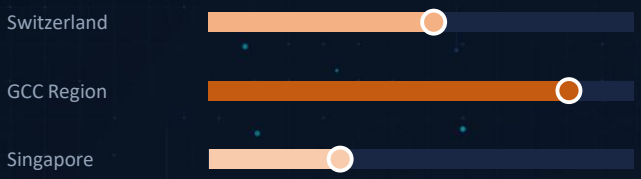
DEFCON BY REGION



TOP THREAT ACTOR — **TeamPCP**

Cloud-native cybercrime group that poisoned Trivy, Telnyx, Checkmarx KICS, and LiteLLM in a single supply chain campaign. Deployed CanisterWorm across npm, Docker, and Kubernetes. Released an Iran-targeted Kubernetes wiper.

TOP ATTACK VECTOR — **ClickFix Social Engineering**

Dominant initial access technique. New variant uses rundll32+WebDAV to evade PowerShell detection. Now targets macOS via fake Cloudflare CAPTCHAs. Apple added Terminal warning in macOS Tahoe 26.4.

STRATEGIC EVENT OF THE MONTH

IRAN-US-ISRAEL CYBER-KINETIC CONFLICT ESCALATION

Following Operation Epic Fury / Roaring Lion (Feb 28), the first openly acknowledged convergence of cyber and kinetic warfare unfolded across the Middle East. Key developments:

- Handala (Iran/MOIS) - Wiped tens of thousands of Stryker medical devices via Intune. Hacked FBI Director Patel's personal Gmail. Attacked 50+ Israeli companies with wiper malware.
- AWS Data Centers - Drone strikes physically damaged AWS facilities in UAE and Bahrain, causing extended cloud outages impacting dozens of services across the region.
- IP Camera Weaponization - Iranian actors compromised hundreds of surveillance cameras across the Middle East for real-time battlefield intelligence and targeting.
- Hacktivist Surge - 149 DDoS attacks hit 110 organizations in 16 countries within days. Keymous+ and DieNet drove the majority of retaliatory cyber activity.

KEY STRATEGIC INSIGHTS

AI THREAT

AI-Assisted Malware Crosses the Threshold

VoidLink (Linux), GhostClaw (macOS), and IBM's Slopoly confirm AI is now embedded in malware production at scale. APT36 mass-produces vibeware implants using generative AI, overwhelming defenses through volume rather than sophistication. McAfee reports AI-generated malware scaling attacks globally.

SUPPLY CHAIN

Supply Chain Attacks at Industrial Scale

TeamPCP compromised Trivy, Telnyx, Checkmarx KICS, and LiteLLM in a coordinated campaign. CanisterWorm self-propagates through npm, Docker, and Kubernetes. GlassWorm hit 400+ repos across GitHub, npm, and OpenVSX. Multiple trusted developer tools were weaponized simultaneously.

RANSOMWARE

Ransomware Business Model Mutates

Mandiant M-Trends 2026 reports ransom payment rates at historic lows. Attackers shift to pure data extortion without encryption. Cobalt Strike abandoned for native Windows tools and RMM platforms. Dwell time increased to 14 days as attackers systematically target backup infrastructure.

NOTABLE DEVELOPMENTS

ESPIONAGE

iOS Exploit Kits Proliferate Globally

DarkSword and Coruna exploit kits, previously nation-state only, now used by commercial surveillance vendors and cybercriminals. CISA added DarkSword iOS flaws to KEV. Hundreds of millions of iPhones at risk across Saudi Arabia, Turkey, Malaysia, and Ukraine.

DEV SECURITY

29M Secrets Leaked on GitHub (+34% YoY)

GitGuardian found 29M new hardcoded secrets in public repos in 2025. Google and GitGuardian confirmed 2,600+ valid TLS certificates protecting Fortune 500 and governments among leaked credentials. Security boffins found ~2,000 API keys across 10M websites.

DATA BREACH

European Commission Breached (350GB)

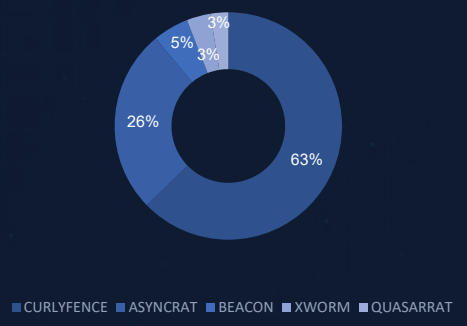
ShinyHunters claimed 350GB exfiltration from Europa.eu cloud infrastructure. The group also abandoned BreachForums, leaking its 300K-user database. Separately targeting ~400 firms via misconfigured Salesforce Experience Cloud portals.

POLICY

FCC Bans Foreign-Made SOHO Routers

The US FCC banned import of new foreign-made consumer routers citing supply chain risks. Critics call it industrial policy disguised as cybersecurity. Meanwhile, Mirai variants evolved into hundreds of botnet strains. DOJ disrupted 4 botnets hijacking 3M devices.

MOST ACTIVE MALWARE



CRITICAL VULNERABILITIES

CVE-2026-20131 CVSS 10.0 EXPLOITED

Cisco Secure FMC

Auth bypass to root. Zero-day exploited by Interlock ransomware since January. Affects enterprise firewall management across all versions.

CVE-2026-3055 CVSS 9.3 EXPLOITED

Citrix NetScaler

Memory overread with active exploitation within days of disclosure. Echoes CitrixBleed pattern. Critical for all NetScaler deployments.

CVE-2025-53521 CVSS 9.8 EXPLOITED

F5 BIG-IP APM

RCE reclassified from DoS. Webshells deployed on unpatched devices. Added to CISA KEV catalog with 3-day federal patch mandate.

TECHNIQUE OF THE MONTH

ClickFix Evolution: Cross-Platform Social Engineering at Scale

ClickFix continues to dominate initial access across multiple campaigns. Key evolutions this month:

- New variant uses rundll32.exe + WebDAV instead of PowerShell, evading most EDR detections
- macOS targeting via fake Cloudflare CAPTCHA pages delivers Infiniti Stealer compiled with Nuitka
- Apple responds with macOS Tahoe 26.4 Terminal warning feature to block paste-and-execute attacks
- SmartApeSG campaign delivers Remcos, NetSupport RAT, StealC, and Sectop RAT via single chain
- Fake Claude Code and VS Code install pages use InstallFix variant to target developers specifically

MONTHLY RECOMMENDATIONS

Immediate Actions

- Patch actively exploited vulnerabilities (Cisco FMC, Citrix NetScaler, F5 BIG-IP)
- Secure internet-facing assets (firewalls, VPNs, gateways)
- Enforce npm minimumReleaseAge to delay install of newly publishedpackages, reducing exposure to supply chain poisoning before detection
- Block ClickFix attack vectors (fake CAPTCHA, rundll32 + WebDAV patterns)
- Audit supply chain dependencies (npm/PyPI/Docker – TeamPCP campaign)
- Monitor cloud & CI/CD for abuse (Intune misuse, unauthorized changes, secret leaks)

Audit Software Supply Chain

- Enforce npm minimumReleaseAge to delay install of newly published packages, reducing exposure to supply chain poisoning before detection
- Review all npm, PyPI, Docker dependencies for TeamPCP-linked packages (Trivy, Telnyx, LiteLLM, KICS)
- Monitor CI/CD pipeline logs for unauthorized GitHub Actions modifications or secret exfiltration
- Audit OpenVSX and VS Code extensions for GlassWorm campaign indicators across 400+ repos
- Implement SBOM validation and dependency lockfiles for all production-critical pipelines

Patch Critical Network Infrastructure

- Deploy endpoint controls blocking paste-to-Terminal and Run dialog execution chains
- Update macOS fleet to Tahoe 26.4 for Apple's new Terminal paste warning protections
- Train SOC analysts on rundll32+WebDAV ClickFix variant that bypasses PowerShell monitoring
- Block fake CAPTCHA and verification domains at DNS layer; monitor Cloudflare impersonation
- Review developer workstations for fake VS Code, Claude Code, and AI tool installers

Harden OT & Industrial Control Systems

- Patch Schneider Electric EcoStruxure (CVSS 9.8) and Honeywell IQ4x controllers (CVSS 10.0, default credentials grant full access)
- Audit Siemens SIMATIC S7-1500 web servers for stored XSS vulnerability enabling session hijack from the engineering network
- Isolate Rockwell Automation ControlLogix modules from internet-facing networks per vendor emergency advisory issued this month
- Review WAGO managed switch configurations after critical 10.0 CVSS undocumented backdoor disclosure enabling full device takeover
- Segment IT/OT boundaries and enforce unidirectional gateways, especially for GCC energy sector assets exposed to Iranian hybrid warfare campaigns

Strengthen GCC & Middle East Defenses

- Audit all internet-exposed IP cameras; isolate from corporate networks or disable remote access
- Review Azure and AWS configurations for Handala-style Intune abuse and cloud wiper patterns
- Deploy BPFdoor detection rules on telecom infrastructure targeting Red Menshen indicators
- Activate DDoS protection and incident response plans given elevated hacktivist activity levels
- Monitor Kubernetes and Docker environments for CanisterWorm propagation indicators

NOTABLE ALLEGED DATA BREACHES

TARGET	SCALE	DETAILS
European Commission	350GB	Cloud infrastructure breached by ShinyHunters via AWS account compromise
Lockheed Martin (alleged)	375TB	Listed on dark web Threat Market by group claiming APT Iran affiliation
Crunchyroll	6.8M users	Customer data stolen from anime streaming platform, investigation ongoing
UH Cancer Center	1.2M people	Ransomware on epidemiology division exposed patient records since 1993
Stryker	200K devices	Iran-linked Handala wiped devices via Microsoft Intune in destructive attack