where hackers accessed its GitHub repositories, and stole various documents. The breach, linked to the threat actor IntelBroker, involved data from various U.S. government agencies. While Acuity claims to have found no evidence of sensitive data impact, the US State Department is investigating the breach, which purportedly compromised classified information from the Five Eyes intelligence alliance, features government, military, and Pentagon employees' details.

- Prudential Insurance experienced a cyberattack in February, resulting in unauthorized access and access to personal information, including names, addresses, and driver's license numbers, of 36,545 individuals. The AlphV ransomware gang claimed responsibility for the attack, which was disclosed after a law enforcement takedown attempt of the gang's infrastructure.

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

- PandaBuy suffered a data breach, after threat actors Sangierro and IntelBroker exploited critical vulnerabilities in its API to steal and leak a database of over 1.3 million customers' information on BreachForums. The data includes full names, contact details, login IPs, order details, home addresses, and zip codes. Cybersecurity experts confirmed the authenticity of the database.

- The Russian-speaking hacktivist group RGB-TEAM claimed to have breached Russia's prosecutor general's website, leaking 100,000 criminal records from 1993 to 2022 on Telegram. The leak includes data on crimes like theft and drug sales. Independent verification confirmed the data's authenticity.

- Jackson County in Missouri is addressing disruptions in its IT systems suspected to be caused by a ransomware attack, affecting tax payments, and various online services. The county has noted operational inconsistencies across its digital infrastructure, with certain systems rendered inoperative.

- Multiple Iranian hacker groups launched #OpIsrael and Quds Day cyberattacks, targeting sectors like education, banking, government, and healthcare in Israel. Key groups included Iran affiliated groups like Malek Team, Lord Nemesis, and Handala Hack, as well as Anonymous. Malek Team hit the "Doctorim" medical site and "Emalon" hotel booking site, claiming to breach over 1.2 million records. Anonymous targeted the Israeli Ministry of Justice, claiming to wipe servers and steal data. Lord Nemesis released data from educational institutions, and Handala Hack claimed attacks on various Israeli companies and a substantial data breach from ArrowNet company.

VULNERABILITIES AND PATCHES

- Security experts have uncovered a sophisticated supply chain attack involving a backdoor planted in the xz/liblzma compression tool, part of the xz-utils package, affecting major Linux distributions. Initiated through a campaign of tampering and social engineering, the XZ Trojan has compromised open-source compression library xz/liblzma versions 5.6.0 and 5.6.1. The backdoor enables remote, unauthorized access and code execution on affected systems, prompting a rapid response from cybersecurity authorities and a call for organizations to revert to secure xz software versions.

- Google issued a security advisory for Android Pixel smartphone owners, warning about targeted attacks exploiting two vulnerabilities (CVE-2024-29745 and CVE-2024-29748) to bypass built-in security features. These vulnerabilities were exploited by "forensic companies", possibly for law enforcement purposes, to extract information and prevent remote wiping of confiscated phones. Google is releasing patches to address these vulnerabilities, which have seen in-the-wild exploitation.

- Researchers disclosed vulnerabilities in Ivanti Connect Secure and Policy Secure gateways, including CVE-2024-21894, which enables unauthenticated attackers to perform DoS attacks and potentially execute arbitrary code. With a CVSS score of 8.2, the vulnerability affects various versions of Ivanti products. Ivanti has released patches for all affected versions to mitigate these high-severity flaws.

  Check Point IPS blade provides protection against this threat *(XZ Utils Backdoor (CVE-2024-3094))*

THREAT INTELLIGENCE REPORTS

- Check Point Research reports on the active usage of AI in election campaigns around the world. AI technologies have been used to create content misleading voters, promoting candidates, attacking political adversaries, and disseminating disinformation on a wide scale. With audio manipulation technology being more mature and harder to detect, it currently poses a larger threat than videos.

- Check Point Research reveals an Agent Tesla malware campaign aimed at U.S. and Australian organizations, initiated by the main threat actor "Bignosa" and associated actor "Gods." The campaign, exploiting email phishing to distribute the malware, utilized advanced obfuscation methods including Cassandra Protector. Detailed investigation linked the activities to specific individuals, highlighting the extent and sophistication of the operation.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat.

- Check Point Research (CPR) recently analyzed several popular dating applications with over 10 million downloads combined to understand how safe they are for users. The research focused on a popular gay dating app called “Hornet” that had vulnerabilities, allowing the precise location of the user, even if users disabled the display of their distances.