TOP ATTACKS AND BREACHES

- Germany has revealed a sophisticated state-sponsored hacking campaign targeting Volkswagen, orchestrated by Chinese hackers since 2010. The attackers successfully infiltrated VW's networks multiple times, extracting thousands of documents critical to automotive technology, including electric and hydrogen vehicle innovations. Evidence points to China due to the tactics and tools used, such as "China Chopper" and "Plug X," although direct governmental involvement remains unconfirmed.
- Medusa ransomware asserted responsibility for a cyberattack on Northeast Ohio Neighborhood Health, exfiltrating 51GB of sensitive data, including Protected Health Information and Personally Identifiable Information. Medusa has demanded a $250,000 ransom to prevent the sale or public release of the data, affecting patients linked to United Healthcare, Optum, and Change Healthcare.
- A campaign dubbed ArcaneDoor abusing Cisco perimeter devices to target government networks around the world has been discovered. The campaign, which security researchers attribute to China, exploits yet undiscovered initial access vulnerabilities affecting Cisco firewalls, as well as potentially other vendors' devices. Cisco has published fixes for some of the vulnerabilities used in the attack.
- 15% of Sweden's alcohol sales volume has been disrupted after a ransomware attack has hit Skanlog, a logistics company which provides distribution for the country's alcohol retail monopoly Systembolaget. According to Skanlog's statement, it has been unable to provide deliveries after its central business system has been affected the ransomware attack.
- Hacktivist group Belarusian Cyber-Partisans claimed to have accessed the Belarus KGB's network, retrieving over 8,600 internal files. This action is said to be in response to the KGB chief's accusations against them of threatening national security. The group's activities, including the previous disabling of state media and affecting Belarusian Railways, aim to oppose political repression.
- North Korean APT groups Lazarus, Kimsuky, and Andariel conducted extensive cyber espionage against 83 South Korean defense contractors from October 2022 to July 2023, successfully extracting confidential data from about ten firms. These operations included using malware and exploiting vulnerabilities to exfiltrate information, impacting South Korea's defense technological edge.
- An unidentified attacker has compromised a Czech news service to post a fake news story about an assassination attempt on Slovak President Peter Pellegrini. The false report, quickly retracted, was part of a disinformation tactic aimed at creating political tension.

VULNERABILITIES AND PATCHES

- Rapid7 researchers have uncovered an unauthenticated, critical, zero-day vulnerability (CVE-2024-4040) in CrushFTP, which allows attackers to completely compromise the server. The vulnerability enables remote execution of arbitrary code on the server without any user interaction. The flaw is currently actively exploited, with patches available.
- Google has shared a security patch for Chrome, which includes fixes for 4 vulnerabilities. Among the vulnerabilities is a critical Type Confusion vulnerability (CVE-2024-4058) in the ANGLE backend, which can allow the execution of arbitrary code on a victim's machine.
- A Proof-of-concept has been released for a critical severity vulnerability (CVE-2024-2389) affecting Flowmon products. This flaw, characterized by improper access controls, allows unauthorized remote attackers to manipulate network traffic data, potentially leading to data breaches. The vulnerability is currently unpatched.

THREAT INTELLIGENCE REPORTS

- Researchers have analyzed the Russia affiliated threat actor APT28 (aka Fancy Bear, Forest Blizzard, Sofacy, STRONTIUM) and its custom tool, GooseEgg, used to exploit CVE-2022-38028 in the Windows Print Spooler service. The research revealed that the tool allows credential theft and privileged actions within targeted systems, primarily affecting government and NGO sectors in the US, Europe, and the Middle East.
- Researchers have unveiled the activities of a Vietnamese-origin threat actor, dubbed "CoralRaider", which specializes in stealing social media and financial data across several Asian countries. Utilizing a customized variant of QuasarRAT named RotBot and XClient stealer, the actor orchestrates credential theft and financial fraud, notably through deceptive Telegram bots and sophisticated malware deployment strategies.
- Researchers have identified a new variant of the LightSpy malware, initially designed for mobile platforms, now targeting macOS devices. The variant exploits system vulnerabilities to perform espionage activities, indicating an escalation in cyber threats against macOS users. The analysis reveals sophisticated techniques including encrypted payloads and dynamic module loading.
- Researchers have detailed the technical aspects of the ToddyCat APT group's traffic tunneling and data extraction tools. Their analysis focuses on two main tools, a reverse SSH tunneling tool and the SoftEther VPN tool, used for bypassing network security measures and extracting sensitive data from targeted entities, primarily governmental organizations in Asia.