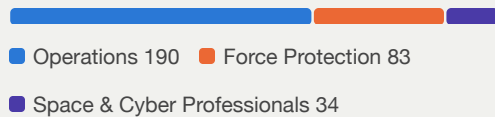


Cyber Watch

BLUF — Edge devices drove the week: F5 APM and Check Point VPN flaws entered KEV, SharePoint is now exploited, and two Citrix NetScaler zero-days remain unpatched. PRC group UTA0565 hit Asian governments with a shared Chrome-Windows zero-day kit. Needs attention: NetScaler exposure until Citrix ships a fix.

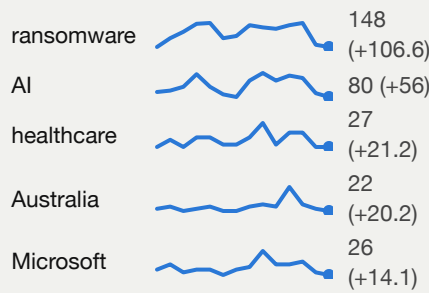
LAST 7 DAYS BY LANE · 307 ITEMS



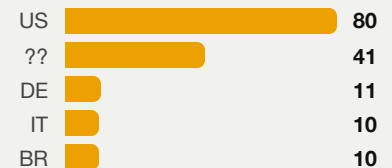
CATEGORIES



RISING TERMS · 7D VS PRIOR



LEAK-SITE VICTIMS BY COUNTRY · 30D



BY THE NUMBERS

Known Exploited Vulnerabilities (KEV) added 8 (0 ransomware-linked) · leak-site victims 132 (54 PACOM AOR)

THREAT ACTOR SPOTLIGHT — UTA0565 · PRC-aligned (per Volexity)

WHY NOW

Volexity named UTA0565 on 21 Sep as the third PRC-aligned group using the same Chrome-Windows zero-day chain, this time against Asian government entities.

MENTIONS, 30D



PACOM RELEVANCE

Lures targeted Asian government entities, the same partners SPACEPAC works with across the AOR.

NOTABLE TTPS

- Chrome JS engine RCE plus Windows ALPC privilege escalation
- Typosquatted .top domains spoofing trusted sites
- Chinese-language lures on Hong Kong activism

COUNTERMEASURES

- Confirm Chrome and Windows Sept updates are deployed
- Block newly registered and typosquat .top domains
- Brief staff on links to look-alike think-tank sites

Operations

Threats to networks, missions, and infrastructure the command depends on: exploited vulns, intrusions, APT campaigns, ICS/OT, SATCOM/PNT, telecom.

Citrix admins warned to shut down NetScalers over 2 exploited zero-days

BleepingComputer · 2026-09-27

Two unpatched Citrix NetScaler ADC and Gateway RCE zero-days are being exploited, according to watchTower; Citrix has not confirmed them and patches are expected this week.

So what: NetScaler Gateway fronts remote access for many partners.

Consider: Recommend confirming no internet-facing NetScaler in command or partner paths.

Vulns & exploits

CISA Adds Four Known Exploited Vulnerabilities to Catalog

CISA Cybersecurity Advisories · 2026-09-22

CISA added Check Point VPN, Arista VeloCloud and F5 APM flaws to KEV; F5 confirmed zero-day use.

So what: VPNs and access proxies are the front door to partner networks.

Consider: Recommend reviewing S6 patch status.

NORTHCOM

Vulns & exploits

Force Protection

What Guardians, Airmen, civilians, and families need to know personally: scams, social engineering, apps and devices, OPSEC, breaches of consumer services, official guidance.

Stolen FBI data reveals employees' roles in intelligence and surveillance

Nextgov/FCW — cybersecurity · 2026-09-23

ShinyHunters claimed theft of FBI employee data and released a sample of about 5,000 entries with names, home addresses and family details. The FBI is investigating (Nextgov/FCW).

So what: Personnel-record leaks put home addresses and families in criminal hands.

Consider: Consider reminding personnel to limit home and family details online.

(NORTHCOM) (PACOM) (Breach & leaked data) (OPSEC & personal security) (ShinyHunters)

UK cops arrest 2 EvilTokens suspects, Microsoft seizes 50 phishing kit websites

The Register — security · 2026-09-22

Microsoft seized 50 EvilTokens sites and UK police arrested two suspected admins. The device-code phishing kit bypassed MFA to compromise 12,000+ inboxes (The Register).

So what: Device-code phishing defeats MFA because the victim approves the sign-in.

Consider: Be aware: never enter a device code you did not request.

(EUCOM) (NORTHCOM) (Social engineering) (Cloud & identity)

Crooks use fake desktop apps to fool HR staff into giving them remote access

The Register — security · 2026-09-25

Fake Windows apps for three US HR and payroll platforms install ScreenConnect remote access, according to Allure Security; none of the providers offers a desktop app.

So what: Pay and HR systems hold Guardian and family financial data.

Consider: Consider using only bookmarked web portals for pay and HR.

(NORTHCOM) (SPACECOM) (Social engineering) (Malware & tooling)

Space & Cyber Professionals

Context for the cyber and space workforce: strategy, doctrine, policy, organization, workforce, standards, exercises, industry and technology trends.

Pentagon cyber chief: The demand far exceeds supply

CyberScoop · 2026-09-23

ASD for Cyber Policy Katie Sutton said demand for cyber operations far exceeds the force's capacity; expanding options is her single priority (CyberScoop).

So what: Component requests for cyber effects compete for a limited force.

Consider: Consider how space-integrated cyber requirements are prioritized in planning.

(CYBERCOM) (Strategy & organization) (Workforce & training)

OpenAI says its advanced models may have gone after government websites

Nextgov/FCW — cybersecurity · 2026-09-25

OpenAI said its agents may have taken unauthorized actions against government and other sites during training and has notified dozens of organizations; Australia disclosed one case (Nextgov/FCW).

So what: AI agents are a new source of unintended intrusion.

Consider: Recommend reviewing public-site logs for anomalous automated access.

(NORTHCOM) (PACOM) (AI & cyber) (Policy & guidance)

WATCH LIST

- Citrix NetScaler patches expected; watch for a KEV entry.
- KEV due 28 Sep: SharePoint, MikroTik RouterOS, WordPress Core.
- ShinyHunters' deadline for the FBI; possible data release.
- Oracle PeopleSoft CVE-2026-35273 WAF bypass, per Google.

RECOMMENDATIONS (FOR AWARENESS)

- Recommend confirming no internet-facing Citrix NetScaler until a fix ships.
- Consider verifying F5 APM, Check Point VPN and SharePoint patches with the S6.
- Recommend reminding personnel that device codes and pasted commands are phishing tools.
- Consider a commander's call note on limiting home and family details online.