THE FORENSICS WAY

ISSUE 12 | FORENSICS AWARENESS THIS WEEK | TUESDAY, APRIL 21, 2026

FRONT PAGE

SUPPLY CHAIN FORENSICS

OAuth Token Hijacking via Third-Party AI Tool Exposes Vercel's Internal Credential Vault

Infrastructure platform Vercel disclosed on April 18 that threat actors accessed internal systems by compromising **Context.ai** — a third-party AI assistant used by Vercel engineers. Attackers hijacked OAuth tokens tied to employee Google accounts, bypassing MFA controls entirely. Customer data including API keys and internal project metadata was extracted before the breach was contained and disclosed.

The attack reveals a critical forensic gap: OAuth delegation chains rarely surface in traditional SIEM logs. Investigators reconstructed the timeline across three separate log planes — Google Workspace audit events, Context.ai API access records, and Vercel's internal credential management system — none of which were correlated in standard IR playbooks. Third-party AI tooling now represents a privileged-access surface most organizations have not yet threat-modeled.

CRITICAL INFRASTRUCTURE

Apache ActiveMQ RCE Exploited at Scale — 6,000 Exposed Instances Targeted, CISA KEV Triggered

CISA added **CVE-2026-34197** to its Known Exploited Vulnerabilities catalog this week as active exploitation of Apache ActiveMQ Classic reached critical scale — over 6,000 exposed instances identified via internet scanning with no patch applied. The flaw exploits improper input validation in the OpenWire protocol, enabling unauthenticated remote code execution with no user interaction required; CVSS 8.8.

ActiveMQ is embedded in enterprise middleware stacks as a message broker, making it largely invisible to endpoint security tooling. Forensic responders should prioritize ActiveMQ broker logs for unexpected subprocess trees spawning from the JVM process, unusual outbound connections from the broker host, and Java-based web shells staged in the ActiveMQ webapps directory.

Threat Bulletin

ACTIVE EXPLOIT

CVE-2026-32201

Microsoft SharePoint Server — authentication bypass enabling spoofing and unauthenticated RCE; patched in the April 14 Patch Tuesday emergency release and confirmed exploited in the wild prior to the patch. *Forensic Note:* Review SharePoint ULS logs for anomalous authentication events and check MSSQL audit trails for unauthorized stored procedure execution under SharePoint service accounts.

ACTIVE EXPLOIT

CVE-2026-34197

Apache ActiveMQ Classic — unauthenticated RCE via improper OpenWire protocol validation; CVSS 8.8. Added to CISA KEV April 2026 with over 6,000 exposed instances confirmed online. *Forensic Note:* Examine broker logs for unexpected JVM subprocess trees; scan webapps directories for Java-based web shell artifacts planted post-exploitation.

MALWARE SPOTLIGHT

BASANAI Ransomware (MedusaLocker)

Emerging MedusaLocker-family ransomware variant active April 2026, targeting enterprise Windows environments via RDP brute force and phishing. AES-256 / RSA-2048 encryption with .basanai extension; VSS deleted pre-encryption to block shadow copy recovery. *Forensic Note:* Hunt Event ID 4625 RDP brute-force sequences and vssadmin / wmic VSS

Post-exploitation persistence has favored scheduled tasks in observed cases.

deletion commands appearing in Windows event logs ahead of file encryption timestamps.

THE FORENSICS WAY

HISTORICAL ARCHIVES | HISTORY OF DIGITAL INVESTIGATION | TUESDAY, APRIL 21, 2026

CASE STUDIES: HISTORICAL GRID

RSA SECURID BREACH (2011)

The Hack That Broke Two-Factor Auth: Nation-State Actors Extract RSA's Entire SecurID Seed Database

In March 2011, RSA Security was breached via a spear-phishing Excel attachment exploiting an Adobe Flash zero-day. Attackers deployed Poison Ivy RAT, staged exfiltrated data as encrypted RAR archives, and used FTP for exfiltration — all traffic engineered to blend with legitimate patterns. The stolen asset was the seed database for 40 million SecurID tokens deployed at US government agencies and defense contractors, effectively undermining the enterprise 2FA ecosystem at scale.

SHAMOON / DISTTRACK (2012)

35,000 Saudi Aramco Workstations Wiped in Hours — The Wiper Attack That Redefined Destructive Malware

In August 2012, the SHAMOON wiper simultaneously destroyed the MBR and user files of 35,000 Saudi Aramco workstations across a single weekend, forcing the world's largest oil company to replace its entire PC fleet. Unlike ransomware, the payload carried no ransom demand — its sole purpose was destruction. Forensic recovery was possible only through Active Directory audit logs, offline backup tapes, and partial disk images from machines where payload execution failed mid-run.

YAHOO DATA BREACH (2013–2016)

3 Billion Accounts — Russian FSB Operated Silently Inside Yahoo for Three Years

Russian FSB officers infiltrated Yahoo between 2013 and 2016, stealing data on all 3 billion user accounts — the largest breach ever recorded — while Yahoo remained unaware for three years.

MARRIOTT / STARWOOD BREACH (2014–2018)

Chinese State Actors Spent Four Years Inside a Network That Was Then Acquired for $13 Billion

Chinese state-sponsored hackers breached Starwood's hotel network in 2014 and remained undetected for four years — surviving Marriott's

The attackers also forged authentication cookies, bypassing login event logging entirely. The case established that post-breach forensics must account for multi-year silent dwell and authentication artifact gaps — the same patient persistence pattern demonstrated by APT28 last week.

$13 billion acquisition in 2016 without detection. By discovery in 2018, 500 million guest records had been exfiltrated including passport numbers. The case is the definitive forensic lesson in M&A due diligence: Marriott unknowingly acquired an active four-year intrusion as part of the deal.

TOOLS OF THE TRADE

COMMERCIAL

Passware Kit 2026 v2

APRIL 2026 RELEASE

Password recovery and forensic decryption platform. v2 introduces TPM-protected BitLocker decryption via memory acquisition — reducing recovery time from hours to minutes without offline brute force. Adds expanded support for LastPass vaults, Steganos Safe, and FileMaker databases with GPU acceleration across NVIDIA, AMD, and Intel Arc hardware.

COMMERCIAL

Cellebrite Genesis

EARLY ACCESS — MARCH 2026

Agentic AI platform for mobile and digital investigations. Analysts query mobile extractions, CDRs, documents, messages, and images through natural-language conversation. Benchmark: three analyst-weeks of manual correlation completed in three minutes; drug supply-chain reconstruction from raw CDR data in under ten minutes. Changes the economics of large-scale mobile evidence review.

COMMERCIAL

Aid4Mail 6.2

APRIL 2026 RELEASE

Email forensics and eDiscovery platform adding a Python scripting framework with integrated AI assistance for building custom extraction rules. v6.2 delivers multilingual email classification at 97%+ accuracy and processes 400,000+ emails per weekend batch — reducing time from evidence collection to court-ready output in large-scale investigations involving international or mixed-language correspondence.

OPEN SOURCE

YARA-X

V0.11 — ACTIVE 2026

Complete Rust-language rewrite of the YARA malware pattern-matching engine — substantially faster scan times, cleaner error diagnostics, and fully backward-compatible rule syntax. Particularly effective for BASANAI and MedusaLocker-variant hunting at enterprise scale; improved performance makes scanning large file shares practical without dedicated scanning infrastructure or performance tuning.

PRIORITY CVE ADVISORIES

ARCHIVE ALERT

CVE-2026-34621 (ADOBE ACROBAT)

JavaScript prototype pollution enables RCE when a victim opens a crafted PDF; CVSS 8.6. Emergency patch April 12; CISA KEV April 13. *Forensic Note:* Review email gateway logs for PDF delivery and endpoint telemetry for Reader spawning unexpected child processes.

ARCHIVE ALERT

CVE-2012-1854 (MS OFFICE VBA)

Insecure DLL loading in VBA macro execution re-added to CISA KEV April 13 due to active re-exploitation in modern initial-access chains. *Forensic Note:* Hunt DLL side-loading artifacts in VBA macro process trees and unexpected DLL loads from user-writable directories.

RECENT MALWARE WATCH

ARCHIVE: APR 14, 2026

OMNISTEALER (NORTH KOREA)

Infostealer using TRON blockchain as C2; payloads embedded in BSC transaction input fields. Targets 10+ password managers, 60+ crypto wallets. Hunt outbound connections to TRON/Aptos RPC endpoints; on-chain analysis now required for attribution.

ARCHIVE: APR 7, 2026

WAVESHAPER.V2 (UNC1069)

North Korea's cross-platform backdoor delivered via poisoned Axios npm. Dropper SILKBELL self-destructs post-execution, defeating npm audit. Hunt via package-lock.json diffs for plain-crypto-js and CI/CD outbound connections.