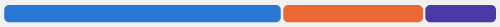
Cyber Watch

2026-W44 · 26 Oct – 01 Nov 2026
Makani Lab · Cyber Watch
Operations · Force Protection · Professionals

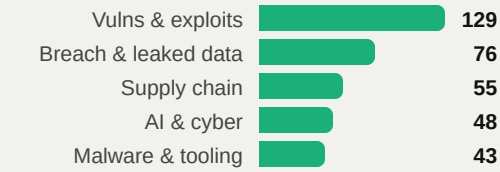
BLUF — According to Lumen, PRC actor Volt Typhoon has held access to U.S. defense, telecom and satellite networks for three years, with Hawaii among the most targeted states. Needs attention: Ivanti Connect Secure KEV due 2 Nov and SD-WAN exposure on partner networks.

LAST 7 DAYS BY LANE · 365 ITEMS

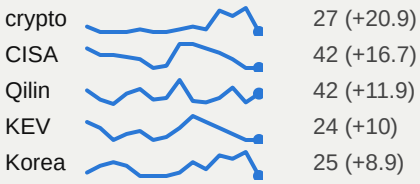


Operations 206 · Force Protection 105 · Space & Cyber Professionals 54

CATEGORIES



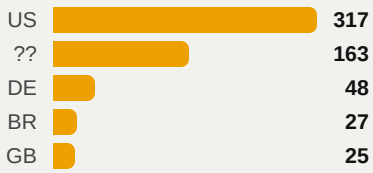
RISING TERMS · 7D VS PRIOR



BY THE NUMBERS

Known Exploited Vulnerabilities (KEV) added 8 (0 ransomware-linked) · leak-site victims 200 (88 PACOM AOR)

LEAK-SITE VICTIMS BY COUNTRY · 30D



THREAT ACTOR SPOTLIGHT — VOLT TYPHOON · PRC (state-sponsored) · Vanguard Panda, BRONZE SILHOUETTE, Insidious Taurus, UNC3236

WHY NOW
Lumen exposed its Silent Train network; Talos tied SD-WAN key theft against space firms to it.

MENTIONS, 30D



6 this week

PACOM RELEVANCE
Hawaii and satellite services are named targets.

NOTABLE TTPS
- Rotating SOHO/IoT relay chains
- Zero-days in SD-WAN and IT management platforms

COUNTERMEASURES
- Keep management interfaces off the internet
- Hunt SD-WAN controllers for KeyDrift

Operations

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

China's 'Volt Typhoon' quietly built another hacking network following US crackdown, new findings say

Nextgov/FCW — cybersecurity · 2026-10-28

Lumen: Silent Train hit government, defense, telecom and satellite networks, focused on Hawaii.

So what: Hawaii networks are named targets.

Consider: Consider reviewing edge logs with Hawaii providers.

PACOM · NORTHCOM · APT & espionage · Critical infrastructure · Volt Typhoon

Inside KeyDrift: Analyzing historical UAT-11473 activity on Cisco SD-WAN

Cisco Talos · 2026-10-28

Talos: Cisco SD-WAN CVE-2026-20127 used to steal keys from space and satellite firms.

So what: SATCOM-adjacent SD-WAN is targeted.

Consider: Recommend checking controllers for KeyDrift.

SPACECOM · PACOM · APT & espionage · Vulns & exploits · Volt Typhoon

CISA Adds Two Known Exploited Vulnerabilities to Catalog

CISA Cybersecurity Advisories · 2026-10-30

KEV: Ivanti Connect Secure (due 2, 13 Nov), Cisco ASA/FTD, GitLab, VMware ESX.

So what: VPNs are Volt Typhoon's way in.

Consider: Recommend confirming gateway patches.

CYBERCOM · 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.

Hackers steal and publish data on 41,000 Homeland Security workers

Malwarebytes Labs · 2026-10-30

Hacktivists published names, phones, job titles and group memberships for 41,000 DHS staff, including intelligence personnel.

So what: Directory data powers pretext calls.

Consider: Be aware of calls citing your role; verify by a known number.

NORTHCOM · Breach & leaked data · Social engineering · ShinyHunters

Defense contractor pleads guilty to aiding North Korean remote worker scheme

CyberScoop · 2026-10-30

A TS-cleared contractor pleaded guilty to lending his identity to DPRK IT workers; Treasury also sanctioned their launderers.

So what: Cleared identities are being rented out.

Consider: Be aware that offers to 'borrow' your identity are crimes.

NORTHCOM · Social engineering · DPRK & crypto theft · DPRK IT workers

U.S. military building resilience against emerging OPSEC risks from automated surveillance networks

DefenseScoop · 2026-10-28

TRANSCOM officials warn that license-plate readers and AI camera networks can track military movements.

So what: Commercial sensors map patterns of life.

Consider: Be aware of these networks in movement planning.

NORTHCOM · OPSEC & personal security · AI & cyber

Space & Cyber Professionals

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

CISA publishes strategy with eye on the next four years

CyberScoop · 2026-10-26

CISA's 'CISA 2030: Defend, Harden, Prevail' starts a 60-day service review and a 180-day rollout.

So what: It is the agency's priorities through 2030.

Consider: Consider tracking what the review changes.

NORTHCOM · Strategy & organization · Critical infrastructure

Tracking AI adoption in North Korean threat actor tradecraft

Microsoft Security / MSTIC · 2026-10-29

Microsoft: DPRK groups use AI for lures, personas and tooling; two use ARTEX. FBI pinned the $6B Binance theft on TraderTraitor.

So what: AI speeds DPRK operations and funding.

Consider: Be aware lure quality is rising.

PACOM · AI & cyber · DPRK & crypto theft · Lazarus Group

Australia reports 20% rise in cyber incidents, nearly 80% jump in threat notifications amid critical infrastructure risks

Industrial Cyber · 2026-10-29

ASD's ACSC handled 1,500+ incidents in 2025-26 (up 20%) and sent 4,400 threat notifications (up ~80%).

So what: The key partner reports AI-driven growth.

Consider: Recommend reading it ahead of partner talks.

PACOM · Critical infrastructure · AI & cyber

WATCH LIST

- Ivanti KEV due 2 Nov; Siemens and Plex 3 Nov.
- Midterms 3 Nov: election-themed scams.
- Commissary freezer hack attribution.
- Vapor Panda ARTEX campaign still active.

RECOMMENDATIONS (FOR AWARENESS)

- Recommend confirming Ivanti, ASA/FTD and GitLab patches.
- Consider reviewing SD-WAN management exposure.
- Consider a reminder to verify 'IT' calls.