THE FORENSICS WAY

ISSUE 14 | FORENSICS AWARENESS THIS WEEK | TUESDAY, MAY 5, 2026

FRONT PAGE

SAAS & CLOUD FORENSICS

ShinyHunters Exfiltrates 3.65 TB from 275 Million Canvas Users via Salesforce Misconfiguration

Educational technology provider Instructure disclosed on May 1 that threat group **ShinyHunters** exploited a Salesforce misconfiguration to exfiltrate data on approximately 275 million users across nearly 9,000 schools worldwide. The stolen 3.65 TB included names, email addresses, student ID numbers, and private student-teacher messages. ShinyHunters claimed responsibility publicly on May 3 and listed the data for sale before Instructure's full disclosure was complete.

Investigators face a multi-cloud forensics challenge: evidence spans Instructure's own systems, Salesforce API access logs, and ShinyHunters' infrastructure — three separate evidence planes with distinct custody requirements. The attack exploited misconfigured Salesforce access controls, not a zero-day, making API activity logs and OAuth token issuance records the primary forensic artifacts. The case reinforces that SaaS misconfiguration now carries the same breach risk as an unpatched critical vulnerability.

CRITICAL INFRASTRUCTURE

CVE-2026-41940: CRLF Injection in cPanel Session Cookies Compromises 40,000+ Hosting Servers Worldwide

A critical CRLF injection vulnerability (CVE-2026-41940, CVSS 9.8) in cPanel and WebHost Manager session cookie handling has been mass-exploited since late April, compromising over **40,000 internet-facing hosting control panels** by May 4. Attackers gain root-level administrative access without credentials — enabling complete server takeover. Multiple threat actors simultaneously deployed "Sorry" ransomware and persistent administrative backdoors on affected hosts.

Unlike endpoint ransomware, a single compromised cPanel host encrypts dozens of hosted websites, databases, and mail servers simultaneously. Forensic responders must examine access logs for

Threat Bulletin

ACTIVE EXPLOIT

CVE-2026-41940

cPanel & WHM — CRLF injection in session cookie handling enables unauthenticated authentication bypass; CVSS 9.8. Actively exploited across 40,000+ hosting control panels with ransomware and backdoor deployment. *Forensic Note:* Examine cPanel access logs for malformed cookie payloads containing CRLF sequences; audit /tmp and /dev/shm directories for dropped ransomware binaries with creation timestamps.

ACTIVE EXPLOIT

CVE-2026-2033

Google Chrome V8 — type confusion in the JavaScript engine enables remote code execution via crafted web pages; CVSS 8.8. Added to CISA KEV May 2026 with confirmed in-the-wild exploitation. *Forensic Note:* Pull Chrome crashpad reports, GPU process logs, and extension history from suspect endpoints; hunt for renderer process sandbox escapes in Windows event telemetry and EDR process-creation logs.

MALWARE SPOTLIGHT

"Sorry" Ransomware (cPanel-Targeting)

Go-based Linux ransomware deployed exclusively via CVE-2026-41940 on cPanel/WHM servers. ChaCha20 stream cipher with RSA-2048 key wrapping encrypts all hosted sites, databases, and mail data simultaneously, appending a .sorry extension. Ransom communication

CRLF injection artifacts in session cookie fields, timestamp ransomware binary drops in /tmp directories, and reconstruct the pre-encryption exfiltration timeline. At 40,000+ affected instances, automated evidence collection is not optional — it is the only viable triage approach.

via Tox messenger; no public decryption utility exists. *Forensic Note:* Prioritize disk imaging and cPanel access log preservation before engaging any ransom demand process; ransomware binary artifacts in /tmp are short-lived.

THE FORENSICS WAY

HISTORICAL ARCHIVES | HISTORY OF DIGITAL INVESTIGATION | TUESDAY, MAY 5, 2026

CASE STUDIES: HISTORICAL GRID

SILK ROAD INVESTIGATION (2013)

Dread Pirate Roberts Unmasked: Live RAM Capture and Bitcoin Forensics Bring Down the Dark Web's First Empire

In October 2013, FBI agents arrested Ross Ulbricht in a San Francisco library with his laptop open and unlocked — capturing running processes, active Silk Road admin sessions, and credentials in live RAM before any encryption could engage. Bitcoin blockchain analysis then linked $13.4 million in transaction proceeds to Ulbricht's real-world identity through wallet clustering. The case established live system forensics and on-chain attribution as foundational DFIR disciplines for dark web investigations.

CARETO / THE MASK APT (2007–2014)

Seven Years Undetected: Kaspersky Uncovers a Multi-Platform Nation-State Operation Spanning 31 Countries

Discovered by Kaspersky Lab in 2014, The Mask (Careto) had operated undetected since 2007 — targeting government institutions, embassies, energy companies, and research organizations across 31 countries. The platform ran simultaneously on Windows, macOS, and Linux with rootkit and bootkit persistence modules. Forensic attribution required multi-platform malware analysis, C2 traffic correlation, and registry artifact reconstruction, establishing the investigative playbook for nation-state multi-platform APTs.

TARGET DATA BREACH (2013)

An HVAC Vendor's Stolen Credentials and 40 Million Payment Cards: The Breach

EQUIFAX DATA BREACH (2017)

A 76-Day Dwell, an Expired SSL Certificate, and 148

That Defined Third-Party Risk

In November 2013, attackers used stolen credentials from Target's HVAC vendor Fazio Mechanical to access the supplier portal and move laterally to POS systems across 1,800 stores. BlackPOS RAM-scraping malware harvested 40 million payment card records in-transit before encryption. Target's own security systems generated alerts that went uninvestigated — the breach was ultimately surfaced by DOJ investigators. The case defined third-party vendor access as retail's primary attack vector.

Million Americans' Data Silently Exfiltrated

In May 2017, attackers exploited an unpatched Apache Struts vulnerability (CVE-2017-5638) in Equifax's online dispute portal — a patch had been available for two months. The attackers spent 76 days inside the network executing 51 unmonitored database queries, exfiltrating 148 million Americans' SSNs, birth dates, and financial records. An expired internal SSL certificate had blinded the security inspection system to outbound traffic for 19 months prior to discovery.

TOOLS OF THE TRADE

OPEN SOURCE

Mirage

SYGNIA — ACTIVE 2026

Open-source forensic evidence collection tool for Google Cloud Platform and Google Workspace. Aggregates audit logs and configurations across GCP components, collects Gmail user activity, and automates authentication prerequisites — enabling investigators to rapidly build a complete cloud evidence package. Directly applicable to SaaS breach investigations involving GCP, complementing native audit logging with structured DFIR output.

OPEN SOURCE

AuraInspector

MANDIANT / GOOGLE — JAN 2026

Open-source command-line tool for detecting access control misconfigurations in Salesforce Aura framework sites. Tests getConfigData endpoints to enumerate exposed objects via action bulking — directly applicable to this week's Instructure/Salesforce breach. Helps investigators reconstruct which Salesforce objects were accessible to an unauthenticated attacker through misconfigured Experience Cloud access controls.

OPEN SOURCE

GWForensic

OWNSECURITY — ACTIVE 2026

Open-source DFIR tool for collecting and analyzing Google Workspace audit events. Automatically extracts logs in universal formats from the Admin SDK, enabling analysts to focus on identifying malicious patterns rather than log parsing. Reconstructs user activity timelines, unauthorized access paths, and data export events from Workspace — a practical counterpart to Mirage for investigations spanning both GCP infrastructure and Workspace user data.

OPEN SOURCE

Plaso

LOG2TIMELINE — JAN 2026 RELEASE

Python-based super-timeline framework aggregating artifacts from disk images, file system metadata, Windows Registry, event logs, browser history, and application databases into a single unified timeline. The January 2026 release adds Firefox 118+ download tracking, improved AppCompatCache parsing, and OpenSearch 2.5+ compatibility. Essential for reconstructing pre-encryption timelines in hosting infrastructure compromise investigations.

PRIORITY CVE ADVISORIES

ARCHIVE ALERT

CVE-2026-33825 (MS DEFENDER)

Insufficient access control enabling local privilege escalation; CISA KEV April 22. *Forensic Note:* Review Windows Security logs for unexpected privilege

ARCHIVE ALERT

CVE-2025-31324 (SAP NETWEAVER)

Unrestricted file upload to Metadata Uploader enabling unauthenticated RCE; CVSS 10.0. Renewed exploitation April 2026. *Forensic Note:* Inspect HTTP access logs for POST requests to /developmentserver/metadatauploader and scan web-accessible directories for JSP/ASPX web shells.

RECENT MALWARE WATCH

ARCHIVE: APR 28, 2026

LOTUS WIPER

Destructive wiper targeting Venezuela's energy sector; two batch scripts overwrite MBR and delete all volumes. No ransom demand — pure geopolitical sabotage. Hunt batch script artifacts and abnormal system

ARCHIVE: APR 21, 2026

BASANAI (MEDUSALOCKER)

MedusaLocker-family ransomware targeting enterprise Windows via RDP brute force; AES-256/RSA-2048 encryption, VSS deletion pre-encryption. Hunt Event ID 4625 RDP sequences and vssadmin

escalation sequences (Event ID 4672/4673) and Defender service modification events preceding detection.

utility process trees in Windows event logs.

commands preceding file encryption timestamps.