CHECK POINT RESEARCH

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Vodafone, a major international telecom, has sustained a source code leak claimed by the Lapsus$ extortion group. The company confirmed limited access to GitHub files through compromised third-party development software, while stating that customer data and core network infrastructure were not affected by the incident.
- Cryptocurrency platform THORChain, based in Switzerland, has encountered a security breach that led to the theft of about $10.7M. Trading was halted after one of six vaults was compromised, and the company said losses were limited to protocol-owned assets across several blockchains.
- West Pharmaceutical Services, a global manufacturer of drug delivery components, has experienced a ransomware attack that disrupted shipping, manufacturing, and shared service functions. The company disclosed that some systems were encrypted and data was stolen, but no ransomware group has publicly claimed responsibility.
- Foxconn, a global electronics manufacturer, has confirmed it was hit by a cyberattack on its North American operations after the Nitrogen ransomware group claimed to have stolen 8TB of data. The company confirmed disruption at some factories and said affected facilities were resuming normal production.

AI THREATS

- Researchers unveiled 'Claw Chain', four vulnerabilities in OpenClaw, an autonomous AI agent platform, that allow attackers to bypass sandbox controls, expose restricted files, leak secrets, and gain owner-level access. The flaws include the critical CVE-2026-44112, rated CVSS 9.6.
- Researchers developed an AI-assisted macOS kernel exploit that bypasses Apple's Memory Integrity Enforcement on M5 chips and grants full system control on macOS 26.4.1. Anthropic's Mythos Preview reportedly accelerated bug discovery, and the findings were privately reported to Apple before public disclosure.
- Researchers detailed how threat actors abuse Vercel's AI website generator, v0.dev, to mass-produce realistic phishing pages mimicking brands such as Microsoft and Spotify. The campaigns utilize Telegram bots to capture credentials and payment details in real time.
- Researchers found a popular Hugging Face repository hiding Windows-targeting malware after it amassed over 200,000 downloads. The package posed as OpenAI's privacy filter and installed an infostealer that harvested browser passwords, cookies, SSH keys, VPN configurations, and cryptocurrency wallets before exfiltrating the data.

VULNERABILITIES AND PATCHES

- Two Windows zero-day vulnerabilities, YellowKey and GreenPlasma, affect Windows 11 and recent Windows Server versions. YellowKey allows BitLocker bypass through Windows Recovery Environment with physical access, while GreenPlasma abuses the CTFMON framework to escalate privileges to SYSTEM. Proof-of-concept code is public, and the vulnerabilities are still unpatched.
- F5 has fixed CVE-2026-42945, a critical memory flaw in the NGINX rewrite module affecting versions 0.6.27 through 1.30.0. The 18-year-old bug enables denial of service and, under specific configurations, possible remote code execution. Public exploit code requires memory protections to be disabled.

  Check Point IPS provides protection against this threat (Nginx Heap Overflow (CVE-2026-42945))
- Cisco has addressed CVE-2026-20182, a critical authentication bypass in Catalyst SD-WAN controllers that is being actively exploited. The flaw allows remote, unauthenticated attackers to gain full administrative control of affected systems. CISA ordered federal agencies to patch vulnerable devices following Cisco's fixes.
- Apple has released security updates for CVE-2026-28819, an out-of-bounds write flaw in the Wi-Fi component affecting iOS, iPadOS, and macOS. Successful exploitation could allow an app to execute code with kernel privileges. The issue was addressed with improved bounds checking.

THREAT INTELLIGENCE REPORTS

- Check Point Research has analyzed an internal leak from The Gentlemen ransomware operation, exposing chats, infrastructure details, affiliate roles, and ransom negotiations. The report links the zeta88 account to the administrator, maps 8 affiliate TOX IDs, and details the use of Fortinet and Cisco vulnerabilities as well as NTLM relay and OWA/M365 for initial access in attacks.

  Check Point Threat Emulation and Harmony Endpoint provide protection against this threat
- Check Point Research has summarized Q1 2026 ransomware trends, recording 2,122 leak-site victims, which is the second-highest Q1 on record, and renewed consolidation. The top 10 groups were responsible for 71% of victims. Qilin led with 338 victims, The Gentlemen rose to third, and LockBit 5.0 returned with 163 victims.
- Check Point Research have quantified a World Cup 2026-driven surge in cyber activity, with weekly attacks per organization rising in Mexico, Canada, and the United States in April, across the media, hospitality, transportation and travel sectors. FIFA-themed domains reached 9,741 in April, and by early May, one in 41 were malicious.
- Researchers attributed a months-long intrusion against an Azerbaijani oil and gas company to the Chinese-linked FamousSparrow group. Attackers exploited an unpatched Microsoft Exchange server to deploy web shells, then alternated between Deed RAT and TernDoor across three waves of persistent activity.