THE FORENSICS WAY

ISSUE 29 | FORENSICS AWARENESS THIS WEEK | TUESDAY, AUGUST 18, 2026

FRONT PAGE

RANSOMWARE

The Reboot That Killed the Ransom: An Akira Affiliate Rebooted Into Safe Mode to Blind EDR — and Broke Its Own Encryptor

Huntress documented an Akira intrusion that began August 4 with a credential-spray attack against an internet-facing SonicWall SSL VPN account lacking MFA — compromised in under seven minutes. Once inside, the affiliate reached for a first-for-Akira evasion trick: rebooting the victim host into Safe Mode with Networking, a startup state that loads only core drivers and routinely blinds EDR agents that depend on normal-mode services. It is a well-worn tactic against defenders — this time it turned on the attacker instead.

Akira's encryptor is built for speed, leaning on concurrent worker threads and heavy memory-mapped I/O rather than simple sequential reads and writes. Safe Mode's minimal driver set restricted storage controllers and pagefile availability enough to break that architecture outright, and the encryption run failed. Forensic priority: alert on bursts of failed VPN logins against multiple usernames from a single source, monitor msconfig.exe and bcdedit activity alongside boot-configuration event log entries, and treat an unexplained Safe Mode reboot as a live indicator of an EDR-evasion attempt in progress, not routine maintenance.

SUPPLY CHAIN

The Build That Lies About Working: 16 Typosquatted RubyGems Fake a Clean Install While Quietly Fetching a Windows Infostealer

OpenSourceMalware disclosed a campaign it calls StubMaker on August 15 — 16 RubyGems packages typosquatting popular Ruby dependencies with clumsy, low-effort misspellings rather than the SEO-polished lookalikes typically seen in supply-chain attacks. Published by accounts "mod8rz41mje" and "rbq95bwt6q," each gem ships a Makefile with empty all, install, and clean targets

Threat Bulletin

ACTIVE EXPLOIT

CVE-2026-59310

VMware vCenter — an unauthenticated directory-traversal flaw in the Syslog server lets a remote attacker with network access execute arbitrary code; CVSS 9.8. A suspected APT began exploiting it just five days after disclosure, hitting 360-plus victim IPs across 47 countries and deploying reverse_ssh via cron for persistence; CISA KEV. *Forensic Note:* Inventory internet- and internal-network-reachable vCenter instances, hunt cron-job persistence and reverse_ssh connections, and patch to 9.1.0.0300, 9.0.2.0100, or the relevant 8.0 branch — no workaround exists.

ACTIVE EXPLOIT

CVE-2026-55040

Microsoft SharePoint — a weak-authentication flaw in JWT validation accepts tokens signed with *alg: none*, letting a remote attacker who knows a target's Windows SID forge an admin session with no password; CVSS 9.1. Patched in July, but attackers began exploiting it within hours of a public PoC on August 11; CISA KEV. *Forensic Note:* Review IIS and ULS logs for forged JWT admin sessions, hunt for unauthorized site-collection administrator changes, and confirm the July patch is applied everywhere.

MALWARE SPOTLIGHT

reverse_ssh — The Open-Source Backdoor Riding vCenter's Coattails

alongside do-nothing Unix and Windows stub scripts, so the extension build phase reports success while the real payload runs from the installer hook itself: a platform beacon that fetches and executes a Windows loader.

Once resident, the loader harvests browser-stored credentials, cryptocurrency wallets and seed phrases, and Telegram session data. The technique's real innovation is procedural rather than technical — a fake successful build is a quieter tell than a failed one, since developers rarely investigate a gem that installs cleanly. Forensic priority: audit Gemfile.lock and installed-gem inventories against the 16 known typosquat names, inspect extconf.rb and Makefile targets for stub scripts that return success without building anything, and treat any Ruby dev machine with unexplained outbound beacon traffic as a credential-theft incident.

The vCenter campaign's persistence mechanism is not custom malware at all but reverse_ssh, a legitimate open-source Go tool for establishing outbound SSH tunnels, dropped by a malicious cron job after initial path-traversal access. Because it is a signed, unmodified open-source binary, it evades signature-based detection that would flag a purpose-built implant, while giving the operator a durable, low-noise shell back into the environment. *Forensic Note:* Hunt unexpected reverse_ssh binaries and outbound SSH sessions from server infrastructure, audit cron and systemd timers for unauthorized entries, and treat any unsanctioned use of legitimate remote-access tooling as a compromise indicator, not a false positive.

THE FORENSICS WAY

HISTORICAL ARCHIVES | HISTORY OF DIGITAL INVESTIGATION | TUESDAY, AUGUST 18, 2026

CASE STUDIES: HISTORICAL GRID

THE CTX PYPI HIJACK (2022)

The Theft That Ran at "pip install": How a Hijacked Maintainer Account Turned Setup Scripts Into an Exfiltration Channel

In May 2022, researchers discovered that the popular PyPI package ctx had been hijacked through a compromised maintainer account, with a malicious setup.py silently exfiltrating environment variables — AWS keys, API tokens, and other secrets — to an attacker-controlled endpoint the instant pip install ran; a companion attack against the PHP package phpass used the

FLAME (2012)

Too Sophisticated to Hide: How the Most Complex Cyberespionage Tool Ever Found Was Uncovered While Investigating Something Else Entirely

Kaspersky researchers stumbled onto Flame in May 2012 while investigating an unrelated data-wiping incident at Iranian oil facilities — and found a 20-megabyte espionage platform so environmentally precise it fingerprinted each target machine, activated modules only under exact matching conditions, and could remotely

identical technique. Because the theft executed during installation rather than at import or runtime, static scanners and casual code review missed it entirely, and only anomalous outbound traffic during a routine build gave it away. It is a direct ancestor of this week's StubMaker campaign — the same install-time execution trick, now dressed up with a Makefile that reports a clean build to keep the theft invisible.

trigger its own suicide command to erase all trace of itself if a target didn't match. That same target-specific precision was the tell: its bloated size and unusual Lua-scripted architecture behaved so strangely outside its intended context that analysts caught it almost by accident. It is a fitting ancestor to this week's Akira failure — malware engineered so tightly for one operating environment that reality outside it exposed the seams.

THE EVENT-STREAM INCIDENT (2018)

A Handshake, Not a Hack: How Asking Nicely for Publish Rights Poisoned a Package Downloaded Millions of Times a Week

In November 2018, a developer using the alias "right9ctrl" simply asked the maintainer of the popular npm package event-stream to take over maintenance — no exploit required — then quietly added a dependency, flatmap-stream, carrying an encrypted payload aimed narrowly at the Copay Bitcoin wallet app. A routine code review by another developer, Jayden Seric, caught the anomaly before it detonated at wider scale, and the incident became a landmark case for social-engineered maintainer takeovers. It remains the clearest historical ancestor of last month's CHAINDROP npm worm — the same trust relationship, automated into self-propagation across hundreds of packages instead of one.

GOOTLOADER (2020–PRESENT)

Poisoning the Search Result Instead of the Inbox: The Malware That Weaponized Google Before It Weaponized a Document

Since 2020, the Gootloader operation has ranked fake legal-document and business-template pages at the top of search results through aggressive SEO poisoning, luring professionals searching for contracts into downloading a JavaScript-based loader disguised as the file they wanted. Investigators traced the campaign's staying power to its manipulation of the search layer itself rather than any single payload, forcing defenders to treat "what a search engine surfaces" as an attack surface in its own right — the same technique now aimed at AI agents instead of humans in recent fake-API-documentation campaigns.

TOOLS OF THE TRADE

OPEN SOURCE

Senrigan

YAMATO SECURITY — V1.X

Hayabusa's cloud-facing sibling, built for fast offline threat hunting across AWS CloudTrail logs. Pair it with vCenter and cloud-hosted infrastructure investigations to surface reconnaissance and

OPEN SOURCE

APT-Hunter

AHMEDKHLIEF — V3.X

An EVTX threat-hunting engine that applies built-in detection logic for common attacker tradecraft without needing a SIEM. Ideal for hunting the boot-configuration and Safe Mode indicators behind

COMMERCIAL

EnCase Endpoint Investigator

OPENTEXT — V25.X

A remote, covert endpoint-investigation platform for scoping a compromise without alerting the subject or disrupting operations. Point it at a developer's machine after a

UTILITY / SCRIPT

RegRipper

HARLAN CARVEY — V4.X

The long-standing registry-hive parsing framework for pulling structured data out of raw hives. Aimed squarely at this week's Akira Safe Mode incident: parse SYSTEM and SOFTWARE hives for

lateral-movement patterns the moment a path-traversal foothold like this week's vCenter flaw starts pivoting into cloud accounts.

Akira's failed EDR-evasion attempt — bcdedit invocations, unexpected reboots, and service-stop events all resolve to timeline-ready detections offline.

StubMaker-style install-time infostealer hit to preserve file access history, browser credential-store timestamps, and outbound-connection artifacts.

boot-configuration entries, Safe Mode–eligible services, and Run-key persistence left behind by the failed encryption attempt.

PRIORITY CVE ADVISORIES

ARCHIVE ALERT

CVE-2026-9198 (LANGFLOW OSS)

An insecure default lets any network caller mint a SUPERUSER token, then execute arbitrary Python via /api/v1/validate/code; CVSS 9.8, unauthenticated. Fixed in 1.10.1; CISA KEV. *Forensic Note:* Review Langflow logs for auto_login calls followed by validate/code POSTs, and hunt dropped payloads on pre-1.10.1 hosts.

ARCHIVE ALERT

CVE-2026-18556 / CVE-2026-18577 (N-ABLE N-CENTRAL)

An authentication bypass (CVSS 8.2) let attackers gain administrative RMM access and reach managed endpoints via Take Control; the first patch proved incomplete and a second bypass was exploited before the follow-up fix. Both CISA KEV. *Forensic Note:* Audit N-central admin logins and Take Control session logs, and treat every managed endpoint as potentially touched.

RECENT MALWARE WATCH

ARCHIVE: AUGUST 11, 2026

NOVA RANSOMWARE — THE RUST ENCRYPTOR THAT BLINDS DEFENDER FIRST

A 64-bit Rust encryptor that reconfigures Microsoft Defender, kills security services, and deletes Volume Shadow Copies before encrypting with XChaCha20-Poly1305 and RSA-2048. Hunt Defender configuration-change events and mass service termination as an early-warning pair.

ARCHIVE: AUGUST 4, 2026

MEDUSAHVNC — THE BROWSER ON THE DESKTOP YOU CANNOT SEE

Sold as MaaS via website and Telegram, MedusaHVNC spawns a hidden Windows desktop and opens a browser with the victim's real profile, so fraud flows from the victim's own IP. Hunt charmap.exe with network connections and enumerate hidden desktops in memory captures.