THE FORENSICS WAY

ISSUE 13 | FORENSICS AWARENESS THIS WEEK | TUESDAY, APRIL 28, 2026

FRONT PAGE

LAW ENFORCEMENT & ATTRIBUTION

OSINT Catches Scattered Spider: 'Tylerb' Pleads Guilty to $8M SIM-Swap Campaign Against Twilio, LastPass & Others

On April 21, Tyler Robert Buchanan — a 24-year-old British national and senior Scattered Spider operator known as 'Tylerb' — pleaded guilty to wire fraud conspiracy and aggravated identity theft in federal court. Buchanan led SMS phishing campaigns that compromised **Twilio**, **LastPass**, **DoorDash**, **Mailchimp**, and at least eight other tech companies in 2022, enabling SIM-swap attacks that stole over $8 million in cryptocurrency from victims.

FBI investigators broke attribution using open-source techniques: Buchanan had reused identical usernames and email addresses across dozens of phishing domain registrations, leaving a recoverable thread through infrastructure records. Spanish authorities arrested him in June 2024 while boarding a flight to Italy before extradition to the US. The case is a textbook example of how repeated identifiers in domain registration data enable OSINT attribution of otherwise sophisticated threat actors.

SOCIAL ENGINEERING & LATERAL MOVEMENT

UNC6692 Weaponizes FTK Imager to Steal Active Directory Databases via Fake Microsoft Teams IT Helpdesk

Google Threat Intelligence Group and Mandiant disclosed **UNC6692** — a newly identified threat group combining email flooding, Microsoft Teams impersonation of IT helpdesk staff, and a custom modular malware suite named SNOW. Active since December 2025, the campaign targets senior employees (77% of March–April incidents were director-level or above). Initial access is pure social engineering — no CVE exploitation required.

Once inside, UNC6692 deploys SNOWBELT (Chrome extension for persistence), SNOWGLAZE (Python tunneler), and

Threat Bulletin

ACTIVE EXPLOIT

CVE-2026-33825

Microsoft Defender — insufficient access control enabling local privilege escalation; added to CISA KEV April 22, 2026 with confirmed active exploitation in the wild. *Forensic Note:* Review Windows Security logs for unexpected privilege escalation sequences (Event ID 4672/4673) and Defender service modification events that may indicate exploitation prior to detection.

CRITICAL

CVE-2025-31324

SAP NetWeaver Visual Composer — unrestricted file upload to Metadata Uploader endpoint enabling unauthenticated RCE; CVSS 10.0. Active exploitation campaigns targeting unpatched instances renewed in April 2026. *Forensic Note:* Inspect SAP HTTP access logs for POST requests to /developmentserver/metadatauploader and scan web-accessible directories for planted JSP or ASPX web shells.

MALWARE SPOTLIGHT

Lotus Wiper (Venezuela Energy Sector)

Data-wiping malware targeting Venezuela's energy and utilities sector; compiled September 2025, active through April 2026. Two batch scripts orchestrate MBR overwrite, drive destruction, defense weakening, and full-volume file deletion — no ransom demand, pure geopolitical sabotage. *Forensic Note:* Disk imaging must be prioritized on triage; hunt batch script

SNOWBASIN (Python backdoor), then spreads via PsExec and LSASS credential dumping. Most forensically significant: the group weaponizes legitimate forensic tool **FTK Imager** to extract the Active Directory database (ntds.dit) and registry hives before exfiltration via LimeWire peer-to-peer sharing — adding FTK Imager to the growing list of DFIR tools turned against defenders.

artifacts and abnormal system utility process trees in Windows event logs preceding the wipe timestamp.

THE FORENSICS WAY

HISTORICAL ARCHIVES | HISTORY OF DIGITAL INVESTIGATION | TUESDAY, APRIL 28, 2026

CASE STUDIES: HISTORICAL GRID

TARGET DATA BREACH (2013)

An HVAC Vendor's Stolen Credentials and 40 Million Payment Cards: The Breach That Defined Third-Party Risk

In November 2013, attackers used stolen credentials from Target's HVAC vendor Fazio Mechanical to access the supplier portal and move laterally to POS systems across 1,800 stores. BlackPOS RAM-scraping malware harvested 40 million payment card records in-transit before encryption. Target's own security systems generated alerts that went uninvestigated — the breach was ultimately surfaced by DOJ investigators. The case defined third-party vendor access as retail's primary attack vector.

EQUIFAX DATA BREACH (2017)

A 76-Day Dwell, an Expired SSL Certificate, and 148 Million Americans' Data Silently Exfiltrated

In May 2017, attackers exploited an unpatched Apache Struts vulnerability (CVE-2017-5638) in Equifax's online dispute portal — a patch had been available for two months. The attackers spent 76 days inside the network executing 51 unmonitored database queries, exfiltrating 148 million Americans' SSNs, birth dates, and financial records. An expired internal SSL certificate had blinded the security inspection system to outbound traffic for 19 months prior to discovery.

RSA SECURID BREACH (2011)

The Hack That Broke Two-Factor Auth: Nation-State Actors Extract RSA's Entire SecurID Seed Database

SHAMOON / DISTTRACK (2012)

35,000 Saudi Aramco Workstations Wiped in Hours — The Wiper Attack That

In March 2011, RSA Security was breached via a spear-phishing Excel attachment exploiting an Adobe Flash zero-day. Attackers deployed Poison Ivy RAT, staged exfiltrated data as encrypted RAR archives, and used FTP for exfiltration — all traffic engineered to blend with legitimate patterns. The stolen asset was the seed database for 40 million SecurID tokens deployed at US government agencies and defense contractors, effectively undermining the enterprise 2FA ecosystem at scale.

Redefined Destructive Malware

In August 2012, the SHAMOON wiper simultaneously destroyed the MBR and user files of 35,000 Saudi Aramco workstations across a single weekend, forcing the world's largest oil company to replace its entire PC fleet. Unlike ransomware, the payload carried no ransom demand — its sole purpose was destruction. Forensic recovery was possible only through Active Directory audit logs, offline backup tapes, and partial disk images from machines where payload execution failed mid-run.

TOOLS OF THE TRADE

OPEN SOURCE

Volatility 3

ACTIVE RELEASE — 2026

Memory forensics framework for Windows, macOS, and Linux RAM image analysis. Directly applicable to this week's UNC6692 LSASS credential theft — Volatility's hashdump and lsadump plugins extract NTLM hashes from memory images without touching the live system. Plugin architecture enables rapid triage of kernel objects, network connections, and process injection artifacts from a single RAM acquisition.

UTILITY / SCRIPT

EvtxECmd

EZ TOOLS — ACTIVE 2026

Command-line Windows Event Log (.evtx) parser from Eric Zimmerman's suite, outputting structured CSV/JSON for timeline analysis. Processes thousands of event log files simultaneously with custom map files for targeted Event ID hunting. Essential for BASANAI and UNC6692 investigations — batch parsing Security, System, and Application logs into a single unified timeline dramatically accelerates lateral movement and privilege escalation reconstruction.

COMMERCIAL

Falcon Forensics

CROWDSTRIKE — ACTIVE 2026

Automated forensic data collection and triage platform for Windows, macOS, and Linux endpoints. Enables wide-aperture, point-in-time or continuous collection of process trees, network connections, file system artifacts, and registry state without requiring full disk imaging. Integrated threat intelligence correlation surfaces IOCs against collected artifacts automatically — particularly effective for distributed IR across enterprise environments during active intrusions like UNC6692.

OPEN SOURCE

Autopsy

V4.21 — ACTIVE 2026

Open-source digital forensics platform with graphical interface for disk image analysis, timeline reconstruction, keyword search, and artifact extraction. Module ecosystem covers browser history, registry analysis, email parsing, and hash filtering against NSRL and custom hash databases. Widely adopted in law enforcement and private IR engagements — a practical starting point for Target- and Equifax-style breach investigations involving acquired disk images.

PRIORITY CVE ADVISORIES

ARCHIVE ALERT

CVE-2026-32201 (MS SHAREPOINT)

Authentication bypass enabling spoofing and unauthenticated RCE; patched April 14 Patch Tuesday, confirmed exploited in the wild prior to patch. *Forensic Note:* Review SharePoint ULS logs for anomalous auth events and MSSQL audit trails for unauthorized stored procedure execution.

ARCHIVE ALERT

CVE-2026-34197 (APACHE ACTIVEMQ)

Unauthenticated RCE via OpenWire protocol; CVSS 8.8. Over 6,000 exposed instances exploited, CISA KEV April 2026. *Forensic Note:* Examine broker logs for unexpected JVM subprocess trees; scan webapps directories for Java-based web shells.

RECENT MALWARE WATCH

ARCHIVE: APR 21, 2026

BASANAI (MEDUSALOCKER)

MedusaLocker-family ransomware targeting enterprise Windows via RDP brute force; AES-256/RSA-2048, VSS deletion pre-encryption. Hunt Event ID 4625 RDP sequences and vssadmin commands preceding file encryption timestamps.

ARCHIVE: APR 14, 2026

OMNISTEALER (NORTH KOREA)

Infostealer using TRON blockchain as C2; payloads embedded in BSC transaction input fields. Targets 10+ password managers, 60+ crypto wallets. Hunt outbound TRON/Aptos RPC connections; on-chain analysis required for attribution.