Check Point Research
WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- UnitedHealth Group confirmed its subsidiary was attacked by the ALPHV ransomware gang. 6 terabytes of data were stolen in the attack, and Change Healthcare, a crucial intermediary between pharmacies and insurance companies, was forced to disconnect its systems on February 21. The disruption impacted U.S. military clinics and hospitals worldwide, necessitating manual prescription processes.

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

- AI-powered photo and video editing service, Cutout.Pro, experienced a data breach that exposed personal data of 20 million users. The breach, disclosed by a cybercriminal on a hacking forum, included email addresses, hashed passwords, IP addresses, and more. Despite the breach, Cutout.Pro has not issued an official statement, and the leaked data has been verified by independent sources.

- Rhysida ransomware gang targeted Lurie Children's Hospital in Chicago, claiming to have stolen 600 GB of sensitive data and demanding a 60 BTC ($3.7 million) ransom. The attack disrupted hospital operations, forcing it offline and affecting patient care. Despite efforts to restore systems, significant disruptions persist, impacting service delivery and data accessibility.

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

- U.S. law firm Houser LLP reported a data breach that exposed personal information of over 325,000 individuals. The breach, discovered in May 2023, included encryption of certain files. The compromised data includes Social Security numbers, financial account information, and medical data.

- Walmart's Spark, a crowdsourcing delivery service, experienced a cyberattack which exposed sensitive data of its drivers. The breach, likely from credential stuffing or phishing, affected over 200 Spark Driver accounts. The attack occurred between early December 2023 and early February 2024, compromising Social Security numbers, driver's license numbers, and contact details. Walmart has notified affected individuals, reset passwords, and added a security mechanism for accessing sensitive data.

- Researchers identified a sophisticated cyber espionage campaign named SPIKEDWINE. The operation targets European diplomats through a malicious PDF disguised as an invitation from the Ambassador of India. This campaign employs a previously undocumented backdoor, WINELOADER, utilizes advanced Tactics, Techniques, and Procedures (TTPs), and exploits geopolitical relations. SPIKEDWINE is believed to be orchestrated by a nation-state actor.

VULNERABILITIES AND PATCHES

- CISA and its international partners have issued a warning that cyber threat actors are exploiting previously identified vulnerabilities in Ivanti Connect Secure and Ivanti Policy Secure gateways. These vulnerabilities, specifically CVE-2023-46805, CVE-2024-21887, and CVE-2024-21893, impact all supported versions and could allow threat actors to bypass authentication, craft malicious requests, and execute arbitrary commands with elevated privileges.

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

- Researchers uncovered exploitation of significant vulnerabilities in ConnectWise ScreenConnect software, tracked as CVE-2024-1708 and CVE-2024-1709, by threat actor groups including Black Basta and Bl00dy Ransomware gangs. These vulnerabilities allow unauthorized access and control over affected systems, prompting urgent security updates.

  Check Point IPS blade provides protection against these threats *(ConnectWise ScreenConnect Remote Code Execution (CVE-2024-1708), ConnectWise ScreenConnect Authentication Bypass (CVE-2024-1709))*

- 3 million Anycubic 3D printers were hacked by an unknown actor. The printers produced a warning note, informing customers of an unspecified critical remote access vulnerability in Anycubic's MQTT service, which allegedly gives an attacker the ability to "connect and control" to customer 3D printers.

THREAT INTELLIGENCE REPORTS

- Check Point Research reports on an increase in attacks on Web Application Programming Interfaces (APIs), affecting 1 in 4.6 organizations worldwide every week, compared to January 2023. This escalation underscores the expanding vulnerabilities within Web APIs, which facilitate essential communication between software applications but also introduce a broad attack surface susceptible to authentication bypasses, unauthorized data access, and other malicious activities.

  Check Point IPS blade provides protection against this threat.

- Researchers have identified ongoing espionage activities by the suspected Iranian threat actor UNC1549, targeting aerospace, aviation, and defense industries in the Middle East. The campaign uses sophisticated social engineering and malware, including MINIBIKE and MINIBUS backdoors, leveraging Microsoft Azure cloud infrastructure for command and control.

- Researchers observe a surge in SocGholish infections targeting WordPress websites through compromised administrator accounts. SocGholish infections are known for impersonating legitimate browser updates to distribute Remote Access Trojans. The malware, part of a longstanding campaign, has seen a notable increase in activity, with infections doubling from the previous year.