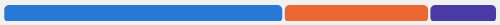
Cyber Watch

2026-W42 · 12 Oct – 18 Oct 2026
Makani Lab · Cyber Watch
Operations · Force Protection · Professionals

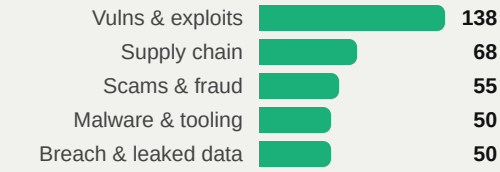
BLUF — PRC edge-device exploitation led the week: CISA added BeyondTrust and Ivanti zero-days to KEV, DOJ charged 14 in a DPRK IT worker scheme, and a BAE Systems incident halted federal bankruptcy notices. Needs attention: BeyondTrust and Fortinet KEV entries are due 19 Oct, and patching alone may not clear access gained before disclosure.

LAST 7 DAYS BY LANE · 356 ITEMS

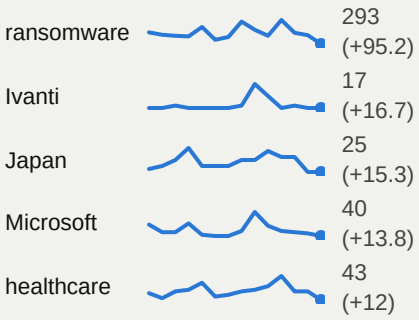


Operations 202 · Force Protection 105 · Space & Cyber Professionals 49

CATEGORIES



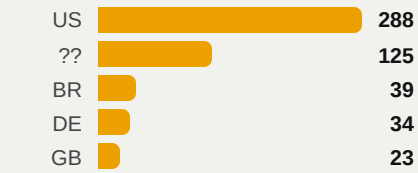
RISING TERMS · 7D VS PRIOR



BY THE NUMBERS

Known Exploited Vulnerabilities (KEV) added 8 (0 ransomware-linked) · leak-site victims 277 (140 PACOM AOR)

LEAK-SITE VICTIMS BY COUNTRY · 30D



THREAT ACTOR SPOTLIGHT — UNC5221 / UNC5174 · PRC · Armory Castle, Warp Panda

WHY NOW

BeyondTrust disclosed a Remote Support zero-day exploited since 29 Aug; Mandiant attributes it to Armory Castle (formerly UNC5221), and CISA added it to KEV.

MENTIONS, 30D



PACOM RELEVANCE

Remote-support tools are common at the IT contractors and partner networks a theater space component depends on.

NOTABLE TTPS

- Zero-days in edge and security products: Ivanti, Citrix NetScaler, now BeyondTrust
- Targets appliances without EDR; Brickstorm dwell time averaged 400 days
- Deletes logs; rotates infrastructure and tools per victim

COUNTERMEASURES

- Apply BT26-05-RS; versions older than 24.3.1 must upgrade first
- Limit external access to remote-support appliances
- Hunt for pre-disclosure activity; send appliance logs off-box

Operations

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

Prolific Chinese espionage group exploits BeyondTrust zero-day

CyberScoop · 2026-10-16

According to Mandiant, PRC-nexus Armory Castle exploited BeyondTrust Remote Support zero-day CVE-2026-102764 from 29 Aug. CISA added it to KEV, due 19 Oct; Canada issued alert AL26-025.

So what: Remote-support appliances hold privileged access; earlier compromises may be unfound.

Consider: Recommend applying BT26-05-RS and hunting for pre-disclosure activity.

PACOM · CYBERCOM · APT & espionage · Vulns & exploits · UNC5221 / UNC5174

CISA Urges Patching Newly Exploited Vulnerability in Ivanti Connect Secure

CISA Cybersecurity Advisories · 2026-10-13

CISA says actors exploited Ivanti Connect Secure zero-day CVE-2026-104935 for credential theft and

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.

North Korean IT Workers Expanding Use of Facilitators, Broadening Recruitment

FBI IC3 Public Service Announcements · 2026-10-13

FBI IC3 warned that DPRK IT workers are using more U.S.-based facilitators and recruiting more widely. In the DOJ case, facilitators hosted company laptops in more than 40 Texas homes.

So what: Laptop-hosting side jobs reach members, spouses and veterans and are a federal crime.

Consider: Be aware of offers to host laptops for a remote employer; recommend reporting them to OSI.

NORTHCOM · Scams & fraud · Social engineering · DPRK IT workers

Microsoft, Health-ISAC dismantle phishing infrastructure targeting critical infrastructure, healthcare sector

Industrial Cyber · 2026-10-16

Microsoft and Health-ISAC, supported by Japan's National Police Agency, seized domains behind the YAM Store, CoGUI and Iron Man phishing kits, which Microsoft says sent over 1 billion messages since January.

So what: Victims were mainly in Japan and the U.S.

Consider: Consider reminding families to reach bank and delivery sites directly, not via links.

PACOM · Scams & fraud · Social engineering

Spyware vendors found a way to make targeted ads even worse

The Register — security · 2026-10-15

According to Citizen Lab, adtech firm Discover-Tech used ad-bidding data to deliver zero-click Candiru spyware through ads, infecting at least 45 Al Jazeera devices. Google had listed it as an approved vendor.

So what: Ad data can single out a person; opening a page was enough.

Consider: Consider Lockdown Mode for high-visibility personnel and limiting ad tracking.

CENTCOM · EUCOM · Apps & devices · OPSEC & personal security

Sextortion “help” firm took $60 million from victims, FTC alleges

Malwarebytes Labs · 2026-10-15

The FTC alleges Digital Forensics Corporation took at least $60 million from sextortion victims for help it often did not provide. A federal court has temporarily halted the firm.

So what: Paid 'recovery' firms add a second loss for sextortion victims.

Consider: Be aware that help is free through OSI, NCMEC Take It Down and the FBI.

NORTHCOM · Scams & fraud

Space & Cyber Professionals

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

Pentagon averts cyber pay cuts — for now — with one-year C-MIP ‘transition plan’

DefenseScoop · 2026-10-15

According to a memo reviewed by DefenseScoop, cyber troops receive the higher of C-MIP or legacy incentive pay until 30 Sep 2027, averting cuts of $100 to $1,000 a month.

So what: Pay is protected for a year; members must still qualify under C-MIP.

Consider: Recommend supervisors review C-MIP qualification paths.

CYBERCOM · Workforce & training

NSA urges zero-trust controls to protect DoW OT systems from evolving cyber threats, unauthorized access

Industrial Cyber · 2026-10-11

An NSA information sheet lists 26 zero-trust activities for DOW critical OT, including legacy systems: secure remote access, asset inventory, segmentation, hardened workstations and Active Directory.

So what: Ground-segment and installation control systems are DOW OT.

Consider: Consider reviewing OT against the 26 activities.

CYBERCOM · NORTHCOM · Standards & compliance · ICS / OT

Space sector faces satellite cybersecurity blind spots, calls for stronger threat intelligence and