THE FORENSICS WAY

ISSUE 07 | FORENSICS AWARENESS THIS WEEK | TUESDAY, MARCH 17, 2026

FRONT PAGE

INSIDER THREAT

The Trusted Responder: US Prosecutors Allege IR Consultant Aided BlackCat Ransomware Actors

US prosecutors have alleged that a licensed incident response consultant deliberately assisted **BlackCat/ALPHV ransomware operators** during live engagements — exploiting privileged network access to facilitate attacker persistence and hamper victim recovery. It is one of the most disturbing insider threat cases in DFIR history.

The implications are industry-wide. Vendor vetting, privileged access governance, and independent remediation verification are now evidentiary necessities. Forensic examiners should document every action taken under external consultant credentials and treat all third-party IR access as a potential privileged-access risk.

LIVING-OFF-THE-LAND ATTACK

Stryker Breach: Attackers Abuse Microsoft Intune to Disrupt Medical Device Supply Chain

Attackers disrupted manufacturing at **Stryker**, one of the world's largest medical device manufacturers, by abusing **Microsoft Intune** and native management tools rather than deploying malware — evading every malware-centric control in the environment. A textbook living-off-the-land execution with no malicious binaries on disk.

Investigators must reconstruct attacker actions entirely from Intune audit logs, Azure AD sign-in records, and device compliance policy change histories. The Stryker case confirms that management-plane forensics is now a core IR competency, and tools like DeepBlueCLI are increasingly essential for hunting these artifact chains.

Threat Bulletin

ACTIVE EXPLOIT

CVE-2026-3910

Chromium V8 Engine — 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; exploitation leaves renderer process anomalies in crash logs.

CRITICAL

CVE-2026-26110

Microsoft Office RCE via Preview Pane — code executes without opening the file; previewing in Explorer is sufficient. One of two zero-days in March Patch Tuesday's 84-fix release. *Forensic Note:* Check Outlook preview events in Windows telemetry alongside the standard file-open artifact chain.

MALWARE SPOTLIGHT

Avrecon Botnet (SocksEscort)

US and European authorities dismantled the SocksEscort proxy-for-hire network — 360,000 compromised routers recruited since 2020 to launder ransomware C2 traffic. *Forensic Note:* Minimal on-device artifacts; hunt via outbound connection anomalies and firmware integrity checks.

THE FORENSICS WAY

HISTORICAL ARCHIVES | HISTORY OF DIGITAL INVESTIGATION | TUESDAY, MARCH 17, 2026

CASE STUDIES: HISTORICAL GRID

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 between third-party vendor risk and catastrophic data loss.

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 Stryker Intune intrusion.

STUXNET / OPERATION OLYMPIC GAMES (2010)

The First Cyberweapon Deployed Against Iran

Jointly developed by the NSA and Israel's Unit 8200, Stuxnet was a precision instrument designed to destroy Iranian centrifuges at Natanz while reporting normal status to operators. Its forensic discovery by Kaspersky and Symantec researchers established the foundational methodology for ICS/SCADA malware analysis still applied today.

NOTPETYA WIPER ATTACK (2017)

The $10 Billion Lesson in Destructive Malware

Disguised as ransomware, Russia's NotPetya was a pure wiper that caused an estimated $10 billion in global damages. Forensic analysts at ESET and Kaspersky determined the ransom facade was deliberate misdirection — a lesson that directly informs how investigators must approach Iran-aligned BaqiyatLock and Sicarii deployments today.

TOOLS OF THE TRADE

UTILITY / SCRIPT

DeepBlueCLI

OPEN SOURCE — ERIC CONRAD

PowerShell-based Windows Event Log analysis tool built specifically to hunt living-off-the-land attacks. Detects suspicious PowerShell usage, pass-the-hash, Mimikatz activity, and user creation events — exactly the artifact chain left behind by Intune-based intrusions like the Stryker breach.

OPEN SOURCE

Autopsy

V4.21 — 2026

The most widely used open-source digital forensics platform. Version 4.21 adds improved ML-based file classifier modules, enhanced timeline analysis, and expanded support for newer Android filesystem structures — a reliable foundation for examiners at every level.

OPEN SOURCE

Wireshark

V4.4 — 2026

The gold standard for network protocol analysis. v4.4 adds improved decryption support for TLS 1.3 sessions when keys are available, enhanced packet filtering, and new dissectors for cloud-native protocols. Essential for tracing Avrecon-style botnet C2 traffic buried inside legitimate service flows.

COMMERCIAL

Semperis ADFR

ACTIVE DIRECTORY FOREST RECOVERY

Purpose-built for Active Directory forensics and recovery following ransomware attacks. Captures a forensic snapshot of AD state pre-encryption, supports tiered forest recovery, and generates change-diff reports that serve as primary evidence in post-incident investigations involving credential-based lateral movement.

PRIORITY CVE ADVISORIES

ARCHIVE ALERT

CVE-2026-0145 (PALO ALTO)

PAN-OS GlobalProtect authentication bypass. Preferred initial-access vector for Iranian APT groups Seedworm and APT42. *Forensic Note:* Audit GlobalProtect session logs for anomalous authentication patterns.

ARCHIVE ALERT

CVE-2026-1834 (FORTINET)

FortiGate SSL-VPN unauthenticated RCE. Actively weaponized by Iran-aligned actors as a secondary access mechanism. *Forensic Note:* Review SSL-VPN session initiations and anomalous HTTPD child processes.

RECENT MALWARE WATCH

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.

ARCHIVE: MAR 10, 2026

WEZRAT (APT42)

Iran's APT42 infostealer persisting via legitimate cloud services to harvest credentials and session tokens. Minimal system footprint — hunt via cloud auth logs and anomalous OAuth token grants.