Cybersecurity Briefing: May 19-26, 2026 — Supply Chain Compromise Crisis Week

May 26, 2026

Contents

What Happened This Week (And Why It Matters)

The week of May 19-26, 2026 was the most consequential for software supply-chain attacks in recorded history. Three simultaneous attack campaigns—each targeting different layers of the developer ecosystem—exposed fundamental architectural weaknesses in how we build and ship software. A poisoned VS Code extension breached GitHub's internal repository vault. A self-propagating npm worm with fraudulent build provenance infected 520 million downstream packages in the span of hours. And a coordinated GitHub Actions workflow attack compromised 5,561 repositories' CI/CD systems in a single 6-hour window. Together, these incidents demonstrate that IDE extensions, build attestations, and CI/CD workflows—the tools developers trust most—have become the primary attack surface for adversaries with financial resources.

If your organization uses npm, PyPI, GitHub, or developer IDEs, assume you've been exposed. The blast radius of this week's incidents spans billions of end-users across education, finance, healthcare, and software sectors. The Canvas breach alone affected 275 million students and faculty. The TanStack worm reached every developer who installed any of 520 million packages in a 12-hour window. And the CISA AWS GovCloud credential leak exposed the infrastructure code and deployment keys for US federal cybersecurity operations.

Beyond supply-chain chaos, federal agencies now have a June 4 deadline to patch 10 newly critical vulnerabilities actively exploited in the wild—including a Microsoft Defender flaw (CVSS 7.8) that grants SYSTEM access, a Drupal SQL injection seeing 15,000+ attack attempts per day, and a LiteSpeed cPanel plugin with a perfect CVSS 10.0 score. This briefing covers the incidents you must action in the next 72 hours, the vulnerabilities requiring emergency patching before the federal deadline, and the threat actors whose credentials and malware you're now fighting across your estate.

Major Breaches & Incidents (May 19-26, 2026)

GitHub Internal Repository Breach via Poisoned Nx Console Extension (May 18-20)

The Attack: On May 18, 2026, a threat actor modified the Nx Console VS Code extension (maintained by Nrwl) after compromising the Nx developer's GitHub credentials via the TanStack npm supply-chain incident. The malicious version (18.95.0) was published to the VS Code Marketplace at 12:36 UTC and remained available for 11 minutes before automated detection removed it. During that window and the subsequent 36 minutes on OpenVSX, the extension was installed 2.2 million times. More critically, 6,000 instances of the extension activated within 72 hours—enough to exfiltrate credentials from a meaningful number of developer workstations. [7] [11] [27] [40]

What the Malware Did: The extension's obfuscated index.js file (498 KB) deployed six parallel credential collectors targeting: GitHub tokens (including gh CLI credentials), npm authentication tokens, AWS IMDS and Secrets Manager, GCP service account credentials, Kubernetes secrets, HashiCorp Vault, SSH private keys, 1Password vaults, and a particularly sensitive target—Claude Code configuration files stored in ~/.claude/settings.json. The payload included a sophisticated technique for bypassing GitHub Actions secret masking: pattern-matching against /proc/*/mem (process memory) to extract unmasked runner credentials. Exfiltration used encrypted HTTPS tunnels (double-encrypted AES-256-GCM + RSA-OAEP) with fallback to DNS tunneling. [40]

Direct Consequence: The stolen GitHub credentials enabled the attacker to run GitHub Actions workflows with elevated permissions, leading directly to the compromise of 3,800 internal GitHub repositories (detailed below). The stolen credentials also cascaded into a secondary compromise of Grafana Labs' GitHub repositories. [26]

Ransom & Attribution: The threat actor, tracked as TeamPCP (also called UNC6780), demanded $50,000+ USD for the exfiltrated internal repository data, posted to underground forums on May 20. [19]

GitHub Internal Repositories (3,800 Repos Exfiltrated)

Scale & Timeline: Between May 18-20, 2026, TeamPCP gained unauthorized access to approximately **3,800 internal GitHub repositories** containing sensitive source code, documentation, and infrastructure configurations. GitHub discovered the compromise on May 19 when monitoring detected unusual access patterns on an employee workstation. The company publicly disclosed the breach on May 20 via official statements. [18] [22] [26] [27]

Root Cause Chain: The attack chain was: TanStack npm worm (May 11) → Nx developer infected → GitHub credentials stolen → Nx Console extension modified → VS Code extension malware distributed → more developer credentials harvested → GitHub Actions credentials leaked → internal repositories accessed via workflow permissions. This represents a "privilege escalation across trust boundaries" where each compromised component provided access to a higher-privilege system. [7] [40]

Aftermath & Remediation: GitHub responded by rotating critical secrets, implementing endpoint isolation, and offering security brief to customers. The company confirmed that this incident was separate from (but enabled) the later Grafana GitHub breach. No evidence of production customer data access was discovered, but GitHub's own internal secrets and source code remain in the attacker's hands. [18] [27]

TanStack npm Supply-Chain Worm: SLSA Provenance Breakthrough (May 11, Cascading May 19-26)

The Exploit: On May 11, 2026, at 19:20 UTC, a threat actor executed a three-step GitHub Actions exploitation chain against the TanStack/router repository. Step 1: Create a fork with pull_request_target workflow access, poisoning the pnpm package store cached across the fork-to-base trust boundary. Step 2: Inject malicious binaries into the cache designed to extract OIDC tokens from the GitHub Actions runner's process memory. Step 3: Exchange the harvested OIDC token (auto-generated with id-token: write permissions) for npm federation credentials via npm's official endpoint (/-/npm/v1/oidc/token/exchange/package/), then publish malicious npm packages using those credentials. [9] [38]

Historic First: Valid SLSA Build Level 3 Attestations on Malicious Packages [9] [38]

Because the attack exploited GitHub Actions itself, the attacker's packages included **legitimate SLSA Build Level 3 provenance attestations signed by GitHub's Sigstore integration**. Every malicious package carried a valid cryptographic certificate proving it was built by GitHub's official runners. This is the first documented supply-chain attack where the malicious artifact includes authentic supply-chain provenance—undermining SLSA as a sole security signal for package safety. Organizations relying on "valid SLSA provenance = trustworthy package" are now at risk.

Scale & Self-Propagation: The attack published 84 malicious versions across 42 @tanstack/* packages in the first 6 minutes. But the worm didn't stop at direct victims: once installed, TanStack packages executed hooks that ran the credential-harvesting payload, stealing npm federation credentials from developer machines and using those credentials to poison downstream packages. By end-of-day May 11, the worm had spread to **373 malicious versions across 169 npm + PyPI packages**, affecting: [8] [9] [28]

- @uipath/* namespace (40+ packages)
- @mistralai/mistralai and variant (@mistralai/azure, @mistralai/gcp)

- @squawk aviation data ecosystem (19 packages)
- guardrails-ai (PyPI equivalent, 15+ versions)
- intercom-client, @tallyui, @draftlab, @beproduct, @mesadev

Estimated Exposure: @tanstack/react-router alone receives 12.7 million downloads weekly. Conservative estimate: **520 million cumulative downloads** of affected packages during the active exploitation window (May 11-12). [9]

Malicious Payload Details: A 2.3 MB obfuscated router_init.js file injected into package dependencies executed six credential-harvesting collectors: AWS IMDS/Secrets Manager, GCP metadata, Kubernetes SA tokens, Vault, .npmrc files, GitHub tokens (deliberately skipping github_token to evade secret scanning), SSH private keys, and decentralized messenger network tokens (Session). Exfiltration occurred to: Session network endpoints (filev2.getsession.org, seed1-3.getsession.org), git-tanstack.com, api.masscan.cloud, litter.catbox.moe, and Ox Cargo network. [9] [38]

Dead-Man's-Switch Persistence: The payload included a gh-token-monitor daemon that polled GitHub every 60 seconds. If the daemon detected that the stolen GitHub token had been revoked (HTTP 40x response), it executed `rm -rf ~/` **wiping the entire home directory of the infected developer's machine**. This mechanism was designed to persist even after token revocation—forcing organizations to clean up machines rather than simply rotating credentials. [9]

Detection & Response Speed: External security researchers detected the attack within 20-26 minutes of initial payload publication. TanStack maintainers deprecated malicious versions within 1 hour. npm removed the malicious package tarballs from mirrors by evening May 11. But because self-propagating worms had already stolen downstream developer credentials, secondary waves of poisoning continued May 12-19. [9]

CVE Assignment: CVE-2026-45321 (CVSS 9.6, VPR 9.2) describing the GitHub Actions exploitation. As of May 22, this CVE is **not** in the CISA Known Exploited Vulnerabilities catalog, a gap requiring immediate attention given active exploitation at scale. [8] [38]

Sources: [7] [8] [9] [28] [38]

Megalodon GitHub Actions CI/CD Attack: 5,561 Repositories in 6 Hours (May 18)

The Attack: Between 11:36 a.m. and 5:48 p.m. UTC on May 18, 2026, a threat actor systematically compromised 5,561 GitHub repositories by injecting malicious base64-encoded bash payloads into .github/workflows/ YAML files. The attacker used throwaway GitHub accounts with randomly generated usernames (rkb8el9r, bhlru9lr, lo6wt4t6, etc.), rotated author identities to evade detection, and used workflow_dispatch triggers instead of on: push to minimize automation pipeline exposure. [23] [39]

Attribution & Root Cause: Hudson Rock's forensic analysis (published May 23) traced the attack to **commodity infostealer infections**. Specifically, 33% of unique GitHub account usernames used in the Megalodon attacks (331 of 978 accounts) were directly matched to computers infected with Redline, Vidar, Raccoon, or related infostealers. The attackers had stolen GitHub credentials from malware-infected developer machines, then used those credentials en masse to compromise public repositories. [23]

Payload & Exfiltration: The malicious workflow payloads harvested: environment variables (28+ types), AWS CLI profiles, GCP service account tokens, Azure credentials, source file grep patterns for hardcoded passwords (150 file types, 29 patterns), and OIDC token generation to query cloud metadata services (AWS IMDS, GCP metadata, Azure IMDS). All exfiltration occurred to C2 infrastructure at 216.126.225.129:8443 with campaign identifier "megalodon". Zero-disk execution ensured in-memory decode without disk artifacts. [39]

Scope Verification: GitHub code search on the malicious base64 prefix (Q0I9Imh0dHA6Ly8yMTYu) returned 3,500+ infected YAML files. OX Security and other independent researchers confirmed 5,000+ total repositories compromised. The attack demonstrated that infostealer-infected developer credentials are sufficient to achieve CI/CD pipeline compromise at scale. [23] [39]

Sources: [23] [24] [39]

Mini Shai-Hulud @antv Ecosystem Wave: 639 Packages in 1 Hour (May 19)

Scale & Timing: At 01:56 UTC on May 19, 2026, attackers published malicious packages using a compromised npm maintainer account. At 02:06 UTC (10 minutes later), a second coordinated wave followed. Together, **639 malicious package versions were published in 1 hour across 323 unique packages**—the largest single-hour poisoning spike of any Shai-Hulud variant to date. [12] [28]

Compromised Account & Target Ecosystem: The attacker controlled the npm account "atool" (email: i@hust.cc), which maintained 100+ packages. The target was Alibaba's @antv data visualization ecosystem (g2, g6, x6, l7, s2, f2, g, g2plot, graphin, data-set, s2-vue)—widely used in charting and analytics applications. Secondary targets included: echarts-for-react (~1.1M weekly downloads), timeago.js, size-sensor, canvas-nest.js. [12] [28]

Payload Evolution: Wave 1 used preinstall hooks with `bun run index.js` (assuming Bun runtime installed). Wave 2 added Bun as an explicit dependency to ensure execution across environments without pre-installed runtimes. This evolution shows attacker adaptation within a 10-minute window. [12]

Credential Harvesting Scope: The 499 KB obfuscated payload ran six parallel collectors targeting GitHub tokens, npm tokens, SSH keys, Git credentials, AWS IMDS, Kubernetes SA tokens, HashiCorp Vault, Docker auth configs, CI/CD platform credentials (18+ types), browser cookies/sessions, and environment variables. Exfiltration to attacker-controlled infrastructure occurred via encrypted channels. [28]

Sources: [12] [28]

CISA AWS GovCloud Credentials Leak: 844 MB of Federal Secrets (May 15-18)

Exposure Details: On May 14, 2026, GitGuardian security researcher Guillaume Valadon discovered a publicly accessible GitHub repository titled "Private-CISA" containing **844 MB of sensitive federal data**—498 MB of active content plus Git history dating to November 13, 2025. The repository had been public for approximately 6 months. [20] [25]

Credentials Exposed: AWS GovCloud administrative credentials (3 servers with plaintext passwords), GitHub personal access tokens, Kubernetes kubeconfig files, Entra ID SAML certificates for Azure federation, Artifactory credentials, SSH private keys, and internal service account passwords stored in CSV format. Operational files included: CI/CD build logs, GitHub Actions automation code, Terraform infrastructure-as-code, ArgoCD deployment manifests, and OneNote/docx backups of internal documentation. [20] [25] [37]

Critical Finding on Repository Owner Conduct: The repository owner **deliberately disabled GitHub's automatic credential detection feature** (commit logs show explicit disable commands). GitHub's default configuration blocks SSH keys and secrets in public repositories; this setting was intentionally overridden. [20] [37]

Blast Radius of Leaked RSA Key: The leaked RSA private key granted full control of a GitHub App installed on the CISA-IT organization with unrestricted repository access. This enabled: read access to all CISA source code, registration of rogue CI/CD runners, pipeline hijacking, extraction of repository secrets, and modification of branch protection rules. [25]

Detection & Response Timeline:

- May 14, 4:14 PM CET: GitGuardian researcher reports to CERT/CC
- May 15, afternoon: CISA directly notified
- May 15, ~6:00 PM EST: Repository owner takes offline (~26 hours after detection)
- May 22 (7+ days later): CISA still invalidating and replacing exposed credentials [20]

Congressional Response: Rep. Bennie Thompson and Sen. Maggie Hassan issued formal demands for answers, citing diminished CISA security culture following recent reorganization that resulted in 1/3 workforce loss. The incident reflects systemic governance failures, not isolated human error. [20]

Quote from Researcher: GitGuardian's Valadon stated: "I honestly believed that it was all fake before analyzing the content deeper. This is indeed the worst leak that I've witnessed in my career." [37]

Sources: [20] [25] [37]

Instructure Canvas Recompromise: 275 Million Students Exposed (May 1 & May 7)

Initial Breach & False Containment: On May 1, 2026, Instructure (Canvas learning management system) suffered a data breach. The company claimed containment by May 2. On May 7, 2026, the same attacker recompromised the system, publishing extortion demands on Canvas login pages—proving the May 2 containment claim was false. [20]

Scale: Canvas serves ~9,000 educational institutions with ~275 million students and faculty. Total data exposure: 3.65 terabytes. [20] [34]

Attack Pattern (8-Month Campaign): Security researcher Dipan Mann (Cloudskope) documented an 8-month campaign: September 2025 University of Pennsylvania Canvas access (proof-of-concept), May 1 production compromise, May 7 recompromise demonstrating failed remediation. [20]

Attribution & Ransom: ShinyHunters claimed responsibility. Ransom demands cited "several billion private messages, names, phone numbers, email addresses." Extortion deadlines were set for May 6, then extended to May 12. The attacker removed Canvas data from their leak site post-deadline, suggesting either payment or negotiation. [20] [34]

Sources: [20] [34]

Incident Summary Table: Major Breaches & Incidents (May 19-

26, 2026)

Date	Organization/Category	Incident	Blast Radius	Immediate Action
May 18-20	GitHub (Internal)	3,800 internal repositories exfiltrated via Nx Console VS Code extension malware (TeamPCP)	Internal source code, secrets, infrastructure configs exposed; downstream Grafana breach enabled	Rotate all GitHub tokens; audit workflow files for malicious commits; check for gh-token-monitor daemon
May 11 (cascade May 19-26)	TanStack (npm/PyPI)	Self-propagating worm with valid SLSA provenance attestations; 373 malicious versions across 169 packages; credential-harvesting payloads [9] [38]	520M cumulative package downloads; 40+ @uipath, 15+ Mistral, 19+ Squawk, 40+ other ecosystem packages poisoned	Audit npm lockfiles for May 11-12 @tanstack/, *@mistralai/*, @uipath/*, intercom-client; revoke developer credentials; rebuild from last known-good baseline
May 18	GitHub (Public Repos)	Megalodon: 5,718 malicious commits to 5,561 repositories in 6-hour window via CI/CD workflow injection; root cause: infostealer-infected developer credentials	CI secrets and cloud credentials harvested at scale; attributed to 33% infostealer-linked machines	Block C2 216.126.225.129:8443; scan for infostealer infections (Redline, Vidar, Raccoon); check GitHub Actions logs for workflow_dispatch triggers
May 19	npm (@antv ecosystem)	Mini Shai-Hulud: 639 malicious package versions in 1 hour (record) across @antv data visualization, echarts-for-react, timeago.js, size-sensor	1.1M+ weekly downloads (echarts-for-react); credential harvesting via package install hooks	Audit lockfiles for @antv/*, echarts-for-react, timeago.js, size-sensor, canvas-nest.js published May 19; remove and rebuild
May 15-18	CISA (AWS GovCloud)	844 MB public GitHub repo "Private-CISA" exposed: AWS credentials, Kubernetes configs, SAML	Compromised AWS GovCloud access; CI/CD pipeline control; federal infrastructure-as-code; CISA	Audit AWS GovCloud CloudTrail logs May 15-22 for unauthorized access; rotate all exposed AWS keys, GitHub

Date	Organization/Category	Incident	Blast Radius	Immediate Action
		certs, Terraform code, build logs; exposed for ~6 months	remediation still ongoing May 22	App credentials, Kubernetes tokens
May 1 & May 7	Instructure (Canvas)	Recompromise proving May 2 containment false; ShinyHunters ransomware double-extortion	275M students/faculty; 9,000 institutions; 3.65TB data; ransom deadline extended to May 12	Assume Canvas credentials compromised; force password reset for all users; audit Learning Analytics for suspicious data exports
May 20-22	CISA (KEV Catalog)	10 vulnerabilities added to Known Exploited Vulnerabilities with June 4 federal deadline: Microsoft Defender (CVE-2026-41091, -45498), Langflow, Trend Micro Apex, Drupal, legacy Windows/IE/Adobe CVEs	Federal agencies must patch by June 4; CVE-2026-41091 (CVSS 7.8) grants SYSTEM; Drupal (CVSS 6.5) seeing 15,000+ attacks/48hr	Prioritize Microsoft Defender engine/platform updates; patch Drupal Core immediately (versions 10.4.10, 10.5.10, 10.6.9, 11.1.10, 11.2.12, 11.3.10)

Exploited Vulnerabilities: Active Exploitation & Urgent Patches

CISA KEV Catalog Additions (May 20-22): 10 Vulnerabilities with June 4 Federal Deadline

Highest Priority (Active Exploitation Confirmed):

CVE-2026-41091 (Microsoft Defender) — CVSS 7.8, Privilege Escalation → SYSTEM Access

- Affected: Malware Protection Engine versions 1.1.26030.3008 through 1.1.26040.7; Antimalware Platform 4.18.26030.3011 through 4.18.26040.6
- Fixed: Engine 1.1.26040.8+; Platform 4.18.26040.7+
- Exploitation: RedSun variant actively exploiting in the wild; privilege escalation to SYSTEM-level access on Windows endpoints
- Remediation: Deploy patched Malware Protection Engine 1.1.26040.8 via Windows Update (automatic) or Microsoft Defender antimalware updates. Verify engine version: `mpcmdrun.exe -version` [1] [15] [4]

CVE-2026-45498 (Microsoft Defender) — CVSS 4.0/7.5, Denial of Service

- Same version ranges as CVE-2026-41091
- Exploitation: UnDefend variant actively exploiting; causes Defender crashes/hangs
- Remediation: Same as CVE-2026-41091; deploy Engine 1.1.26040.8+. No separate patch. [1] [15] [4]

CVE-2026-9082 (Drupal Core SQL Injection) — CVSS 6.5, Unauthenticated SQL Injection

- All supported Drupal Core versions affected
- Exploitation: **15,000+ attack attempts within 48 hours of patch release on 6,000 sites** (Imperva, May 20)
- Exploitation tools already available; reconnaissance + data extraction/privilege escalation capability confirmed
- Affected versions: 10.x, 10.5.x, 10.6.x, 11.1.x, 11.2.x, 11.3.x
- Fixed versions: 10.4.10, 10.5.10, 10.6.9, 11.1.10, 11.2.12, 11.3.10
- **Deadline: May 27, 2026** (7 days from KEV addition)
- Remediation: Update Drupal Core immediately via composer or security update mechanism. Verify: `drush status | grep "Drupal version"` [5] [16] [17] [32]

CVE-2025-34291 (Langflow) — Origin Validation Error, RCE

- Unauthenticated cross-origin RCE via overly permissive CORS + SameSite=None refresh token cookie
- Affected: Langflow versions prior to 1.9.3
- Remediation: Update to v1.9.3+ or disable CORS if not required. Check: `pip show langflow | grep Version` [1] [2]

CVE-2026-34926 (Trend Micro Apex One) — Directory Traversal

- On-premises version directory traversal via update mechanism
- Trend Micro patches available
- Remediation: Update Apex One via Trend Micro Security Console [1] [3]

Legacy Windows/IE/Adobe Vulnerabilities (Low Remediation Urgency for Modern Infrastructure):

- CVE-2010-0249, CVE-2010-0806 (IE use-after-free, end-of-life products)
- CVE-2008-4250 (Windows RPC buffer overflow, legacy)
- CVE-2009-1537 (DirectX NULL byte, legacy)
- CVE-2009-3459 (Adobe Reader buffer overflow)

NOT in CISA KEV but Actively Exploited:

CVE-2026-45321 (TanStack GitHub Actions Exploitation) — CVSS 9.6

- Described above; not added to KEV as of May 22, despite widespread exploitation
- Organizations should treat as equivalent to KEV-level urgency [8] [38]

Additional Critical Vulnerabilities in Active Exploitation

LiteSpeed User-End cPanel Plugin CVE-2026-48172 — CVSS 10.0 (Perfect Score)

- **Any cPanel user can execute arbitrary scripts with root privileges**
- Affected: Versions 2.3 through 2.4.4
- Fixed: v2.4.7 (bundled with WHM 5.3.1.0)

- Actively exploited in the wild; previous cPanel flaw (CVE-2026-41940, CVSS 9.8) deployed Mirai botnet + "Sorry" ransomware
- Remediation: Update to v2.4.7 or uninstall via `/usr/local/lsws/admin/misc/lscmctl cpanelplugin --uninstall`. Detection: `grep -rE "cpanel_jsonapi_func=redisAble" /var/cpanel/logs /usr/local/cpanel/logs/` [13] [32]

Ghost CMS CVE-2026-26980 — CVSS 9.4, SQL Injection

- Unauthenticated SQL injection in Content API
- Fixed: February 2026 (v6.19.1)
- Weaponized: 700+ websites compromised by May 7, 2026
- Attack: Malicious JavaScript injected into article footers via ClickFix (fake CAPTCHA) campaigns
- Sectors affected: Universities, blockchain, AI, SaaS, security, media, fintech
- Remediation: Update to v6.19.1+. Audit article content for injected scripts. [14] [21] [32]

Drupal Reconnaissance Activity: 15,000+ attack attempts identified within 48 hours of patch release (May 20) on 6,000 sites; tooling designed for data extraction + privilege escalation; remediation window is critical. [16] [17]

Chart: Cybersecurity Incidents by Category (May 19-26, 2026)

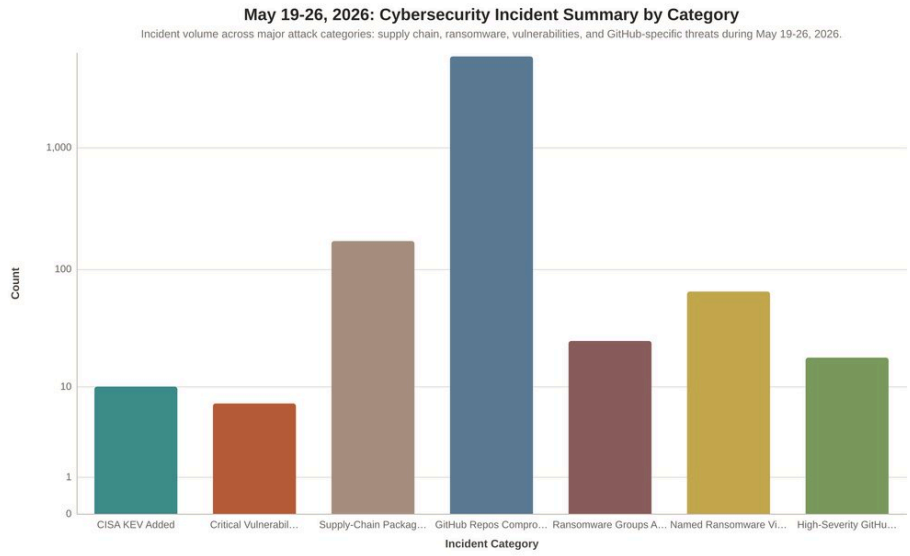

Figure 1: May 19-26, 2026: Cybersecurity Incident Summary by Category: Incident volume across major attack categories: supply chain, ransomware, vulnerabilities, and GitHub-specific threats during May 19-26, 2026.

Critical Actions: Next 24-72 Hours

Immediate (Next 24 Hours)

1. Patch Microsoft Defender (CVE-2026-41091, CVE-2026-45498)

- Deploy Malware Protection Engine 1.1.26040.8+ across all Windows endpoints
- Verify: `mpcmdrun.exe -version` shows 1.1.26040.8 or higher
- Automated via Windows Update; monitor for completion

2. Audit npm Lockfiles for Poisoned Packages

- Search package-lock.json and yarn.lock for:
  - @tanstack/* versions published May 11, 2026
  - @antv/* versions published May 19, 2026
  - @mistralai/*, @uipath/*, intercom-client, laravel-lang/*, echarts-for-react versions published May 11-12, 19, 22-23
- If found: delete node_modules/, lockfile, and reinstall from trusted backup or known-safe baseline

3. Rotate All Cloud & Developer Credentials

- GitHub tokens (Personal Access Tokens, Deploy Keys, GitHub Actions secrets)
- npm authentication tokens (.npmrc, GitHub Packages, npm registry)
- AWS credentials (Access Keys, Temporary Credentials, IMDS role assumptions)
- GCP service accounts (JSON keys)
- Azure credentials (SPN credentials, managed identities)
- SSH keys (regenerate and redeploy)
- Kubernetes API tokens
- **Assume compromise if developers used GitHub, VS Code, npm, or GitHub Actions between May 11-26, 2026**

4. Block C2 Infrastructure (Network/WAF/DNS)

- 216.126.225.129:8443 (Megalodon campaign)
- flipboxstudio.info (Laravel-Lang campaign)
- t.m-kosche.com (GitHub Actions issues-helper campaign)
- Session/Oxen network endpoints: filev2.getsession.org, seed1-3.getsession.org (TanStack worm)
- git-tanstack.com, api.masscan.cloud, litter.catbox.moe (TanStack secondary C2)

5. Patch Drupal Core (CVE-2026-9082 — SQL Injection)

- Update to: 10.4.10, 10.5.10, 10.6.9, 11.1.10, 11.2.12, 11.3.10
- Deploy via composer update drupal/core
- Verify: `drush status | grep "Drupal version"`
- **Federal deadline: May 27, 2026** (5 days away)

6. Uninstall/Update LiteSpeed cPanel (CVE-2026-48172 — CVSS 10.0)

- If running cPanel with LiteSpeed: `/usr/local/lsws/admin/misc/lscmctl cpanelplugin --uninstall`
- OR update to v2.4.7 (bundled with WHM 5.3.1.0)
- Verify: `ls -la /usr/local/lsws/` returns empty or v2.4.7+

Short-Term (1-2 Weeks)

7. IDE Extension & CI/CD Security Hardening

- VS Code: Implement corporate allowlist for extensions; disable auto-update; restrict to approved marketplace
- GitHub: Enable branch protection on all repositories; require pull request reviews; audit and restrict workflow file modifications
- Enable secret scanning + push protection for all repositories (not just public)
- Audit recent .github/workflows/ additions for malicious patterns (unusual C2 domains, credential harvesting, archive commands)

8. GitHub Actions Secrets Audit & Rotation

- Rotate all GitHub Actions secrets (GITHUB_TOKEN, AWS_ACCESS_KEY_ID, NPM_TOKEN, GCP_SA_JSON, etc.)
- Audit Actions logs for unexpected workflow_dispatch triggers or unusual step definitions
- Check for gh-token-monitor daemon process (sign of dead-man's-switch persistence)

9. Supply-Chain SCA & Reachability Analysis

- Implement or upgrade software composition analysis (SCA) tooling to include reachability analysis
- Identify transitive dependencies (not just direct); assess breaking-change impact of supply-chain poisoning
- Use tools like Socket.dev, Snyk, or Dependabot to detect malicious package patterns

10. Ghost CMS CVE-2026-26980 (700+ Sites Compromised)

- If running Ghost: Update to v6.19.1+
- Audit article content for injected JavaScript (especially in article footers/metadata)
- Search Content API audit logs for unauthorized SQL-injection payloads
- Remediation: `npm update ghost && npm run prod`

Watchlist: Next 7 Days (May 26-June 2)

1. CISA KEV June 4 Remediation Deadline (9 days away)

- All 10 known-exploited vulnerabilities must be patched by June 4 for federal agencies
- Non-federal organizations should treat this as a hard deadline as well
- Monitor CISA alerts daily for additional KEV additions or exploited zero-day disclosures

2. Ransomware Group Activity Escalation

- **ShinyHunters:** 42 million Charter Communications records (May 23 disclosure); expected May 27 deadline
- **Play Ransomware:** 7 victims discovered May 25; targeting VPN/remote-access infrastructure
- **Qilin:** 13+ active victims; weak authentication on remote-access systems
- **Akira:** 84 victims in March 2026 alone; known for NAS/tape destruction tactics
- **Expected:** Continued double-extortion campaigns with data-leak-site monetization

3. Nation-State Operations Intensification

- **Iranian Screening Serpens (UNC1549/Nimbus Manticore):** Aerospace, defense, telecom targeting; fake job-offer lures

- **Chinese Salt Typhoon:** Ongoing telecom/government intrusions; 50+ recent victims across 42 countries
- **Russian APT28 (Forest Blizzard):** Infrastructure (WorkTitans, MIRhosting) seized May 18-25; renewed campaign likely

4. Supply-Chain Worm Variants & Secondary Waves

- TanStack worm self-propagation may continue as newly-infected developer credentials are leveraged
- Mini Shai-Hulud waves historically cluster; additional @antv or similar ecosystem waves possible
- Expected: Continued GitHub Actions workflow poisoning (Megalodon-style)

5. Government & Law Enforcement Activity

- **FBI/CISA Joint Operations:** Ongoing disruption of infrastructure used in ransomware, botnets
- **Expected:** Additional arrests/charges related to Kimwolf botnet (May 21 arrest), First VPN shutdown (May 22)
- **Expected:** New sanctions against Russian/Iranian/Chinese cyber operators

6. Additional CVE Exploitations

- **Ghost CMS (700+ sites):** Ongoing malware injection into articles
- **Drupal (6,000 sites under attack):** Reconnaissance phase; exploitation tooling maturing
- **Copy.fail Linux kernel variants:** AWS Fargate/ECS endpoints exposed May 26-29 deadline
- **NGINX CVE-2026-42945:** 5.7M+ public servers; active exploitation likely

---

Summary & Critical Takeaways

The Bottom Line: May 19-26, 2026 exposed a fundamental architectural weakness: developer tools (IDE extensions, CI/CD workflows, build artifacts) have become as critical to security as application firewalls or network segmentation. A single compromised VS Code extension exposed 3,800 GitHub repositories. A single poisoned npm package reached 520 million downstream consumers in 12 hours, complete with fraudulent SLSA attestations that bypassed supply-chain verification systems.

Three Concurrent Attack Patterns:

1. **IDE → Credential Theft → CI/CD Compromise** (Nx Console → Megalodon)
2. **Package Ecosystem Self-Propagation via Credential Harvesting** (TanStack → Mini Shai-Hulud waves)
3. **Ransomware Double-Extortion Targeting Backup Systems** (ShinyHunters, Play, Qilin, Akira)

Your Immediate Priorities (Next 72 Hours):

1. Rotate all developer credentials (GitHub, npm, AWS, GCP, SSH)
2. Patch Microsoft Defender (CVE-2026-41091, -45498) and Drupal Core (CVE-2026-9082)
3. Audit npm/PyPI lockfiles for poisoned packages from May 11-12, 19, 22-23
4. Block identified C2 infrastructure via firewall/WAF/DNS
5. Assume GitHub Actions secrets, npm tokens, and cloud credentials are compromised

By June 4: All CISA KEV vulnerabilities must be patched (federal deadline); private organizations should treat this as standard practice.

[1] [2] [3] [4] [5] [6] [7] [8] [9] [10] [12] [13] [14] [15] [16] [17] [18] [19] [20] [21] [22] [23] [25] [26] [27] [28] [29] [30] [31] [32] [33] [34] [35] [36] [38] [39] [40]

Sources

- [1] CISA Adds Two Known Exploited Vulnerabilities to Catalog | CISA - https://www.cisa.gov/news-events/alerts/2026/05/21/cisa-adds-two-known-exploited-vulnerabilities-...
- [2] Langflow: CISA adds Langflow Vulnerability to Known Exploited Vulnerabilities Catalog - https://blog.rankiteo.com/lan1779452952-langflow-vulnerability-may-2026/
- [3] Trend Micro: CISA Warns Trend Micro Apex One Vulnerability Is Being Exploited in Attacks - https://blog.rankiteo.com/tre1779438294-trend-micro-vulnerability-may-2026/
- [4] Microsoft Defender vulnerabilities are being exploited in the wild | Malwarebytes - https://www.malwarebytes.com/blog/bugs/2026/05/microsoft-defender-vulnerabilities-are-being-explo...
- [5] CISA Adds One Known Exploited Vulnerability to Catalog | CISA - https://www.cisa.gov/news-events/alerts/2026/05/22/cisa-adds-one-known-exploited-vulnerability-ca...
- [6] CISA Adds Seven Known Exploited Vulnerabilities to Catalog | CISA - https://www.cisa.gov/news-events/alerts/2026/05/20/cisa-adds-seven-known-exploited-vulnerabilitie...
- [7] GitHub links repo breach to TanStack npm supply-chain attack - https://www.bleepingcomputer.com/news/security/github-links-repo-breach-to-tanstack-npm-supply-ch...
- [8] Mini Shai-Hulud Supply Chain Attack CVE-2026-45321 FAQ | Tenable® - https://www.tenable.com/blog/mini-shai-hulud-frequently-asked-questions
- [9] TanStack npm Supply Chain Attack: Detailed Analysis of the May 2026 GitHub Actions Breach and Multi-Ecosystem Impact – Rescana - https://www.rescana.com/post/tanstack-npm-supply-chain-attack-detailed-analysis-of-the-may-2026-g...
- [10] GitHub Breach May 2026: All You Need to Know | Axipro - https://axipro.co/github-breach-may-2026/
- [11] GitHub confirms 3,800 internal repos stolen through poisoned VS Code extension as supply chain worm hits Microsoft's Python SDK | VentureBeat - https://venturebeat.com/security/github-confirms-3800-repos-stolen-poisoned-vs-code-extension-sup...
- [12] Shai-Hulud: Here We Go Again. Mass npm Supply Chain Attack Hits the AntV Ecosystem - StepSecurity - https://www.stepsecurity.io/blog/shai-hulud-here-we-go-again-mass-npm-supply-chain-attack-hits-th...
- [13] LiteSpeed cPanel Plugin CVE-2026-48172 Exploited to Run Scripts as Root - https://thehackernews.com/2026/05/litespeed-cpanel-plugin-cve-2026-48172.html
- [14] Ghost CMS CVE-2026-26980 Exploited to Hijack 700+ Sites for ClickFix Attacks - https://thehackernews.com/2026/05/ghost-cms-cve-2026-26980-exploited-to.html
- [15] Microsoft Defender vulnerabilities exploited in the wild (CVE-2026-41091, CVE-2026-45498) - Help Net Security - https://www.helpnetsecurity.com/2026/05/21/microsoft-defender-vulnerabilities-cve-2026-41091-cve-...
- [16] NEWS ROUNDUP - 22nd May 2026 - Digital Forensics Magazine - https://digitalforensicsmagazine.com/news-roundup-22nd-may-2026/
- [17] Cybersecurity News - WIU Cybersecurity Center - WIU - https://www.wiu.edu/cybersecuritycenter/cybernews.php
- [18] CISO Platform Breach Report 21 May 2026 - All Articles - CISO Platform - https://www.cisoplatform.com/profiles/blogs/ciso-platform-breach-report-21-may-2026
- [19] Cybersecurity News | Daily Recap [20 May 2026] - https://www.hendryadrian.com/cybersecurity-news-daily-recap-20-may-2026/
- [20] Krebs on Security – In-depth security news and investigation - https://krebsonsecurity.com/
- [21] Cybersecurity News, Insights and Analysis | SecurityWeek - https://www.securityweek.com/
- [22] CISOPlatform Breach Report - May 22, 2026 | Key Breach Incidents Overview - All Articles - CISO Platform - https://www.cisoplatform.com/profiles/blogs/cisoplatform-breach-report-may-22-2026-key-breach-inc...
- [23] Megalodon GitHub Attack Targets 5,561 Repos with Malicious CI/CD Workflows - https://thehackernews.com/2026/05/megalodon-github-attack-targets-5561.html
- [24] Popular GitHub Action Tags Redirected to Imposter Commit to Steal CI/CD Credentials - https://thehackernews.com/2026/05/github-actions-supply-chain-attack.html

- [25] How We Got a CISA GitHub Leak Taken Down in Under a Day - https://blog.gitguardian.com/how-we-got-a-cisa-github-leak-taken-down-in-26-hours/
- [26] GitHub Security Breach Raises Supply Chain Risks for Crypto Developers | MEXC News - https://www.mexc.com/news/1103579
- [27] GitHub internal repositories breached | SOPHOS - https://www.sophos.com/en-us/blog/github-internal-repositories-breached
- [28] The npm Threat Landscape: Attack Surface and Mitigations (Updated May 21) - https://unit42.paloaltonetworks.com/monitoring-npm-supply-chain-attacks/
- [29] Postmortem: TanStack NPM supply-chain compromise | Hacker News - https://news.ycombinator.com/item?id=48100706
- [30] Railway Offline Eight Hours After GCP Error - webhosting.today - https://webhosting.today/2026/05/20/google-cloud-incorrectly-suspended-railways-account-eight-hou...
- [31] GitHub Advisory Database · GitHub - https://github.com/advisories
- [32] Vulnerability Intelligence Report — May 23, 2026 - Threat-Modeling.com - https://threat-modeling.com/vulnerability-intelligence-report-may-23-2026/
- [33] Security Bulletin - May 19 2026 | Atlassian Support | Atlassian Documentation - https://confluence.atlassian.com/security/security-bulletin-may-19-2026-1786839142.html
- [34] Ransomware.live - https://www.ransomware.live/
- [35] Verizon DBIR: Vulnerability exploitation is the dominant initial access vector - Help Net Security - https://www.helpnetsecurity.com/2026/05/20/verizon-2026-dbir-findings/
- [36] 2026 Data Breach Investigations Report (DBIR) | Verizon - https://www.verizon.com/business/resources/reports/dbir/
- [37] CISA GitHub Leak Exposes AWS GovCloud Secrets | eSecurity Planet - https://www.esecurityplanet.com/threats/cisa-github-leak-exposes-aws-govcloud-secrets/
- [38] Threat Advisory: TanStack Supply Chain Attack - https://www.uvcyber.com/resources/reports/threat-advisory-tanstack-supply-chain-attack
- [39] MEGALODON_CI: GitHub Actions Workflow Poisoning Attack - https://phoenix.security/megalodon-ci-github-actions-workflow-poisoning-credential-harvesting/
- [40] VS Code Extension Malware: How TeamPCP Breached GitHub - https://phoenix.security/vs-code-extension-malware-github-breach-teampcp-2026/