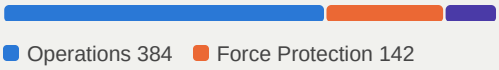
# Cyber Watch

**2026-W47 · 16 Nov – 22 Nov 2026**
Makani Lab · Cyber Watch
Operations · Force Protection · Professionals

**BLUF** — PRC-nexus actors led the week: Google tied ARMORY CASTLE to a vCenter zero-day used to forge SSO admin access, and Bitdefender says the EggStreme group rebuilt its tools against Philippine government targets. The FBI warned the ARTEX AI framework can take intrusions to privileged access in under three hours. Attention: vCenter and Cisco Expressway KEV entries are due 23 Nov.

### LAST 7 DAYS BY LANE · 589 ITEMS



Operations 384 · Force Protection 142 · Space & Cyber Professionals 63

**CATEGORIES**

| | |
|---|---|
| Vulns & exploits | 284 |
| Supply chain | 120 |
| Breach & leaked data | 88 |
| AI & cyber | 85 |
| Cloud & identity | 62 |

### RISING TERMS · 7D VS PRIOR

| | |
|---|---|
| AI | 166 (+70.7) |
| ransomware | 312 (+66.7) |
| healthcare | 69 (+39.2) |
| Microsoft | 53 (+26.5) |
| energy | 33 (+15.7) |

**BY THE NUMBERS**

Known Exploited Vulnerabilities (KEV) added 9 (0 ransomware-linked) · leak-site victims 276 (147 PACOM AOR)

### LEAK-SITE VICTIMS BY COUNTRY · 30D

| | |
|---|---|
| US | 420 |
| ?? | 177 |
| DE | 50 |
| CA | 48 |
| GB | 34 |

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

**WHY NOW**

Google and Mandiant tied vCenter zero-day CVE-2026-123890 to ARMORY CASTLE, exploited since early Sep, with entry via the BeyondTrust zero-day (W42).

**MENTIONS, 30D**



6 this week

**PACOM RELEVANCE**

vCenter hosts mission-support systems at AOR contractors and partners.

**NOTABLE TTPS**

- BeyondTrust zero-day, then pivot to Linux
- Steals vCenter SAML key; forges SSO admins
- SSH keys on ESXi; Slack-based C2

**COUNTERMEASURES**

- Apply Broadcom's 19 Nov vCenter fix
- Review SSO admins; rotate SAML keys
- Audit ESXi SSH and authorized keys

## Operations

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

### KEV: CVE-2026-76466 — Cisco Expressway Series

CISA Known Exploited Vulnerabilities · 2026-11-19

Exploited Cisco Expressway hard-coded credentials give remote root; ThaiCERT also warned. KEV due 23 Nov.

**So what:** Expressway bridges VTC and voice to the internet.

**Consider:** Recommend confirming patch status.

PACOM · NORTHCOM · Vulns & exploits

### New EggStreme Malware Variant Goes Silent to Evade Security Tools in Government Attacks

The Hacker News · 2026-11-18

According to Bitdefender, the suspected Chinese APT behind EggStreme rebuilt its toolkit and still targets Philippine government bodies.

**So what:** Treaty-ally networks remain a PRC target.

**Consider:** Be aware older EggStreme indicators may not match.

PACOM · APT & espionage · Malware & tooling

## 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.

### Pakistani hackers are spying on defense workers with fake job sites

CyberScoop · 2026-11-17

According to Lookout, Pakistan-aligned SpaceCobra used fake defense recruiter sites to push GravityRAT Android spyware.

**So what:** Job-seeking and separating members fit the lure.

**Consider:** Be aware an app offered outside the store is a red flag.

PACOM · Social engineering · Apps & devices

### Russian National Indicted for Acting as a Foreign Agent of Russia to Target Silicon Valley Technology and Defense Company

Department of Justice press releases · 2026-11-18

DOJ indicted a Russian national for surveilling a defense firm's employees; an FBI affidavit points to FSB tasking, per The Register.

**So what:** Defense staff and families can be targeted at home.

**Consider:** Be aware; report suspicious contact or devices to OSI.

NORTHCOM · EUCOM · OPSEC & personal security · APT & espionage

### Alaska, Hawaiian investigate website security incident

Hawaii News Now · 2026-11-18

An Optimizely flaw let attackers plant card-stealing code on 178 sites on 16 Nov, including Alaska and Hawaiian Airlines.

**So what:** Families booking travel may have entered card data.

**Consider:** Consider checking card statements for 16 Nov.

PACOM · NORTHCOM · Supply chain · Breach & leaked data

## Space & Cyber Professionals

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

### Pentagon CIO replaces White House cyber director Sean Cairncross in major shakeup

Nextgov/FCW — cybersecurity · 2026-11-19

Pentagon CIO Kirsten Davies replaces fired National Cyber Director Sean Cairncross; senators plan holds on the CISA nominee.

**So what:** The DOW CIO now leads national cyber policy.

**Consider:** Be aware CISA may lack a confirmed director into 2027.

NORTHCOM · CYBERCOM · Strategy & organization

### FBI warns hackers weaponizing ARTEX AI framework to automate attacks on energy, manufacturing, telecom

Industrial Cyber · 2026-11-17

FBI FLASH: the ARTEX AI framework has driven intrusions to privileged access in under three hours; Google saw a similar tool in a US aerospace hack.

**So what:** Patch-to-exploit time is shrinking.

**Consider:** Consider reviewing exposed supplier and legacy portals.

PACOM · NORTHCOM · AI & cyber · Supply chain

**WATCH LIST**

- KEV due 23 Nov: vCenter, Expressway, SAP, Roller.
- KEV due 24 Nov: Office, Chromium, BroadWorks, Openwave.
- FBI probing an apparent NCIC database breach.
- Senate holds on CISA nominee LoSapio.

**RECOMMENDATIONS (FOR AWARENESS)**

- Recommend confirming vCenter and Expressway patches by 23 Nov.
- Consider reviewing exposed supplier portals and APIs.
- Be aware fake recruiter sites push mobile spyware.
- Recommend reviewing Microsoft's Entra Connect Health notice.