TOP ATTACKS AND BREACHES

- The ransomware-as-a-service group Medusa has breached Water for People nonprofit organization, which aims to improve access to clean water in different countries including Guatemala, Honduras, Mozambique and India. The cybercriminals are asking for a $300K extortion fee to not leak the stolen data. The organization says its financial systems and business operations have not been impacted.

  Check Point Threat Emulation provides protection against this threat (Trojan.Wins.Imphash.ta.CV)

- The Paraguayan military has published a warning following an attack against Paraguayan top internet provider, Tigo. The ISP suffered a ransomware attack in the beginning of January which also affected over 300 organizations hosted at Tigo Business. Black Hunt group took the responsibility for the attack.

- Rhysida ransomware gang claimed responsibility for a Christmas-season attack on the Lutheran World Federation, a member of the World Council of Churches (a global Christian inter-church organization). The breach affected 77 million Lutherans globally, while the Rhysida gang has set a $280K ransom for the data, threatening to release it publicly after seven days.

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

- The U.S. Securities and Exchange Commission's (SEC) official X (formerly Twitter) account was hijacked by cryptocurrency scammers. A fake X message posted, falsely claiming regulatory approval for multiple bitcoin ETFs, briefly spiked Bitcoin prices, influencing investor confidence and regulatory scrutiny in the cryptocurrency space.

- Lush, the privately-owned British cosmetics retailer with stores in North America, has confirmed a cyber-attack and is working to limit its the impact on company's operations. The nature of the attack is unclear, and no threat actor has claimed responsibility for the attack yet.

- The United States largest nonbank mortgage lender LoneDepot is handling a ransomware incident. Customers of the firm have complained about not being able to access the company's payment portal, as the firm's spokesperson acknowledged that it had taken its systems offline to address the attack.

- Recent findings, revealed in documents filed with regulators in Maine this week, highlight that an April ransomware attack on a U.S. Navy shipbuilder, Fincantieri Marine Group, had exposed the personal information of nearly 17,000 individuals. This includes names and Social Security Numbers.

VULNERABILITIES AND PATCHES

- Researchers revealed active exploitation of two zero-day vulnerabilities (CVE-2023-46805 and CVE-2024-21887) in Ivanti Connect Secure & Ivanti Policy Secure gateways. These vulnerabilities, allowing remote authentication bypass and code execution, have been used since at least December by threat group UTA0178 associated with China. Despite a published patch, security experts caution that it doesn't fully mitigate ongoing compromises initiated by the attackers.
- Microsoft's January 2024 Patch Tuesday included fixes for 49 vulnerabilities, out of which two (CVE-2024-20674 and CVE-2024-20700) are rated critical and high in severity. The patch release included additional four high severity Google Chrome vulnerabilities that could allow remote attackers to potentially exploit heap corruption via a crafted HTML page.
- SAP shared ten new security alerts in their Security Patch Day, including four critical escalation of privileges vulnerabilities. These are SAP BTP Security Services Integration Library vulnerabilities that can allow escalation of privileges.
- GitLab has released fixes for a critical-severity vulnerability (CVE-2023-7028) in several versions of its GitLab Community Edition (CE) and Enterprise Edition (EE). If successfully exploited, the flaw could allow attackers to take control of accounts without user interaction.

THREAT INTELLIGENCE REPORTS

- Check Point's latest Global Threat Index for December 2023's Most Wanted Malware highlighted the resurgence of the Qbot malware in targeted phishing attacks on the hospitality sector, just four months after its infrastructure was dismantled in Operation Duck Hunt. Meanwhile, JavaScript downloader FakeUpdates jumped into first place and Education remained the most impacted industry worldwide.
- Check Point Research has released its Brand Phishing Report for Q4 2023, revealing the brands that were frequently imitated by cybercriminals in their attempts to steal individuals' personal information or payment credentials. During Q4, Microsoft has topped Checkpoint's list by a large margin (33%), followed by Amazon (9%), Google (8%) and Apple (4%).
- Check Point Research provides an introduction to .NET managed hooking using the Harmony library. The research covers the most common examples of its implementation and provides practical examples on this matter.
- Cloudflare's Q4 2023 DDoS Threat Report reveals a sharp 117% YoY increase in network-layer DDoS attacks. Noteworthy spikes include a 3,370% surge in attacks on Taiwan, potentially linked to the general election and China tensions.