Check Point Research
WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Cybersecurity and Infrastructure Security Agency (CISA) has taken offline two systems following a breach that occurred as a result of the recent vulnerabilities exploitation in Ivanti products. The affected systems potentially include the Infrastructure Protection Gateway and the Chemical Security Assessment Tool, holding sensitive US infrastructure and chemical security data.

  Check Point IPS blade provides protection against this threat *((Ivanti Authentication Bypass (CVE-2023-46805), Ivanti Command Injection (CVE-2024-21887), Ivanti Server-Side Request Forgery (CVE-2024-21893))*

- Microsoft disclosed additional implications behind the intrusion to their systems by Russia affiliated threat actor Midnight Blizzard (aka Nobelium) that was reported in January. Reportedly, Midnight Blizzard is using information exfiltrated from company's corporate email systems to gain, or attempt to gain, unauthorized access to some of Microsoft source code repositories and internal systems.

- Play ransomware group has claimed responsibility for an attack on the IT vendor Xplain, leaking 65,000 Swiss government documents, including classified data. Swiss authorities discovered that 5% of the 1.3 million leaked files are linked to federal agencies, mainly affecting the Federal Department of Justice and Police, and to a lesser extent the Federal Department of Defence, Civil Protection, and Sport. The leak contained personal info, technical details, and passwords.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat *(Ransomware.Win.Play.B, Ransomware.Wins.PLAY.A)*

- Stormous ransomware gang has attacked Duvel Moortgat Brewery, halting production by shutting down servers in Belgium and the U.S. after stealing 88 gigabytes of data. The company was given a March 25 deadline to pay the ransom.

  Check Point Threat Emulation provides protection against this threat.

- Financial services firm Paysign is investigating a reported data breach after a threat actor named "emo" claimed to sell a database on dark web forum. The alleged leaked database contains 1,242,575 records, including customers' full names, addresses, dates of birth, phone numbers, and account balances.

- The Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) was hit by a cyber incident, leading to the precautionary shutdown of its corporate systems. Although the attack did not compromise FINTRAC's intelligence or classified systems, it prompted collaboration with federal partners to restore operations and strengthen defenses.

VULNERABILITIES AND PATCHES

- QNAP has issued an alert regarding critical vulnerabilities in its NAS software, with a notable authentication bypass flaw (CVE-2024-21899) that permits unauthorized remote access. While two other vulnerabilities (CVE-2024-21900 and CVE-2024-21901) require authenticated access, posing less risk, CVE-2024-21899's low complexity raises significant security concerns. Affected products include QTS, QuTS hero, and others, with updates available to mitigate these risks.

- JetBrains has released an advisory for two critical vulnerabilities (CVE-2024-27198 and CVE-2024-27199) in all on-premises versions of TeamCity. These flaws could allow unauthenticated attackers with HTTP(S) access to bypass authentication checks and gain administrative control of a TeamCity server.

  Check Point IPS blade provides protection against this threat *(JetBrains TeamCity Authentication Bypass (CVE-2024-27198))*

- VMware has released security updates to fix critical vulnerabilities (CVE-2024-22252 - CVE-2024-22255) in VMware ESXi, Workstation, and Fusion, which allow for code execution and sandbox escape. These vulnerabilities, ranging in severity with CVSS scores up to 9.3, impact multiple products and versions.

- Cisco has shared patches to address a high-severity security flaw (CVE-2024-20337) impacting its Secure Client software. Successful exploitation could allow an attacker to execute arbitrary script code in the browser or access sensitive, browser-based information, including a valid SAML token. Attackers could use the token to establish a remote access VPN session with the privileges of the affected user.

THREAT INTELLIGENCE REPORTS

- Check Point Research has been tracking the financially motivated threat actor Magnet Goblin exploiting 1-day vulnerabilities in servers like Ivanti Connect Secure VPN, Magento, and Qlik Sense. The actor deploys a new Linux version of NerbianRAT and WARPWIRE JavaScript credential stealer, while proving quick adoption of exploits.

  Check Point IPS and Harmony Endpoint provide protection against this threat *(RAT_Linux_Nerbian_*)*

- Researchers have analyzed an attack case by the APT group Earth Kapre, where threat actors used Impacket and the Windows Program Compatibility Assistant service in later stages of the attack process. The group has been actively conducting phishing campaigns targeting organizations in Russia, Germany, Ukraine, the United Kingdom, Slovenia, Canada, Australia, and the US

- Researchers have uncovered a new malware campaign targeting the Popup Builder WordPress plugin, exploiting a stored XSS vulnerability. Over 3,300 websites have been infected, with malicious code found in the plugin's Custom JS or CSS sections, leading to unauthorized redirections and malware injections.