January 29 – February 4, 2024

Check Point Research WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- AnyDesk Software GmbH , the company behind the popular remote desktop application, has confirmed a cybersecurity incident in which the attackers gained access to company's production systems. Reportedly, source code and private code signing keys were stolen during the attack. As part of the response, AnyDesk have revoked security-related certificates and remediated or replaced systems as necessary. Out of caution, AnyDesk is also revoking all passwords to their web portal and suggests changing the password if it's used on other sites.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat (Trojan.Win.Anydesk.* , Trojan.Wins.AnyDeskCert.*)

- The French energy giant Schneider Electric has confirmed a ransomware attack conducted by Cactus ransomware gang. The attack disabled some of the company's systems and possibly caused a theft of large amount of organizational information. The ransomware group has not yet published Schneider on its leak site, which possibly indicates ongoing negotiations between the two.

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

- ALPHV (BlackCat) ransomware group has claimed responsibility for an attack on the US IT service firm Techinca, which supplies services to federal security agencies. ALPHV claims to have gained access to documents belonging to the Defense Counterintelligence and Security Agency, which conducts background investigations. The group has leaked documents that allegedly include names, social security numbers and clearance levels of American military and FBI members.

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

- Medusa ransomware group has stolen approximately 400GB of data belonging to 9 companies in an attack against Italian cloud service provider CloudFire. The attack resulted in the exposure of sensitive information, including personal identification documents, notarial deeds, sales contracts and more.

- Fulton County in Georgia has been a victim of a cyber-attack that resulted in a significant IT outage, affecting county office phone systems and online transactions. The incident is under active investigation by law enforcement, including the FBI. While the attacker remains unidentified, the attack has disrupted essential services like court and tax systems, with no specific timeframe for system restoration.

VULNERABILITIES AND PATCHES

- Ivanti has disclosed two vulnerabilities affecting its Connect Secure VPN product. A high-severity flaw, tracked as CVE-2024-21893, allows unauthenticated access to restricted resources, and has been reportedly exploited in the wild. The other flaw, tracked as CVE-2024-21888, is a high-severity privilege escalation flaw that could allow a user to elevate privileges to those of an administrator. CISA directed agencies running affected products—Ivanti Connect Secure or Ivanti Policy Secure solutions—to immediately disconnect all instances from the networks, until a required mitigation is done.

  Check Point Harmony IPS provides protection against this threat (Ivanti Server-Side Request Forgery (CVE-2024-21893))

- Researchers have identified a high-severity vulnerability in Google Chrome's V8 JavaScript engine, tracked as CVE-2024-0517. The flaw could allow a remote attacker to potentially exploit heap corruption via a crafted HTML page.

  Check Point Harmony IPS provides protection against this threat (Google Chrome Out of Bounds Write (CVE-2024-0517))

- GitLab has released fixes addressing a security flaw in its Community Edition (CE) and Enterprise Edition (EE), tracked as CVE-2024-0402. With a CVSS score of 9.9, this critical vulnerability allows an authenticated user to write files to arbitrary locations on the GitLab server while creating a workspace.

THREAT INTELLIGENCE REPORTS

- Check Point Research found that cybercriminals are increasingly using generative AI for sophisticated cybercrimes, including social media impersonation, spam campaigns, and KYC verification services. The research shows the rise of AI-driven platforms for creating and managing fake social media accounts, offering services to automate content generation and account activity for illicit purposes.

- The US Department of Justice has disrupted the KB botnet, which is known to be used by China-affiliated APT Volt Typhoon. The botnet was used to conceal affiliation to China in attacks targeting critical infrastructure organizations in the US. Volt Typhoon used Cisco and NetGear end-of-life SOHO (small office / home office) vulnerable devices for purpose of gaining initial access. CISA and the FBI released guidance for vendors regarding securing SOHO router devices.

  Check Point Threat Emulation provides protection against this threat (APT.Wins.VoltTyphoon; InfoStealer.Wins.VoltTyphoon)

- Recent reports show that the Russia affiliated APT28 (AKA Pawn Storm and Forest Blizzard) continues using its traditional tactics, combined with sophisticated TTPs. Among those, also NTLMv2 hash relay attacks and stealthy infrastructures.