CHECK POINT RESEARCH

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Luxury retailer Louis Vuitton has suffered a cyber-attack that resulted in the exfiltration of certain personal data of customers from the UK, South Korea, Turkey, Italy, and Sweden after unauthorized access to its systems. No payment information was compromised, but sensitive client data was exposed, reportedly due to a breach of a third-party vendor's database. The ShinyHunters extortion group is believed to be responsible for the attack.

- UK retail giant Co-op has officially disclosed by a cyber-attack that resulted in the theft of personal data belonging to all 6.5 million of its customers, following a massive breach in April that led to system shutdowns and food shortages in its stores. The attack exposed customers' contact information but did not include financial or transaction data. The Scattered Spider threat group, known for deploying DragonForce ransomware, is suspected to be behind the attack.

- NovaBev Group, a major Russian spirits producer and distributor, has been a victim of a ransomware attack that resulted in temporary disruption of critical IT infrastructure. The attack has severely affected the operations of the group and its subsidiary, WineLab, disrupting services across more than 2,000 stores. The attack involved sophisticated techniques that bypassed existing security protocols. No threat actor has claimed responsibility yet.

- Thailand's Ministry of Labor has experienced a cyber-attack that resulted in the defacement of its website and the alleged theft of 300GB of sensitive data. The impact includes the claimed encryption of 2,000 laptops and dozens of servers, as well as the potential exposure of citizen data, information on foreign visitors, and supposed classified documents. The Devman ransomware group, which has been linked to the DragonForce malware family, has claimed responsibility for the attack and is demanding a $15 million ransom.

- Singapore's critical infrastructure was hit by a cyber-attack that resulted in targeted infiltration attempts against systems delivering essential services, with a focus on sectors such as defense, technology, and telecommunications. The impact includes ongoing attacks that could undermine national security and disrupt business operations and supply chains; however, there is no information regarding any specific data leak or number of affected users. The China affiliated espionage group UNC3886 has been identified as responsible for the attack.

- Gaskar Group, a major drone supplier to Russia's military, has confirmed a cyber-attack that destroyed over 250 systems, wiping 57 terabytes of data and backups, and exposed employees' personal details. Ukrainian hacktivists BO Team, Ukrainian Cyber Alliance, and Ukraine's military intelligence claimed responsibility.

VULNERABILITIES AND PATCHES

- Following Microsoft disclosure of a critical SharePoint 0-day vulnerability dubbed **"ToolShell"** (CVE-2025-53770, a variant of the authentication-bypass bug CVE-2025-49706), Check Point Research released an advisory with key findings on the vulnerability. Check Point Research identified the first signs of the exploitation on July 7th, and dozens of compromise attempts across government, telecommunications, and software sectors in North America and Western Europe.

  Check Point IPS provides protection against this threat *(Microsoft SharePoint Server Insecure Deserialization (CVE-2025-53770), Microsoft SharePoint Server Authentication Bypass (CVE-2025-49706))*

- A patch has been released for a high-severity Chrome vulnerability, CVE-2025-6558 (CVSS 8.8), which was actively exploited in the wild and allows remote attackers to escape the browser's sandbox via insufficient input validation in the ANGLE and GPU components. This zero-day flaw affects Chrome versions prior to 138.0.7204.157 and enables arbitrary code execution in the GPU process through a specially crafted HTML page.

- VMware fixed four zero-day vulnerabilities (CVE-2025-41236 to CVE-2025-41239) in ESXi, Workstation, Fusion, and Tools exploited at Pwn2Own Berlin 2025. Three critical flaws (score 9.3) allow guest-to-host code execution, and one high-severity issue (7.1) impacts VMware Tools.

THREAT INTELLIGENCE REPORTS

- Check Point Research reported a 21% year-over-year surge in global weekly cyber-attacks per organization in Q2 2025, reaching 1,984 attacks. Education is the most targeted sector, and Europe is seeing the highest regional growth at 22%. Around 1,600 ransomware incidents were disclosed, mainly affecting business services, manufacturing, and construction. North America and Europe accounted for 53% and 25% of ransomware cases, respectively.

- Check Point Research uncovered that FileFix, a social engineering method that opens File Explorer from a malicious site and copies a hidden PowerShell command to the clipboard, is actively tested by threat actors. Pasting it into the address bar executes malware without exploiting software flaws.

  Check Point Harmony Endpoint provides protection against this threat

- Researchers found that threat actors abuse Microsoft Teams calls to impersonate IT support and deliver Matanbuchus 3.0 via Quick Assist. A PowerShell script uses DLL side-loading to deploy the malware, which supports memory execution, obfuscation and data theft.

  Check Point Threat Emulation and Harmony Endpoint provide protection against this threat *(Trojan-Downloader.Wins.Matanbuchus.ta.*; Trojan-Downloader.Win.Matanbuchus)*

- European and US authorities disrupted the operations of NoName057(16), a pro-Russian hacktivist group known for large-scale DDoS attacks against Ukraine and its allies. Operation Eastwood dismantled over 100 servers and took down the group's core infrastructure. Seven arrest warrants were issued, and over 1,000 suspected supporters were notified of potential legal consequences.