THE FORENSICS WAY

ISSUE 08 | FORENSICS AWARENESS THIS WEEK | TUESDAY, MARCH 24, 2026

FRONT PAGE

ZERO-DAY EXPLOITATION

36 Days in the Dark: Interlock Ransomware Exploited Cisco FMC Before Anyone Knew the Flaw Existed

The Interlock ransomware group exploited **CVE-2026-20131**, a CVSS 10.0 critical flaw in Cisco Secure Firewall Management Center, as an active zero-day for 36 days before Cisco patched it on March 4. Amazon's threat intelligence team uncovered the campaign after Interlock's own infrastructure server was misconfigured — exposing their full attack toolkit.

Interlock blended into admin activity using legitimate tools — ConnectWise ScreenConnect, Volatility, and the AD exploitation tool Certify — leaving no obvious malware signatures. Compromising the FMC grants root-level access to an entire firewall estate; FMC audit logs and connected Firepower device artifacts must now be treated as primary forensic evidence.

SUPPLY CHAIN ATTACK

Scanner to Stealer: The Trivy Compromise Spawned a Blockchain-C2 Worm Across 141 npm Packages

On March 19, threat group **TeamPCP** hijacked the trivy-action GitHub repository and published a weaponized v0.69.4 that silently stole CI/CD credentials — SSH keys, cloud configs, Kubernetes secrets, and .env files — while continuing to run legitimate Trivy scans, making detection nearly impossible without artifact-level analysis.

The follow-on **CanisterWorm** uses an Internet Computer blockchain canister as its C2 resolver — the first documented ICP abuse for malware command-and-control — rendering DNS takedown useless. Any org that ran trivy-action between March 19–22 should treat build runners as compromised; hunt for the *pgmon* systemd service and *~/.config/sysmon.py*.

Threat Bulletin

ACTIVE EXPLOIT

CVE-2026-20131

Cisco Secure FMC — Unauthenticated RCE via insecure Java deserialization; CVSS 10.0. Zero-day exploited by Interlock ransomware since January 26; added to CISA KEV March 20. *Forensic Note:* Audit FMC HTTP request logs and Firepower devices for lateral movement artifacts.

CRITICAL

CVE-2026-3564

ConnectWise ScreenConnect — ASP.NET machine key exposure allows session token forgery and support session hijacking; CVSS 9.0. Patched in v26.1 on March 18. *Forensic Note:* In MSP-linked intrusions, audit ScreenConnect session logs and config files for machine key extraction.

MALWARE SPOTLIGHT

CanisterWorm (TeamPCP)

Self-propagating npm worm — spawned by the Trivy supply chain compromise — that spreads autonomously by harvesting npm auth tokens and publishing malicious packages. Uses an ICP blockchain canister for C2, the first such documented abuse, making network-layer defenses ineffective. *Forensic Note:* Hunt via pgmon systemd service, ~/.config/sysmon.py, and ICP canister beacon traffic.

THE FORENSICS WAY

HISTORICAL ARCHIVES | HISTORY OF DIGITAL INVESTIGATION | TUESDAY, MARCH 24, 2026

CASE STUDIES: HISTORICAL GRID

SOLARWINDS ORION SUPPLY CHAIN (2020)

SUNBURST: The Supply Chain Attack That Reached 18,000 Organizations

In December 2020, state-sponsored attackers embedded a backdoor called SUNBURST into SolarWinds Orion software updates, compromising 18,000 organizations including nine US federal agencies. The malware lay dormant for two weeks before activation, communicating via DNS beaconing that mimicked legitimate Orion traffic. Its discovery forced investigators to develop new methodologies to distinguish compromised telemetry from authentic network data — a foundational challenge directly mirrored in this week's Trivy compromise.

COLONIAL PIPELINE RANSOMWARE (2021)

One Compromised Password Shut Down 45% of US East Coast Fuel Supply

The DarkSide ransomware attack on Colonial Pipeline in May 2021 forced a six-day shutdown of 5,500 miles of fuel pipeline serving 45% of the US East Coast. Attackers gained initial access via a single compromised VPN credential with no MFA enforced — the account had not been used in months but remained active. The incident became the primary basis for CISA's OT/ICS network segmentation guidance and defined critical infrastructure incident response planning for years.

OPM DATA BREACH (2014–2015)

21.5 Million Fingerprints — The Worst Espionage Breach in US History

Chinese state actors exfiltrated the complete security clearance files — including fingerprints, personal histories, and foreign contacts — of 21.5 million federal employees and contractors from the Office of Personnel Management. The breach went undetected for over a year. Forensic investigators found the attackers had used stolen credentials from an OPM contractor as their initial access vector, establishing a direct line

TARGET POS BREACH (2013)

40 Million Cards Stolen Through an HVAC Vendor

Attackers stole 40 million credit and debit card numbers from Target's point-of-sale systems by first compromising Fazio Mechanical, a small HVAC contractor with remote network access. The case pioneered retail DFIR methodology, introduced RAM scraping malware to mainstream incident response, and remains the definitive case study in third-party supply chain risk — directly applicable to this week's Trivy CI/CD pipeline intrusion.

between third-party vendor risk and catastrophic data loss.

TOOLS OF THE TRADE

OPEN SOURCE

Hindsight

V2026.01 — FEBRUARY 2026

Web artifact forensics for Chrome and all Chromium-based browsers — URLs, downloads, cache, cookies, passwords, and extensions. The v2026.01 release adds Chrome Sync Data parsing from local LevelDB files, enabling cross-device attribution for synced visits. Exports to XLSX, JSONL, and SQLite for direct Timesketch ingestion.

OPEN SOURCE

MalChela

MARCH 2026 UPDATE

Rust-based malware analysis suite covering static analysis, string extraction, entropy detection, PE parsing, YARA scanning, and ATT&CK technique mapping. The March 2026 update adds MCP integration — run all tools via natural language through an AI assistant. Well-suited for rapid triage of suspicious npm package artifacts like those in the CanisterWorm campaign.

UTILITY / SCRIPT

Velociraptor MCP Server

ACTIVE RELEASE — MARCH 2026

Model Context Protocol bridge between Velociraptor and LLMs — exposes VQL hunt execution, artifact collection, and fleet management as AI tool calls. Analysts issue natural language hunts instead of writing VQL manually. Directly applicable for hunting CanisterWorm IOCs (pgmon service, sysmon.py) across entire CI/CD runner fleets at speed.

UTILITY / SCRIPT

DFIR Toolkit

INITIAL RELEASE — MARCH 2026

Zero-install, browser-based forensic utilities — IOC extraction, timestamp conversion, file hashing, and email header analysis — processed entirely client-side with no data leaving the browser. Built for live-response on locked-down endpoints where installing tools is prohibited. Ideal for rapid IOC triage of CanisterWorm npm package artifacts in regulated environments.

PRIORITY CVE ADVISORIES

ARCHIVE ALERT

CVE-2026-3910 (CHROMIUM V8)

Type confusion RCE via malicious web content. Added to CISA KEV March 13; emergency Chrome 146 patch released. *Forensic Note:* Preserve browser profiles and V8 crash telemetry; renderer process anomalies appear in crash logs.

ARCHIVE ALERT

CVE-2026-26110 (MICROSOFT OFFICE)

Office RCE via Preview Pane — code executes without opening the file; Explorer preview is sufficient. One of two zero-days in March Patch Tuesday. *Forensic Note:* Check Outlook preview events in Windows telemetry alongside the standard file-open artifact chain.

RECENT MALWARE WATCH

ARCHIVE: MAR 17, 2026

AVRECON BOTNET (SOCKSESCORT)

360,000 compromised routers recruited since 2020 to launder ransomware C2 traffic. Dismantled by US and European authorities. Minimal on-device artifacts — hunt via outbound connection anomalies and firmware integrity checks.

ARCHIVE: MAR 10, 2026

BAQIYATLOCK WIPER

Iran-aligned wiper deployed as a ransomware facade — no decryption key ever issued. Targets MBR and file headers for permanent destruction. Volatile memory capture is the only viable forensic path post-execution.