THE FORENSICS WAY

ISSUE 15 | FORENSICS AWARENESS THIS WEEK | TUESDAY, MAY 12, 2026

FRONT PAGE

CYBERSECURITY INTELLIGENCE

RansomHouse Claims Trellix Breach, Publishing Evidence of Source Code and Internal Infrastructure Access

RansomHouse named cybersecurity vendor Trellix on its dark web leak site on May 7, claiming a compromise initiated April 17. The group published screenshots showing access to source code repositories alongside what researchers identified as internal VMware, Rubrik, and Dell EMC system interfaces.

Trellix confirmed unauthorized access to "a portion" of its source code repository and engaged forensic experts while notifying law enforcement. The primary investigative concern is whether the breach extended to development secrets, code-signing credentials, or exploitable product logic that could be weaponized against Trellix's enterprise customer base.

LINUX SECURITY

"Copy Fail" (CVE-2026-31431): Page-Cache Privilege Escalation Creates an Undetectable Forensic Blind Spot on Linux

CVE-2026-31431, dubbed "Copy Fail," enables local root escalation by corrupting the page-cache representation of privileged binaries without touching on-disk files. An attacker abuses the AF_ALG socket interface and splice() to write into cached copies of executables such as /usr/bin/su, yielding root upon next execution.

CISA added CVE-2026-31431 to its Known Exploited Vulnerabilities catalog, with FCEB agencies required to patch by May 15. Standard disk forensics find nothing — the on-disk binary is unmodified. Live memory acquisition at the moment of exploitation is the only reliable detection method, making volatile-memory collection a first-response requirement on any suspected Linux host.

Threat Bulletin

ACTIVE EXPLOIT

CVE-2026-0300

Palo Alto PAN-OS — buffer overflow in the User-ID Authentication Portal enables unauthenticated RCE with root privileges; CVSS 9.3. Exploited since April 9 by state-sponsored cluster CL-STA-1132 for espionage. *Forensic Note:* Capture PA-Series disk images before patching; examine management-process core dumps and auth portal access logs for shellcode injection artifacts.

HIGH

CVE-2026-23918

Apache HTTP Server 2.4.66 mod_http2 — double-free in stream cleanup enables DoS and potential RCE via HTTP/2 early RST attack; CVSS 8.8. Fixed in version 2.4.67. *Forensic Note:* Examine worker-process core dump files and httpd error logs for double-free crash signatures; review HTTP/2 stream identifiers in access logs preceding service disruptions.

MALWARE SPOTLIGHT

BARADAI Ransomware

File-encrypting ransomware identified by CYFIRMA researchers in May 2026 through underground forum monitoring. BARADAI targets a wide range of local and network file types, appending a distinct extension and deploying a ransom note — no public decryptor currently exists. *Forensic Note:* Preserve shadow copy metadata and Volume Change Journal before any recovery action; encrypted file

timestamps reveal the encryption sweep order.

THE FORENSICS WAY

HISTORICAL ARCHIVES | HISTORY OF DIGITAL INVESTIGATION | TUESDAY, MAY 12, 2026

CASE STUDIES: HISTORICAL GRID

BANGLADESH BANK SWIFT HEIST (2016)

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.

ASHLEY MADISON BREACH (2015)

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.

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

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 —

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.

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.

TOOLS OF THE TRADE

OPEN SOURCE

WAInsight

AKHIL DARA — MAY 2026

New open-source forensic analysis suite for WhatsApp data released on GitHub in May 2026. Provides comprehensive extraction and analysis of WhatsApp message databases, media files, and contact records — streamlining evidence collection from the world's most widely used encrypted messaging platform.

COMMERCIAL

Cyber Triage

SLEUTH KIT LABS — 2026 EDITION

Automated endpoint forensics platform for rapid incident response with agentless remote data collection across Windows, Linux, and memory. Identifies malicious activity through YARA scanning, Sigma rule processing, hash analysis, and internal heuristics — enabling simultaneous triage across large numbers of endpoints without on-site agent deployment.

COMMERCIAL

Magnet AXIOM

MAGNET FORENSICS — 2026

Unified forensics platform that builds a single correlated timeline from mobile devices, cloud sources, computer artifacts, and memory captures. AI-assisted artifact triage and automated cloud and mobile extraction surface connections that span disparate evidence sources — widely deployed in enterprise IR and law enforcement multi-source investigations.

OPEN SOURCE

LiME

LINUX MEMORY EXTRACTOR — V1.9

Loadable kernel module for acquiring volatile memory from live Linux systems over the network or to disk, producing images compatible with Volatility and other analysis frameworks. Given CVE-2026-31431's page-cache attack model — where binary corruption exists only in RAM — live memory acquisition via LiME is the sole forensic method capable of capturing Copy Fail evidence.

PRIORITY CVE ADVISORIES

ARCHIVE ALERT

CVE-2026-41940 (CPANEL/WHM)

CRLF injection in session cookie handling enables unauthenticated root-level access; CVSS 9.8. Mass-exploited across 40,000+ hosting servers with ransomware and backdoor deployment. *Forensic Note:* Audit cPanel access logs for malformed cookie payloads and /tmp for ransomware binary drop timestamps.

ARCHIVE ALERT

CVE-2026-2033 (CHROME V8)

Type confusion in Chrome V8 enables RCE via crafted web pages; CVSS 8.8. Added to CISA KEV with confirmed in-the-wild exploitation. *Forensic Note:* Collect Chrome crashpad reports and renderer process sandbox escape events from EDR telemetry and Windows event logs.

RECENT MALWARE WATCH

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. No public decryptor. Hunt ransomware binary artifacts in /tmp and CRLF injection sequences in cPanel access logs.

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 utility process trees in Windows event logs.