THE FORENSICS WAY

ISSUE 21 | FORENSICS AWARENESS THIS WEEK | TUESDAY, JUNE 23, 2026

FRONT PAGE

DEFENSE EVASION

Killing the Watchdogs: The Gentlemen RaaS Ships an In-House "GentleKiller" Framework That Blinds 400+ Security Tools

ESET this week detailed GentleKiller, an in-house EDR-killing framework that the Gentlemen ransomware-as-a-service gang — one of 2026's most active, with roughly 478 victims — hands to its affiliates as a turnkey suite. The framework ships at least eight variants, each impersonating a different legitimate security product and abusing a unique signed-but-vulnerable kernel driver. Using Bring Your Own Vulnerable Driver, it terminates protection from kernel space, beneath user-mode defenses, targeting more than 400 processes across some 48 products from Microsoft Defender and CrowdStrike to Sophos and ESET's own agents.

The operation industrializes evasion: it weaponizes freshly published BYOVD proof-of-concepts — tools like UnknownKiller and PoisonKiller — within days of their GitHub disclosure, and folds in third-party killers (HexKiller, ThrottleBlood, HavocKiller) behind a shared evasion layer wrapped in Enigma or Themida. A 90% affiliate cut and a focus on Southeast Asia, South America, and Western Europe round out the model. Forensic priority: hunt signed-but-vulnerable driver writes and Service Control Manager driver-load events, correlate abrupt security-service terminations, and cross-check loaded drivers against known-vulnerable catalogs — because once the killer runs, the endpoint's own telemetry goes dark.

MAC FORENSICS

What the Mac Still Remembers: A New macOS Tahoe Biome Stream Logs Every Menu Click — and Can Reconstruct Deliberate User Actions

Even as attackers race to blind real-time defenses, examiners just gained a quiet new witness. Researchers featured in Forensic Focus's June 17 round-up documented a newly identified artifact

Threat Bulletin

ACTIVE EXPLOIT

CVE-2026-48907

Joomla Content Editor (JCE) — an improper access-control flaw lets an unauthenticated attacker create a rogue editor profile and abuse the profile-import workflow to upload and execute arbitrary PHP, planting a persistent web shell; CVSS 10.0. It chains missing authorization, weak file validation, and disabled upload safeguards in JCE 1.0.0 through 2.9.99.4 (fixed in 2.9.99.5). CISA added it to the KEV on June 16 with a June 19 federal deadline. *Forensic Note:* Hunt newly imported editor profiles, rogue PHP under media/upload directories, and web-shell callbacks; inventory JCE versions across all Joomla sites.

CRITICAL

CVE-2026-42530

NGINX (F5) — a use-after-free in the HTTP/3 module (*ngx_http_v3_module*) lets an unauthenticated remote attacker trigger denial of service or, where ASLR is disabled or bypassed, remote code execution in the worker process; CVSS 9.2. F5 shipped out-of-band fixes on June 18 alongside companion bug CVE-2026-42055 (an HTTP/2 and gRPC heap overflow), spanning NGINX Open Source, Plus, Gateway Fabric, and Instance Manager. *Forensic Note:* Review HTTP/3 (QUIC) traffic and worker-process crash artifacts, hunt malformed gRPC and proxy requests, and confirm upgrade to OSS 1.31.2 or Plus R37 P2 / R36 P6.

MALWARE SPOTLIGHT

in macOS Tahoe 26: an *App.MenuItem* Biome stream, at *~/Library/Biome/streams/restricted/App.MenuItem/local*, that timestamps every menu selection a user makes across applications. Correlated with file-system and unified-log records, it lets investigators reconstruct intent — evidence that a user deliberately compressed, encrypted, or deleted files rather than a process doing so on its own.

Biome is Apple's on-device behavioral store, and these protected streams accumulate a high-resolution record of activity that survives even when an application keeps no logs of its own — exactly the residue that outlasts an attacker's clean-up or an insider's denials. The same round-up tempers the find with a Daubert-flavored caution: examiners must test alternate explanations before asserting causation. Forensic priority: preserve the restricted Biome streams during acquisition, decode their SEGB/protobuf records, and corroborate every menu event against file-system and unified-log timestamps before drawing conclusions.

Rokarolla — Android Banker With Full Device Takeover

Zimperium's zLabs detailed Rokarolla, an Android banking trojan that targets 217 banking and cryptocurrency apps through a toolkit of 137 remote commands. Spread by fake sites posing as TikTok or Chrome, it leans entirely on a single granted Accessibility permission to overlay fake login pages, harvest lock-screen credentials, SMS, and contacts, keylog input, and block or intercept calls to suppress bank fraud alerts — and it rewrites the clipboard to swap in attacker crypto-wallet addresses. *Forensic Note:* Examine Accessibility-service grants, sideload origins, overlay-injection artifacts, and clipboard-tampering hooks; check for call-blocking configuration.

THE FORENSICS WAY

HISTORICAL ARCHIVES | HISTORY OF DIGITAL INVESTIGATION | TUESDAY, JUNE 23, 2026

CASE STUDIES: HISTORICAL GRID

ROBBINHOOD & THE GIGABYTE DRIVER (2019–2020)

The Ransomware That Brought Its Own Kernel Key: How BYOVD Was Born as a Way to Murder Antivirus

Documented by Sophos in 2020, the RobbinHood ransomware — the strain that crippled Baltimore and Greenville — pioneered a now-ubiquitous trick: it dropped a legitimately signed Gigabyte motherboard driver carrying CVE-2018-19320, exploited that signed driver to gain kernel write access, switched off Windows driver-signature enforcement, and loaded its

CASEY ANTHONY DIGITAL FORENSICS (2008–2011)

The Searches the Computer Kept: How Browser Artifacts — and One Forensic Misstep — Defined a Murder Trial

The 2011 trial of Casey Anthony turned on what her family's computer had quietly recorded: browser and search-history artifacts, including a notorious query about a "fool-proof" method of suffocation made on the day her daughter was last seen alive. The case also became a cautionary tale in forensic rigor when the examination software miscounted how many times a key page

own malicious driver to kill antivirus and EDR processes before encrypting. It was the first widely analyzed case of attackers carrying a trusted, signed driver onto a host purely to dismantle its defenses. Six years on, this week's GentleKiller framework has turned that one-off technique into an industrialized, affiliate-ready EDR-killing arsenal.

had been visited — reporting one visit instead of dozens — a discrepancy that surfaced only after the verdict. It stands as a lasting lesson that systems silently log deliberate user actions, and that examiners must validate every artifact before relying on it — the same discipline now demanded by the macOS Biome menu-logging stream on Page 1.

XZ UTILS BACKDOOR (2024)

The Backdoor That Almost Owned Linux: A Patient Maintainer, a Poisoned Build, and a One-in-a-Million Catch

In March 2024, a Microsoft engineer chasing a half-second SSH delay uncovered CVE-2024-3094 — a backdoor buried in the xz/liblzma compression library by "Jia Tan," a contributor who had spent roughly two years earning maintainer trust before slipping malicious build-time code into release tarballs. The implant hooked OpenSSH's authentication path and would have handed a chosen attacker remote access across countless Linux distributions. Discovered almost by accident days before it reached stable releases, it remains the canonical lesson in how trusted, signed components get weaponized — the same abuse of legitimacy that lets GentleKiller load signed-but-vulnerable drivers to blind defenders on Page 1.

LOCKBIT 3.0 BUILDER LEAK (2022)

When Ransomware Went Open Source: A Leaked Builder Put Click-to-Encrypt Malware in Anyone's Hands

In September 2022, a disgruntled developer leaked LockBit's 3.0 ("Black") builder, publishing the encryptor, decryptor, and a configuration tool that let anyone generate fully functional, customized ransomware in minutes. The leak spawned a wave of copycat operations that simply rebranded LockBit's code, badly muddying attribution for investigators who could no longer assume a LockBit payload meant the LockBit crew. It marked the moment ransomware capability detached from skill — the same commoditization now embodied by the Gentlemen RaaS on Page 1, which hands affiliates a prepackaged EDR-killer suite and a 90% cut.

TOOLS OF THE TRADE

OPEN SOURCE

LOLDrivers

MAGICSWORD — LIVE CATALOG

Community-curated catalog of known vulnerable and malicious Windows drivers, complete with hashes, certificate details, and ready-made detection rules. It is the direct counter to Page 1's GentleKiller: cross-reference any loaded kernel driver against the list to spot the signed-but-exploitable drivers

UTILITY / SCRIPT

Sigcheck

SYSINTERNALS — V2.X

Command-line utility that verifies file signatures, certificate chains, and VirusTotal status, flagging signed-but-revoked or anomalously signed binaries. Run it against suspect drivers in %TEMP% or system32\drivers to confirm the legitimately-signed-yet-vulnerable

OPEN SOURCE

mac_apt

YOGESH KHATRI — V1.X

macOS Artifact Parsing Tool that processes disk images and live systems for hundreds of artifacts, including Biome streams, Spotlight, and unified logs. The right tool to extract and timeline the new App.MenuItem stream from Page 1 and corroborate deliberate-user-action evidence across data sources.

COMMERCIAL

Binalyze AIR

BINALYZE — SAAS / ON-PREM

Automated DFIR platform that remotely collects hundreds of evidence types and triages endpoints at fleet scale. Valuable precisely when an EDR killer has blinded agent telemetry — gather raw driver, service, and event-log artifacts independently of the very tool the attacker just disabled.

attackers carry in to kill EDR.

driver behind an EDR blackout.

PRIORITY CVE ADVISORIES

ARCHIVE ALERT

CVE-2026-35273 (ORACLE PEOPLESOFT)

Unauthenticated SSRF-to-RCE in the PeopleTools Environment Management Hub (PSEMHUB) lets a remote attacker run code with no credentials; CVSS 9.8. Exploited as a zero-day by ShinyHunters from May 27; CISA KEV June 12. *Forensic Note:* Review PSEMHUB and web-server logs for unauthenticated requests and hunt web shells; inventory PeopleTools 8.61/8.62.

ARCHIVE ALERT

CVE-2026-20253 (SPLUNK ENTERPRISE)

An unauthenticated PostgreSQL sidecar (added in v10) accepts any credentials on its recovery endpoints, letting an attacker write files and chain a malicious DB restore into code execution; CVSS 9.8. *Forensic Note:* Audit the postgres recovery endpoints, hunt attacker-written files, and confirm upgrade to 10.0.7 or 10.2.4.

RECENT MALWARE WATCH

ARCHIVE: JUNE 16, 2026

BACKDOOR.TURN — DRAGONFORCE TEAMS-RELAY C2

A RAT linked to DragonForce (tied to Scattered Spider) tunnels its command-and-control through Microsoft Teams TURN relay servers, riding an anonymous visitor token so traffic blends into ordinary conferencing and slips past egress filtering. Hunt unexpected TURN negotiations, correlate Teams-relay connections from servers that never host meetings, and pull Symantec's IOCs.

ARCHIVE: JUNE 9, 2026

MAGECART — GTM & STRIPE SKIMMING

A renewed Magecart campaign loads client-side card-skimming code through Google Tag Manager and the Stripe API from trusted, already-allow-listed domains, sailing past CSP rules and blocklists to harvest payment data at checkout. Hunt the GTM container's change history, rogue localStorage staging captured cards, and CSP exceptions for Google and Stripe origins.