# THE FORENSICS WAY

ISSUE 37 | FORENSICS AWARENESS THIS WEEK | TUESDAY, OCTOBER 13, 2026

## FRONT PAGE

OPERATIONAL TECHNOLOGY

### The Fridges Were the Attack Surface: Hundreds of French Supermarkets Lose the Cold Chain to Controllers Nobody Was Still Patching

Overnight on October 11–12, attackers remotely drove refrigeration setpoints at hundreds of French supermarkets as high as 50°C. Intermarché reported up to 200 stores affected, Coopérative U nearly 100, Carrefour 80 and Monoprix around 30, with Netto, E.Leclerc and Auchan also named in reporting. Affected Intermarché stores were told to discard all fresh and frozen stock, and the Paris prosecutor's office — which has opened an investigation — attributes fires to the incident. The Prime Minister asked ANSSI to examine it; no actor has claimed responsibility.

Danfoss has confirmed its AK-SM800 and AK-SC355 controllers among the affected equipment, describing most of it as legacy hardware no longer receiving software or security updates, with one AK-SM800 found running outdated firmware. The initial access path is not officially established, though the controllers are widely reported as internet-reachable and Danfoss's own guidance is to remove direct internet access. Forensic priority: this evidence spoils faster than the stock. Capture controller configuration, setpoint-change history and alarm logs *before* swapping hardware out, because replacement destroys the only record of what was commanded and when. Treat the temperature logs as the proof of harm, and reconcile each setpoint change against an authorised maintenance action — and note that Claroty-reported flaws in the newer AK-SM 800A, fixed in 2025, have not been linked to this attack.

VULNERABILITY MANAGEMENT

### Eleven Years Late: CISA Flags Five Legacy Flaws as Actively Exploited, the Oldest Disclosed in 2015

On October 8 the Known Exploited Vulnerabilities catalogue took five additions in a single batch, and not one of them is new: CVE-2015-5477 in ISC BIND, CVE-2015-3306 in ProFTPD, CVE-2016-3081 in Apache Struts, CVE-2021-3199 in ONLYOFFICE Docs and

## THREAT BULLETIN

**Active Exploit**

**CVE-2026-104286** — Fortinet FortiMail. A path traversal (CWE-22) combined with improper NULL-byte handling (CWE-158) lets an unauthenticated attacker write arbitrary files via crafted HTTP/HTTPS requests, reportedly via the webmail IBE component. CVSS 9.8, disclosed as an exploited zero-day in FG-IR-26-175 on October 1 with no fix then available; CISA KEV due October 4. *Forensic Note:* Interim guidance is to disable IBE where unused and restrict interface access — then hunt for files written outside expected directories, since arbitrary write is the foothold.

**Critical**

**CVE-2026-89111 / CVE-2026-89107** — SAP, October 13 Patch Day. The first is an unauthenticated SSRF in SAP Cloud SDK for Python (CVSS 10.0): an attacker controlling a tenant subdomain value can redirect OAuth2 token requests to their own server and capture client credentials. The second is ABAP code injection in S/4HANA (CVSS 9.9). No in-the-wild exploitation reported yet. *Forensic Note:* Credential capture leaves no failed authentication, so audit OAuth2 token endpoints for requests

CVE-2023-22894 in Strapi, with a remediation due date of October 11. Fixes for the oldest two have existed for eleven years.

A 2015 flaw exploited in 2026 is rarely a patching failure; it is an inventory failure. Software that old is generally not sitting on a tracked server — it is embedded in an appliance, bundled inside a vendor-managed box, or running on a host that no longer appears in anyone's asset register, which is precisely the condition that put unsupported refrigeration controllers in this week's other story. Forensic priority: pivot from "are we patched" to "do we know this is here." Hunt for these components by service fingerprint and file artefact rather than by asset list, since the systems most likely to be running them are the ones your inventory has already lost track of, and treat an unexplained BIND, ProFTPD or Struts instance as a scoping question rather than a closed finding.

resolved to unexpected hosts and rotate any client secrets issued to multi-tenant BTP apps.

---

**Malware Spotlight**

### MATCHBOIL / MATCHWOK — The Downloader That Moved From Ministries to the Power Grid

ESET research published this week tracks Russia-aligned UAC-0099's continued refinement of MATCHBOIL, a C# downloader whose usual payload is the MATCHWOK backdoor. Delivery runs through phishing impersonating Ukrainian court summonses, carrying an archive with a script inside; command-and-control sits on BitLaunch VPS hosts partly screened behind Cloudflare, and some operations also deploy the DRAGSTARE stealer. The notable shift is targeting: ESET now sees transport, manufacturing and energy victims rather than the usual government, financial and media set. *Forensic Note:* Sandbox evasion and heavy .NET obfuscation make dynamic triage unreliable, so anchor hunting on the archive-plus-script delivery pattern and on egress to VPS ranges behind a CDN.



THE FORENSICS WAY

HISTORICAL ARCHIVES | HISTORY OF DIGITAL INVESTIGATION | TUESDAY, OCTOBER 13, 2026

# CASE STUDIES: HISTORICAL GRID

THE GERMAN STEEL MILL (2014)

## A Furnace That Could Not Be Shut Down: The Case That Proved Code Could Break Metal

Germany's federal information security agency, the BSI, disclosed in its December 2014 annual report that attackers had phished their way into a steel mill's office network, pivoted into the production network, and left a blast furnace unable to be shut down in a controlled manner — causing what the agency called massive physical damage. The report credited the attackers with detailed knowledge of industrial control systems, named neither the plant nor an actor, and published almost no technical indicators. That silence became its own lesson: it remains one of the most-cited OT incidents precisely because so little evidence was ever released, a problem this week's refrigeration attack risks repeating if controller state is discarded during the rush to restore cooling.

MAROOCHY SHIRE (2000)

## Forty-Six Radio Commands: The First OT Intrusion Investigated Well Enough to Convict

Across February to April 2000, Vitek Boden used a laptop and a two-way radio to issue commands to sewage pumping stations in Maroochy Shire, Queensland, releasing on the order of 800,000 litres of raw sewage into parks, waterways and hotel grounds. He had worked for the contractor that installed the SCADA system, so his instructions were indistinguishable from legitimate ones in isolation. Investigators built the case by correlating radio telemetry against pump-station alarms to separate attack from malfunction, then recovered the control software and command traces from the seized laptop. It stands as the earliest OT compromise investigated thoroughly enough to secure a conviction — and the original demonstration that in control systems, the evidence lives in the command history.

JUNIPER SCREENOS (2015)

## Unauthorized Code in the Firewall: When the Appliance Itself Was the Thing That Could Not Be Trusted

On December 17–18, 2015, Juniper disclosed that an internal source-code review had turned up unauthorized code in ScreenOS, the operating system behind its NetScreen firewalls. The advisory covered two separate backdoors: a hardcoded master password granting administrative access over SSH and Telnet (CVE-2015-7755), and an altered Q parameter in the Dual_EC_DRBG random number generator that let a passive eavesdropper decrypt VPN traffic (CVE-2015-7756). The earliest affected builds shipped in 2012, leaving the code in production for roughly three years, and Fox-IT recovered

THE UBER BREACH AND COVER-UP (2016)

## The Keys Were in the Repository: A Credential Leak That Became a Criminal Case About the Response

In October 2016, attackers reached a private GitHub repository used by Uber engineers, lifted AWS credentials committed into it, and used them to pull an S3 datastore holding records on roughly 57 million riders and drivers, including some 600,000 driver's licence numbers. Uber paid the attackers $100,000 routed through its bug-bounty programme and obtained non-disclosure agreements, and the breach stayed unreported until November 2017; the company's security chief was convicted of obstruction of justice and misprision of a felony in October 2022.

the backdoor password within six hours of disclosure.

# TOOLS OF THE TRADE

OPEN SOURCE

### Scalpel3

LSU — NEW RELEASE

File carver aimed at automatically reconstructing fragmented files from damaged or partially wiped media, validated against the DFRWS 2006 and 2007 carving challenges. Built for the case where the filesystem is gone but the content is not — recovering logs and configuration from embedded or failing storage.

OPEN SOURCE

### ntfsfind & ntfsdump

COMMAND LINE — NTFS

Paired command-line utilities that search for and extract files directly out of Windows disk images without mounting them. Avoiding the mount keeps the examiner's host from touching the evidence filesystem, which matters when the image is the subject of a prosecution rather than an internal review.

COMMERCIAL

### MD-LIVE

GMDSOFT — BLOCK HASH SCAN

Mobile triage tool whose Block Hash Scan matches a device against a prepared hash set, hashing only the blocks needed rather than whole files. A quick pass flags candidates and a deeper pass confirms them, so on-scene examiners can decide what to seize without taking a full image first.

UTILITY / SCRIPT

### VESTIGEX

BETA V1.1.1 — FREE

Free Windows desktop DFIR platform, currently in beta, that produces hash-chained audit logs alongside chain-of-custody reports in HTML, PDF, Word and Excel. Useful where the output has to survive challenge — the audit chain documents what the examiner did, not only what was found.

## PRIORITY CVE ADVISORIES

**ARCHIVE ALERT**

**CVE-2026-76504 (CISCO CATALYST SD-WAN MANAGER)**

URI hex-encoding mishandling (CWE-177) slips a crafted request past the rule guarding an API endpoint, giving unauthenticated admin access; CVSS 9.8, CISA KEV September 30. *Forensic Note:* Hunt an encoded "j" in the *j_security_check* path in raw web logs.

**ARCHIVE ALERT**

**CVE-2026-102489 / CVE-2026-102490 (ZAMMAD)**

Session fixation alongside improper privilege management in the help-desk platform, both added to CISA KEV October 2. *Forensic Note:* Session fixation leaves no failed-login trail — audit session identifiers that predate their own successful authentication.

## RECENT MALWARE WATCH

**ARCHIVE: OCTOBER 6, 2026**

**SC — THE WORDPRESS BACKDOOR THAT REBUILDS ITSELF**

Sucuri's "self-healing mesh" living in at least eight places at once across files, a database options row and a System V shared-memory segment, where any survivor restores the rest on the next page load. Enumerate all persistence classes before removing any.

**ARCHIVE: SEPTEMBER 29, 2026**

**KREMLIN — BANKING THEFT FROM INSIDE THE BROWSER**

Brazilian toolkit chaining JavaScript loaders and C++ installers to plant malicious Chrome and Edge extensions, harvesting session tokens from an already-authenticated browser and so bypassing MFA. Inventory extensions against an approved list.