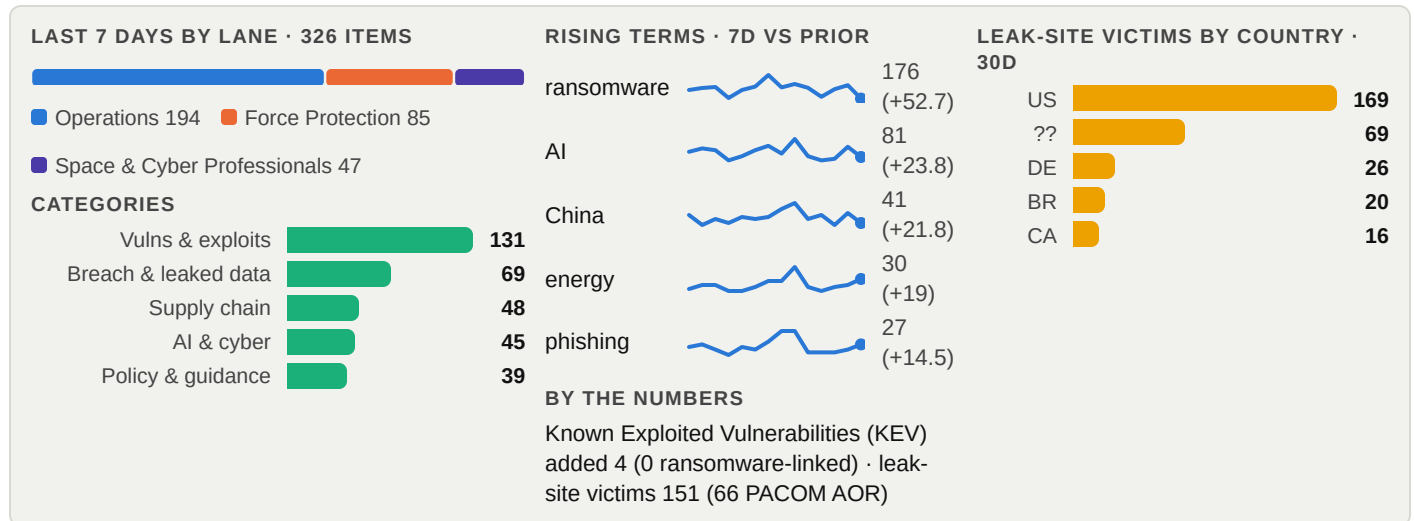


Cyber Watch

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.



THREAT ACTOR SPOTLIGHT — SHINYHUNTERS · Criminal extortion group · UNC6040

WHY NOW

Data theft and extortion via cloud/SaaS and enterprise app exploitation (Salesforce, Oracle); leak threats against government and corporate victims

NOTABLE TTPS

—

COUNTERMEASURES

—

MENTIONS, 30D

11 this week

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

Risky Bulletin: Authorities dismantle KillSec group, arrest members across Europe

Risky Business News · 2026-10-01

In other news: Ransomware attack could have crippled South Africa's air traffic operations; US sanctions Venezuelan ATM hackers; Chinese APT targets AI experts.

[EUCOM](#) [PACOM](#) [Ransomware](#) [Vulns & exploits](#) [Qilin](#)

Centrii warns nation-state access and renewable supply-chain risks raise energy sector financial exposure

Industrial Cyber · 2026-10-05

New analysis from Centrii identified that cyber risk in the energy sector is increasingly becoming a financial and...

[EUCOM](#) [NORTHCOM](#) [Supply chain](#) [APT & espionage](#) [Volt Typhoon](#)

Symantec reports Warlock ransomware group targets water, telecom, government organizations through SharePoint flaws

Industrial Cyber · 2026-10-01

New data from Symantec observed that the China-nexus group behind Warlock ransomware, tracked as Longlegs or Storm-2603, has...

[NORTHCOM](#) [PACOM](#) [Telecom & cables](#) [Vulns & exploits](#) [Warlock / Storm-2603](#)

Pentagon personnel breach — undetected for months — renews cyber standard scrutiny

Nextgov/ECW — cybhersecurity · 2026-10-05

UNCLASSIFIED · open-source reporting only · 8 sources · built 2026-10-06 06:49 HST

Cyber Watch · 2026-W41 · page 1 of 2

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.

AI policy circles targeted in China-linked phishing operation

CyberScoop · 2026-10-01

Cybersecurity firm Proofpoint said TA419 impersonated officials and AI industry figures in an effort to gain access to cloud accounts held by U.S. think tank, university and legal-sector experts.

PACOM NORTHCOM Supply chain Social engineering TA419

7th Air Force seeks new counter-drone capabilities for point defense modernization in South Korea

DefenseScoop · 2026-10-05

The RFI release comes amid growing concerns about North Korea's drone arsenal.

PACOM EUCOM OPSEC & personal security Supply chain

China-linked hackers posed as former US officials, Anthropic employee to target AI experts

Nextgov/FCW — cybersecurity · 2026-09-30

According to Proofpoint, China-aligned TA419 posed as a former OSTP official, a former State economist and an Anthropic employee, inviting AI policy experts to a fake advisory committee and then phishing their Microsoft logins.

So what: Staff who work with think tanks get the same invitations.

Consider: Be aware that known names can be spoofed; verify out of band.

PACOM NORTHCOM Social engineering Cloud & identity TA419

Suspected Chinese spies spoofed an Anthropic exec, ex-White House official in AI phishing

The Register — security · 2026-10-01

Your invite to a fake AI policy advisory committee has strings attached

PACOM NORTHCOM Social engineering Supply chain TA419

China-Aligned TA419 Targets U.S. AI Policy Experts With Microsoft AitM Phishing

The Hacker News · 2026-10-03

A new China-nexus cyber espionage group known as TA419 has been attributed to multiple credential phishing campaigns targeting artificial intelligence (AI) experts working for U.S. think tanks,...

PACOM NORTHCOM Social engineering APT & espionage TA419

Space & Cyber Professionals

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

National cyber director: Government-industry collaboration vital to managing AI risks, competition with nations

CyberScoop · 2026-10-01

Sean Cairncross talked about regulations, China, pilot projects and more Thursday.

PACOM NORTHCOM AI & cyber Strategy & organization

Inside Maritime OT's Isolation Problem: Tanker Cyber Incidents, an AI Test Breakout, and APT36's USB Route to Air-Gapped Networks

Industrial Cyber · 2026-10-04

In mid-September, the US Coast Guard and FBI confirmed they had boarded US-bound energy tankers after indications that...

NORTHCOM EUCOM APT & espionage Apps & devices

NIST outlines secure remote access strategies to strengthen water and wastewater OT cybersecurity

Industrial Cyber · 2026-10-04

The National Institute of Standards and Technology (NIST) published practical guidance to help U.S. water and wastewater utilities...

NORTHCOM SPACECOM ICS / OT Critical infrastructure

The Pentagon's new cyber mastery incentive model promised a 'new era.' Troops are bracing for pay cuts.

DefenseScoop · 2026-10-01