THE FORENSICS WAY

ISSUE 22 | FORENSICS AWARENESS THIS WEEK | TUESDAY, JUNE 30, 2026

FRONT PAGE

TAKEDOWN

Endgame Strikes Again: A Global Operation Rips Out the SocGholish, Amadey and StealC Stealer-Loader Backbone

In coordinated action carried out June 15–19 and announced this week, Operation Endgame — led by Europol and Eurojust with law enforcement from Canada, Denmark, Germany, the Netherlands, the United Kingdom, and the United States — dismantled the infrastructure behind three malware families that sit at the heart of the cybercrime economy. SocGholish pushes fake browser-update lures through compromised websites; Amadey is a downloader-and-stealer hybrid; StealC harvests passwords and authentication tokens while doubling as a loader. The strike disrupted 326 servers and 142 domains, flagged more than €41 million in criminal cryptocurrency, and recovered roughly 27 million credentials stolen from over 385,000 compromised systems.

These loaders and stealers are the initial-access and credential-theft layer that precedes ransomware and fraud, so the seized command panels and loader-to-victim mappings — bolstered by private-sector help from Microsoft, ESET, Proofpoint, IBM X-Force, Shadowserver, Have I Been Pwned, and Spamhaus — are an evidentiary goldmine for scoping who was infected and what was taken. Forensic priority: ingest the released IOCs and recovered-credential sets, hunt SocGholish fake-update injects and Amadey/StealC staging and persistence on suspect hosts, and treat any credential that touched an infected machine as burned. The caveat that always applies: takedowns disrupt, they rarely eradicate — expect rebrands and rebuilt infrastructure.

FINANCIAL CRACKDOWN

Cutting Off the Cash-Out: DOJ Seizes Huione's Cloud Infrastructure as Treasury Targets a Laundering Hub

On June 23, the U.S. Justice Department seized a cloud account allegedly supporting the Huione Group, the Southeast Asian

Threat Bulletin

ACTIVE EXPLOIT

CVE-2026-20230

Cisco Unified Communications Manager (and Session Management Edition) — a server-side request forgery from improper input validation lets an attacker send a crafted HTTP request to write files to the underlying OS, a foothold that can later be escalated to root; CVSS 8.6. Exploitation (which requires the WebDialer service enabled) was observed from the weekend of June 21–22, with public exploit code available; CISA KEV June 25, with a three-day BOD 26-04 deadline of June 28. *Forensic Note:* Confirm whether WebDialer is enabled, hunt attacker-written files and anomalous outbound SSRF requests in CUCM logs, and watch for follow-on root-escalation activity.

CRITICAL

CVE-2026-12569

PTC Windchill & FlexPLM — an unauthenticated remote code execution flaw caused by insecure deserialization of untrusted data; CVSS 9.3. Attackers are actively dropping persistent JSP web shells under */Windchill/login/* for command execution and data theft, making this the first PTC product ever added to the KEV (June 25, fix by June 28). Because PLM systems hold CAD, BOM, and engineering IP, the blast radius is intellectual property. *Forensic Note:* Hunt JSP web shells under /Windchill/login/, review the deserialization endpoints for crafted payloads, and treat engineering and

conglomerate long tied to laundering proceeds from "pig-butchering" crypto-investment scams and other cyber-enabled fraud, while the Treasury pressed sanctions citing alleged North Korean laundering links. Where Operation Endgame went after the malware that steals, this action goes after the financial plumbing that launders — the cash-out layer that turns stolen value into clean money.

For investigators, the prize is the linkage data: cloud-account metadata, domain mappings, and on-chain payment flows are what connect scam infrastructure to its banking conversion and, in turn, to state actors. The two operations are a matched pair — one severs the supply of stolen credentials, the other the demand-side laundering rails. Forensic priority: preserve cloud-account metadata and access logs before disruption scatters them, trace cryptocurrency through mixers and exchanges to identify off-ramps, and correlate scam-victim payment rails against the seized infrastructure to map the full money cycle.

manufacturing data as exfiltration targets.

MALWARE SPOTLIGHT

CryptoBandits — Stealer-Backdoor With Tor-Hidden C2

A newly profiled threat, CryptoBandits operates as both an information stealer and a backdoor, abusing the Tor network and local proxying to conceal its command-and-control while it targets cryptocurrency wallets, stages additional payloads, and plants persistence keys for long-term access. Its reliance on anonymized C2 mirrors the same evasion-through-legitimate-infrastructure playbook investigators keep meeting. *Forensic Note:* Hunt Tor process artifacts and local proxy listeners, audit wallet-file and keystore access, enumerate Run/registry and scheduled-task persistence, and recover staged payloads from temp and profile directories.

THE FORENSICS WAY

HISTORICAL ARCHIVES | HISTORY OF DIGITAL INVESTIGATION | TUESDAY, JUNE 30, 2026

CASE STUDIES: HISTORICAL GRID

OPERATION TOVAR — GAMEOVER ZEUS (2014)

The Botnet That Took a Global Posse to Kill: Sinkholing a Peer-to-Peer Empire and Naming Its Architect

In June 2014, an international coalition of law enforcement and private-sector partners executed Operation Tovar, seizing control of the

OPERATION LADYBIRD — EMOTET TAKEDOWN (2021)

Dismantling "the World's Most Dangerous Malware": When Police Seized the Botnet and Pushed the Uninstall

In January 2021, Europol and Eurojust coordinated Operation Ladybird, seizing the infrastructure of Emotet — then branded "the world's most dangerous malware" — across more

GameOver Zeus peer-to-peer banking botnet that had stolen an estimated $100 million and served as the delivery vehicle for CryptoLocker ransomware. Because GameOver Zeus had no central server, investigators had to map and poison its resilient P2P topology, redirecting infected nodes to sinkholes while indicting its architect, Evgeniy Bogachev. It became the template for modern coordinated takedowns — the same multinational, public-private model that powered this week's Operation Endgame strike on the SocGholish, Amadey, and StealC networks.

than a hundred servers worldwide. In an unprecedented move, investigators leveraged control of the botnet to deliver a time-delayed update that uninstalled Emotet from infected machines, and they harvested vast troves of stolen credentials for victim notification. The loader-takedown playbook it pioneered — seize the infrastructure, recover the credentials, notify the victims — is exactly the model Operation Endgame ran again this week on Page 1.

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 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 — the downstream ransomware tradecraft that loaders and stealers like those dismantled in this week's Operation Endgame exist to enable.

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 had been visited — reporting one visit instead of dozens — a discrepancy that surfaced only after the verdict. It stands as a lasting lesson that the evidence is only as good as its validation — the same discipline investigators must apply to the seized panels and recovered-credential troves behind this week's takedowns.

TOOLS OF THE TRADE

OPEN SOURCE

OpenCTI

FILIGRAN — V6.X

Open cyber-threat-intelligence platform for storing, relating, and visualizing IOCs and adversary infrastructure. Ingest the SocGholish, Amadey, and StealC

COMMERCIAL

Maltego

MALTEGO — 2026 RELEASE

Link-analysis and graphing platform that maps relationships across domains, infrastructure, identities, and crypto addresses. Built for exactly the entity-

OPEN SOURCE

GraphSense

IKNAIO / AIT — V25.X

Open-source cryptocurrency analytics platform for tracing flows across multiple blockchains and clustering addresses. A free counterpart for

UTILITY / SCRIPT

DeepBlueCLI

SANS / ERIC CONRAD — V3.X

PowerShell module that rapidly triages Windows event logs for attacker behavior — suspicious account use, service creation, encoded commands, and lateral

indicators released after Operation Endgame and link the 142 seized domains and hashes to your own observed victims to scope the blast radius.

mapping behind this week's takedowns — pivoting from a seized server to its domains, operators, and the wallets in the financial cash-out chain.

following the €41M flagged by Operation Endgame and the laundering rails behind the Huione seizure — from victim payment to exchange off-ramp.

movement. A fast first pass on a host suspected of Amadey or StealC infection to surface the credential theft and follow-on activity those loaders enable.

PRIORITY CVE ADVISORIES

ARCHIVE ALERT

CVE-2026-48907 (JOOMLA JCE)

Improper access control in the Joomla Content Editor lets an unauthenticated attacker create a rogue editor profile and abuse profile-import to upload and execute PHP, planting a web shell; CVSS 10.0. Actively exploited; CISA KEV June 16. *Forensic Note:* Hunt newly imported editor profiles and rogue PHP under media/upload directories; upgrade to JCE 2.9.99.5.

ARCHIVE ALERT

CVE-2026-42530 (NGINX / F5)

A use-after-free in the HTTP/3 module lets an unauthenticated remote attacker cause denial of service or, where ASLR is bypassed, remote code execution; CVSS 9.2. Out-of-band fixes shipped June 18 alongside an HTTP/2 and gRPC heap overflow. *Forensic Note:* Review HTTP/3 (QUIC) traffic and worker-process crashes; upgrade to OSS 1.31.2 or Plus R37 P2 / R36 P6.

RECENT MALWARE WATCH

ARCHIVE: JUNE 23, 2026

ROKAROLLA — ANDROID DEVICE-TAKEOVER BANKER

An Android banking trojan that targets 217 banking and crypto apps with 137 remote commands, leaning on a single granted Accessibility permission to overlay fake login pages, intercept calls to suppress fraud alerts, and rewrite the clipboard to swap in attacker wallet addresses. Examine Accessibility-service grants, sideload origins, overlay-injection artifacts, and clipboard-tampering hooks.

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 and correlate Teams-relay connections from servers that never host meetings.