TOP ATTACKS AND BREACHES

- The US and UK governments have announced a criminal indictment and sanctions against APT31, a group of Chinese hackers, for their role in allegedly conducting attacks against companies in the US, as well as government officials in the UK. Check Point has shared its insights on the event and referenced a past report about APT31, including a deep dive into how the group used zero-day vulnerabilities.

- INC ransomware gang has launched a cyberattack on the healthcare system of the Scottish NHS Dumfries and Galloway, claiming to have stolen 3 terabytes of sensitive patient data. Threatening to leak the data unless their demands are met, the gang provided "Proof pack" screenshots as evidence. NHS has confirmed the leak of clinical data for a small number of patients.

- Qilin ransomware gang has disrupted the operations of "The Big Issue", a well-known street newspaper sold by homeless individuals in the UK. The gang claimed to have stolen 550GB of confidential data including files related to commercial and personnel operations.

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

- Threat actor IntelBroker has been observed selling data of the England and Wales Cricket Board's icoachcriket platform. Over 40K users' personal information, including email addresses and hashed passwords from 2014 to 2021, has been compromised and is now up for sale on dark web forums. The ECB has yet to confirm the breach.

- The city of St. Cloud, Florida, has suffered a ransomware attack, impacting multiple city services and departments. Essential services like Police and Fire Rescue continue to operate, and certain payments have been shifted to cash-only transactions. No ransomware group has yes claimed responsibility for the attack.

- A new UK-based health insurance firm Harvard Pilgrim Health Care has disclosed a ransomware attack that has compromised the data of nearly 2.9M individuals in April 2023, 12% higher than initially reported. The exposed data may contain personal data and protected health information of current and former subscribers and dependents, as well as current contracted providers.

- American retailer Hot Topic has been a victim of credential stuffing attacks that exposed clients' personal data and partial payment data. The threat actors targeted the company's website and mobile application in automated attacks using login information obtained from an unknown source.

VULNERABILITIES AND PATCHES

- Researchers have discovered an active attack campaign exploiting a vulnerability in Ray, an open-source AI framework, impacting various sectors such as education and biopharma. Despite being disclosed, one critical vulnerability (CVE-2023-48022) remains unpatched. The vulnerability, termed ShadowRay, allows attackers to take over victims' computing power and leak sensitive data.

  Check Point IPS provides protection against this threat *(Anyscale Ray Remote Code Execution (CVE-2023-48022))*

- Google has published a summary of zero-day vulnerability exploits in the wild for the year of 2023, revealing a more-than 50% increase compared to previous year. Among their finding, exploiting zero-day flaws in third-party components has been observed as a key attack method, affecting multiple products.

- Researchers have revealed a novel exploitation of a double-free vulnerability (CVE-2024-1086) in Linux kernel's nf_tables, impacting versions between v5.14 and v6.6.14. Utilizing Dirty Pagedirectory among other techniques, the exploit achieves a universal root shell without recompilation across different kernels. Additionally, researchers have discovered a use-after-free vulnerability (CVE-2024-0582) Linux kernel's io_uring interface, which allows attackers to potentially gain root privileges through a data-only exploit, modifying certain data without altering code execution flow.

- Researchers have found a high-severity CSRF vulnerability (CVE-2024-1538) in the popular WordPress File Manager plugin, impacting versions up to 7.2.4. Successful exploitation could allow attackers to inject JavaScript, potentially leading to Remote Code Execution.

THREAT INTELLIGENCE REPORTS

- Check Point Research reports on a wave of scam attacks in which attackers use various scam methods, including malicious QR codes and phishing emails to gain US taxpayers' credentials to steal IRS refunds. Also, a flourishing market for sensitive tax return documents was identified in the Darkweb.

- Check Point researchers detected a typosquatting campaign that comprised over 500 malicious packages, deployed in two distinct waves on PyPI (Python Package Index). Installation of these packages exposed users to potential theft of their personally identifiable information (PII) and the installation of malware on their systems.

  Check Point CloudGuard Code Security provides protection against this threat.

- Researchers have uncovered DinodasRAT, a multi-platform backdoor malware targeting Linux systems, particularly Red Hat-based distributions and Ubuntu. The malware ensures persistence, collects system information to create unique identifiers for each infected machine, and establishes communication with a command-and-control server for data exfiltration and espionage.