Check Point Research
WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Japanese tech company Fujitsu discovered malware on its work computers, risking exposure of customer data. The company, a leading IT firm, detected unauthorized access that potentially allowed personal and customer information to be illicitly extracted. Immediate actions included isolating affected computers and enhancing monitoring to prevent further breaches, with ongoing investigations into the malware's entry point and the extent of data leakage.

- Researches have unveiled a cyber espionage campaign by APT29, a group associated with Russian intelligence services, targeting German political entities through the deployment of Wineloader malware. This operation aims at data exfiltration and espionage, highlighting APT29's persistent threat to global political organizations.

- An alleged AT&T database, containing more than 70M records, including personal data like Social Security Numbers and DOBs, was leaked on a cyber-crime forum. The threat actor claims the breach originally occurred in 2021, and researchers confirmed its validity. The American telecom giant, however, claimed the data was not taken from its own network.

- Popular video game Apex Legends was forced to call off its global championship tournament, after competitors were hacked by unknown attackers while streaming their gameplay. According to unconfirmed reports, the attackers used an RCE vulnerability that exists within the game and can allow them to install malware onto any player's system.

- Russian state affiliated hackers, identified as subgroup UAC-0165 of the Sandworm operation run by Russia's GRU, likely orchestrated recent cyberattacks on four small Ukrainian ISPs. The group, known as Solntsepek, disrupted operations, and claimed responsibility, hinting at the attacks' focus on entities providing services to Ukrainian government agencies and armed forces.

- Nations Direct Mortgage, a Nevada-based lender, reported a significant data breach impacting more than 83,000 customers, where unauthorized access led to the potential exfiltration of sensitive data, including Social Security numbers.

- Researchers have uncovered Chinese APT group Earth Krahang’s latest activity, targeting government entities worldwide. This cyber espionage campaign, active since early 2022, included targeting of 70 organizations in 23 countries. Utilizing vulnerabilities in internet-facing servers and spear-phishing tactics, the group has deployed custom backdoors, XDealer and Reshell, for intelligence gathering.

VULNERABILITIES AND PATCHES

- Mozilla released patches for two critical vulnerabilities in the Firefox browser. The vulnerabilities, CVE-2024-29943 and CVE-2024-29944, allowed sandbox escape and remote code execution were demonstrated on hacking convention Pwn2Own earlier this week.
- Trend Micro researchers disclosed a critical file read vulnerability, CVE-2024-23897, in Jenkins' args4j library, affecting versions up to 2.441 and LTS 2.426.2. This flaw, enabling unauthenticated file reads, could lead to unauthorized access and potential remote code execution. Over 45,000 Jenkins instances remain unpatched, highlighting the urgency for updates.

  Check Point IPS blade provides protection against this threat *(Jenkins Information Disclosure (CVE-2024-23897))*
- Rhino Security Labs researchers discovered an unauthenticated command injection vulnerability in the administrator web interface of the Progress Kemp LoadMaster load balancer. Assigned CVE-2024-1212, this critical flaw allows full compromise of the LoadMaster through the administrator web user interface. The issue was identified in version 7.2.59.0.22007 and patched in version 7.2.59.2.22338.
- Ivanti released a patch for critical remote code execution vulnerability affecting its Standalone Sentry product. The vulnerability, tracked as CVE-2023-41724, allows an unauthenticated adjacent-network attacker to execute arbitrary commands on the appliance's operating system.

THREAT INTELLIGENCE REPORTS

- Check Point Research reports on a wave of attacks abusing prominent cryptocurrency Ethereum's CREATE2 function. The function allows attackers to cause users to approve undeployed smart contracts, which the attackers can later deploy to drain wallets.
- Nemesis Market, a prominent darknet marketplace known for trading narcotics, weapons, and stolen data, was seized in Operation Dark Hunt. This collaborative law enforcement effort used advanced digital forensics techniques to identify the market's operators and subsequent take-down.
- Researchers published a report delving into the negotiation tactics of Akira and Black Basta ransomware groups, highlighting their extortion methods, ransom demands based on victim revenue percentages, and the services offered upon payment. Both groups, employing double extortion by encrypting and exfiltrating data, demonstrate willingness to negotiate ransom amounts and follow through on decryption and data removal services.
- Researchers have uncovered the techniques of KamiKakaBot, a malware deployed by the DarkPink APT group targeting the Asia-Pacific region. The malware utilizes ISO files for phishing, sideloads malicious DLLs via Microsoft Office vulnerabilities, and establishes persistence through registry modifications.