THE FORENSICS WAY

ISSUE 11 | FORENSICS AWARENESS THIS WEEK | TUESDAY, APRIL 14, 2026

FRONT PAGE

NATION-STATE INFRASTRUCTURE

Operation Masquerade Dismantled: DOJ and Allies Seize APT28's 18,000-Router DNS Hijacking Network

The DOJ, FBI, UK NCSC, and allied agencies revealed on April 8 the court-authorized disruption of **Operation Masquerade** — a Russian GRU (APT28 / Fancy Bear) botnet of 18,000 compromised SOHO routers across 120+ countries. The GRU hijacked router DNS resolvers to redirect traffic to fraudulent servers impersonating Microsoft Outlook Web Access, silently harvesting passwords, authentication tokens, and email content.

The FBI deployed court-authorized commands directly to compromised US routers — collecting forensic evidence, resetting malicious DNS resolvers, and blocking the original access vector. DNS hijacking leaves no malware on victim endpoints; investigators must work entirely from router configuration snapshots, DNS query histories, and cloud-service authentication logs.

CLOUD FORENSICS

CERT-EU's Kill Chain: How TruffleHog Became the Attacker's Pivot Tool Inside the Commission's AWS Environment

CERT-EU's April 12 reconstruction confirmed the Trivy breach reached **71 EU entities** — 42 Commission bodies plus 29 other EU organizations. After obtaining the initial AWS API key, the attacker immediately used **TruffleHog** to harvest additional cloud credentials, then created a new IAM key attached to an existing user to blend into normal account activity.

The 340 GB of uncompressed data appeared on ShinyHunters nine days after initial access — compressing the remediation window to hours. Security tooling in CI/CD pipelines must itself be subject to integrity verification, and DFIR teams must add secrets-scanning tools like TruffleHog to their threat models as attacker pivot instruments.

Threat Bulletin

ACTIVE EXPLOIT

CVE-2026-34621

Adobe Acrobat & Reader — JavaScript prototype pollution enables RCE when a victim opens a crafted PDF; CVSS 8.6. Exploited since late 2025; emergency patch April 12; CISA KEV April 13 with April 27 federal deadline. *Forensic Note:* Review email gateway logs for PDF delivery and endpoint telemetry for Reader spawning unexpected child processes.

ACTIVE EXPLOIT

CVE-2012-1854

Microsoft Office VBA — Insecure library loading (DLL hijacking) originally disclosed 2012; re-added to CISA KEV April 13 due to active re-exploitation combined with modern initial-access chains. *Forensic Note:* Hunt for DLL side-loading artifacts in VBA macro process trees and unexpected DLL loads from user-writable directories.

MALWARE SPOTLIGHT

Omnistealer (North Korea)

North Korea-linked infostealer using TRON blockchain as C2 — payloads embedded in BSC transaction input fields, making sinkholing useless. Targets 10+ password managers, 60+ crypto wallets, and cloud credentials; ~300,000 credentials stolen. *Forensic Note:* Hunt outbound connections to TRON and Aptos RPC endpoints; on-chain transaction analysis is now a required DFIR capability for this class of malware.

THE FORENSICS WAY

HISTORICAL ARCHIVES | HISTORY OF DIGITAL INVESTIGATION | TUESDAY, APRIL 14, 2026

CASE STUDIES: HISTORICAL GRID

YAHOO DATA BREACH (2013–2016)

3 Billion Accounts — Russian FSB Operated Silently Inside Yahoo for Three Years

Russian FSB officers infiltrated Yahoo between 2013 and 2016, stealing data on all 3 billion user accounts — the largest breach ever recorded — while Yahoo remained unaware for three years. The attackers also forged authentication cookies, bypassing login event logging entirely. The case established that post-breach forensics must account for multi-year silent dwell and authentication artifact gaps — the same patient persistence pattern demonstrated by APT28 this week.

MARRIOTT / STARWOOD BREACH (2014–2018)

Chinese State Actors Spent Four Years Inside a Network That Was Then Acquired for $13 Billion

Chinese state-sponsored hackers breached Starwood's hotel network in 2014 and remained undetected for four years — surviving Marriott's $13 billion acquisition in 2016 without detection. By discovery in 2018, 500 million guest records had been exfiltrated including passport numbers. The case is the definitive forensic lesson in M&A due diligence: Marriott unknowingly acquired an active four-year intrusion as part of the deal.

XCODEGHOST (2015)

4,000 Infected iOS Apps: When China Poisoned the Developer Toolchain Itself

In 2015, Chinese attackers distributed a counterfeit version of Apple's Xcode through domestic file-sharing sites, causing thousands of iOS developers to unknowingly compile malware into their own apps. Over 4,000 infected apps — including WeChat — passed Apple's code-signing process and reached end users worldwide. The case proved developer toolchain compromise is more dangerous than

EVENT-STREAM NPM POISONING (2018)

Ownership Transfer as an Attack Vector: The npm Compromise That Foreshadowed the Supply Chain Era

In November 2018, a malicious contributor convinced the maintainer of event-stream — 2 million weekly downloads — to transfer package ownership, then quietly added a dependency containing a cryptocurrency stealer targeting Copay Bitcoin wallet users. The package sat undetected for two months. The case first demonstrated that npm ownership transfer itself

direct payload delivery — the developer becomes an unwitting distributor at scale.

was an attack vector, directly foreshadowing the social engineering of the Axios maintainer by UNC1069.

TOOLS OF THE TRADE

OPEN SOURCE

Spectacular

NEW RELEASE — APRIL 2026

Open-source forensic parser for Meta Ray-Ban smart glasses artifacts in mobile extractions. Parses settings files, sync logs, linked accounts, Meta AI prompt histories, and EXIF data from glasses-captured media that may reveal geolocation. Fills a gap left by all major mobile forensics platforms — smart glasses are a rapidly expanding evidence surface with no prior tool support.

OPEN SOURCE

TruffleHog

V3 — ACTIVE 2026

Open-source secrets scanner detecting exposed credentials and API keys across Git repositories, CI/CD pipelines, and cloud environments. This week TruffleHog was weaponized by the EU Commission attacker to pivot from one AWS key to a broader credential set — confirming DFIR tooling itself must be in investigators' threat models. Also the fastest way to assess what secrets were visible to an attacker in a breached pipeline.

OPEN SOURCE

Zeek

ACTIVE RELEASE — 2026

Network security monitoring framework generating structured logs from traffic or PCAPs — DNS, HTTP, SSL, and 50+ protocol records. Zeek's dns.log captures every resolver query and response, making it ideal for hunting APT28-style DNS manipulation: malicious resolver substitutions in router configs leave a distinct trail in DNS response anomalies. Core to most enterprise network forensics workflows.

COMMERCIAL

Chainalysis Reactor

CHAINALYSIS — ACTIVE 2026

Blockchain forensics platform used by law enforcement in 70+ countries to trace cryptocurrency transactions and de-anonymize wallet clusters. Directly applicable to Omnistealer investigations — Reactor can trace TRON and BSC transactions used as C2 back to exchanges and link wallet clusters to the North Korean operators. The industry standard for on-chain attribution in nation-state and financial crime cases.

PRIORITY CVE ADVISORIES

ARCHIVE ALERT

CVE-2026-35616 (FORTICLIENT EMS)

Unauthenticated API bypass and arbitrary code execution on the EMS host; CVSS 9.1. CISA KEV April 6. *Forensic Note:* EMS controls enterprise endpoint policy — review API call patterns and scheduled tasks for signs of unauthorized lateral movement.

ARCHIVE ALERT

CVE-2026-3502 (TRUECONF)

Update mechanism skips integrity verification, enabling malicious executable delivery to all connected clients; CVSS 7.8. Exploited against Southeast Asian governments. *Forensic Note:* Compare binary hashes to known-good; hunt processes spawned from the update service.

RECENT MALWARE WATCH

ARCHIVE: APR 7, 2026

WAVESHAPER.V2 (UNC1069)

North Korea's cross-platform backdoor delivered via poisoned Axios npm. Dropper SILKBELL self-destructs post-execution, defeating npm audit. Hunt via package-lock.json diffs for plain-crypto-js and CI/CD outbound connections.

ARCHIVE: MAR 31, 2026

INFINITI STEALER (CLICKFIX)

Python macOS infostealer via fake Cloudflare browser prompts using Bash one-liners. No traditional binary footprint — requires script-execution monitoring for detection.