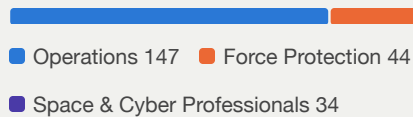


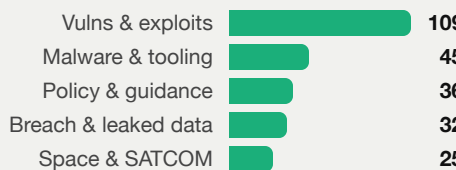
Cyber Watch

BLUF — A five-nation advisory tied the WaterPlum fake-recruiter campaign to the DPRK 313 General Bureau: 30,000+ devices in 100+ countries, \$10.71M stolen. CISA added Cisco Secure Email Gateway CVE-2026-76461 to KEV on disclosure day. AAFES is investigating suspicious messages pushed to military customers through its own channels.

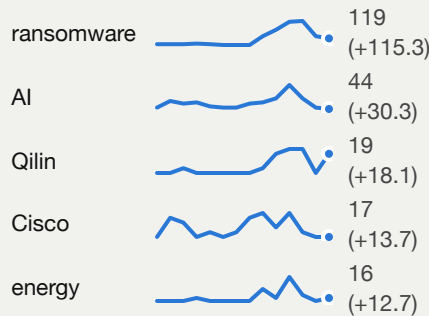
LAST 7 DAYS BY LANE · 225 ITEMS



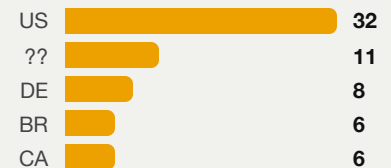
CATEGORIES



RISING TERMS · 7D VS PRIOR



LEAK-SITE VICTIMS BY COUNTRY · 30D



BY THE NUMBERS

Known Exploited Vulnerabilities (KEV) added 6 (0 ransomware-linked) · leak-site victims 111 (42 PACOM AOR)

THREAT ACTOR SPOTLIGHT — WATERPLUM · DPRK (313 General Bureau, Munitions Industry Department) · Contagious Interview, DeceptiveDevelopment, Famous Chollima (overlap), CL-STA-0240

WHY NOW

An 18 Sep FBI/DC3 advisory with Japan, Australia, and Germany named WaterPlum a DPRK state campaign: 30,000+ devices, \$10.71M stolen, and Japan's first laptop farm dismantled.

MENTIONS, 30D



PACOM RELEVANCE

Japan is a primary target; the campaign hunts IT talent across Japan and the ROK.

NOTABLE TTPS

- Fake AI/crypto recruiters targeting developers
- Weaponized GitHub 'coding assignment' repos
- RATs and stealers for credentials and wallets

COUNTERMEASURES

- Run interview code only in a disposable VM
- Assume credential theft; rotate and enforce MFA
- Alert on egress to non-standard package registries

Operations

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

International security agencies warn about North Korean hackers exploiting job seekers to steal crypto, data

CyberScoop · 2026-09-18

A five-nation advisory attributed WaterPlum (Contagious Interview) to the DPRK 313 General Bureau.

So what: 30,000+ devices in 100+ countries and \$10.71M from 7,000+ wallets; the lure also harvests credentials and IDs.

Consider: Consider warning technical staff and job-hunting families never to run interview code.

(PACOM) (NORTHCOM) (APT & espionage) (Social engineering) (WaterPlum)

KEY: CVE-2026-76461 — Cisco Secure Email Gateway

CISA Known Exploited Vulnerabilities · 2026-09-13

CISA added Cisco Secure Email Gateway CVE-2026-76461 (CVSS 9.8) to KEV the day Cisco disclosed it.

So what: Per Rapid7, a crafted email gives root command execution pre-authentication on an internet-facing gateway.

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.

AAFES investigating 'suspicious' messages sent to military customers through email and store's official app

DefenseScoop · 2026-09-18

AAFES is investigating suspicious messages sent to military customers via its official email and the My Exchange app, including a fake 'AAFES Security Team' wish-list link. It has not said whether a breach occurred.

So what: It came through a channel Guardians and families are trained to trust; AAFES serves ~30M shoppers.

Consider: Recommend telling families to delete the message and verify by calling AAFES support.

(NORTHCOM) (PACOM) (Scams & fraud) (Social engineering)

FBI: Fake cop and government impersonation scams cost victims \$1.6B

The Register — security · 2026-09-18

FBI IC3 reports law-enforcement and government impersonation scams have cost victims over \$1.6B across ~61,000 complaints since January 2025, averaging more than \$26,000 each.

So what: Rank, unit, and duty status are easy to research, and a fake police caller carries extra weight.

Consider: Be aware no agency or court demands payment by phone, gift card, wire, or crypto.

(NORTHCOM) (Scams & fraud)

Google Pixel phones pwned in zero-click attacks

The Register — security · 2026-09-16

Google disclosed CVE-2026-58704, an improper authorization flaw in Pixel cellular modems exploitable with no user interaction, and warned of limited targeted exploitation. CISA added it to KEV the next day.

So what: A personal-device risk needing no user mistake; targeted spyware follows people, not networks.

Consider: Recommend Pixel users apply the September update; careful browsing does not mitigate zero-click.

(GLOBAL) (mobile_device) (vulnerability_exploitation)

Space & Cyber Professionals

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

SecAF announces on-orbit space control weapons

U.S. Space Force · 2026-09-15

Secretary of the Air Force Troy Meink announced on-orbit space control weapons at the 2026 Air, Space and Cyber Conference, saying both services must defeat AI-enabled threats inside a slower budget process.

So what: An on-orbit space control mission raises the value of SPACEPAC ground stations as targets.

Consider: Recommend reviewing how S36 priorities map to the supporting ground segment.

(GLOBAL) (space_policy) (strategy)

Joint Chiefs chairman says U.S. forces must prepare to be 'hunted' by autonomous systems

DefenseScoop · 2026-09-16

Chairman of the Joint Chiefs Gen. Dan Caine said U.S. forces must assume they will be 'hunted by autonomous systems, jammed across the spectrum, and tracked in real time,' citing Ukrainian FPV drones using AI vision.

So what: Autonomy that survives GPS denial shifts the burden onto space-based PNT and comms resilience.

Consider: Recommend reviewing how resilience planning handles PNT-degraded threats.

(GLOBAL) (EUCOM) (strategy) (ai_security)

WATCH LIST

- KEV due: Linux kernel 21 Sep, Windows 22 Sep, V8 23 Sep.
- JFrog Artifactory KEV entries due 25 Sep.
- Whether AAFES confirms a breach at the Exchange.

RECOMMENDATIONS (FOR AWARENESS)

- Confirm Cisco Secure Email Gateway and ISE are patched.
- Push the AAFES warning to families: delete, verify by phone.
- Pixel users: apply the September update (CVE-2026-58704).