THE FORENSICS WAY

ISSUE 19 | FORENSICS AWARENESS THIS WEEK | TUESDAY, JUNE 9, 2026

FRONT PAGE

WEB THREAT

Hiding in Plain Sight: 2,000 Hacked WordPress Sites Pull Their Orders From Steam Profile Comments

A campaign uncovered this week compromised nearly 2,000 WordPress sites and stashed its command-and-control instructions where almost no defender thinks to look — inside the comment fields of legitimate Steam Community profiles. Invisible Unicode characters encode a payload that, once decoded, resolves to a malicious script URL.

By turning Valve's trusted platform into a dead-drop resolver, the operators skip standing up their own C2 infrastructure and slide past reputation- and domain-based blocking entirely; a takedown means editing a Steam profile, not seizing a server. Forensic priority: capture the injected plugin and theme code, decode the zero-width Unicode strings to recover the resolver URL, and pivot on outbound requests to Steam profile endpoints from server-side hosts that have no business talking to a gaming platform.

SUPPLY CHAIN

IronWorm Burrows Through npm: 36 Packages Turned Into a Self-Spreading Harvester of AI and Cloud Keys

Researchers disclosed IronWorm, an infostealing worm that infected 36 npm packages and hunts a sweeping target list — 86 environment variables and 20 credential files spanning Anthropic, OpenAI, AWS, and npm tokens, Vault configuration files, SSH keys, and Exodus cryptocurrency wallets. Each compromised maintainer becomes a launch pad for the next wave of infections.

The shift is notable: AI-provider API keys now sit alongside cloud and crypto secrets as first-class loot, a reflection of how deeply LLM gateways have wired themselves into modern build pipelines. Forensic priority: reconstruct npm publish events and maintainer-token usage, diff package-lock histories to scope the blast radius, and treat every secret exposed to an affected CI runner — AI keys most of all — as burned and rotate it.

Threat Bulletin

CRITICAL

CVE-2026-50751

Check Point Remote Access & Mobile Access VPN — an improper-authentication logic flaw in how IKEv1 validates certificates lets an unauthenticated attacker establish a VPN session without valid credentials; CVSS 9.3. Exploited in the wild since May 7 and tied with medium confidence to a Qilin ransomware affiliate; added to CISA KEV June 8. *Forensic Note:* Audit VPN and IKEv1 logs from May 7 onward for sessions lacking a machine certificate, flag gateways still accepting legacy IKEv1 clients, and check for the related site-to-site MitM bug CVE-2026-50752.

ACTIVE EXPLOIT

CVE-2026-42271

BerriAI LiteLLM (AI gateway) — two Model Context Protocol preview endpoints accept full stdio-transport server configs, letting any authenticated API-key holder spawn subprocesses and run arbitrary commands as the proxy; CVSS 8.7. Chained with Starlette's CVE-2026-48710 for unauthenticated RCE; CISA KEV June 8, fix v1.83.7. *Forensic Note:* Hunt POSTs to */mcp-rest/test/connection* and */tools/list*, review proxy process-spawn telemetry, and rotate every model-provider key the gateway holds.

MALWARE SPOTLIGHT

Magecart — GTM & Stripe Skimming

A renewed Magecart campaign abuses Google Tag Manager and the Stripe API to load client-side card-skimming code from inside trusted, already-allow-listed domains. Because the skimmer rides Google and Stripe infrastructure, it sails straight past Content-Security-Policy rules and network blocklists that implicitly trust those origins, harvesting payment data at checkout without ever touching attacker-owned hosts. *Forensic Note:* Inspect the GTM container's change history, hunt rogue localStorage artifacts staging captured card data, review CSP exceptions and Stripe customer metadata, and capture the live checkout DOM at the moment of payment to preserve the injected logic.

THE FORENSICS WAY

HISTORICAL ARCHIVES | HISTORY OF DIGITAL INVESTIGATION | TUESDAY, JUNE 9, 2026

CASE STUDIES: HISTORICAL GRID

HAMMERTOSS / APT29 (2015)

When Cozy Bear Took Orders From Twitter: The Dead-Drop Blueprint Behind Today's Steam-Profile C2

In July 2015, FireEye detailed HAMMERTOSS, a backdoor wielded by Russia's APT29 (Cozy Bear) that fetched its marching orders from an ever-rotating set of daily Twitter handles, pulled images from GitHub, and hid commands inside them with steganography before exfiltrating to cloud storage. By blending malicious traffic into ordinary visits to wildly popular services, it defeated domain blocklists and frustrated network forensics. A decade on, this week's WordPress-on-Steam campaign runs the

BRITISH AIRWAYS MAGECART BREACH (2018)

380,000 Card Payments Skimmed in Plain Sight: The Breach That Made Magecart a Boardroom Word

Between August and September 2018, Magecart operators injected a small block of JavaScript into British Airways' website and mobile app, silently skimming payment-card and personal data from roughly 380,000 transactions as customers checked out. Investigators traced the theft to a single modified script and a malicious look-alike domain harvesting the data in real time. The UK's ICO ultimately fined BA £20 million, and the case turned client-side skimming into a board-level risk — the very

identical playbook — proof the social-media dead drop never went out of style, it only changed venue.

trusted-script abuse powering this week's Google Tag Manager campaign.

MOONLIGHT MAZE (1996–1999)

The First Nation-State Hunt: Years of Stealthy Exfiltration That Seeded the Turla Lineage

Between 1996 and 1999, U.S. investigators traced a sprawling intrusion set — later codenamed Moonlight Maze — siphoning military, NASA, and university research data to Russia-linked infrastructure through a web of compromised relay hosts. It was among the first cyber-espionage cases to demand systematic log correlation, honeypots, and cross-agency forensics, and researchers later tied its LOKI2-based tooling to the code lineage behind Turla and today's Kazuar botnet. The case proved that patient, low-and-slow state intrusions could evade detection for years — the very playbook Secret Blizzard still runs three decades later.

OPERATION AURORA (2009–2010)

An Internet Explorer Zero-Day Opens Google, Adobe, and Dozens More to Persistent Theft

Disclosed by Google in January 2010, Operation Aurora was a China-linked campaign that weaponized an Internet Explorer zero-day (CVE-2010-0249) to breach at least 20 major companies and steal source code and intellectual property. Forensic teams reconstructed the intrusions through memory analysis, encrypted C2 traffic, and the IE use-after-free exploit chain. The case pushed the industry toward threat-intelligence sharing and made "advanced persistent threat" a board-level term — and that same CVE-2010-0249 resurfaced in CISA's May 20, 2026 KEV batch, proving old exploits never truly die.

TOOLS OF THE TRADE

OPEN SOURCE

CyberChef

GCHQ — V10.X

Browser-based "cyber Swiss Army knife" for chaining decode, decrypt, and extract operations without writing code. It is purpose-built for unwinding exactly the layered obfuscation in this week's stories — recovering zero-width Unicode dead-drop URLs from Steam comments and peeling back the Base64 and packing that hides skimmer and worm payloads.

COMMERCIAL

urlscan.io

URLSCAN GMBH — SAAS

Sandboxed URL scanner that loads a page and records every request, script, and resource it pulls in, with a generous free tier. Ideal for replaying a malicious link to watch a Magecart skimmer inject through Google Tag Manager or a hijacked WordPress page resolve its Steam-hosted second stage — all without touching it on a live endpoint.

OPEN SOURCE

GuardDog

DATADOG — V1.X

Heuristic CLI scanner that flags malicious npm and PyPI packages by detecting install-time hooks, obfuscated code, and suspicious network or filesystem access. It targets precisely the IronWorm class of supply-chain threat, surfacing the preinstall scripts and credential-exfiltration behavior that worm-style packages use to spread through a registry.

COMMERCIAL

VirusTotal

GOOGLE — ENTERPRISE / FREE

Multi-engine analysis and intelligence platform for files, URLs, and domains that doubles as a pivot graph across shared infrastructure. Use it to enrich indicators from all three of this week's campaigns — package hashes, dead-drop resolver domains, and skimmer endpoints — and map the relationships that tie disparate intrusions back to a common operator.

PRIORITY CVE ADVISORIES

RECENT MALWARE WATCH

ARCHIVE ALERT

CVE-2026-48172 (LITESPEED CPANEL)

Incorrect privilege assignment lets any authenticated cPanel user invoke the lsws.redisAble function via the cPanel JSON API to run scripts as root; CVSS 10.0. Exploited as a zero-day, auto-uninstalled in cPanel's emergency patch, CISA KEV May 27. *Forensic Note:* Hunt cPanel API logs for lsws.redisAble calls and root-owned scripts created by non-root users.

ARCHIVE ALERT

CVE-2026-41091 (MICROSOFT DEFENDER)

Elevation-of-privilege flaw lets a local attacker abuse the antimalware service to obtain SYSTEM; CVSS 7.8. Added to CISA KEV May 20 alongside DoS bug CVE-2026-45498. *Forensic Note:* Review Defender operational logs and process-creation telemetry for unexpected SYSTEM-level child processes spawned from the antimalware service.

ARCHIVE: JUNE 2, 2026

KAZUAR — SECRET BLIZZARD P2P BOTNET

Turla rebuilt its Kazuar backdoor into a modular peer-to-peer botnet with Kernel, Bridge, and Worker modules and a leader-election scheme that keeps all but one node silent; C2 rides HTTP, WebSockets, or Exchange Web Services with AMSI/ETW/WLDP bypasses. Favor behavioral detection — hunt anomalous IPC and irregular EWS traffic.

ARCHIVE: MAY 26, 2026

MINI SHAI-HULUD WORM

Self-propagating npm/PyPI worm from TeamPCP; 170+ packages across 404 malicious versions, 518M monthly downloads, harvesting CI/CD, cloud, and Vault credentials and defeating SLSA Build Level 3 provenance. Hunt rogue preinstall scripts, unexpected Bun downloads, and the gh-token-monitor persistence daemon.