THE FORENSICS WAY

ISSUE 16 | FORENSICS AWARENESS THIS WEEK | TUESDAY, MAY 19, 2026

FRONT PAGE

SUPPLY CHAIN ATTACK

Grafana GitHub Token Breach: Forked-PR Workflow Abuse Exfiltrates Codebase, Canary Token Triggers Detection

Grafana disclosed on May 16 that CoinbaseCartel — an offshoot of the ShinyHunters, Scattered Spider, and Lapsus$ ecosystem — obtained a privileged GitHub token by abusing a misconfigured *pull_request_target* workflow. The attacker forked a public Grafana repository, injected a curl command, and dumped environment variables when the trusted CI runner executed the fork.

The intrusion was detected only because one of thousands of seeded canary tokens fired the moment it was touched. Grafana refused the extortion demand citing FBI guidance, and confirmed no customer data was exposed. Forensic priority: reconstruct GitHub Actions run logs, workflow YAML diffs, and token usage timelines across every repo the leaked token could access.

WEB SERVER SECURITY

"NGINX Rift" (CVE-2026-42945): 18-Year-Old Rewrite Module Heap Overflow Hits Active Exploitation With Public PoC

CVE-2026-42945, dubbed "NGINX Rift," is a heap buffer overflow in ngx_http_rewrite_module affecting versions 0.6.27 through 1.30.0 — code paths present since 2008. A state mismatch between the rewrite engine's length-calculation and copy passes lets an unauthenticated attacker overflow worker memory with a single crafted HTTP request.

The bug yields reliable DoS via worker crashes, and full RCE on hosts where ASLR is disabled; a working PoC is on GitHub and active exploitation is confirmed. Forensic priority: preserve worker core dumps, error_log entries showing repeated SIGSEGV events, and access logs containing the trigger URI pattern before they roll. Patches: NGINX 1.30.1 / 1.31.0, NGINX Plus R32 P6 / R36 P4.

Threat Bulletin

CRITICAL

CVE-2026-20182

Cisco Catalyst SD-WAN Controller — peering authentication bypass over DTLS (UDP 12346) lets unauthenticated attackers gain administrative access and pivot to NETCONF; CVSS 10.0. Limited exploitation by UAT-8616 confirmed; added to CISA KEV. *Forensic Note:* Preserve vdaemon logs, DTLS session captures on UDP 12346, and NETCONF configuration-change records — controller compromise propagates to every fabric edge device.

ACTIVE EXPLOIT

CVE-2026-44338

PraisonAI Flask API server — AUTH_ENABLED hardcoded to False exposes /agents and /chat endpoints without a token; CVSS 7.3. Probed within 3h 44m of disclosure (May 11) by scanner CVE-Detector/1.0; fix in 4.6.34. *Forensic Note:* Hunt access logs for unauthenticated GET /agents returning 200 OK, and review agents.yaml workflow history for unauthorized invocation chains.

MALWARE SPOTLIGHT

Tycoon2FA — OAuth Device-Code Phishing

The Tycoon2FA phishing-as-a-service kit returned in May 2026 with OAuth 2.0 device-authorization-grant abuse, hijacking Microsoft 365 accounts after victims enter the attacker's device code into Microsoft's legitimate *microsoft.com/devicelogin* page. The completed MFA flow issues access and

refresh tokens directly to attacker-controlled devices — bypassing every conditional-access policy keyed to credential phishing. *Forensic Note:* Audit AzureAD sign-in logs for *authenticationProtocol = deviceCode* events, and enumerate newly registered devices in the affected tenant.

THE FORENSICS WAY

HISTORICAL ARCHIVES | HISTORY OF DIGITAL INVESTIGATION | TUESDAY, MAY 19, 2026

CASE STUDIES: HISTORICAL GRID

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 — exactly the threat model now playing out at Grafana.

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.

BANGLADESH BANK SWIFT HEIST (2016)

ASHLEY MADISON BREACH (2015)

Lazarus Group Steals $81 Million via SWIFT Credential Theft, Forged Transfers, and Custom Banking Malware

In February 2016, Lazarus Group deployed keylogger malware inside Bangladesh Bank to steal SWIFT credentials, then issued 35 fraudulent transfer requests — five succeeded, moving $81 million to Philippines casinos. Mandiant investigators recovered custom malware that interfaced directly with SWIFT Alliance Access software, and the FBI identified evidence of an insider accomplice. The heist established financial sector forensics as a discipline requiring SWIFT audit log reconstruction and cross-border transaction tracing.

The Impact Team Wipes Its Tracks and Vanishes: 37 Million Records, PGP-Signed Leaks, No Identified Suspects

In July 2015, the Impact Team compromised extramarital dating site Ashley Madison, stealing records on 37 million users and releasing 9.7 GB publicly in August with PGP-signed authenticity. Forensic investigation found attackers escalated to administrator level and wiped logs that would have contained their indicators of compromise, rendering attribution impossible. Despite FBI and RCMP investigation, no suspects were ever identified — a landmark study in attacker log-wiping tradecraft and the limits of log-dependent forensics.

TOOLS OF THE TRADE

OPEN SOURCE

Canarytokens

THINKST — FREE SERVICE

Free tripwire token service generating decoy credentials, files, URLs, and AWS keys that fire alerts the moment they are touched. This is the exact mechanism that caught the Grafana CoinbaseCartel breach in May 2026 — a single seeded token triggered detection before any data was exfiltrated.

OPEN SOURCE

gitleaks

ZACHARY RICE — V8.X

Static-analysis scanner for detecting hardcoded secrets in git repositories and CI/CD pipelines using regex and entropy heuristics. Designed to be wired into pre-commit hooks and GitHub Actions — the kind of guardrail that would have flagged the privileged token leaked through Grafana's forked pull-request workflow.

OPEN SOURCE

Hayabusa

YAMATO SECURITY — V3.X

Fast Windows event log timeline analyzer powered by Sigma rules; converts raw EVTX files into severity-ranked detections in minutes. Ideal for hunting Tycoon2FA OAuth device-code authentication artifacts and AzureAD-connected workstation anomalies during M365 token-theft investigations.

COMMERCIAL

Microsoft Defender for Cloud Apps

MICROSOFT — 2026 BUILD

SaaS-aware CASB providing OAuth-app discovery, anomaly detection on token issuance, and real-time policy enforcement across Microsoft 365 and connected cloud apps. Surfaces rogue device registrations and impossible-travel sign-ins — exactly the signal class needed to catch Tycoon2FA device-code phishing in progress.

PRIORITY CVE ADVISORIES

ARCHIVE ALERT

CVE-2026-0300 (PAN-OS)

Palo Alto User-ID Authentication Portal buffer overflow enables unauthenticated RCE as root; CVSS 9.3. Exploited since April 9 by state-sponsored cluster CL-STA-1132. *Forensic Note:* Capture PA-Series disk images and management-process core dumps before patching to preserve shellcode artifacts.

ARCHIVE ALERT

CVE-2026-23918 (APACHE MOD_HTTP2)

Double-free in Apache HTTP Server 2.4.66 mod_http2 stream cleanup enables DoS and potential RCE via HTTP/2 early RST; CVSS 8.8. Fixed in 2.4.67. *Forensic Note:* Examine worker core dumps and HTTP/2 stream identifiers in access logs preceding service disruption.

RECENT MALWARE WATCH

ARCHIVE: MAY 12, 2026

BARADAI RANSOMWARE

File-encrypting ransomware identified by CYFIRMA in May 2026 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 Volume Change

ARCHIVE: MAY 5, 2026

"SORRY" RANSOMWARE

Go-based Linux ransomware targeting cPanel/WHM servers via CVE-2026-41940; ChaCha20/RSA-2048 encryption appends .sorry extension across all hosted sites and databases. Hunt ransomware binary artifacts in /tmp and CRLF injection sequences in cPanel access logs.

Journal before any recovery action.