THE FORENSICS WAY

ISSUE 05 | FORENSICS AWARENESS THIS WEEK | TUESDAY, MARCH 3, 2026

FRONT PAGE

CRITICAL INFRASTRUCTURE

RESURGE Malware Haunts Ivanti Devices as Edge Forensics Blind Spots Widen

CISA issued updated indicators of compromise this week for **RESURGE**, a persistent malware strain targeting **Ivanti Connect Secure** appliances that has confounded forensic responders by lying dormant well outside the reach of standard endpoint detection tools. Edge network devices — VPN gateways, routers, and remote access appliances — rarely generate the telemetry that investigators rely on, leaving significant gaps in timeline reconstruction.

CISA's guidance urges teams to move beyond host-based triage and adopt appliance-specific acquisition methods alongside network-side flow analysis. For examiners, the RESURGE case is a stark reminder that perimeter devices now represent one of the least-understood and most actively targeted blind spots in modern forensic investigations.

DATA BREACH INVESTIGATION

1.15 Million SSNs Exposed: Ransomware Hits University of Hawai'i Cancer Center

A ransomware incident at the **University of Hawai'i Cancer Center** exposed Social Security numbers for up to 1.15 million individuals, including patients and staff whose data resided in clinical and administrative systems. The scale of identity exposure demands a dual-track forensic response — maintaining clinical continuity while simultaneously managing evidence preservation across access logs, backup systems, and encrypted data stores.

Healthcare DFIR teams are increasingly confronting this challenge: the same systems that must stay operational for patient care are also the primary evidence sources. Examiners working this case type are urged to prioritize immutable log extraction and chain-of-custody documentation early, before operational recovery efforts overwrite critical artifacts.

Threat Bulletin

CRITICAL

CVE-2026-20127

Cisco Catalyst SD-WAN — Remote Root Exploitation. NSA and international partners issued a joint alert on active exploitation granting full root-level device access. Compromised routing infrastructure can enable traffic redirection and log tampering, undermining evidence integrity. *Forensic Note:* Perform control-plane forensics and diff running configs against known-good baselines.

ACTIVE EXPLOIT

CVE-2026-25108

FileZen Command Injection — CISA has ordered emergency mitigations for this actively exploited file-transfer appliance vulnerability. *Forensic Note:* FileZen's native file-monitoring logs may serve as a primary evidence source for validating compromise timelines and scoping data exfiltration.

MALWARE SPOTLIGHT

"Sandworm_Mode" NPM Packages

A supply-chain campaign deploying typosquatted NPM packages via stolen developer credentials to harvest CI/CD pipeline secrets and poison AI coding assistants through rogue MCP server behavior. Targets developer environments directly, making pipeline integrity logs the critical forensic artifact.

THE FORENSICS WAY

HISTORICAL ARCHIVES | HISTORY OF DIGITAL INVESTIGATION | TUESDAY, MARCH 3, 2026

CASE STUDIES: HISTORICAL GRID

THE KEVIN MITNICK MANHUNT (1995)

A Digital Trail Through Stolen Networks

The world's most wanted hacker was caught when security expert Tsutomu Shimomura traced Mitnick's intrusions through cellular network logs and TCP/IP sequence number fingerprinting. Shimomura rebuilt the attack timeline in real time, pioneering techniques in network forensics and live digital pursuit that are foundational to modern incident response.

SONY PICTURES HACK (2014)

When Attribution Became a Geopolitical Act

The FBI attributed the catastrophic Sony Pictures breach to North Korea's Lazarus Group through meticulous malware code analysis, linguistic pattern matching in embedded strings, and infrastructure correlation across shared IP ranges. It was the first time a nation-state cyberattack produced official government sanctions — establishing digital attribution as an instrument of foreign policy.

OPERATION AURORA (2009–2010)

Nation-State Attribution via Code Fingerprints

When China-linked actors breached Google and thirty-plus corporations, investigators used binary analysis, compiler timestamps, and malware reverse engineering to attribute the campaign to specific infrastructure in Shanghai. The case established the foundational methodology for nation-state attribution still applied today.

OPERATION PACIFIER (2014–2015)

FBI Deploys NIT to Break Tor Anonymity

Rather than immediately shutting down the seized Playpen dark web server, the FBI operated it for thirteen days and deployed a court-authorized Network Investigative Technique, capturing real IP addresses, MAC addresses, and hostnames from over 1,300 Tor users. The case remains the most legally debated example of offensive hacking as lawful evidence collection.

TOOLS OF THE TRADE

OPEN SOURCE

Azul

NEW RELEASE — MAR 2026

Australia's Cyber Security Centre (ACSC) released this open-source malware analysis and correlation utility this week. Designed to help defenders analyze malware at scale, Azul accelerates threat investigation and correlation during active incidents. Available now on GitHub.

COMMERCIAL

Magnet AXIOM Cyber

V9.10 — FEB 2026

Fresh off Magnet Virtual Summit 2026, AXIOM Cyber v9.10 brings Event Snapshots for point-in-time cloud state capture, AI-powered synthetic media and video authentication, and expanded remote endpoint collection for hybrid cloud environments.

UTILITY / SCRIPT

KAPE

KROLL ARTIFACT PARSER & EXTRACTOR

Eric Zimmerman's triage powerhouse continues to be the first tool deployed in most Windows IR engagements. KAPE collects and processes forensic artifacts in minutes using community-maintained Targets and Modules — essential for rapid evidence triage on live systems.

COMMERCIAL

Belkasoft Evidence Center X

LATEST — FEB 2026

Belkasoft's latest update adds AI-powered facial recognition, Magnet AXIOM case import for cross-tool workflow continuity, and expanded mobile device support. Particularly strong for social media and messaging artifact extraction across iOS and Android.

PRIORITY CVE ADVISORIES

ARCHIVE ALERT

CVE-2026-21519 (WINDOWS)

Windows Desktop Window Manager privilege escalation to SYSTEM. Actively exploited in the wild. *Forensic Note:* Hunt for low-privilege processes spawning elevated children in security event logs.

ARCHIVE ALERT

CVE-2026-2441 (CHROME)

Use-after-free zero-day in Chrome CSS engine enabling drive-by code execution. Added to CISA KEV. *Forensic Note:* Preserve browser profiles and check renderer crash logs for exploitation indicators.

RECENT MALWARE WATCH

ARCHIVE: FEB 24, 2026

PROMPTSPY (ANDROID)

First Android malware using Google Gemini AI at runtime to adapt its persistence across device configurations. Embeds a VNC module for real-time remote screen control once Accessibility permissions are granted.

ARCHIVE: FEB 24, 2026

REYNOLDS RANSOMWARE

Ships with a built-in BYOVD module that terminates endpoint security tools before deploying encryption. Look for signed-but-vulnerable driver artifacts in %TEMP% on compromised hosts.