THE FORENSICS WAY

ISSUE 03 | FORENSICS AWARENESS THIS WEEK | TUESDAY, FEBRUARY 17, 2026

FRONT PAGE

THREAT ACTOR SPOTLIGHT

Velociraptor Turned Weapon: Attackers Deploy DFIR's Own Framework as a RAT

In a striking reversal, threat actors exploiting **SolarWinds Web Help Desk** vulnerabilities have been observed deploying *Velociraptor*—a legitimate open-source digital forensics and incident response framework—as a remote access and data collection tool. After gaining initial entry, operators pivot through **Cloudflare tunnels** and Zoho infrastructure to establish covert command channels, then weaponize Velociraptor's VQL query engine to harvest system artifacts, enumerate credentials, and exfiltrate data.

DFIR teams investigating these intrusions must hunt specifically for unauthorized MSI installs, VQL script activity, and Cloudflare tunnel artifacts—while moving fast. Attackers are actively erasing traces, making volatile evidence preservation the immediate priority upon detection.

EVIDENTIARY CHALLENGE

Deepfakes Are Outpacing Forensics: The Coming Admissibility Crisis

Digital forensics pioneer **Hany Farid** warned this week that generative AI has made convincing synthetic media faster and cheaper to produce than the forensic tools available to authenticate it. Courts in New York and California, operating under new AI provenance laws enacted in January, now require verifiable cryptographic markers on AI-generated media—but enforcement depends entirely on examiner capability to detect their absence.

Farid's central concern for practitioners is a credibility gap: jurors who cannot distinguish authentic footage from sophisticated deepfakes may begin to doubt all digital evidence. The implication for forensic examiners is stark—media authentication must now be treated as a foundational competency, not a specialist skill.

Threat Bulletin

CRITICAL

CVE-2026-21510

Windows Shell SmartScreen Security Feature Bypass. Attackers trick users into opening malicious .lnk shortcut files, silently bypassing SmartScreen warnings and executing untrusted code. One of six zero-days patched in Microsoft's February Patch Tuesday. *Forensic Note:* Check recent items, jump lists, and prefetch for unsigned .lnk launches.

ACTIVE EXPLOIT

CVE-2026-1731

BeyondTrust Remote Support & Privileged Remote Access — Unauthenticated RCE. Internet-exposed helpdesk platforms are a primary initial-access vector. *Forensic Note:* Review remote support session logs and look for anomalous child processes spawned by BeyondTrust agents.

MALWARE SPOTLIGHT

Reynolds Ransomware

A newly disclosed ransomware family shipping with a built-in Bring Your Own Vulnerable Driver (BYOVD) module that terminates endpoint security tools before deploying encryption. *Forensic Note:* Look for signed-but-vulnerable driver artifacts in %TEMP% and event logs showing abrupt security service terminations.

THE FORENSICS WAY

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

CASE STUDIES: HISTORICAL GRID

THE GOLDEN STATE KILLER (2018)

Genealogical DNA Closes a 40-Year Cold Case

Joseph James DeAngelo evaded capture for four decades until investigators submitted crime-scene DNA to a public genealogy database, built a family tree, and narrowed suspects to one individual. Discarded items confirmed the match. The case pioneered investigative genetic genealogy as a forensic discipline and sparked major legal debate over DNA privacy.

COLONIAL PIPELINE RECOVERY (2021)

DOJ Traces and Seizes $2.3M in Ransom Bitcoin

After Colonial Pipeline paid DarkSide ransomware operators 75 Bitcoin, the DOJ's Digital Currency Unit traced the funds through blockchain analysis and seized 63.7 BTC within weeks. The case demonstrated that cryptocurrency transactions—though pseudonymous—leave an immutable, forensically traceable ledger, establishing a new standard for crypto-asset recovery operations.

CASE STUDY: LYNX RANSOMWARE

The RDP Pivot Point

In a recent forensic engagement, Lynx operators gained access via a single non-MFA RDP account. Within six hours, they had mapped the entire network using legitimate tools, demonstrating the speed of modern ransomware pivots.

ARTIFACT ANALYSIS: LYNX

Persistence and Evasion

Detailed investigation into the Lynx execution chain reveals the use of custom scripts to disable security software prior to the deployment of the encryption engine, highlighting a need for immutable logging.

PRIORITY CVE ADVISORIES

ARCHIVE ALERT

CVE-2026-4411 (RDS)

Remote Desktop Services Arbitrary File Execution. Actively leveraged by Lynx operators to drop initial-stage loaders. *Forensic Note:* Review RDP

ARCHIVE ALERT

CVE-2026-5522 (WINDOWS)

Windows Service Persistence Vulnerability. Allows attackers to maintain elevated access without triggering system integrity alarms. *Forensic Note:* Audit

RECENT MALWARE WATCH

ARCHIVE: FEB 3, 2026

LYNX RANSOMWARE

Sophisticated C++ strain prioritizing shadow copy destruction and network share encryption via compromised

ARCHIVE: FEB 2026

SECTOPRAT V.2

Remote Access Trojan using "ClickFix" browser-update lures for credential exfiltration. Frequently observed as a

session logs and prefetch artifacts for unsigned loader activity.

service registry keys against known-good baselines.

administrative tokens. Favors exposed RDP for initial access.

secondary payload during the Lynx initial access phase.