WEEKLY EXECUTIVE SUMMARY · CYBER THREAT INTELLIGENCE

Global Cyber Threat Report

Coverage period: June 7 – June 13, 2026 · Prepared June 16, 2026

Major incidents
8
Confirmed this week

Records exposed
~11M+
Confirmed; billions claimed

Law enforcement actions
1
DOJ/FBI domain seizure

Key threat actor
Miasma worm
Self-replicating supply chain

NOTABLE INCIDENTS

Miasma Worm — Microsoft GitHub & PyPI Escalation

Critical

June 5–7, 2026 (active through report window)

The self-replicating Miasma supply-chain worm escalated against Microsoft's open-source estate, with a compromised contributor account pushing a malicious commit into the Azure/durabletask GitHub repository. GitHub's automated enforcement disabled 73 repositories across the Azure, Azure-Samples, Microsoft, and MicrosoftDocs organizations in a 105-second sweep. The payload plants configuration files that execute a credential-harvesting script the moment a repository is opened in Claude Code, Gemini CLI, Cursor, or VS Code. On June 7, the campaign expanded again when researchers identified 37 malicious Python wheel artifacts across 19 PyPI packages, continuing a wave that has already hit npm and PyPI ecosystems since June 1.

73 repos disabled · Targets AI coding agents · Software / developer ecosystem

Kyushu Electric Power Transmission and Distribution (Japan)

Critical

Disclosed June 8, 2026

A utility subsidiary disclosed that a palm-sized, unencrypted SSD containing personal records for up to 10.9 million customers went missing from a biometrically secured server room. A contractor performing a routine backup copied the database to the portable drive on April 27; it was discovered missing on May 26. Fifty-seven individuals from ten contracting firms had access to the room during the window. This is being called the largest personal data breach in Japanese history, and Japan's METI has ordered a full investigation.

Up to 10.9M customers · Unencrypted physical media · Utilities / energy

DOJ / FBI — Chinese Recruitment Network Disrupted

Confirmed

Announced June 10, 2026

Federal authorities seized 13 internet domains tied to an alleged Chinese intelligence-gathering operation active since November 2023. The network used fake consulting firms with names like Centrik Global Consulting and Catalyst Global Solutions to advertise "Senior Analyst" and "International Affairs Consultant" roles aimed at current and former U.S. government and military personnel holding security clearances. Operators reportedly used AI-generated headshots, stolen identities, encrypted messaging, and cryptocurrency to mask payments for sensitive insider information.

China-linked espionage · 13 domains seized · Government / defense workforce

Ivanti Sentry — Max-Severity Flaw Exploited

Critical

Patched June 9; exploited within 24 hours

Ivanti disclosed CVE-2026-10520, a maximum-severity (CVSS 10) OS command injection flaw in its Sentry mobile gateway product, alongside a second critical authentication bypass (CVE-2026-10523). Despite Ivanti initially reporting no evidence of in-the-wild exploitation, the Shadowserver Foundation observed mass exploitation attempts within 24 hours of a public proof-of-concept, confirming at least two backdoored instances and warning that most exposed gateways are likely compromised. CISA issued a binding directive giving federal agencies three days to patch.

CVSS 10 — root RCE · Exploited in 24 hours · CISA emergency directive

TikTok — Claimed 2.4 Billion Record Leak

Unverified

Posted June 11, 2026

A threat actor advertised a dataset allegedly containing 2.4 billion TikTok user records — including emails, phone numbers, dates of birth, and in some cases names and location data — on a known leak forum. Researchers assess the data most likely originates from infostealer malware rather than a direct breach of TikTok's systems, and were unable to verify the claim; the seller's download link led to a near-empty private Telegram channel. A separate, smaller listing of 3,000 records with plaintext passwords surfaced around the same time.

Unconfirmed claim · Likely infostealer-sourced

Wise — Disputed 4.9 Million Record Breach Claim

Unverified

Posted ~June 12, 2026

A threat actor advertised a database of approximately 4.9 million records allegedly exfiltrated from fintech platform Wise, primarily affecting Spanish users and including national ID numbers (NIF) and contact details. Timestamps in sample records suggest a recent exfiltration rather than a repackaged old dump. Wise stated it found no evidence its systems were compromised and called the data unrelated to its platform, suggesting the listing may repackage data from a previous, unrelated leak.

Spanish national IDs claimed · Fintech / financial services

Arch User Repository (AUR) — Supply Chain Hijack

High

Disclosed June 11, 2026

Security researchers and the Arch Linux community disclosed a large-scale supply-chain attack against the Arch User Repository, in which attackers hijacked more than 400 community packages and converted them into a malware delivery network. While the immediate blast radius is limited to Arch Linux systems, the incident is a continuation of the broader 2026 pattern of attackers compromising developer trust in open-source package ecosystems.

400+ packages hijacked · Open-source ecosystem

University of Nottingham

Medium

Reported week of June 8, 2026

The university confirmed a hacking group gained access to its student records system, affecting both current students and alumni. Further details on the scope of compromised data and the responsible threat actor have not yet been publicly disclosed.

Education sector · Students & alumni affected

KEY TRENDS THIS WEEK

AI coding agents are now an attack surface

Miasma's pivot to triggering payloads when a repository is simply opened in Claude Code, Cursor, or VS Code — rather than waiting for code execution — marks a meaningful shift. Trust boundaries built around "running" untrusted code no longer hold when agentic tools auto-read repository contents on open.

Exploitation timelines keep shrinking

The Ivanti Sentry flaw went from patch to mass exploitation in under 24 hours, despite the vendor reporting no known in-the-wild activity at disclosure. Patch-now windows are compressing industry-wide, and "no evidence of exploitation" statements are increasingly stale within a day.

Physical media remains a blind spot

The Kyushu Electric incident — an unencrypted SSD physically removed from a secured room — is a reminder that the largest breaches aren't always remote exploits. Encryption-at-rest policies for portable media often lag far behind network-layer defenses.

Unverifiable mega-leak claims are noise and signal

Both the TikTok and Wise claims this week illustrate a recurring pattern: forum-posted "mega leaks" that researchers can neither confirm nor fully debunk. Infostealer-aggregated data increasingly gets rebranded as fresh corporate breaches, complicating incident response prioritization.

RECOMMENDED EXECUTIVE ACTIONS

- **Audit AI coding agent exposure:** Treat any repository opened in Claude Code, Cursor, Gemini CLI, or VS Code between June 1–9, 2026 as potentially compromised if it touched the affected npm, PyPI, or GitHub namespaces. Rotate developer and cloud credentials accordingly.

- **Patch Ivanti Sentry immediately:** Upgrade to R10.5.2, R10.6.2, or R10.7.1 without delay. Given the 24-hour exploitation timeline, assume compromise on any unpatched, internet-exposed instance and investigate for backdoors.
- **Review portable media encryption policy:** Following the Kyushu Electric incident, confirm that all portable storage devices used for backups or data transfer enforce mandatory encryption, and audit physical access logs for sensitive server rooms.
- **Brief security-cleared and government-adjacent staff:** In light of the DOJ domain seizures, alert employees with security clearances or government backgrounds to scrutinize unsolicited "consulting" job offers, especially those sourced via LinkedIn or freelance platforms.
- **Treat unverified mega-leak claims with measured caution:** Avoid overreacting to unconfirmed claims like the TikTok and Wise postings, but monitor credential-stuffing and phishing attempts that may exploit public attention on these stories.

THREAT ACTOR SPOTLIGHT

Miasma Worm Operators (Unattributed)

A self-replicating campaign active since June 1 that has evolved through three distinct waves: malicious npm preinstall hooks, a "Phantom Gyp" technique using binding.gyp files to bypass scanners, and direct credential-harvesting commits to GitHub repositories targeting AI coding agents. A variant of the Mini Shai-Hulud worm released by TeamPCP in mid-May, Miasma has compromised the same contributor account across multiple incidents, suggesting the credential theft itself remains unresolved. Expect continued waves against additional package ecosystems.

Alleged Chinese Intelligence Recruitment Network (Disrupted)

Operating since November 2023 through a network of fake consulting firms, this campaign specifically targeted U.S. security-clearance holders and former government personnel displaced by federal workforce reductions. The operation's use of AI-generated headshots and stolen identities reflects a broader trend of nation-state actors adopting commercial AI tooling for tradecraft. The Five Eyes alliance issued a joint warning about similar job-platform recruitment tactics just one week prior to the takedown.

Sources: Cybernews, Dark Reading, BleepingComputer, TechTimes, The Hacker News, StepSecurity, Phoenix Security, GovInfoSecurity, Help Net Security, Reuters, Nextgov/FCW, dev.ua. This report covers disclosed incidents and law enforcement actions from June 7–13, 2026. Several incidents (Miasma, AUR) began before the reporting window but remained active or escalated during this period. Ongoing investigations may yield updated figures. Prepared by Threat Intelligence Unit — June 16, 2026.