INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-04 19:23 UTC

Ransomware Ecosystem Fragmentation Drives Surge in Victims and Multi-Layered Extortion

THREAT CAMPAIGN | HIGH

SCC Item ID	SCC-CAM-2026-0412
Type	Threat Campaign
Severity	HIGH
Affected Products	Organizations across all sectors; identity infrastructure and credential stores particularly at risk
Published	2026-06-04
Discovery Source	Gemini

Executive Summary

Ransomware groups Qilin and Akira are actively expanding operations following law enforcement disruptions of larger ransomware-as-a-service platforms. These groups combine encryption, data theft, and public exposure threats to maximize pressure on victims, with compromised credentials obtained via infostealer malware serving as the predominant initial access mechanism. Organizations that cannot detect early-stage credential compromise face elevated risk of full ransomware deployment and the compounding liability of data exfiltration.

Technical Analysis

This campaign reflects structural fragmentation in the ransomware ecosystem, not a single CVE-bound vulnerability. Qilin and Akira operate as opportunistic RaaS successors following disruptions to larger platforms. The attack chain follows a consistent pattern: infostealer malware (delivered via phishing, T1566) harvests credentials from browser stores and session tokens (T1005, T1083); compromised valid accounts (T1078) provide initial access without exploiting patched vulnerabilities; lateral movement and data collection precede encryption (T1486); exfiltrated data is staged and exfiltrated (T1041); and financial extortion is applied via multi-layered leverage (T1657). No CVE or CWE is associated with this campaign; the primary attack vector is identity infrastructure, not unpatched software. CVSS/EPSS scoring is not applicable. Defenders should treat credential telemetry and identity anomalies as primary detection surfaces. Detection countermeasures include Local Account Monitoring (per SANS Diamond Model / D3 framework) and System File Analysis, supplemented by NIST AU-6 (Audit Record Review, Analysis, and Reporting) for log review cadence.

Action Checklist

1. Step 1: Containment. Audit all externally exposed authentication surfaces immediately. Enforce MFA on VPN, RDP, cloud consoles, and SSO providers per NIST IA-2 (Authentication) and CIS Benchmarks v8 Control 1. Disable or restrict any accounts flagged with suspicious login activity, particularly those with access to backup infrastructure or privileged consoles.
2. Step 2: Detection. Query your SIEM for indicators of infostealer activity: new processes spawning from browser directories, credential database file access (e.g., Login Data on Chromium-based browsers), and anomalous outbound connections to unknown IPs on ports 443/80 (T1041). Correlate against impossible travel, off-hours logins, and new device enrollments (T1078). Cross-reference user accounts against known infostealer log markets where possible via threat intelligence feeds. Reference NIST AU-6 (Audit Record Review, Analysis, and Reporting) for log review cadence. Apply Local Account Monitoring (D3-LAM per SANS Diamond Model) and System File Analysis (D3-SFA) countermeasures.
3. Step 3: Eradication. Rotate all credentials for accounts where infostealer exposure is confirmed or suspected, prioritizing privileged accounts, service accounts, and accounts with access to backups. Per NIST AC-2 (Account Management) and AC-6 (Least Privilege), revoke excessive permissions identified during investigation. Invalidate all active sessions for affected accounts. Remove any unauthorized persistence mechanisms identified in startup configurations. Apply credential rotation and credential hardening countermeasures per NIST IA-4 (Credential Management).
4. Step 4: Recovery. Validate backup integrity before restoring any encrypted systems; confirm backups are offline or immutable and were not accessible from compromised accounts. Monitor restored systems for re-infection indicators for a minimum of 30 days. Verify MFA enrollment status across all accounts post-recovery. Confirm logging is fully operational per NIST AU-2 (Event Logging) and CIS Benchmarks v8 Control 8 before declaring systems clean.
5. Step 5: Post-Incident. Update incident response playbooks to include infostealer activity as an early-warning indicator preceding ransomware deployment. Formalize identity compromise as a standalone escalation trigger. Review privileged access management gaps per NIST AC-2 (Account Management) and CIS Benchmarks v8 Control 5. Assess separation of duties between backup administrators and general IT staff per NIST AC-5 (Separation of Duties). Document control gaps for GRC tracking against CIS Benchmarks v8 Control 13 (Security Awareness and Skills Training).

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to senior leadership, legal counsel, and cyber insurance carrier if any of the following are confirmed: (1) backup infrastructure was accessed or encrypted by compromised credentials, eliminating clean recovery options; (2) data exfiltration to Qilin or Akira leak site infrastructure is confirmed or suspected, triggering breach notification assessment under applicable regulations (HIPAA, state breach notification laws); (3) more than 10% of privileged accounts show evidence of infostealer credential exposure, indicating systemic identity compromise rather than isolated incident.

Recovery Notes	Do not restore systems from backup until backup integrity is independently verified and the accounts used to access backup infrastructure have been fully rotated and audited — Qilin and Akira affiliates consistently target backup deletion or encryption as a parallel workstream to maximize ransom leverage. Monitor all restored systems for a minimum of 30 days using Sysmon event logging, specifically hunting for the pre-encryption indicator commands (`vssadmin delete shadows`, `wbadmin delete catalog`, `bcdedit /set recoveryenabled no`, and `net stop` targeting backup and AV services) that both groups execute in the final stage before deploying the encryptor. Verify that all accounts re-enabled for production access post-recovery have confirmed MFA enrollment and that no session tokens or Kerberos tickets issued before the credential rotation event remain valid.
Forensic Artifacts	Browser credential store files: %LOCALAPPDATA%\Google\Chrome\User Data\Default\Login Data (SQLite), %APPDATA%\Mozilla\Firefox\Profiles\\logins.json and key4.db — primary targets of RedLine, Vidar, and Raccoon infostealer variants used as Qilin/Akira initial access precursors; preserve originals with hash verification before any remediation | Windows Prefetch directory (C:\Windows\Prefetch\): execution artifacts for infostealer binaries persist here even after deletion, providing binary name, execution count, and last execution timestamp — critical for establishing the initial access timeline in this campaign's infostealer-to-ransomware attack chain | Windows Security Event Log — Event IDs 4624/4625/4648 filtered on Logon Types 3 and 10: documents the attacker's use of stolen credentials for lateral movement and privileged console access following infostealer exfiltration, which is the documented initial access pattern for both Qilin and Akira | Backup software access and job logs (Veeam veeam_backup_and_replication.log, Commvault CommServe logs, Windows Server Backup event logs under Microsoft-Windows-Backup/Operational): Qilin and Akira affiliates prioritize backup destruction or encryption as a parallel workstream — unauthorized access events in these logs confirm backup infrastructure was targeted and directly impacts recovery planning | Network flow records (firewall/proxy logs) showing outbound HTTPS sessions to IPs with no prior organizational history in the 72 hours preceding encryption: documents the data exfiltration stage of double-extortion operations, establishes breach notification scope, and may contain C2 or leak site staging infrastructure IPs attributable to Qilin or Akira based on threat intelligence feeds

Per-Action IR Details

Step 1: Containment — Audit all externally exposed authentication surfaces immediately. Enforce MFA on VPN, RDP, cloud consoles, and SSO providers per CIS 6.3 (Require MFA for Externally-Exposed Applications) and CIS 6.4 (Require MFA for Remote Network Access). Disable or restrict any accounts flagged with suspicious login activity, particularly those with access to backup infrastructure or privileged consoles.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.4 (Require MFA for Remote Network Access), CIS 6.2 (Establish an Access Revoking Process), NIST AC-17 (Remote Access), NIST AC-7 (Unsuccessful Logon Attempts)

Compensating: Without enterprise IAM tooling, run the following PowerShell one-liner against Active Directory to enumerate accounts with no MFA claim and active VPN/RDP access: `Get-ADUser -Filter {Enabled -eq $true} -Properties LastLogonDate,MemberOf | Where-Object {$_.MemberOf -match 'VPN|RDP'}`. For Azure/M365 tenants without Conditional Access, use the free Microsoft Entra ID (formerly Azure AD) sign-in logs via the Azure Portal — filter on 'Authentication requirement: Single-factor' and cross-reference with risky sign-in alerts. Immediately disable identified accounts via `Disable-ADAccount -Identity ` and force password reset via `Set-ADAccountPassword`.

Evidence: Before disabling accounts, capture the following: (1) Active Directory Security Event Log — Event ID 4624 (successful logon) and 4625 (failed logon) filtered on Logon Type 3 (network) and Type 10 (RemoteInteractive/RDP) for the past 30 days, focusing on accounts with access to backup infrastructure; (2) VPN authentication logs from your concentrator (Cisco ASA, Fortinet, Palo Alto) showing source IPs, timestamps, and user-agent strings — Qilin and Akira initial access frequently originates from residential proxy or VPN exit node IPs inconsistent with the user's normal geography; (3) Microsoft Entra ID or on-prem ADFS sign-in logs showing device registration events (new device fingerprints) and impossible travel flags for accounts with backup console or privileged access; (4) Cloud console access logs (AWS CloudTrail, Azure Activity Log, GCP Audit Log) for IAM role assumption or console login events from unfamiliar source IPs in the 14 days prior to detection.

Step 2: Detection — Query your SIEM for indicators of infostealer activity: new processes spawning from browser directories, credential database file access (e.g., Login Data on Chromium-based browsers), and anomalous outbound connections to unknown IPs on ports 443/80 (T1041). Correlate against impossible travel, off-hours logins, and new device enrollments (T1078). Cross-reference user accounts against known infostealer log markets where possible via threat intelligence feeds. Reference NIST AU-6 (Audit Record Review, Analysis, and Reporting) for log review cadence. Apply D3-LAM (Local Account Monitoring) and D3-SFA (System File Analysis) countermeasures.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AU-2 (Event Logging), NIST AU-12 (Audit Record Generation), CIS 8.2 (Collect Audit Logs)

Compensating: Deploy Sysmon with SwiftOnSecurity's config (github.com/SwiftOnSecurity/sysmon-config — verify URL before use) and hunt for: Event ID 1 (Process Create) where ParentImage matches `*\chrome.exe`, `*\msedge.exe`, or `*\firefox.exe` and the child process is `cmd.exe`, `powershell.exe`, or any binary outside `C:\Program Files`; Event ID 11 (File Created) targeting `%LOCALAPPDATA%\Google\Chrome\User Data\Default\Login Data` or `%APPDATA%\Mozilla\Firefox\Profiles\*.default\logins.json`; Event ID 3 (Network Connect) from browser-directory parent processes to external IPs. For a 2-person team without SIEM, use `Get-WinEvent -LogName Microsoft-Windows-Sysmon/Operational | Where-Object {$_.Id -eq 11 -and $_.Message -match 'Login Data'}` on endpoints of concern. Cross-reference outbound connections using Wireshark captures on egress points, filtering `tcp.port == 443 and ip.dst != `.

Evidence: Capture before analysis concludes: (1) Browser credential store files — `%LOCALAPPDATA%\Google\Chrome\User Data\Default\Login Data` (SQLite, contains encrypted credentials), `%APPDATA%\Mozilla\Firefox\Profiles\\logins.json` and `key4.db` — hash and preserve originals before any remediation; (2) Sysmon Event ID 1 and 11 logs from all endpoints showing access to browser profile directories within the suspected compromise window — infostealers such as those associated with Qilin/Akira precursor access (RedLine, Vidar, Raccoon variants) characteristically read these files and exfiltrate within minutes; (3) Windows Prefetch files (`C:\Windows\Prefetch\`) for execution evidence of infostealer binaries — prefetch entries persist up to 128 most-recently-used executables and will show the stealer binary name and execution timestamp even after deletion; (4) Network flow data (NetFlow, firewall logs) showing outbound HTTPS connections to IPs with no prior history in your environment, particularly short-duration high-data-volume sessions consistent with credential dump exfiltration; (5) Memory image (via WinPmem or Magnet RAM Capture) from any endpoint suspected of active infostealer execution — stealer malware frequently operates in-memory and decrypted credential material may only exist in RAM.

Step 3: Eradication — Rotate all credentials for accounts where infostealer exposure is confirmed or suspected, prioritizing privileged accounts, service accounts, and accounts with access to backups. Per NIST AC-6 (Least Privilege), revoke excessive permissions identified during investigation. Invalidate all active sessions for affected accounts. Remove any unauthorized persistence mechanisms identified in startup configurations (D3-SICA). Apply D3-CRO (Credential Rotation) and D3-CH (Credential Hardening) countermeasures.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-6 (Least Privilege), NIST AC-2 (Account Management), NIST AC-3 (Access Enforcement), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 5.2 (Use Unique Passwords), CIS 5.3 (Disable Dormant Accounts), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts)

Compensating: For credential rotation at scale without a PAM tool: use `Get-ADUser -Filter * -Properties PasswordLastSet,MemberOf | Where-Object {$_.MemberOf -match 'Backup|Domain Admins|Enterprise Admins'}` to identify privileged accounts requiring immediate rotation; force rotation via `Set-ADAccountPassword -Identity -Reset -NewPassword (ConvertTo-SecureString -AsPlainText '' -Force)` followed by `Set-ADUser -Identity -ChangePasswordAtLogon $true`. For service accounts, enumerate with `Get-ADServiceAccount -Filter *` and manually rotate secrets in dependent services. Invalidate Kerberos tickets by running `klist purge` on affected endpoints and resetting the KRBTGT account password twice (spaced 10 hours apart) if domain admin compromise is suspected. For startup persistence, audit `HKCU\Software\Microsoft\Windows\CurrentVersion\Run`, `HKLM\Software\Microsoft\Windows\CurrentVersion\Run`, and `C:\Users\\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup` using `reg query` and manual directory inspection on all endpoints accessed by compromised accounts.

Evidence: Before rotating credentials or removing persistence, preserve: (1) Registry exports of all Run/RunOnce keys from HKCU and HKLM on compromised endpoints — Qilin and Akira affiliates frequently install lightweight persistence (scheduled tasks, registry run keys) during the dwell period between initial infostealer access and ransomware deployment; (2) Scheduled task XML exports via `schtasks /query /xml` — look for tasks created within the infostealer access window that execute from `%TEMP%`, `%APPDATA%`, or user-writable paths; (3) Active Directory replication metadata (`repadmin /showattr * dc= /filter:(whenChanged>=) /subtree /atts:pwdLastSet,adminCount`) to identify accounts whose passwords were recently changed by the attacker to maintain access; (4) Service account usage logs — Windows Security Event ID 4769 (Kerberos Service Ticket) filtered on service accounts with backup or administrative SPNs, which may indicate pass-the-ticket or Kerberoasting activity used to escalate from initial infostealer credentials toward backup infrastructure access.

Step 4: Recovery — Validate backup integrity before restoring any encrypted systems; confirm backups are offline or immutable and were not accessible from compromised accounts. Monitor restored systems for re-infection indicators for a minimum of 30 days. Verify MFA enrollment status across all accounts post-recovery. Confirm logging is fully operational per NIST AU-2 (Event Logging) and CIS 8.2 (Collect Audit Logs) before declaring systems clean.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-2 (Event Logging), NIST AU-11 (Audit Record Retention), NIST AU-4 (Audit Storage Capacity), NIST AC-3 (Access Enforcement), CIS 8.2 (Collect Audit Logs), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: Before restoring from backup, verify backup integrity without relying on the backup software itself — if backup agent credentials were exposed to infostealer exfiltration, the backup console may be compromised. For Veeam, use the Veeam Backup Validator standalone utility offline; for Windows Server Backup, mount the VHD in a clean VM and run `sfc /scannow` against the mounted volume. To confirm immutability, verify object lock status on S3-compatible targets via AWS CLI: `aws s3api get-object-lock-configuration --bucket `. Post-restore, deploy Sysmon on all recovered systems immediately and monitor for Event ID 1 (Process Create) matching known Qilin/Akira execution patterns — lateral movement tools (e.g., `PsExec`, `wmic`, `cobalt strike beacon` artifacts) and encryption staging activity (`vssadmin delete shadows`, `wbadmin delete catalog`, `bcdedit /set recoveryenabled no`) which are consistently observed in Qilin and Akira pre-encryption phases.

Evidence: Before beginning restore operations, capture and preserve: (1) VSS snapshot inventory via `vssadmin list shadows` on all affected systems — Qilin and Akira both execute VSS deletion commands as a pre-encryption step; any surviving shadow copies confirm the attack timeline and represent potential recovery points; (2) Backup software access logs (Veeam, Commvault, Backup Exec) filtered on logon events and job execution during the suspected compromise window — if backup jobs were modified, deleted, or accessed from compromised account credentials, this confirms backup infrastructure was targeted; (3) File system metadata (MAC times) on encrypted files to establish the precise encryption start time and confirm whether backup access preceded or followed encryption; (4) Network

segmentation validation — confirm via firewall rule audit whether backup server interfaces were accessible from endpoints where compromised credentials were used, establishing the blast radius of potential backup compromise.

Step 5: Post-Incident — Update incident response playbooks to include infostealer activity as an early-warning indicator preceding ransomware deployment. Formalize identity compromise as a standalone escalation trigger. Review privileged access management gaps per NIST AC-2 (Account Management) and CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts). Assess separation of duties between backup administrators and general IT staff per NIST AC-5 (Separation of Duties). Document control gaps for GRC tracking against CIS 7.1 (Establish and Maintain a Vulnerability Management Process).

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: NIST AC-2 (Account Management), NIST AC-5 (Separation Of Duties), NIST AC-6 (Least Privilege), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 6.5 (Require MFA for Administrative Access)

Compensating: For a 2-person team producing GRC-grade post-incident documentation without a GRC platform: document control gaps in a structured spreadsheet mapping each gap to the control ID, the observed deficiency, the affected asset, and the planned remediation date — this satisfies the intent of CIS 7.1 and CIS 7.2 for organizations without enterprise tooling. For playbook updates, publish infostealer detection logic as Sigma rules (yaml format, free, integrates with any log tool) targeting the browser credential access and suspicious child process patterns identified during this investigation — commit to a Git repository for version control. For separation of duties assessment, generate an AD group membership report (`Get-ADGroupMember -Identity 'Backup Operators' -Recursive` and `Get-ADGroupMember -Identity 'Domain Admins' -Recursive`) and flag any account appearing in both — this is the primary structural gap exploited in Qilin/Akira campaigns where backup access and IT admin access overlap.

Evidence: The post-incident documentation package for this campaign type must include: (1) Full timeline reconstruction from first infostealer execution (via Prefetch/Sysmon) through credential exfiltration, lateral movement, backup access, and encryption — this is specifically required for cyber insurance claims and regulatory breach notifications triggered by Qilin/Akira double-extortion data theft; (2) Evidence of data exfiltration scope — network flow records showing volume and destination of outbound transfers prior to encryption, needed to assess whether breach notification obligations are triggered under applicable regulations (HIPAA, state breach notification statutes); (3) Attacker tooling artifacts (dropped binaries, PowerShell transcript logs, `C:\Windows\Temp` and `%APPDATA%` contents from compromised endpoints) preserved as forensic images for potential law enforcement referral, given active FBI/CISA advisories on Akira and Qilin; (4) Lessons-learned documentation specifically addressing the infostealer-to-ransomware dwell time observed — this metric directly informs the updated detection SLA in the revised IR playbook.

Detection Guidance

Primary detection surface is identity and credential telemetry, not network signatures. Key indicators: (1) Infostealer behavior, file read events targeting browser credential stores (e.g., '%LOCALAPPDATA%\Google\Chrome\User Data\Default\Login Data'), credential dumping from memory, and short-lived outbound HTTPS sessions to newly registered or uncategorized domains. (2) Valid account abuse (T1078), logins from new ASNs or geographies, off-hours access to privileged systems, lateral movement via legitimate remote management tools (RDP, WMI, PSExec). (3) Data staging and exfiltration (T1041, T1005), large archive creation (7z, zip, rar) in temp directories, bulk file enumeration (T1083), and sustained outbound data transfers to cloud storage endpoints or unfamiliar IPs. (4) Pre-encryption signals, shadow copy deletion commands (vssadmin delete shadows), Windows event ID 7045 (new service installation), and scheduled task creation by non-standard accounts. Apply Local Account Monitoring (D3-LAM per SANS Diamond Model Application Framework) for account anomaly correlation. NIST AU-6 and AU-12 govern the log review and

generation requirements supporting these detections. Readers should cross-reference these TTPs against primary threat intelligence sources from law enforcement or dedicated threat intelligence vendors (CISA, Mandiant, CrowdStrike) before high-confidence attribution.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`no confirmed IOCs available in source data`	Source data for this item is rated T3 quality; no specific IOC values were provided. Obtain current Qilin and Akira IOCs from ISAC feeds, CISA advisories, or vetted threat intelligence platforms before ingesting into detection tools.	LOW

Framework Mappings

MITRE-ATTACK

- **T1657** — Financial Theft
- **T1005** — Data from Local System
- **T1566** — Phishing
- **T1486** — Data Encrypted for Impact
- **T1083** — File and Directory Discovery
- **T1078** — Valid Accounts
- **T1041** — Exfiltration Over C2 Channel

NIST-800-53R5

- **AT-2** — Literacy Training and Awareness
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-8** — Spam Protection
- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **IR-4** — Incident Handling
- **SC-13** — Cryptographic Protection

NIST-CSF-2

- **RS.MI-01** — Incidents are contained
- **DE.CM-01** — Networks and network services are monitored

HIPAA-SECURITY

- **164.308(a)(7)(ii)(A)** — Data Backup Plan
- **164.312(d)** — Person or Entity Authentication
- **164.308(a)(6)(ii)** — Response and Reporting
- **164.312(e)(1)** — Transmission Security

ISO-27001-2022

- **A.5.29** — Information security during disruption
- **A.5.34** — Privacy and protection of personal information
- **A.8.24** — Use of cryptography

CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications
- **8.2** — Collect Audit Logs

SOC2-TSC

- **CC6.1** — Logical access security software, infrastructure, and architectures
- **CC7.4** — Responds to identified security incidents

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1657	Financial Theft	Impact
T1005	Data from Local System	Collection
T1566	Phishing	Initial-Access
T1486	Data Encrypted for Impact	Impact
T1083	File and Directory Discovery	Discovery
T1078	Valid Accounts	Defense-Evasion
T1041	Exfiltration Over C2 Channel	Exfiltration

Sources

Source	URL	Tier
gemini	https://securityboulevard.com/2026/06/fragmentation-extortion-the-n...	T3

Source	URL	Tier
6 Vulnerability Types Your Organization Must Address - Swimlane	https://swimlane.com/blog/vulnerability-types/	T3
Cyber Security Vulnerabilities: Prevention & Mitigation - SentinelOne	https://www.sentinelone.com/cybersecurity-101/cybersecurity/cyber-s...	T3
What Is a Security Vulnerability? Definition, Types, and How They're ...	https://www.picussecurity.com/resource/glossary/what-is-a-security-...	T3
CVE Trends by Industry Sector | Bitsight Research	https://www.bitsight.com/blog/cve-trends-by-sector	T3

Generated 2026-06-04 19:23 UTC by TJS Security Command Center