THE FORENSICS WAY

ISSUE 17 | FORENSICS AWARENESS THIS WEEK | TUESDAY, MAY 26, 2026

FRONT PAGE

SUPPLY CHAIN ATTACK

GitHub Breached Through Its Own Backyard: Malicious "Nx Console" VS Code Extension Lets TeamPCP Clone 3,800 Internal Repos

GitHub confirmed on May 20 that a threat actor self-identifying as TeamPCP — tracked as UNC6780 — cloned roughly 3,800 internal private repositories after an employee installed a trojanized build of the Nx Console VS Code extension (nrwl.angular-console v18.95.0). The poisoned version was live on the Visual Studio Marketplace for just 18 minutes on May 18.

The extension harvested developer secrets and access tokens from the local IDE environment, which the attacker replayed to pull source code, deployment scripts, and config material now listed on a criminal forum for $50,000+. GitHub says customer repos and enterprise accounts are unaffected. Forensic priority: reconstruct extension install/update telemetry, IDE token-store access, and clone events in audit logs across every repo the harvested tokens could reach.

THREAT DISRUPTION — CODE-SIGNING

Microsoft Dismantles "Fox Tempest": Malware-Signing Service That Minted 1,000+ Fraudulent Code-Signing Certificates

Microsoft's Digital Crimes Unit disrupted Fox Tempest on May 19, revoking more than 1,000 fraudulent code-signing certificates and seizing the domain signspace.cloud through a sealed lawsuit in the Southern District of New York. Paying customers uploaded malware for signing; the certificates — valid for only 72 hours — let payloads masquerade as AnyDesk, Microsoft Teams, PuTTY, and Cisco Webex.

The $5,000–$9,000 service fed ransomware crews including Vanilla Tempest, Storm-0501, Storm-2561, and Storm-0249, whose signed loaders and stealers initially slipped past Windows trust checks. Forensic priority: inventory binaries signed by

Threat Bulletin

CRITICAL

CVE-2025-34291

Langflow — origin-validation error; an overly permissive CORS config plus a refresh-token cookie set SameSite=None lets a malicious web page make credentialed cross-origin calls to the refresh endpoint, yielding tokens for authenticated RCE and full compromise; CVSS 9.4. Added to CISA KEV May 21; Iran's MuddyWater is using it for initial access. *Forensic Note:* Review Langflow access logs for cross-origin refresh-endpoint calls and anomalous token issuance, then hunt post-exploitation execution under the app service account.

ACTIVE EXPLOIT

CVE-2026-34926

Trend Micro Apex One (on-premise) — directory-traversal flaw lets a pre-authenticated local attacker modify a server key table to inject malicious code that is then deployed to managed agents; CVSS 6.7. Added to CISA KEV May 21 with a June 4 federal deadline. *Forensic Note:* Verify integrity of the Apex One key table and agent-deployment packages, and audit management-console logs for unauthorized table writes preceding mass agent updates.

MALWARE SPOTLIGHT

Mini Shai-Hulud — Self-Propagating Package Worm

Microsoft flagged a major resurgence of TeamPCP's Shai-Hulud campaign on May 11, with "Mini Shai-Hulud" compromising 170+ npm packages and

recently revoked certificates, correlate Authenticode timestamps against the 72-hour validity windows, and treat any signspace.cloud-linked signature as an indicator of compromise.

2 PyPI packages across 404 malicious versions touching 518M monthly downloads. The worm uses preinstall/import hooks to fetch the Bun runtime, decrypt hidden payloads, and harvest GitHub Actions, npm, AWS, Kubernetes, and Vault credentials — even defeating SLSA Build Level 3 provenance. *Forensic Note:* Hunt rogue preinstall scripts, unexpected Bun downloads, and the *gh-token-monitor* persistence daemon; treat any CI/CD secret reachable from an affected build as compromised.

THE FORENSICS WAY

HISTORICAL ARCHIVES | HISTORY OF DIGITAL INVESTIGATION | TUESDAY, MAY 26, 2026

CASE STUDIES: HISTORICAL GRID

CODECOV BASH UPLOADER BREACH (2021)

A Single Tampered CI Script Quietly Drains Secrets From Thousands of Build Pipelines for Two Months

In April 2021, Codecov disclosed that an attacker had used a flaw in its Docker image build to extract credentials and modify the widely used Bash Uploader script. For roughly two months, the altered script silently exfiltrated environment variables — tokens, keys, and credentials — from customers' CI/CD pipelines to an attacker-controlled server. Investigators reconstructed the intrusion via Git history of the uploader and outbound traffic analysis, and the case became the textbook example of why every secret exposed to a build runner must be treated as compromised — the exact lesson now echoing through Mini Shai-Hulud.

ASUS SHADOWHAMMER (2019)

Stolen Code-Signing Certificates Push a Backdoored Live Update to a Million Machines — Aimed at 600

Kaspersky's Operation ShadowHammer revealed that attackers had trojanized the ASUS Live Update utility and signed it with legitimate, stolen ASUS code-signing certificates, distributing it through official channels to roughly one million users. The implant checked each host's MAC address against a hardcoded list of about 600 targets before fetching a second-stage payload. Forensic teams matched the malicious binaries by certificate serial and timestamp — a direct historical parallel to this week's Fox Tempest takedown and the enduring danger of trusted signatures.

SOLARWINDS SUNBURST (2020)

APT29 Implants a Signed Backdoor in the Build Pipeline: 18,000 Orion Customers, Months of Undetected Beaconing

In December 2020, FireEye discovered that APT29 (Cozy Bear) had compromised SolarWinds' build server and inserted the SUNBURST backdoor into a signed Orion Platform DLL, distributed via routine update to ~18,000 customers. Forensic teams identified DGA-based C2 over avsvmcloud.com, in-memory loaders, and pre-staged TEARDROP and RAINDROP payloads. The case forced DFIR to treat code-signing certificates and CI/CD pipelines as crown-jewel assets — the threat model defining this entire week.

KASEYA VSA / REVIL (2021)

Supply-Chain Ransomware Hits 1,500+ Downstream Customers in a Single Patch Push

On July 2, 2021, REvil exploited zero-day CVE-2021-30116 in Kaseya VSA's authentication and dropped an encryptor through the platform's own software-management agent, hitting 60 MSPs and an estimated 1,500+ end customers worldwide. Sophos and Mandiant reconstructed the attack chain through VSA agent procedure logs and the malicious "Kaseya VSA Agent Hot-fix" task. The FBI later recovered a universal decryptor; the case codified MSP and management-plane software as the highest-leverage supply-chain target class.

TOOLS OF THE TRADE

OPEN SOURCE

Socket

SOCKET.DEV — CLI

Dependency firewall that analyzes npm, PyPI, and other packages for malicious behavior — install scripts, obfuscated code, network/filesystem access, and credential exfiltration. Built to catch exactly the preinstall-hook tradecraft behind Mini Shai-Hulud before a poisoned version ever reaches a build runner.

OPEN SOURCE

OSV-Scanner

GOOGLE — V2.X

Command-line scanner that matches a project's lockfiles and SBOMs against the OSV database to flag known-vulnerable and compromised dependency versions. Wired into CI, it surfaces the specific malicious package releases pulled in transitively during supply-chain worm events.

OPEN SOURCE

cosign (Sigstore)

SIGSTORE PROJECT — V2.X

Signs and verifies container images and software artifacts with keyless, transparency-logged signatures. Verifying provenance with cosign before deploying is the direct countermeasure to Fox Tempest-style fraudulent code-signing and unverified build outputs.

COMMERCIAL

ExtensionTotal

EXTENSIONTOTAL — 2026

Risk-scoring platform for IDE extensions that analyzes VS Code Marketplace publishers, permissions, and behavioral indicators to flag malicious or trojanized add-ons. Precisely the control class that would have caught the poisoned Nx Console extension used to breach GitHub.

PRIORITY CVE ADVISORIES

ARCHIVE ALERT

CVE-2026-20182 (CISCO SD-WAN)

Catalyst SD-WAN Controller peering authentication bypass over DTLS (UDP 12346) grants unauthenticated admin access and NETCONF pivot; CVSS 10.0. Exploited by UAT-8616; in CISA KEV. *Forensic Note:* Preserve

ARCHIVE ALERT

CVE-2026-44338 (PRAISONAI)

PraisonAI Flask API ships with AUTH_ENABLED hardcoded False, exposing /agents and /chat without a token; CVSS 7.3. Probed within 3h 44m of disclosure; fix in 4.6.34. *Forensic Note:* Hunt unauthenticated GET /agents

RECENT MALWARE WATCH

ARCHIVE: MAY 19, 2026

TYCOON2FA — DEVICE-CODE PHISHING

Phishing-as-a-service kit abusing the OAuth 2.0 device-authorization grant to hijack Microsoft 365 accounts; issues tokens to attacker devices after victims enter a code at the legitimate devicelogin page.

ARCHIVE: MAY 12, 2026

BARADAI RANSOMWARE

File-encrypting ransomware identified by CYFIRMA via underground-forum monitoring; targets a wide range of local and network file types with a distinct extension and ransom note. No public decryptor. Preserve shadow copy metadata and the

vdaemon logs and NETCONF change records — controller compromise propagates to every fabric edge.

returning 200 OK and review agents.yaml workflow history.

Audit AzureAD sign-ins for deviceCode authentication and enumerate newly registered devices.

Volume Change Journal before any recovery action.