INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-07-07 15:05 UTC

Interpol-Impersonation Phishing Campaign Delivers Ransomware via Proton Drive Archives

THREAT CAMPAIGN | **HIGH** | CVSS 8.1

SCC Item ID	SCC-CAM-2026-0632
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	8.1
Affected Products	Small businesses across Europe, Asia, the Middle East, and North America, multiple sectors
Published	2026-07-06
Discovery Source	Gemini

Executive Summary

An active phishing campaign impersonates Interpol to pressure small business employees into downloading ransomware from Proton Drive. Victims receive emails falsely claiming their organization is under criminal investigation; the urgency drives clicks on a password-protected archive containing a ransomware executable disguised with a video-file extension (.mp4, .avi, .mov). Small businesses across Europe, Asia, the Middle East, and North America face encryption of critical systems, operational shutdown, and potential ransom demands, with limited IT resources to recover quickly.

Technical Analysis

This campaign targets small businesses via spearphishing attachments (T1566.001) and link-based lures (T1566.002). The lure impersonates Interpol, invoking fear of criminal investigation to manipulate targets into action (CWE-1021: Improper Restriction of Rendered UI Layers; CWE-693: Protection Mechanism Failure; CWE-345: Insufficient Verification of Data Authenticity). The payload, ransomware masquerading as a video file (T1036: Masquerading), is hosted on Proton Drive (T1537: Transfer Data to Cloud Account), a legitimate service with strong URL reputation, likely chosen to bypass email gateway URL filters and sandboxing. The archive is password-protected, a technique consistent with CWE-693, intended to prevent automated attachment detonation. User execution is required (T1204.002). Upon execution, the ransomware encrypts files (T1486: Data Encrypted for Impact). Confidence in campaign existence is medium; confidence in specific payload technical details and attribution is low. No threat actor group has been identified. No CVE, specific payload hash, or C2 infrastructure is confirmed in available reporting.

Action Checklist

1. Step 1: Containment. At the email gateway, block or quarantine password-protected archive attachments from external senders and flag any inbound email referencing Interpol, criminal investigation, or legal action. At the web proxy or DNS filter, restrict downloads from proton.me and drive.proton.me for any organization that does not have a documented business need for Proton Drive access. Do not open any password-protected archive received via unsolicited email.
2. Step 2: Detection. Search email gateway logs for messages containing keywords 'Interpol', 'criminal investigation', 'legal notice', or links to proton.me/drive.proton.me delivered to small-business employee accounts. Review endpoint detection logs for execution of files with video-file extensions (.mp4, .avi, .mov) that trigger process creation or file encryption activity. Monitor for mass file rename or extension-change events consistent with ransomware staging (NIST AU-2: Event Logging; CIS Control 8.2: Collect Audit Logs). Check for lateral movement or credential access following any suspected execution.
3. Step 3: Eradication. If a host has executed the payload, isolate it from the network immediately. Terminate any active encryption processes. Remove the malicious archive and any dropped executables identified by endpoint detection tooling. Reset credentials for any accounts accessed on the compromised host (NIST IA-4: Identifier Management). Audit cloud storage access logs for unauthorized data staging or exfiltration activity (T1537).
4. Step 4: Recovery. Restore encrypted files from verified, offline or immutable backups. Confirm backup integrity before restoration. Validate that no ransomware persistence mechanisms (scheduled tasks, startup entries) remain using system initialization configuration analysis (NIST SI-7: Software, Firmware, and Information Integrity). Monitor restored systems for re-infection indicators for a minimum of 72 hours post-restoration. Reintroduce systems to the network only after clean validation.
5. Step 5: Post-Incident. Conduct targeted phishing awareness training focused on authority-impersonation lures (law enforcement, regulatory body) and the risk of password-protected archives from unsolicited email. Review email gateway policies to enforce attachment sandboxing and block password-protected archives from unknown senders. Implement or validate MFA on all externally exposed and administrative accounts (NIST IA-2: Authentication; CIS Control 6.3, CIS Control 6.4, CIS Control 6.5). Audit user account permissions to enforce least privilege, limiting blast radius of any future endpoint compromise (NIST AC-6).

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately if any host confirms payload execution (mass file extension changes, ransom note dropped, VSS deletion detected), if more than one business unit is affected indicating lateral movement beyond initial phishing victim, or if regulated data (PII, PHI, payment card data) was accessible on encrypted systems triggering breach notification obligations under GDPR, HIPAA, or PCI-DSS.

Recovery Notes	Restoration must use only offline or immutable backups verified by hash comparison — do not restore from any backup stored on a network share accessible from the compromised host, as ransomware commonly traverses mapped drives before encrypting. Before reintroducing any restored system to the network, confirm shadow copy status, validate all persistence locations (scheduled tasks, run keys, startup folders) are clean via Autoruns, and reimage rather than in-place recover any host where the encryption process ran with SYSTEM or administrator privileges. Maintain Sysmon monitoring on all restored hosts for a minimum of 72 hours, specifically watching for re-execution of any binary with the same hash or process lineage as the original payload.
Forensic Artifacts	Original phishing .eml file with full SMTP headers (Return-Path, Received chain, DKIM/SPF results, Message-ID) — identifies sender infrastructure and spoofing technique used to impersonate Interpol | Password-protected archive file (e.g., ZIP/RAR containing the ransomware disguised as .mp4/.avi/.mov) — hash the container and the extracted payload for threat intelligence submission and AV/EDR rule development | Sysmon Event ID 1 logs showing process creation from a video-extension image name, including parent process (likely explorer.exe or a mail client), command line, and SHA-256 hash of the executed file | Windows Security Event Log Event ID 4663 (Object Access) and file system audit entries showing the directories and file types targeted by the encryption routine, plus Event ID 4688 (Process Creation) for the ransomware process and any child processes it spawned | Ransom note files dropped in encrypted directories — filename pattern, embedded payment/contact addresses, and any unique strings identify the ransomware family and variant for cross-referencing with threat intelligence sources such as ID Ransomware or NoMoreRansom

Per-Action IR Details

Step 1: Containment — Block downloads from proton.me and drive.proton.me at the email gateway and web proxy for any organization that does not have a documented business need for Proton Drive access. Flag and quarantine any inbound email referencing Interpol, criminal investigation, or legal action as a lure keyword. Do not open any password-protected archive received via unsolicited email.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: NIST AC-4 (Information Flow Enforcement), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices)

Compensating: At the email gateway (e.g., Postfix + SpamAssassin), add header/body regex rules matching 'Interpol', 'criminal investigation', 'legal notice' to route to quarantine. At the web proxy (e.g., Squid), add ACL deny entries for *.proton.me and drive.proton.me. On Windows hosts without a proxy, use Windows Firewall (netsh advfirewall) or a hosts-file block for proton.me to prevent drive downloads. Both actions require only CLI access and take under 15 minutes for a 2-person team.

Evidence: Before pushing gateway and proxy rules, capture the current email gateway queue and any already-delivered messages matching the lure keywords — export raw .eml files preserving full headers (Return-Path, Received chain, X-Mailer, Message-ID) to establish sender infrastructure. Capture web proxy access logs (e.g., /var/log/squid/access.log) showing any prior requests to proton.me/drive.proton.me, including timestamps, source IPs, and full URLs, to identify hosts that may have already downloaded the archive before the block is applied. These logs are at risk of rotation and must be archived before rule changes flush cache state.

Step 2: Detection — Search email gateway logs for messages containing keywords 'Interpol', 'criminal investigation', 'legal notice', or links to proton.me/drive.proton.me delivered to small-business employee accounts. Review endpoint detection logs for execution of files with video-file extensions (.mp4, .avi, .mov) that trigger process creation or file encryption activity. Monitor for mass file rename or extension-change events consistent with ransomware staging (NIST AU-2: Event Logging; CIS 8.2: Collect Audit Logs). Check

for lateral movement or credential access following any suspected execution.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, And Reporting), CIS 8.2 (Collect Audit Logs)

Compensating: Deploy Sysmon (SwiftOnSecurity config baseline) with Event ID 1 (Process Create) filtering for image names ending in .mp4, .avi, or .mov; Event ID 11 (File Create) for rapid sequential writes to user-profile directories indicative of encryption staging; and Event ID 3 (Network Connect) for outbound connections from video-extension processes. Use PowerShell to sweep delivered mail: Get-MessageTrackingLog -EventId DELIVER | Where-Object {$_.MessageSubject -match 'Interpol|investigation|legal notice'}. Use a Sigma rule targeting Sysmon Event ID 1 where ParentImage is explorer.exe and Image matches *.mp4 or *.avi to catch the disguised payload launch — Sigma rules can be converted to native Windows Event Log queries via sigmac without a SIEM.

Evidence: This step is analytical and does not alter live host state; however, if any endpoint shows process creation from a video-extension file, treat that host as actively compromised and capture before any further action: (1) full RAM image using WinPmem or DumpIt to preserve in-memory encryption keys and injected code; (2) netstat -ano or Get-NetTCPConnection output to record active C2 or exfiltration connections; (3) tasklist /svc and Get-Process to record all running processes and their parent PIDs; (4) Sysmon EVTX export from %SystemRoot%\System32\winevt\Logs\Microsoft-Windows-Sysmon%4Operational.evtx; (5) VSS snapshot enumeration via vssadmin list shadows to determine whether the ransomware has already deleted shadow copies.

Step 3: Eradication — If a host has executed the payload, isolate it from the network immediately. Terminate any active encryption processes. Remove the malicious archive and any dropped executables identified by endpoint detection tooling. Reset credentials for any accounts accessed on the compromised host (D3-CRO: Credential Rotation). Audit cloud storage access logs for unauthorized data staging or exfiltration activity (T1537).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-2 (Account Management), NIST AC-6 (Least Privilege), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 6.2 (Establish an Access Revoking Process)

Compensating: Network isolation: disable the NIC via Device Manager or run netsh interface set interface 'Ethernet' admin=disable to sever connectivity without full power-off (preserving volatile state). Terminate encryption processes: use taskkill /F /PID targeting the process identified in Step 2 Sysmon logs — do NOT reboot, which destroys in-memory evidence. Remove the malicious archive and dropped executables using their SHA-256 hashes (computed prior to deletion via certutil -hashfile SHA256) and log the file paths. For credential rotation on a small-business domain, run net user /domain for all accounts with interactive or remote sessions on the host. For Proton Drive exfiltration audit, if the organization has a Proton for Business account, review the account's activity log via the Proton admin panel; otherwise, query proxy logs for POST/PUT requests to api.protonmail.ch or drive.proton.me originating from the compromised host.

Evidence: CRITICAL — volatile capture MUST precede every eradication action listed in this step. Before isolating the host: acquire full RAM image (WinPmem/DumpIt) and run Get-NetTCPConnection | Where-Object {$_.State -eq 'Established'} to document active connections including any C2 beaconing or cloud exfiltration sessions to Proton infrastructure. Before terminating encryption processes: capture the full process tree (Get-CimInstance Win32_Process | Select ProcessId, ParentProcessId, Name, CommandLine) and note the PID, parent PID, and command line of the ransomware process spawned from the video-extension lure file. Before removing files: hash all artifacts with certutil and copy them to a forensic hold location. Before credential rotation: export Windows Security Event Log Event ID 4624 (Successful Logon) and 4648 (Explicit Credential Use) from the compromised host covering the period from suspected execution through isolation, to identify all accounts used during the attack window.

Step 4: Recovery — Restore encrypted files from verified, offline or immutable backups. Confirm backup integrity before restoration. Validate that no ransomware persistence mechanisms (scheduled tasks, startup entries) remain using system initialization configuration analysis (D3-SICA: System Init Config Analysis).

Monitor restored systems for re-infection indicators for a minimum of 72 hours post-restoration. Reintroduce systems to the network only after clean validation.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: CIS 4.6 (Securely Manage Enterprise Assets and Software), CIS 11.3 (Protect Recovery Data)

Compensating: Verify backup integrity before restoration using hash comparison: on Windows, certutil -hashfile SHA256 matched against the hash recorded at backup creation time. Enumerate all persistence mechanisms using Autoruns (Sysinternals) — run autorunsc.exe -a * -c > autoruns_output.csv and review for any entries with non-standard publishers, unsigned binaries, or paths in %APPDATA%, %TEMP%, or %PUBLIC% consistent with a dropped ransomware payload. Check scheduled tasks via schtasks /query /fo LIST /v and registry run keys at HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run and HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run. Deploy Sysmon post-restoration and monitor for Event ID 1 (Process Create) triggering from paths or hashes matching the original payload for the 72-hour watch window.

Evidence: Before restoring from backup, document the full scope of encrypted files: run Get-ChildItem -Path C:\ -Recurse | Where-Object {$_.Extension -match ''} to enumerate affected files and record the ransomware's appended extension (which identifies the specific ransomware family or variant). Preserve the ransom note files (typically dropped in each encrypted directory) — their filename, contents, and embedded contact/payment addresses are key intelligence for variant identification and law enforcement reporting. Capture a final VSS snapshot state via vssadmin list shadows before restoration to confirm whether shadow copies were deleted by the ransomware (deletion is a known ransomware behavior and confirms payload execution reached that stage). These artifacts must be preserved in forensic hold before restoration overwrites the encrypted file state.

Step 5: Post-Incident — Conduct targeted phishing awareness training focused on authority-impersonation lures (law enforcement, regulatory body) and the risk of password-protected archives from unsolicited email. Review email gateway policies to enforce attachment sandboxing and block password-protected archives from unknown senders. Implement or validate MFA on all externally exposed and administrative accounts (CIS 6.3, CIS 6.4, CIS 6.5; D3-MFA: Multi-factor Authentication). Audit user account permissions to enforce least privilege, limiting blast radius of any future endpoint compromise (NIST AC-6; D3-UAP: User Account Permissions).

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: NIST AC-6 (Least Privilege), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.4 (Require MFA for Remote Network Access), CIS 6.5 (Require MFA for Administrative Access), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: For phishing simulation targeting authority-impersonation lures, use GoPhish (free, open-source) to craft a test campaign mimicking the Interpol lure format — sender display name spoofing a law enforcement body, urgency language, and a Proton Drive link — and measure click-through rates as a baseline before and after training. For email gateway hardening without an enterprise secure email gateway, configure Postfix/SpamAssassin to reject or quarantine password-protected ZIP/RAR/7z attachments from external senders using mime_header_checks rules. For MFA on a small-business budget, enable TOTP-based MFA via free tiers of Duo Security or use Windows Hello for Business for administrative accounts. For least-privilege audit, run Get-ADUser -Filter * -Properties MemberOf | Select Name, MemberOf and compare against a documented need-to-know matrix to identify over-privileged accounts.

Evidence: Post-incident, preserve and archive all collected forensic artifacts from Steps 2-4 into a structured incident record before closing the case: the original phishing .eml file with full headers, the password-protected archive (do not execute — store in an encrypted forensic container), hashes of all malicious files, Sysmon EVTX exports, RAM images, ransom note copies, and proxy/gateway logs showing delivery and download activity. This evidence package supports law enforcement referral (Interpol impersonation is itself a criminal offense in most jurisdictions), insurance claims, and lessons-learned documentation. Retain per your organization's audit record retention policy in alignment with NIST AU-11 (Audit Record Retention).

Detection Guidance

No confirmed IOCs (hashes, IPs, domains, C2 addresses) are available in the provided source material. Detection must rely on behavioral and heuristic indicators. Search email gateway logs for inbound messages referencing Interpol or criminal investigation with links to proton.me or attachments with video-file extensions inside password-protected archives. At the endpoint, alert on execution of files bearing video extensions (.mp4, .avi, .mov, .mkv) that spawn child processes, access registry run keys, or initiate file enumeration and bulk renaming, behavioral patterns consistent with ransomware staging. Enable and review audit logs for mass file modification or extension-change events (NIST AU-2, AU-6; CIS Control 8.2). Monitor for user account activity anomalies following any suspected execution event, including new local accounts, privilege escalation, or access to network shares. Flag Proton Drive download activity from business endpoints where it has no documented use case. Because the archive is password-protected, automated sandbox detonation will not execute the payload; therefore, user education and pre-delivery filtering are the primary preventive controls.

Framework Mappings

MITRE-ATTACK

- **T1566.001** — Spearphishing Attachment
- **T1566.002** — Spearphishing Link
- **T1537** — Transfer Data to Cloud Account
- **T1036** — Masquerading
- **T1486** — Data Encrypted for Impact
- **T1204.002** — Malicious File

NIST-800-53R5

- **AT-2** — Literacy Training and Awareness
- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-8** — Spam Protection
- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **SI-7** — Software, Firmware, and Information Integrity
- **IR-4** — Incident Handling

OWASP-TOP10-2021

- **A08:2021** — Software and Data Integrity Failures

CIS-V8

- **2.5** — Allowlist Authorized Software
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks

NIST-CSF-2

- **RS.MI-01** — Incidents are contained

HIPAA-SECURITY

- **164.308(a)(7)(ii)(A)** — Data Backup Plan
- **164.308(a)(5)(i)** — Security Awareness and Training

ISO-27001-2022

- **A.5.29** — Information security during disruption
- **A.5.34** — Privacy and protection of personal information
- **A.5.23** — Information security for use of cloud services

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1566.001	Spearphishing Attachment	Initial-Access
T1566.002	Spearphishing Link	Initial-Access
T1537	Transfer Data to Cloud Account	Exfiltration
T1036	Masquerading	Defense-Evasion
T1486	Data Encrypted for Impact	Impact
T1204.002	Malicious File	Execution

Sources

Source	URL	Tier
Cyber Guidance for Small Businesses - CISA	https://www.cisa.gov/cyber-guidance-small-businesses	T1
Vulnerability Assessment for SMBs: Complete Guide to ... - SensCy	https://senscy.com/vulnerability-assessment-for-small-businesses-co...	T3
Study: Small Businesses Underestimate Cyber Risk Reality - Coalition	https://www.coalitioninc.com/blog/security-labs/small-business-cybe...	T3
Small and Medium Businesses Under Siege - Halcyon	https://www.halcyon.ai/resources/whitepapers/small-and-medium-busin...	T3

Source	URL	Tier
Three Ways Businesses are Vulnerable to Security Attacks	https://stratixsystems.com/three-ways-businesses-are-vulnerable-to-...	T3

Generated 2026-07-07 15:05 UTC by TJS Security Command Center