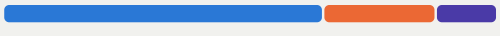
Cyber Watch

2026-W46 · 09 Nov – 15 Nov 2026
Makani Lab · Cyber Watch
Operations · Force Protection · Professionals

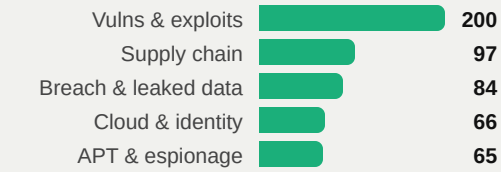
BLUF — China-nexus telecom espionage led the week: Enea exposed SilentAir intercepting calls and SMS 2FA on Asian mobile networks, mostly in Taiwan. The FBI disrupted DPRK's FaceStealer deepfake video-call scheme. Attention: exploited Check Point gateway KEV CVE-2026-123039 is due 16 Nov.

LAST 7 DAYS BY LANE · 474 ITEMS

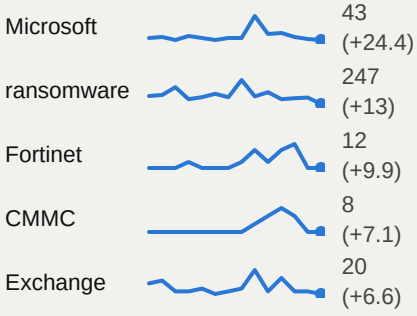


Operations 307 · Force Protection 108 · Space & Cyber Professionals 59

CATEGORIES



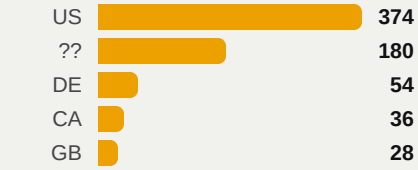
RISING TERMS · 7D VS PRIOR



BY THE NUMBERS

Known Exploited Vulnerabilities (KEV) added 8 (0 ransomware-linked) · leak-site victims 225 (115 PACOM AOR)

LEAK-SITE VICTIMS BY COUNTRY · 30D



THREAT ACTOR SPOTLIGHT — SALT TYPHOON · PRC (MSS) · GhostEmperor, FamousSparrow, Earth Estries, UNC2286, RedMike

WHY NOW

Check Point tied three China-nexus campaigns on telecoms and militaries to CopperDragon, supplier of the Sparrow framework used by FamousSparrow and Earth Estries.

MENTIONS, 30D



PACOM RELEVANCE

Hits telecoms and militaries in Taiwan and Southeast Asia.

NOTABLE TTPS

- Watering holes showing a fake Chrome certificate error
- 'Certificate Fix' MSI drops SquadC or SparrowDoor
- Internet-facing Linux first, then Windows

COUNTERMEASURES

- Treat any 'certificate fix' download as hostile
- Block user-run MSIs from browser downloads
- Patch and log internet-facing Linux hosts

Operations

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

KEV: CVE-2026-123039 — Check Point Multiple Products

CISA Known Exploited Vulnerabilities · 2026-11-12

Check Point Research says attackers chained PHP2Shell with this root flaw on Security Gateways, then wiped ESXi hosts; ThaiCERT also warned.

So what: Edge firewalls front partner networks.

Consider: Recommend confirming patch status before 16 Nov.

PACOM · CENTCOM · Vulns & exploits · Malware & tooling

SilentAir Hijacks Asian Telecom Networks to Intercept SMS 2FA Codes and Spy on Taiwanese Users

The Hacker News · 2026-11-13

According to Enea, China-nexus SilentAir backdoored telecom gear in six Asian countries to track subscribers and intercept calls and SMS.

So what: SMS 2FA on partner networks is interceptable.

Consider: Consider app or hardware MFA over SMS codes.

PACOM · Telecom & cables · APT & espionage

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.

FBI disrupts intricate North Korean fake-call scheme tied to $400M in crypto theft

Nextgov/FCW — cybersecurity · 2026-11-12

FBI: DPRK used hijacked Telegram, LinkedIn and Slack accounts to set up fake video calls showing a known face, then pushed an audio 'fix'; over $400M stolen.

So what: A familiar face on a call is not proof.

Consider: Be aware: never run a script a meeting asks for.

PACOM · NORTHCOM · Social engineering · DPRK & crypto theft · Lazarus Group

Operation Endgame Takes Down Gootloader, CastleRAT and StealC Servers, Seizes 6.4M Stolen Logins

The Hacker News · 2026-11-13

Operation Endgame took down StealC, CastleRAT and Gootloader servers and seized about 6.4 million stolen logins, according to Germany's BKA.

So what: Stealer logs mix personal and work passwords.

Consider: Consider passkeys and changing reused passwords.

EUCOM · NORTHCOM · Malware & tooling · Cloud & identity

Spyware attacks trend toward hitting just about anyone

CyberScoop · 2026-11-10

According to iVerify, Apple spyware alerts this year reached people with no public profile, including a limousine driver in Australia.

So what: Spyware is no longer aimed only at VIPs.

Consider: Be aware Apple threat alerts are real; consider Lockdown Mode.

PACOM · NORTHCOM · Malware & tooling · Apps & devices

Space & Cyber Professionals

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

CISA, NSA, Australian cyber agencies urge early vendor readiness for PQC transition across critical systems

Industrial Cyber · 2026-11-08

CISA, NSA and Australia's ASD/ACSC issued joint questions for judging vendor post-quantum readiness and urged PQC terms in contracts.

So what: Ground segment and ICS have long lifecycles.

Consider: Recommend using the questions at contract renewal.

PACOM · CYBERCOM · Standards & compliance · Supply chain

Trump nominates Palantir security chief Michael LoSapio to lead CISA

Nextgov/FCW — cybersecurity · 2026-11-09

Palantir CISO Michael LoSapio was nominated to lead CISA, which has had no confirmed director since January 2025.

So what: CISA leadership shapes KEV and advisories.

Consider: Be aware it may roll to the next Congress.

NORTHCOM · Strategy & organization

WATCH LIST

- KEV due: Check Point, UnrealIRCd 16 Nov; Apple 18 Nov; SonicWall SSLVPN 20 Nov.
- KEV due 24 Nov: Outlook spoofing, Chromium, Cisco BroadWorks; Barracuda ESG exploited.
- Commissary refrigeration: France names IRGC Shahid Kaveh.
- CISA 2015 info-sharing protections lapse 11 Dec.

RECOMMENDATIONS (FOR AWARENESS)

- Recommend confirming Check Point, Barracuda ESG and SonicWall patch status.
- Consider app or hardware MFA instead of SMS codes.
- Be aware video calls from known faces can be faked.
- Consider reviewing contractor ScreenConnect extensions.