THE FORENSICS WAY

ISSUE 09 | FORENSICS AWARENESS THIS WEEK | TUESDAY, MARCH 31, 2026

FRONT PAGE

STATE-SPONSORED ESPIONAGE

Sleeper Cells in the Backbone: China's Red Menshen Pre-Positioned BPFdoor Inside Global Telecom Networks

Rapid7 Labs confirmed on March 26 that Chinese state-nexus group **Red Menshen** has spent years systematically embedding **BPFdoor** implants inside telecommunications backbone infrastructure worldwide — not for immediate data theft, but as dormant sleeper cells that can be activated on command for espionage or large-scale disruption.

BPFdoor abuses the Linux kernel's BPF subsystem to inspect raw packets, awakening only on a trigger buried in normal HTTPS traffic — exposing no listening ports and generating zero C2 traffic at rest. Rapid7 released a free detection script; investigators must hunt for raw socket usage, anomalous BPF filter installations, and process spoofing artifacts on all Linux network edge hosts.

SUPPLY CHAIN ESCALATION

CanisterWorm Goes Ransomware: TeamPCP Pivots to Vect RaaS After Stealing 300 GB of Developer Credentials

The **TeamPCP** CanisterWorm campaign escalated dramatically this week as the group partnered with Vect ransomware-as-a-service and confirmed first ransomware deployments using 300 GB of stolen CI/CD credentials harvested from 474 compromised GitHub repositories and 1,750 Python packages.

Within eight days, TeamPCP expanded targeting from Linux to Windows, pivoted delivery from Base64 inline encoding to WAV steganography, and extended the blast radius to Checkmarx, LiteLLM, and Telnyx SDK. Any organization that consumed affected packages must treat downstream endpoint compromise — not just credential exposure — as a live incident.

Threat Bulletin

ACTIVE EXPLOIT

CVE-2025-53521

F5 BIG-IP APM — Unauthenticated RCE triggered by malicious traffic when an APM access policy is active; CVSS 9.3. Added to CISA KEV March 27; federal patch deadline March 30. *Forensic Note:* BIG-IP APM sits at the auth perimeter — audit all systems that authenticated through the affected appliance for lateral movement.

CRITICAL

CVE-2026-21643

Fortinet FortiClient EMS — Pre-auth SQL injection via unsanitized tenant header extracts full admin credentials from the PostgreSQL backend; CVSS 9.8. 2,000+ exposed instances tracked by Shadowserver. *Forensic Note:* Audit EMS policy deployment chains and endpoint telemetry for unauthorized policy changes.

MALWARE SPOTLIGHT

Infiniti Stealer (ClickFix)

Python-based macOS infostealer delivered via Cloudflare-branded fake browser verification prompts using Bash one-liners — the ClickFix technique — that bypass Gatekeeper assumptions. Targets credentials, browser data, and crypto wallets. *Forensic Note:* No traditional binary footprint; detection requires user-behavior telemetry and script-execution monitoring.

THE FORENSICS WAY

HISTORICAL ARCHIVES | HISTORY OF DIGITAL INVESTIGATION | TUESDAY, MARCH 31, 2026

CASE STUDIES: HISTORICAL GRID

MOONLIGHT MAZE (1996–1999)

The First State Cyber Espionage Campaign — Russia's Multi-Year Infiltration of US Military Networks

From 1996 to 1999, Russian state actors systematically exfiltrated terabytes from US military, NASA, and DoE networks in what became the first publicly attributed state-sponsored cyber espionage campaign — Moonlight Maze. Investigators traced the attack through telephone records and sustained international cooperation, establishing the attribution framework still applied in state-nexus telecom cases like BPFdoor today.

OPERATION APT1 / COMMENT CREW (2006–2013)

The Mandiant Report That Named Names: How China's PLA Stole Terabytes From 141 US Organizations

In February 2013, Mandiant publicly attributed years of systematic IP theft to China's PLA Unit 61398 — designating them APT1. The Comment Crew maintained persistent access to 141 US organizations across 20 industries for an average of 356 days per victim, stealing terabytes of intellectual property. The report pioneered the modern threat-actor attribution methodology that every state-nexus investigation now follows.

SOLARWINDS ORION SUPPLY CHAIN (2020)

SUNBURST: The Supply Chain Attack That Reached 18,000 Organizations

In December 2020, state-sponsored attackers embedded a backdoor called SUNBURST into SolarWinds Orion software updates, compromising 18,000 organizations including nine US federal agencies. The malware lay dormant for two weeks before activation, communicating via DNS beaconing that mimicked legitimate Orion traffic. Its discovery forced investigators to develop new

COLONIAL PIPELINE RANSOMWARE (2021)

One Compromised Password Shut Down 45% of US East Coast Fuel Supply

The DarkSide ransomware attack on Colonial Pipeline in May 2021 forced a six-day shutdown of 5,500 miles of fuel pipeline serving 45% of the US East Coast. Attackers gained initial access via a single compromised VPN credential with no MFA enforced — the account had not been used in months but remained active. The incident became the primary basis for CISA's OT/ICS network segmentation guidance and defined critical infrastructure IR planning for years.

methodologies to distinguish compromised telemetry from authentic network data.

TOOLS OF THE TRADE

OPEN SOURCE

MalHunt

MAJOR REWRITE — MARCH 2026

Python suite that orchestrates Volatility3 plugin runs and YARA scanning across memory dumps. The March 2026 rewrite migrates fully to Volatility3, auto-fetches and compiles the 3,300-rule Yara-Forge bundle daily, and adds modular packaging for pipeline integration. Directly applicable for memory forensics on BPFdoor-infected Linux hosts where kernel-resident artifacts must be recovered.

UTILITY / SCRIPT

Rapid7 BPFdoor Detector

RELEASED MARCH 26, 2026

Open-source scanner from Rapid7 Labs designed to detect BPFdoor implants on Linux systems, released alongside their telecom backbone research. Hunts for kernel-level BPF filter anomalies, raw socket usage, and process masquerading artifacts consistent with Red Menshen TTPs. The first purpose-built open-source tool addressing BPFdoor's kernel-resident evasion techniques.

OPEN SOURCE

NIST OpenLQM

RELEASED MARCH 2026

NIST's open-source latent fingerprint quality assessment tool — formerly restricted to US law enforcement as LQMetric — now available cross-platform worldwide. Scores print quality from 0–100, enabling triage prioritization across hundreds of latent prints from a scene. Accompanied by NIST Special Database 302: 10,000 annotated latent fingerprint images for examiner and AI training.

COMMERCIAL

Magnet One Mobile Case Stream

GA LAUNCH — MARCH 27, 2026

Cloud-powered mobile evidence platform combining GrayKey acquisition, cloud-based artifact processing, and collaborative case review in one streaming workflow. Moves processing off lab workstations, cutting time-to-evidence from days to minutes and enabling parallel multi-source analysis. Designed for distributed teams working mobile-heavy ransomware and supply chain investigations.

PRIORITY CVE ADVISORIES

ARCHIVE ALERT

CVE-2026-20131 (CISCO FMC)

Unauthenticated RCE via Java deserialization; CVSS 10.0. Zero-day exploited by Interlock ransomware for 36 days before patch. *Forensic Note:* Audit FMC HTTP request logs and connected Firepower devices for lateral movement artifacts.

ARCHIVE ALERT

CVE-2026-3564 (SCREENCONNECT)

ASP.NET machine key exposure allows session token forgery and support session hijacking; CVSS 9.0. *Forensic Note:* In MSP-linked intrusions, audit ScreenConnect session logs and config files for machine key extraction.

RECENT MALWARE WATCH

ARCHIVE: MAR 24, 2026

CANISTERWORM (TEAMPCP)

Self-propagating npm worm using ICP blockchain C2 — the first documented case. Seeded via Trivy supply chain compromise; autonomously spreads by harvesting npm auth tokens and publishing malicious packages.

ARCHIVE: MAR 17, 2026

AVRECON BOTNET (SOCKSESCORT)

360,000 compromised routers recruited to launder ransomware C2 traffic. Dismantled by US and European authorities. Hunt via outbound connection anomalies and firmware integrity checks.