THE FORENSICS WAY

ISSUE 20 | FORENSICS AWARENESS THIS WEEK | TUESDAY, JUNE 16, 2026

FRONT PAGE

SUPPLY CHAIN

Poisoned at the Source: 400+ Arch Linux Packages Spiked With an eBPF Rootkit and Credential Stealer

A campaign disclosed this week poisoned more than 400 packages in the Arch User Repository, planting a Linux ELF binary that pairs a credential stealer with an eBPF-based rootkit able to run in kernel space and hide its own processes. The operator spoofed a trusted maintainer and hijacked at least 20 orphaned packages by quietly rewriting their PKGBUILD files.

The stealer rakes in GitHub credentials, SSH keys, HashiCorp Vault tokens, browser cookies, and chat data from Slack, Discord, Teams, and Telegram before exfiltrating over HTTP. Because the rootkit can survive ordinary cleanup, Sonatype and IFIN researchers tell responders to rotate every secret and rebuild affected hosts from scratch. Forensic priority: capture PKGBUILD and pre-install-script changes, hunt eBPF program loads and hidden-PID discrepancies, and treat any developer secret exposed to an infected machine as burned.

AI THREAT

Ransomware, Assembled by Agents: Sophos Finds an 80-Module Attack Toolkit Built With AI Coding Assistants

Investigating a customer intrusion, Sophos uncovered a sprawling, AI-assembled attack framework — roughly 80 modules tested against more than 70 evasion techniques and against Sophos, CrowdStrike, and Microsoft EDR. It automates Active Directory discovery and bundles Cobalt Strike profiles, Telegram-bot command-and-control, Python shellcode injectors, and Cloudflare Workers redirectors.

Most striking is the assembly line behind it: a Claude Opus 4.5 agent coordinated the R&D while specialized agents handled coding, OPSEC hardening, proxy testing, and documentation of bypass research lifted from major vendors, generating payloads in Rust and Go. Russian-language scripts, a Git repo holding an AD-discovery panel, and Cobalt Strike operator logs referencing

Threat Bulletin

ACTIVE EXPLOIT

CVE-2026-35273

Oracle PeopleSoft Enterprise PeopleTools — an unauthenticated SSRF-to-RCE flaw in the Environment Management Hub (PSEMHUB) lets a remote attacker run code over HTTP with no credentials and no user interaction; CVSS 9.8. Mandiant tracked zero-day exploitation by ShinyHunters (UNC6240) from May 27, with stolen university data posted to the group's leak site on June 9; CISA KEV June 12. *Forensic Note:* Review PSEMHUB and web-server logs for unauthenticated requests, hunt exfiltration staging and web shells, and inventory PeopleTools 8.61/8.62 builds.

CRITICAL

CVE-2026-20253

Splunk Enterprise — an unauthenticated PostgreSQL sidecar service (added in v10 and proxied through the web port) accepts any credentials on its */v1/postgres/recovery* backup and restore endpoints, letting an attacker write arbitrary files and chain a malicious database restore into code execution; CVSS 9.8. Internet-facing instances, especially on AWS, are immediately at risk. *Forensic Note:* Audit access to the postgres recovery endpoints, hunt attacker-written *.py* files and unexpected DB restores, and confirm upgrade to 10.0.7 or 10.2.4.

MALWARE SPOTLIGHT

Backdoor.Turn — DragonForce Teams-Relay C2

ransom notes and leak sites round out the evidence. Forensic priority: preserve developer-tool and AI-agent artifacts, profile the Rust/Go loaders, and watch for Telegram and Cloudflare Workers egress.

DragonForce — a cartel-structured ransomware operation linked to Scattered Spider — is deploying Backdoor.Turn, a RAT that tunnels its command-and-control through Microsoft Teams TURN relay servers. By grabbing an anonymous Teams visitor token and riding legitimate Microsoft relay infrastructure, its traffic blends into ordinary conferencing and slips past egress filtering; the implant runs commands, scans networks, captures TLS certificates, searches LDAP/AD, and steals credentials. *Forensic Note:* Hunt unexpected processes negotiating TURN sessions, correlate Teams-relay connections from servers that never host meetings, and pull Symantec's published IOCs.

THE FORENSICS WAY

HISTORICAL ARCHIVES | HISTORY OF DIGITAL INVESTIGATION | TUESDAY, JUNE 16, 2026

CASE STUDIES: HISTORICAL GRID

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.

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

Discovered almost by accident days before it reached stable releases, it became the canonical near-miss of open-source supply-chain compromise — the direct ancestor of this week's Arch AUR maintainer-spoofing campaign.

ransomware capability detached from skill — the same democratization now accelerating through the AI-assembled toolkit on Page 1.

HAMMERTOSS / APT29 (2015)

When Cozy Bear Took Orders From Twitter: The Dead-Drop Blueprint Behind Today's Trusted-Infrastructure 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 Backdoor.Turn — routing its C2 through Microsoft Teams relay servers — runs the identical playbook: hide inside infrastructure too trusted to block.

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 trusted-code abuse that resurfaces whenever attackers poison a dependency users already trust, from checkout scripts to this week's Arch packages.

TOOLS OF THE TRADE

OPEN SOURCE

Tracee

AQUA SECURITY — V0.X

Runtime security and forensics tool that uses eBPF to trace kernel and system events in real time. It is built to catch exactly the AUR threat on Page 1 — surfacing the eBPF program loads, hidden processes, and anomalous syscalls a kernel-resident rootkit uses to cloak itself from ordinary tooling.

OPEN SOURCE

Suricata

OISF — V7.X

High-performance network IDS/IPS and packet-capture engine with deep protocol awareness. Point it at egress traffic to flag the odd TURN negotiations behind Backdoor.Turn's Teams-relay C2 and to fingerprint the unauthenticated HTTP hitting PeopleSoft and Splunk endpoints in this week's exploitation.

UTILITY / SCRIPT

rkhunter

ROOTKIT HUNTER — V1.4

Lightweight Linux scanner that checks for rootkits, backdoors, and local exploits by comparing binaries, kernel modules, and system files against known-good baselines. A fast first pass on a suspected AUR-compromised host — though, as researchers warn, a kernel rootkit that survives cleaning still demands a full rebuild.

COMMERCIAL

Censys

CENSYS — SAAS

Internet-wide scanning and attack-surface platform that indexes exposed services, certificates, and software versions. Use it to find your own internet-facing PeopleSoft and Splunk instances before ShinyHunters does, and to map the exposed-appliance footprint this week's unauthenticated RCEs turn into instant entry points.

PRIORITY CVE ADVISORIES

ARCHIVE ALERT

CVE-2026-50751 (CHECK POINT VPN)

Improper authentication in IKEv1 certificate validation lets an unauthenticated attacker establish a Remote Access / Mobile Access VPN session without valid credentials; CVSS 9.3. Exploited since May 7 and tied to a Qilin ransomware affiliate; CISA KEV June 8. *Forensic Note:* Audit IKEv1 sessions lacking a machine certificate and flag gateways still accepting legacy clients.

ARCHIVE ALERT

CVE-2026-42271 (BERRIAI LITELLM)

Two Model Context Protocol preview endpoints accept full stdio server configs, letting any API-key holder spawn subprocesses and run 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 rotate every model-provider key the gateway holds.

RECENT MALWARE WATCH

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 Content-Security-Policy rules and network 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.

ARCHIVE: JUNE 2, 2026

KAZUAR — SECRET BLIZZARD P2P BOTNET

Turla rebuilt its Kazuar backdoor into a modular peer-to-peer botnet with 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.