December 30, 2024 – January 5, 2025

CHECK POINT RESEARCH

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Check Point elaborated on the US Treasury Department cyber-attack that compromised employee workstations and classified documents. The breach, attributed to a China state-sponsored threat actor, involved unauthorized remote access using a security key from third-party provider BeyondTrust. The attackers exploited two vulnerabilities in BeyondTrust’s remote support software: CVE-2024-12356, critical API access flaw, and CVE-2024-12686, token management vulnerability.
- Japan’s largest mobile carrier, NTT Docomo, has been a victim of a distributed denial-of-service (DDoS) attack that disrupted multiple of its services for 12 hours, including news, video streaming, mobile payments, and webmail. No threat actor has claimed responsibility yet.
- UK photography company DEphoto has suffered a security breach. The threat actor behind the attack claims to have exfiltrated the personal information of more than 500,000 of the company’s customers, including over 15,000 records which contain full unredacted payment card information. The company has begun notifying its customers of their data being leaked.
- Campaign targeting Chrome extension developers, led to the compromise of at least thirty-five browser extensions. The threat actors aim to gain developer credentials to the extensions to replace them with malicious versions. The compromised extensions were collectively used by more than 2.5 million users.
- Space Bears ransomware gang took credit for an alleged cyber-attack on French tech giant Atos, which secures communications for France’s military and intelligence services. The gang claimed to have compromised the company’s internal database and threatened to leak proprietary data. Atos has dismissed these claims as unfounded, stating that no infrastructure managed by the company was breached and no sensitive data was exposed.
- Websites of multiple French cities, including Marseille and Nantes, have been victims of DDoS attacks that resulted in widespread website outages and service disruptions. The attacks affected 23 municipal sites, making them temporarily inaccessible to millions of users. The attacks were claimed by the pro-Russian hacktivist group NoName057(16).
- Iran-linked hacktivist group Handala has claimed responsibility for a supply chain attack targeting Israeli companies via ReutOne, a CRM solutions provider and Microsoft 365 Dynamics reseller. The group alleges access to databases containing personal information from multiple companies in Israel, France, and Ukraine. Researchers revealed the attack involved malicious software updates that collected system data and enabled unauthorized access and data exfiltration.

VULNERABILITIES AND PATCHES

- A proof-of-concept exploit named "LDAPNightmare" has been published, targeting an out-of-bounds read vulnerability CVE-2024-49113 in Windows Lightweight Directory Access Protocol (LDAP). This exploit can crash the Local Security Authority Subsystem Service (LSASS) on unpatched Windows Servers, leading to a system reboot. The same exploit chain can be modified to achieve remote code execution, corresponding to CVE-2024-49112, which has a CVSS score of 9.8.
- DoubleClickjacking, a newly identified vulnerability, evades existing clickjacking protections on major websites by leveraging a double-click sequence to manipulate user interactions. This vulnerability allows attackers to perform UI manipulation and account takeovers by stealthily redirecting users during the double-click process, potentially affecting virtually all major web applications.
- Progress Software Corporation has issued an advisory, addressing three vulnerabilities in its WhatsUp Gold network monitoring platform. Two of the vulnerabilities, CVE-2024-12106 and CVE-2024-12108, are considered critical. The first allows unauthenticated attackers to configure LDAP settings, while the second allows complete remote takeover of the WhatsUp Gold server.

THREAT INTELLIGENCE REPORTS

- PLAYFULGHOST, a new backdoor that shares functionality with Gh0st RAT, has been distributed via phishing emails and SEO poisoning, resulting in the compromise of users' systems through trojanized VPN applications like LetsVPN. The malware enables attackers to collect sensitive data, including keystrokes, screenshots, audio recordings, and system information, potentially leading to unauthorized access and data breaches.

  Check Point Threat Emulation and Harmony Endpoint provide protection against this threat (RAT.Win.Gh0st; Trojan.Wins.Gh0st.ta.)*

- Researchers have uncovered a malicious npm campaign targeting the Nomic Foundation and Hardhat platforms, two integral components of the Ethereum development ecosystem. The campaign involves 20 malicious packages which impersonate legitimate plugins to inject data-stealing code, exfiltrating sensitive information such as private keys and mnemonics, and leverage Ethereum smart contracts to dynamically retrieve command-and-control server addresses.
- Researchers identified a new Android malware named FireScam, disguised as a premium version of the Telegram app. Distributed via phishing websites mimicking Russia's RuStore app market, FireScam uses a dropper module to install the malicious 'Telegram Premium.apk'. It then requests extensive permissions to monitor notifications, access clipboard data and intercept SMS services.
- Researchers discovered NonEuclid RAT, a sophisticated C# malware that enables unauthorized remote control of victim computers. It uses advanced evasion techniques like antivirus bypass, privilege escalation, and dynamic DLL loading. NonEuclid RAT also includes ransomware encryption targeting critical files and is promoted in underground forums and social media.