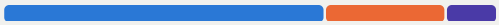
Cyber Watch

2026-W48 · 23 Nov – 29 Nov 2026
Makani Lab · Cyber Watch
Operations · Force Protection · Professionals

> **BLUF** — Rule-based issue (the AI curation stage has not run for this week). Items below are the highest-scoring open-source reports from the last seven days, one section per lane.

LAST 7 DAYS BY LANE · 556 ITEMS



Operations 362 · Force Protection 136 · Space & Cyber Professionals 58

CATEGORIES

Vulns & exploits	276
Supply chain	112
Breach & leaked data	89
Cloud & identity	65
AI & cyber	65

RISING TERMS · 7D VS PRIOR

ransomware		306 (+47.6)
AI		151 (+44.8)
healthcare		61 (+26.6)
Microsoft		54 (+24.5)
energy		34 (+16.3)

BY THE NUMBERS

Known Exploited Vulnerabilities (KEV) added 8 (0 ransomware-linked) · leak-site victims 276 (142 PACOM AOR)

LEAK-SITE VICTIMS BY COUNTRY · 30D

US	428
??	176
DE	52
CA	52
GB	38

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

WHY NOW
Ivanti and edge-device zero-day exploitation

MENTIONS, 30D

9 this week

NOTABLE TTPS
—

COUNTERMEASURES
—

Operations

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

Government tech debt is a national security risk

CyberScoop · 2026-11-18

With 80% of federal IT budgets spent maintaining aging legacy systems, fragmented government networks are struggling to defend against AI-accelerated cyberattacks from foreign adversaries.

NORTHCOM · PACOM · Supply chain · Vulns & exploits · Volt Typhoon

National-level hacker group SilentAir targets mobile users in Taiwan and over ten other countries, abusing telecom signals to intercept SMS and calls

iThome Security (Taiwan) · 2026-11-16

Telecom security firm Enea disclosed the activities of the nation-state hacker group SilentAir. These hackers have long infiltrated the networks of telecom operators worldwide, and their attack targets…

PACOM · Telecom & cables · APT & espionage · Salt Typhoon

Chinese Hackers Exploit VMware vCenter Zero-Day Vulnerability to Intrude, Deploy Backdoors for Data Theft

iThome Security (Taiwan) · 2026-11-20

Google Threat Intelligence Group (GTIG) and Mandiant disclosed that a Chinese hacking group known as Armory Castle or UNC5221 leveraged the VMware vCenter zero-day vulnerability CVE-2026-123890 to launch…

PACOM · NORTHCOM · Vulns & exploits · Malware & tooling · UNC5221 / UNC5174

UAT-12643: Suspected North Korea-aligned actor blends blockchain resilience with targeted infostealing

Cisco Talos · 2026-11-18

Cisco Talos discovered malicious infrastructure associated with a financially motivated threat group we are

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.

Huawei case enters jury deliberations after 2-month battle in US courtroom

South China Morning Post (China) · via TJFSCC Daily · 2026-11-18

Jurors began deliberating on Wednesday in the US government’s criminal case against Huawei Technologies, following a two-month trial that has been one of the most high-profile prosecutions of a Chinese…

NORTHCOM · PACOM · Scams & fraud · Apps & devices

FBI Says North Korean Hackers Stole Over $400 Million in Crypto Using Deepfake Video Calls

DataBreaches.net · 2026-11-16

Ravie Lakshmanan reports: The U.S. Federal Bureau of Investigation (FBI) has established that threat actors tied to the Democratic People’s Republic of Korea (DPRK aka North Korea) have stolen more than…

NORTHCOM · PACOM · DPRK & crypto theft · Social engineering

Japan to postpone launch of sex offense check system over data leak risk

DataBreaches.net · 2026-11-18

The Mainichi reports: Japan decided to postpone the planned Dec. 25 launch of a new system to check the sex offense histories of people working with children after vulnerabilities were found, the minister…

PACOM · SPACECOM · Ransomware · Breach & leaked data

Android Phones Turned Into Fraud Call Relay Stations, Puff Boxes Hide Hundreds of SIM Cards! Criminal Investigation Bureau Exposes Fraudsters' New Call Forwarding Method

iThome Security (Taiwan) · 2026-11-20

To evade international call voice warning mechanisms, overseas fraud groups use DMT equipment set up in Taiwan to forward scam calls as domestic numbers. Recently, some fraud groups have switched to using…

PACOM · NORTHCOM · Scams & fraud · Apps & devices

Sens. Wicker and Luján offer bill to prohibit 'stealth bots,' exclude legitimate users

Inside Defense · via TJFSCC Daily · 2026-11-20

Sens. Roger Wicker (R-MS) and Ben Ray Luján (D-NM) are invoking a threat from China in promoting legislation they’ve introduced to ban the use of artificial intelligence agents that obscure a user’s…

PACOM · NORTHCOM · Policy & guidance · Scams & fraud

Space & Cyber Professionals

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

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

US FCC proposes three-year Cyber Trust Mark renewal cycle, seeks stronger oversight of certified IoT products

Industrial Cyber · 2026-11-22

The Federal Communications Commission (FCC) published Monday a notice seeking public comment on proposed requirements for the U.S....

NORTHCOM · SPACECOM · Apps & devices · APT & espionage

Texas Cyber Command adds 63 companies to Project Watershed 250 to bolster water utility security

Industrial Cyber · 2026-11-20

Texas Cyber Command (TXCC) announced that 63 technology and cybersecurity companies have joined Project Watershed 250, a pilot...

NORTHCOM · CYBERCOM · Critical infrastructure · ICS / OT