CHECK POINT RESEARCH

# WEEKLY INTELLIGENCE REPORT

## TOP ATTACKS AND BREACHES

- The United States Office of the Comptroller of the Currency (OCC), an independent bureau of the Department of the Treasury, has suffered a significant security breach. Threat actors have gained access to the bureau's email messages for a period of a year and a half. According to the agency's disclosure, the messages included "highly sensitive information relating to the financial condition of federally regulated financial institutions".

- American car racing giant NASCAR has allegedly been hit with a ransomware attack. The Medusa ransomware group claims to have breached NASCAR's network, exfiltrated sensitive material and is demanding $4M in ransom. The group has begun leaking documents allegedly stolen from the company's network.

  *Check Point Harmony Endpoint and Threat Emulation provide protection against this threat*
  *(Ransomware.Wins.MedusaLocker.ta.*; Ransomware.Wins.MedusaLocker.*; Trojan.WIN32.Medusalocker.*)*

- Morocco's Institute of Social Security, CNSS, was breached by an Algerian hacker group named 'JabaROOT'. The group claims to have stolen personal information of 2 million Moroccan citizens, which includes personal as well as financial information, such as names, addresses and bank details. The threat group has also defaced the website of Morocco's Ministry of Labor.

- Laboratory Services Cooperative, a Seattle-based nonprofit medical services provider, has disclosed that it had suffered a cyber-attack late last year. The threat actors have stolen personal and medical information of 1.6 million individuals, which includes Social Security numbers as well as diagnosis and treatment details. This information is considered particularly sensitive, as LSC provides services for Planned Parenthood patients.

- United States food manufacturer WK Kellogg Co has notified regulators that it had suffered a data breach. According to the company's statement, it has learned that threat actors had gained access to a Cleo server that held sensitive employee information late last year. The Clop ransomware group, which has added WK Kellogg Co to its victim site, had exploited zero-day vulnerabilities in Cleo servers to breach a large number of companies last year.

  *Check Point Harmony Endpoint, Threat Emulation and IPS provide protection against this threat*
  *(Ransomware.Win.Clop; Ransomware.Wins.Clop; Ransomware.Wins.Clop.ta.* ; Cleo Arbitrary File Upload (CVE-2024-50623))*

- The Czech Republic's Primer Minister's X (formerly Twitter) account was hacked and used to publish false posts. The posts involved foreign policy, including announcements of a fake attack by Russia on Czech Republic soldiers, as well as a fake Czech response to the United States' tariffs. According to the Czech Prime Minister, foreign threat actors were responsible for the breach.

## VULNERABILITIES AND PATCHES

- Microsoft has released April's Patch Tuesday, addressing a total of 134 vulnerabilities across the company's products. Among the vulnerabilities, 11 are considered Critical, and one (CVE-2025-29824) was an actively exploited zero-day vulnerability in Windows CLFS, which was used to deliver ransomware. Microsoft has also published an in-depth report regarding ransomware group Storm-2460's exploitation of the vulnerability.
- Adobe has published 12 security advisories addressing 54 vulnerabilities across the company's products. Of the vulnerabilities, 30 affected Adobe ColdFusion, 11 of which were tagged as critical, and could be exploited to gain arbitrary code execution and file read.
- Google has released April's security patch for Android. The patch addresses 62 vulnerabilities in total, including 2 zero-day vulnerabilities affecting Android devices. Among them is CVE-2024-53197, a privilege escalation flaw in devices' Linux Kernel's USB audio component. This vulnerability was allegedly recently exploited by Israeli firm Cellebrite for Serbia's law enforcement agencies.
- Meta has disclosed a vulnerability affecting WhatsApp Windows Desktop client. The vulnerability, CVE-2025-30401, involved displaying attachments according to their MIME type, but opening them based on the file's name. This allowed attackers to send malicious executables that would appear as JPEG images.

## THREAT INTELLIGENCE REPORTS

- Check Point Research has released March 2025's Most Wanted Malware report, showing the continued dominance of FakeUpdates, a downloader malware that remains the most prevalent threat worldwide. Meanwhile, education remains the most impacted industry globally, with both malware and ransomware attacks increasingly targeting this sector.
- As the tax season is now on its last days, Check Point Research highlights recent tax scams observed in the US and the UK impersonating the relevant tax authorities. The blog offers tips on how to recognize these cyber threats and how to proactively protect yourself.
- Researchers have discovered a campaign by APT group 'ToddyCat' exploiting CVE-2024-11859, a vulnerability in ESET's Command line scanner, which is a security solution. This attack vector allowed the threat actors to operate undetected within a trusted security ecosystem, as they used the Command line scanner to load malicious payloads.
- Researchers have identified a new campaign by Russia-aligned APT group Shuckworm, which tends to target Ukrainian entities with espionage payloads. This campaign targeted a foreign military mission stationed in Ukraine and used an updated variant of the GamaSteel payload to maintain persistence, exfiltrate data, and conduct surveillance.