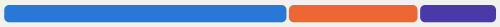
Cyber Watch

2026-W45 · 02 Nov – 08 Nov 2026
Makani Lab · Cyber Watch
Operations · Force Protection · Professionals

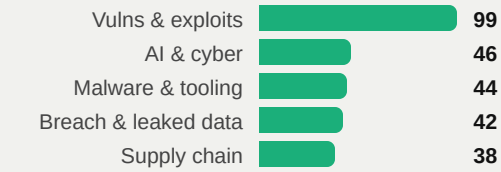
BLUF — The FBI tied the record $6.3B Binance theft to DPRK's TraderTraitor; entry was a fake job interview, a lure that also reaches cleared staff and Guardians. U.S. agencies warned that refrigeration controls are being sabotaged; Nextgov/FCW reports six commissaries hit. Attention: Ivanti VPN KEV due 13 Nov.

LAST 7 DAYS BY LANE · 309 ITEMS

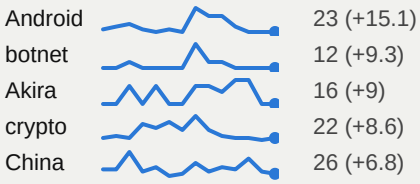


Operations 178 · Force Protection 82 · Space & Cyber Professionals 49

CATEGORIES



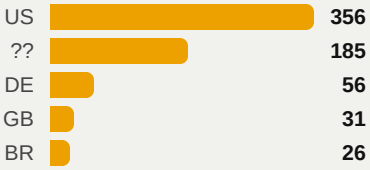
RISING TERMS · 7D VS PRIOR



BY THE NUMBERS

Known Exploited Vulnerabilities (KEV) added 3 (0 ransomware-linked) · leak-site victims 214 (96 PACOM AOR)

LEAK-SITE VICTIMS BY COUNTRY · 30D



THREAT ACTOR SPOTLIGHT — LAZARUS GROUP · DPRK (RGB) · Hidden Cobra, Diamond Sleet, TraderTraitor, BlueNoroff, APT38

WHY NOW

FBI and Secret Service tied the $6.3B Binance theft, the largest crypto heist on record, to TraderTraitor.

MENTIONS, 30D



PACOM RELEVANCE

DPRK theft funds its weapons; job lures target cleared staff.

NOTABLE TTPS

- Fake recruiter and job interview with a malicious coding assignment
- Tampered installer for an AI coding tool
- Pivot via an internal AI tool to wallet engineers

COUNTERMEASURES

- No recruiter tests on work devices
- Verify recruiters via known contacts
- Block downloaded code on admin hosts

Operations

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

US agencies warn of refrigeration hacks amid suspected attacks on military bases

Nextgov/FCW — cybersecurity · 2026-11-05

Five U.S. agencies warned refrigeration controls are being forced into heat or defrost cycles; Nextgov/FCW says Iran-linked actors are suspected at six commissaries.

So what: Commissaries and medical cold chain are on base.

Consider: Consider asking facilities whether refrigeration controllers are internet-reachable.

NORTHCOM · PACOM · ICS / OT · Critical infrastructure

KEV: CVE-2026-19868 — SonicWall SonicOS SSLVPN

CISA Known Exploited Vulnerabilities · 2026-11-05

KEV adds: SonicWall SSLVPN MFA bypass (due 20 Nov), Apple (18 Nov), WordPress (6 Nov).

So what: VPN MFA bypass opens the edge.

Consider: Recommend confirming SonicWall and Ivanti patch status.

PACOM · Vulns & exploits · Cloud & identity

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.

Binance says fake job interview helped North Korean hackers steal $6.3 billion in crypto

Nextgov/FCW — cybersecurity · 2026-11-03

Binance: a fake recruiter ran two interviews, then sent a coding assignment that ran malware on the engineer's work laptop.

So what: Job seekers and cleared staff are the target.

Consider: Be aware that recruiter 'tests' should never run on work or government devices.

PACOM · Social engineering · DPRK & crypto theft · Lazarus Group

Russian state-linked hackers target iPhone, Android devices in zero-click espionage campaign

The Record (Recorded Future) · 2026-11-05

Researchers tie APT29 to a zero-click campaign on iPhone and Android users in Ukraine, the U.S. and Europe; Google patched Android RCE CVE-2026-58868.

So what: Personal phones are espionage targets.

Consider: Consider reminding personnel to install the 2026-11-01 Android patch and current iOS.

EUCOM · NORTHCOM · Apps & devices · APT & espionage · APT29

Former U.S. Government Contractor Pleads Guilty to Spying for Ethiopia

Department of Justice press releases · 2026-11-03

DOJ: a former IT contractor at NRO, State and DOJ pleaded guilty to conspiring to spy for Ethiopia; The Register says he copied files for 2+ years.

So what: Insider risk reaches space intelligence networks.

Consider: Be aware of insider-threat reporting channels.

SPACECOM · APT & espionage · OPSEC & personal security

Space & Cyber Professionals

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

VAPOR PANDA hackers use multi-agent AI to target government, pharmaceutical, semiconductor, defense organizations

Industrial Cyber · 2026-11-05

CrowdStrike: PRC-nexus VAPOR PANDA used ARTEX AI agents against 200+ orgs in 14 countries, including U.S. defense and telecoms.

So what: AI agents let small PRC teams run parallel intrusions.

Consider: Consider sharing CrowdStrike indicators with partners.

PACOM · NORTHCOM · APT & espionage · AI & cyber

Post-Quantum Questions to Ask Your Vendors

CISA Cybersecurity Advisories · 2026-11-05

CISA, ASD's ACSC and NSA issued questions for assessing vendor post-quantum readiness, flagging hard-to-update ICS and IoT.

So what: Ground systems have long crypto lifecycles.

Consider: Recommend reviewing it for ground and facility systems.

PACOM · Standards & compliance · Supply chain

WATCH LIST

- KEV due: Brotli, Adobe 10 Nov; VMware ESX 11 Nov; Ivanti 13 Nov.
- sshole SSH exploitation (CVE-2026-123158).
- Commissary freezer attribution.
- CISA 2015 stopgap ends 11 Dec.

RECOMMENDATIONS (FOR AWARENESS)

- Recommend confirming Ivanti, ESX and SonicWall patches.
- Consider checking refrigeration controller exposure.
- Consider a recruiter-lure reminder to personnel.
- Be aware phones need November patches.