THE FORENSICS WAY

ISSUE 18 | FORENSICS AWARENESS THIS WEEK | TUESDAY, JUNE 2, 2026

FRONT PAGE

NETWORK INTRUSION

SonicWall Gen6 VPNs Under Siege: An Incomplete Patch Lets Akira Bypass MFA and Land in Under an Hour

Defenders confirmed a coordinated campaign that began May 20 brute-forcing credentials against end-of-life SonicWall Gen6 SSL-VPN appliances and sailing past multi-factor authentication via CVE-2024-12802 — a missing MFA enforcement for the UPN login format. SonicWall rated the flaw 6.5; CISA's data publisher independently assessed it at 9.1, Critical.

The trap: the firmware fix alone does not close the hole — Gen6 owners must manually reconfigure the LDAP server, and the hardware reached end-of-life on April 16 with no further updates coming. Intrusions ran a tidy 30–60 minutes — log in, recon, test credential reuse, log out — with Akira ransomware tied to the bulk of follow-on claims. Forensic priority: preserve SSL-VPN authentication logs for UPN-format logins, snapshot LDAP configuration, and trace lateral movement from VPN-adjacent hosts before reimaging.

DATA BREACH

ShinyHunters Talks Its Way Into Carnival: A Social-Engineered Account Exposes 5.9 Million Travelers

Carnival began notifying 5,995,277 people in late May after an attacker socially engineered an employee on April 14 into granting access to part of the cruise operator's IT estate. Using the compromised account, the intruder reached a limited portion of systems by April 22 and copied personal data before being blocked; the extortion crew ShinyHunters claimed the theft.

Exposed records vary by individual but include names, addresses, dates of birth, email addresses, phone numbers, and government-issued ID numbers — effectively a ready-made identity-theft kit. Carnival is offering 24 months of credit monitoring. Forensic priority: reconstruct the help-desk and identity-verification workflow abused for initial access, scope the compromised

Threat Bulletin

CRITICAL

CVE-2026-48172

LiteSpeed User-End cPanel Plugin — incorrect privilege assignment lets any authenticated cPanel user invoke the *lsws.redisAble* function through the standard cPanel JSON API to run arbitrary scripts as root; CVSS 10.0. Exploited as a zero-day and auto-uninstalled in cPanel's May 19 emergency patch; added to CISA KEV May 27. *Forensic Note:* Hunt cPanel API logs for lsws.redisAble calls, audit root-owned scripts and cron entries created by non-root users, and confirm the plugin was upgraded to v2.4.7 or later.

ACTIVE EXPLOIT

CVE-2026-41091

Microsoft Defender — elevation-of-privilege flaw lets a local attacker who already holds limited access abuse the antimalware service to obtain SYSTEM; CVSS 7.8. Added to CISA KEV May 20 alongside a Defender denial-of-service 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 — a hallmark of post-access privilege escalation.

MALWARE SPOTLIGHT

Kazuar — Secret Blizzard P2P Botnet

Russia's Secret Blizzard (Turla) has rebuilt its long-running Kazuar backdoor into a modular peer-to-peer botnet engineered for stealthy, long-term espionage against government,

account's full data-access timeline, and map exposed identifiers against downstream fraud and account-takeover reports.

diplomatic, and defense targets. Three module types — Kernel, Bridge, and Worker — split the work, and a leader-election scheme keeps all but one node silent to shrink the detection surface; C2 rides HTTP, WebSockets, or Exchange Web Services, with AMSI, ETW, and WLDP bypasses built in. *Forensic Note:* Favor behavioral detection over static signatures — hunt anomalous named-pipe/IPC patterns between hosts, irregular EWS traffic, and ETW/AMSI tampering, and treat any single beaconing "leader" as one node of many.

THE FORENSICS WAY

HISTORICAL ARCHIVES | HISTORY OF DIGITAL INVESTIGATION | TUESDAY, JUNE 2, 2026

CASE STUDIES: HISTORICAL GRID

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

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

evade detection for years — the very playbook Secret Blizzard still runs three decades later.

20, 2026 KEV batch, proving old exploits never truly die.

CODECOV BASH UPLOADER BREACH (2021)

A Single Tampered CI Script Quietly Drains Secrets From Thousands of Build Pipelines for Two Months

In April 2021, Codecov disclosed that an attacker had used a flaw in its Docker image build to extract credentials and modify the widely used Bash Uploader script. For roughly two months, the altered script silently exfiltrated environment variables — tokens, keys, and credentials — from customers' CI/CD pipelines to an attacker-controlled server. Investigators reconstructed the intrusion via Git history of the uploader and outbound traffic analysis, and the case became the textbook example of why every secret exposed to a build runner must be treated as compromised.

ASUS SHADOWHAMMER (2019)

Stolen Code-Signing Certificates Push a Backdoored Live Update to a Million Machines — Aimed at 600

Kaspersky's Operation ShadowHammer revealed that attackers had trojanized the ASUS Live Update utility and signed it with legitimate, stolen ASUS code-signing certificates, distributing it through official channels to roughly one million users. The implant checked each host's MAC address against a hardcoded list of about 600 targets before fetching a second-stage payload. Forensic teams matched the malicious binaries by certificate serial and timestamp — an enduring lesson in the danger of trusted signatures and surgically targeted supply-chain delivery.

TOOLS OF THE TRADE

UTILITY

Sysmon

MICROSOFT SYSINTERNALS — V15.X

Free Windows system-monitoring driver and service that logs process creation, network connections, image loads, and named-pipe activity with rich detail. The high-fidelity telemetry it produces is foundational for spotting Kazuar-style inter-process communication, persistence, and ETW/AMSI tampering that default Windows logging misses entirely.

OPEN SOURCE

Chainsaw

WITHSECURE LABS — V2.X

Fast command-line tool for hunting threats across Windows event logs and the MFT using built-in detection logic and Sigma rules. It turns raw EVTX into ranked detections in seconds — ideal for surfacing the privilege-escalation and bypass artifacts left by Defender abuse (CVE-2026-41091) and stealthy implants.

OPEN SOURCE

RITA

ACTIVE COUNTERMEASURES — V5.X

Framework that analyzes Zeek network logs to detect command-and-control beaconing, unusually long connections, and DNS tunneling through statistical scoring. Built to expose the regular, low-volume callbacks of a botnet leader node — precisely the signal Kazuar's peer-to-peer design tries to bury in normal traffic.

COMMERCIAL

SentinelOne Singularity

SENTINELONE — 2026 PLATFORM

Autonomous endpoint and XDR platform that detects and rolls back threats using on-device behavioral AI rather than static signatures. Microsoft's own Kazuar guidance — favor behavioral detection over signatures — is exactly the defensive model this class of EDR is engineered to deliver at scale.

PRIORITY CVE ADVISORIES

RECENT MALWARE WATCH

ARCHIVE ALERT

CVE-2025-34291 (LANGFLOW)

Origin-validation error; a permissive CORS config plus a SameSite=None refresh-token cookie enables credentialed cross-origin calls to the refresh endpoint, yielding authenticated RCE; CVSS 9.4. In CISA KEV; used by Iran's MuddyWater for initial access. *Forensic Note:* Review access logs for cross-origin refresh-endpoint calls and anomalous token issuance.

ARCHIVE ALERT

CVE-2026-34926 (TREND MICRO APEX ONE)

On-premise directory traversal lets a pre-authenticated local attacker modify a server key table to inject code pushed to managed agents; CVSS 6.7. CISA KEV with a June 4 deadline. *Forensic Note:* Verify key-table integrity and agent-deployment packages, and audit console logs for unauthorized table writes.

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.

ARCHIVE: MAY 19, 2026

TYCOON2FA — DEVICE-CODE PHISHING

Phishing-as-a-service kit abusing the OAuth 2.0 device-authorization grant to hijack Microsoft 365 accounts; issues tokens to attacker devices after victims enter a code at the legitimate devicelogin page. Audit AzureAD sign-ins for deviceCode authentication and enumerate newly registered devices.