DEFCON BY REGION

TOP THREAT ACTOR — **ShinyHunters**

Extortion crew behind the largest-ever education breach: 275M Canvas/Instructure records (the actor's claim), plus Charter Communications (4.9M) and 7-Eleven. Runs a pay-or-leak data-extortion model, leaking stolen data when victims refuse to pay.

TOP ATTACK VECTOR — **OAuth Device-Code Phishing**

Attackers harvest tokens via device-code flows and consent-grant apps (EvilTokens, Tycoon2FA), bypassing MFA. Russia-aligned actors (Storm-2372, APT29) drove device-code phishing; lures pose as HR, file-sharing and voicemail portals.

STRATEGIC EVENT OF THE MONTH

EXPLOITATION OVERTAKES CREDENTIALS AS TOP BREACH VECTOR

Verizon's 2026 DBIR confirms a structural shift: for the first time in 19 years of reporting, vulnerability exploitation (31%) overtook stolen credentials (13%) as the way breaches begin. Key signals:

- Exploitation surge - Vulnerability exploitation is now the No.1 breach vector at 31% (up from 20% the prior year), with attackers turning newly disclosed flaws into working attacks within hours to days.
- AI-built exploits - Researchers disclosed the first in-the-wild zero-day believed to be AI-developed, a 2FA bypass staged for mass exploitation and disrupted before launch; PRC and DPRK actors are already using AI for vulnerability discovery.
- Edge and infrastructure first - Cisco Catalyst SD-WAN (CVSS 10.0, CISA Emergency Directive) and cPanel (9.8, around 1.5M servers) drew mass exploitation within days of disclosure.
- Credentials still matter - Phishing (16%, now the No.2 single vector) and credential abuse (13%) still open many breaches; exploitation simply scaled faster and overtook them this year.

KEY STRATEGIC INSIGHTS

DIGITAL TRUST

Signed No Longer Means Safe

Digital signatures, the mark that tells systems software is safe, took two hits. The certificate authority DigiCert was tricked into issuing trusted certificates that were later used to sign malware, and Microsoft found its own code-signing service abused at scale to disguise malware as legitimate. A valid signature is no longer proof of trust, weakening a defense that businesses and security tools have long relied on.

OT / ICS

Iran Pivots to Gulf Energy and OT

Iranian state espionage is intensifying. APT42's SpearSpecter campaign used the TAMECAT backdoor with conference and interview lures against senior defense and government officials. In the Gulf, Cyber Av3ngers keep targeting OT and water systems, while Nimbus Manticore (Charming Kitten/APT35) and MuddyWater add espionage pressure. Energy, water and industrial operators face sustained, state-grade targeting.

SWITZERLAND

G7 Évian: Geneva Corridor in Scope

The G7 summit at Évian (15-17 June) sits on the French shore, but delegations fly into Geneva, sleep Swiss-side and cross the lake daily, putting the Geneva-Lausanne-Vaud corridor in scope: DDoS, hotel and telecom collection, deepfakes, SMS blasters and mobile spyware. The peak state-exfiltration window runs for 30 days after the summit. Full risk map on the ZENDATA blog.

NOTABLE DEVELOPMENTS

LAW ENFORCEMENT

Coordinated Takedowns Disrupt Crime Networks

Authorities pressed a wave of disruptions in May: INTERPOL's Operation Ramz drove 201 arrests across MENA, takedowns hit the Fox Tempest malware-signing crew and the First VPN criminal anonymization service, and defenders disrupted the Glassworm OpenVSX campaign. The tempo signals a more aggressive, cross-border push against extortion and access-broker networks.

STATE THREATS

DPRK Nuclear Test; China and Russia Press On

DPRK Crypto Theft; China and Russia Press OnBody replacement: DPRK cyber units (APT43, Kimsuky, UNC4899) are intensifying cryptocurrency theft and IT-worker fraud to fund the regime's weapons program. The FBI calls China's hacker-for-hire ecosystem out of control as Salt Typhoon persists in telecoms, while Russia's Turla fielded a new Kazuar P2P botnet.

AI SECURITY

AI Tooling Becomes the Target

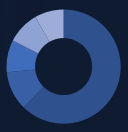
Attackers are now hunting the AI stack itself. The OpenClaw and Claw Chain campaigns and a Claude Code MCP hijack reached developer environments, while China-nexus APT31 abused Gemini through the Model Context Protocol. Exposed ChromaDB stores leaked data, and the Five Eyes issued joint guidance on securing agentic AI.

POLICY

AI and Encryption Rules Shift Worldwide

Regulators moved on AI and privacy. The White House weighed an FDA-style vetting regime for frontier AI, the EU advanced AI Act enforcement and a ban on non-consensual deepfake nudification, and Discord turned on default end-to-end encryption for voice and video calls as Apple began rolling out encrypted RCS. Governance is racing to catch up with agentic AI and pervasive data exposure.

MOST ACTIVE MALWARE



- ASYNCRAT
- CURLYFENCE
- DCRAT
- BEACON

MOST ACTIVE RANSOMWARE

- QILIN
- THE GENTLEMEN
- DRAGONFORCE
- AKIRA

CRITICAL VULNERABILITIES

CVE-2026-20182 | **CVSS 10.0** | EXPLOITED

Cisco Catalyst SD-WAN Manager

Authentication bypass to a high-privileged account in Catalyst SD-WAN Manager (vManage). Exploited by UAT-8616, with 10+ clusters joining after PoC release; CISA Emergency Directive 26-03, added to KEV 14 May. Patch immediately.

CVE-2026-41940 | **CVSS 9.8** | EXPLOITED

cPanel & WHM

Authentication bypass granting full control of the hosting panel across roughly 1.5M internet-facing servers. Mass-exploited; GTIG and Proofpoint track Southeast-Asian government, military and MSP targeting. Patch and rotate tokens.

CVE-2026-31431 | **CVSS 7.8** | EXPLOITED

Linux Kernel - All Distributions

Deterministic local root via page-cache write in the kernel crypto subsystem (the Copy Fail flaw), affecting every mainstream distro since 2017. Now under active in-the-wild exploitation and chained into multi-stage intrusions. Blacklist algif_aead and patch immediately.

TECHNIQUE OF THE MONTH

Trusted-Pipeline Compromise: OIDC Token Theft and CI Cache Poisoning

Attackers are subverting the trusted machinery of software delivery, turning CI/CD systems and developer tools into a distribution channel. Observed behaviors:

- OIDC token hijack - Short-lived OIDC tokens and CI cache entries are stolen and replayed to push malicious artifacts through pipelines that pass provenance checks.
- Cache poisoning - The Mini Shai-Hulud worm poisoned build caches to self-propagate without stored credentials, defeating SLSA Build L3 and reaching OpenAI and Mistral.
- Malicious IDE extensions - A trojanized Nx Console extension distributed via OpenVSX harvested credentials from developer machines and was used to exfiltrate roughly 3,800 of GitHub's own internal repositories.00
- Downstream blast radius - A single poisoned dependency or extension cascades to every consumer, turning one compromise into an industry-wide event.

MONTHLY RECOMMENDATIONS

Secure CI/CD & Dev Tooling

- Enforce minimumReleaseAge on npm and PyPI to delay installs of newly published packages and blunt fast-moving supply-chain attacks.
- Pin and verify dependencies; require signed commits and SLSA provenance, and treat OIDC tokens as short-lived secrets.
- Audit IDE and OpenVSX extensions for Glassworm and Nx Console indicators across all repositories.
- Monitor CI/CD logs for unauthorized GitHub Actions changes, cache tampering and token exfiltration.
- Maintain SBOMs and dependency lockfiles for all production-critical pipelines.

Identity & MFA Hardening

- Enforce phishing-resistant MFA (FIDO2 or passkeys) and block legacy device-code and OAuth consent-grant flows where possible.
- Review and restrict third-party OAuth app consents; alert on new consent grants and risky token scopes.
- Watch for trusted-SaaS abuse in lures: Evernote, Calendly, Upwork and Okendo were used to host phishing in May.
- Brief staff on FIFA World Cup themed phishing (tournament opens 11 June); we anticipate it as a top espionage and scam driver.
- Stand up heightened identity monitoring for the G7 Evian window and the 30 days that follow.

Harden OT & Industrial Control Systems

- Hunt for APT42 TAMECAT indicators; treat podcast and interview lures to energy and nuclear staff as targeted phishing.
- Segment IT/OT boundaries and enforce unidirectional gateways, especially for GCC energy, water and industrial assets.
- Monitor for Cyber Av3ngers and MuddyWater or Nimbus Manticore activity against Gulf critical infrastructure.
- Review remote-access paths into OT; require MFA and just-in-time access for engineering workstations.
- Validate offline backups and recovery for ICS and SCADA before the summer threat peak.

Vulnerability Management Sprint

- Patch Cisco Catalyst SD-WAN (CVE-2026-20182, CVSS 10.0) per CISA Emergency Directive 26-03; hunt for UAT-8616 activity.
- Patch cPanel & WHM (CVE-2026-41940, CVSS 9.8) across hosting estates and rotate API tokens.
- Patch the Linux kernel Copy Fail flaw (CVE-2026-31431) and blacklist algif_aead where patching lags.
- Prioritize internet-facing edge, VPN and management interfaces; market median time-to-patch near 43 days.
- Track CISA KEV daily and align emergency change windows to actively exploited CVEs.

NOTABLE ALLEGED DATA BREACHES

TARGET	SCALE	DETAILS
Canvas (Instructure)	275M users	Largest-ever education breach; ShinyHunters exfiltrated student and teacher records in a pay-or-leak campaign.
Charter Communications	4.9M users	Subscriber and account data stolen and listed for extortion by ShinyHunters.
GitHub (Nx Console)	3,800 repos	GitHub's internal repositories exfiltrated via a trojanized Nx Console extension; OpenAI and Grafana confirmed affected.
Lithuania State Registry	600K+ records	National registry data exposed, affecting a large share of the population.
7-Eleven	185K people	Customer and loyalty data stolen, tied to the wider ShinyHunters extortion wave.