CHECK POINT RESEARCH

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Romania's Constitutional Court annulled the first round of its presidential election after declassified intelligence revealed Russian interference favoring right wing candidate Călin Georgescu. The interference involved a sophisticated social media campaign on TikTok, with $381,000 spent to promote Georgescu without proper disclosure, and cyberattacks targeting electoral infrastructure, leading to vote recounts. The annulment has postponed the runoff election.

- Brain Cipher ransomware group, which payloads are based on LockBit 3.0, claimed responsibility for a breach of Deloitte UK's systems, alleging the theft of 1TB of compressed data, including sensitive information. Deloitte has denied the claims, asserting that the attack likely involved a single client's system external to Deloitte's network.

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

- Refinadora Costarricense de Petróleo (RECOPE), Costa Rica's state-owned entity overseeing the fuel supply chain, suffered a ransomware attack detected in November. This forced the company to switch to manual operations, disrupting digital payment systems and complicating fuel distribution. Despite these challenges, RECOPE assured the public of sufficient fuel reserves.

- ENGlobal Corporation, an energy industry contractor for the US government, reported a ransomware attack discovered in November, which led to the encryption of certain data files and limited access to its IT systems. Currently, no ransomware group has claimed responsibility for the attack, and the potential impact on financial performance is under assessment.

- Conferencing division of the telecommunication giant BT Group has experienced an attempted ransomware attack. It was claimed by the Black Basta group that they have stolen approximately 500 GB of data, including financial records, non-disclosure agreements, and personal documents.

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

- Ukrainian intelligence agency HUR confirmed executing a DDoS against Russia's Gazprombank, one of Russia's largest banks. This led to users experiencing difficulties accessing services, an interference aimed to disrupt financial operations tied to Russia's war efforts in Ukraine.

- Stoli Group USA has filed for Chapter 11 bankruptcy after an August 2024 ransomware attack severely disrupted its IT infrastructure, forcing manual operations and hindering financial reporting. The company faces approximately $84 million in debt, with systems expected to be fully restored no earlier than the first quarter of 2025.

VULNERABILITIES AND PATCHES

- A newly discovered zero-day vulnerability in Windows allows attackers to capture NTLM credentials by having the user view a malicious file in Windows Explorer. This flaw affects all Windows versions from Windows 7 and Server 2008 R2 up to the latest Windows 11 24H2 and Server 2022. While Microsoft has yet to release an official fix, the 0patch platform has shared an unofficial micropatch.

- A critical remote code execution vulnerability (CVE-2024-8785) in Progress WhatsUp Gold versions 2023.1.0 and earlier, enables unauthenticated attackers to modify Windows registry keys, potentially leading to arbitrary code execution. With a proof-of-concept (PoC) exploit now published, administrators are strongly urged to update to version 24.0.1 to mitigate this risk.

- Veeam has released security updates to fix two vulnerabilities in its Service Provider Console (VSPC), including a critical remote code execution flaw (CVE-2024-42448) with a severity score of 9.9 out of 10. This vulnerability allows attackers to execute arbitrary code on unpatched servers via the VSPC management agent. Another high-severity flaw (CVE-2024-42449) enables attackers to steal NTLM hashes and delete files on the VSPC server.

THREAT INTELLIGENCE REPORTS

- Check Point Research analyzed the design and control flow of Akira ransomware's latest variant, written in Rust, that has been primarily targeting ESXi bare metal hypervisor servers in early 2024. The report analyses the unique features of this version of the ransomware, showing how Rust idioms, boilerplate code, and compiler strategies have been used to create complex assembly.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat *(Ransomware_Linux_Akira_C/D, Ransomware.Wins.Akira.G/H)*

- The FBI and CISA have published guidance to assist telecommunications infrastructures defend against the detected ongoing access of the China affiliated Salt Typhoon to U.S. systems. The attacks have enabled the Chinese state affiliated group to exfiltrate extensive metadata and the interception of call audio and text messages, particularly targeting individuals linked to the U.S. government.

- Researchers have uncovered a cyber intrusion targeting a U.S. organization in China, attributed to a China-based threat actor. The attackers used DLL-sideloading with legitimate applications and tools like Impacket, FileZilla, and PowerShell to exfiltrate data and emails. Multiple computers were compromised over the four-month campaign.

- Researchers report on Russian nation-state actor known as Secret Blizzard (Turla) leveraging the infrastructure of six other threat actors, both state-sponsored and cybercriminals, for facilitating their espionage operations. The actor has particularly targeted the infrastructure used by other threat actors to deploy backdoors and gather intelligence on targets, notably in South Asia.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat *(APT.Win.Turla.*, APT.Wins.Turla.*, Backdoor.WIN32.Turla.*, APT.Wins.Turla.ta.*, Trojan.Win.Turla.*)*