INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-05 08:18 UTC

Silver Fox APT Deploys Undocumented ABCDoor Backdoor in Tax-Themed Spear-Phishing Campaign Targeting India and Russia

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0268
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Organizations across multiple sectors in India and Russia; no specific software products identified as exploited
Published	2026-05-04T10:39:26
Discovery Source	Rss

Executive Summary

Silver Fox, a China-linked espionage group, ran a coordinated spear-phishing campaign using tax-themed lures to compromise organizations across multiple sectors in India and Russia. The campaign delivered two malware payloads, including ABCDoor, a previously undocumented backdoor with no existing signatures in major endpoint security engines. The primary risk is prolonged undetected access to sensitive organizational data, consistent with strategic intelligence collection objectives.

Technical Analysis

Silver Fox APT (tracked by Palo Alto Unit 42 as CL-UNK-1068) delivered two malware payloads via spear-phishing: ABCDoor, an undocumented backdoor not currently catalogued in major malware signature databases, and ValleyRAT, a known remote access trojan previously associated with this group. Initial access was achieved through spear-phishing with malicious attachments (T1566.001) and links (T1566.002), requiring user execution (T1204.002). Post-compromise activity includes command-and-control over HTTP/S (T1071.001), remote tool ingestion (T1105), defense evasion via obfuscation (T1027), and persistence via service creation (T1543) and registry run keys (T1547). No CVE is associated; applicable CWEs are CWE-494 (Download of Code Without Integrity Check) and CWE-506 (Embedded Malicious Code). ABCDoor-specific signatures are not published in open-source malware repositories as of the campaign date. No patch exists; this is a malware campaign, not a software vulnerability. Detection gap risk is elevated for organizations relying on signature-based controls alone. Source quality is moderate; primary sourcing relies on vendor threat blog

reporting (Unit 42, Cyble) and security news outlets. Direct law enforcement or CISA confirmation is not available.

Action Checklist

1. Containment: Block known ValleyRAT indicators and any identified ABCDoor network callbacks at perimeter and endpoint controls. Isolate any endpoints showing sustained outbound HTTPS connections to newly registered domains (WHOIS age < 30 days) or low-reputation IP addresses with regular connection patterns consistent with C2 beaconing. Restrict inbound email delivery of archive and executable attachment types if not already enforced.
2. Detection: Hunt for ValleyRAT IOCs using Unit 42 published indicators from the CL-UNK-1068 report. Search EDR telemetry for unsigned process creation from user-writable directories, abnormal child processes spawned by email clients, and outbound HTTP/S connections to newly registered or low-reputation domains. Review SIEM for T1547 (registry run key modifications) and T1543 (new service creation) events on endpoints that received tax-themed emails.
3. Eradication: Remove any confirmed malware artifacts identified during the hunt. Revoke and reissue credentials for accounts on compromised endpoints. Audit and remove any unauthorized persistence mechanisms (scheduled tasks, run keys, new services) discovered during investigation.
4. Recovery: Reimage confirmed compromised endpoints before returning them to production. Validate no lateral movement occurred by reviewing authentication logs for unusual access patterns originating from affected systems. Monitor previously infected endpoints and associated accounts for 30 days post-remediation.
5. Post-Incident: Assess coverage gaps for behavioral detection of undocumented malware families; signature-only endpoint controls provide insufficient coverage here. Review email gateway configuration for attachment sandboxing and link detonation. Map current detection rules to T1566.001, T1566.002, T1204.002, T1105, T1027, T1543, and T1547 to identify rule gaps. If targeting aligns with your sector or geography, evaluate threat intelligence feed coverage for Silver Fox / CL-UNK-1068 activity.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate to senior IR leadership and legal/compliance immediately if forensic evidence indicates ABCDoor achieved persistent access for more than 72 hours, if data staging or exfiltration artifacts are identified (consistent with Silver Fox intelligence-collection objectives), or if compromised accounts held access to PII, export-controlled data, or regulated information requiring breach notification under applicable law (e.g., India DPDP Act, applicable sector regulations).

Recovery Notes	All confirmed ABCDoor- or ValleyRAT-infected endpoints must be reimaged from a known-good baseline rather than cleaned in place, as ABCDoor is undocumented and its full persistence mechanism cannot be verified as fully removed without a clean image. Post-reimage, enforce 30-day enhanced monitoring of reconstituted endpoints and all associated user accounts using Sysmon EventID 1/3/11/13 collection, focusing specifically on process creation from user-writable paths and outbound HTTP/S to low-reputation domains that match Silver Fox C2 infrastructure patterns. Given Silver Fox's strategic intelligence-collection mandate, validate that no sensitive documents, credentials, or internal network maps were accessed or staged for exfiltration during the dwell period by reviewing file access audit logs (Windows Security Event ID 4663) on file servers and SharePoint/OneDrive access logs for accounts present on compromised systems.
Forensic Artifacts	Sysmon Event ID 1 (ProcessCreate) logs filtered for processes executing from %APPDATA%, %TEMP%, %PUBLIC%, or %PROGRAMDATA% with unsigned or low-prevalence binaries — consistent with ABCDoor and ValleyRAT staging behavior observed in Silver Fox campaigns | Email server delivery logs (Exchange Message Tracking or Postfix mail.log) filtered on tax-themed subject lines and inbound archive/executable attachments mapping to the 1,600+ Silver Fox lure distribution events, to establish full organizational targeting scope | Windows Registry export of HKCU\Software\Microsoft\Windows\CurrentVersion\Run and HKLM\SYSTEM\CurrentControlSet\Services capturing T1547 run key and T1543 service persistence artifacts installed by ValleyRAT or ABCDoor on compromised endpoints | Sysmon Event ID 3 (NetworkConnect) and host-based firewall logs documenting outbound HTTP/S connections from endpoint processes to newly registered or low-reputation domains, preserving ABCDoor C2 callback infrastructure for IOC development and potential attribution corroboration with Unit 42 CL-UNK-1068 indicators | Full memory acquisition (WinPmem/DumpIt) from live suspected-infected endpoints capturing ABCDoor in-memory execution artifacts — critical because ABCDoor is undocumented with no existing signatures, making memory forensics the primary mechanism for behavioral analysis and YARA rule development

Per-Action IR Details

Containment — Block known ValleyRAT indicators and any identified ABCDoor network callbacks at perimeter and endpoint controls. Isolate any endpoints flagged with anomalous outbound HTTP/S connections to unrecognized infrastructure. Restrict inbound email delivery of archive and executable attachment types if not already enforced.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST SC-7 (Boundary Protection), NIST SI-3 (Malicious Code Protection), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Without enterprise EDR, deploy Sysmon with a network-connection logging config (SwiftOnSecurity baseline) and parse Event ID 3 (NetworkConnect) for outbound connections to domains registered within the last 90 days. Use Windows Firewall with `netsh advfirewall firewall add rule` to block specific ValleyRAT C2 IPs published in Unit 42 CL-UNK-1068 report. At the mail gateway or MX level, configure a transport rule (Exchange) or milter rule (Postfix) to quarantine inbound ZIP, RAR, ISO, and EXE attachments pending manual review. Use Wireshark or tcpdump on a network tap/span port to capture and review outbound HTTP/S sessions to flag ABCDoor-style low-volume beaconing patterns.

Evidence: Before isolating endpoints, capture full memory with WinPmem or DumpIt to preserve ABCDoor in-memory artifacts (it may not persist fully to disk pre-detonation). Preserve a forensic image of browser and email client cache

directories (e.g., `%APPDATA%\Microsoft\Outlook`, `%LOCALAPPDATA%\Temp`) to recover the original tax-themed spear-phishing lure attachment. Collect Sysmon Event ID 3 (NetworkConnect) and Windows Firewall logs (`%SystemRoot%\System32\LogFiles\Firewall\pfirewall.log`) from all candidate endpoints to document ABCDoor or ValleyRAT C2 callback attempts before network-level blocking destroys active session evidence. Snapshot DNS resolver cache (`ipconfig /displaydns`) on flagged endpoints before network isolation clears it.

Detection — Hunt for ValleyRAT IOCs using Unit 42 published indicators from the CL-UNK-1068 report. Search EDR telemetry for unsigned process creation from user-writable directories, abnormal child processes spawned by email clients, and outbound HTTP/S connections to newly registered or low-reputation domains. Review SIEM for T1547 (registry run key modifications) and T1543 (new service creation) events on endpoints that received tax-themed emails.

NIST Phase: Detection Analysis

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

Controls: NIST IR-5 (Incident Monitoring), NIST SI-4 (System Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-12 (Audit Record Generation), CIS 8.2 (Collect Audit Logs), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Without SIEM/EDR, use Sysmon Event ID 1 (ProcessCreate) filtered for processes whose image path resolves to `%APPDATA%`, `%TEMP%`, `%PUBLIC%`, or other user-writable directories — these are consistent with ABCDoor staging behavior. Query Windows Security Event Log for Event ID 4688 (Process Creation) filtering on OUTLOOK.EXE, WINWORD.EXE, or EXCEL.EXE as parent processes spawning cmd.exe, powershell.exe, mshta.exe, or wscript.exe. For T1547, query registry key `HKCU\Software\Microsoft\Windows\CurrentVersion\Run` and `HKLM\Software\Microsoft\Windows\CurrentVersion\Run` manually or via PowerShell: `Get-ItemProperty -Path 'HKLM:\Software\Microsoft\Windows\CurrentVersion\Run'`. For T1543, run `sc query type= all state= all` or check Event ID 7045 (New Service Installed) in the System Event Log. Use YARA rules derived from ValleyRAT string signatures (available from Unit 42 CL-UNK-1068 disclosure) against `%APPDATA%`, `%TEMP%`, and `C:\Users` recursively via `yara64.exe -r rule.yar C:\Users`.

Evidence: Collect Sysmon Event ID 1, 3, 7 (ImageLoad), 11 (FileCreate), and 13 (RegistryValueSet) from endpoints that received tax-themed emails per mail server delivery logs. Preserve Windows Security Event Log entries for Event ID 4688 and 4624/4625 (logon events) around the time window of identified phishing delivery. Export mail server logs (Exchange Message Tracking Log or Postfix mail.log) filtered on the 1,600+ tax-themed lure subject patterns identified in Unit 42 reporting to map the full delivery scope. Capture `%APPDATA%\Roaming` and `%LOCALAPPDATA%\Temp` directory listings with timestamps to identify ABCDoor staging artifacts (DLL side-loading components or dropper executables consistent with Silver Fox TTPs). Document process tree snapshots from any live suspected-infected systems using Sysinternals Process Explorer before remediation destroys runtime evidence.

Eradication — Remove any confirmed malware artifacts identified during the hunt. Revoke and reissue credentials for accounts on compromised endpoints. Audit and remove any unauthorized persistence mechanisms (scheduled tasks, run keys, new services) discovered during investigation.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST IR-4 (Incident Handling), NIST SI-2 (Flaw Remediation), NIST SI-7 (Software, Firmware, and Information Integrity), NIST IA-5 (Authenticator Management), CIS 5.3 (Disable Dormant Accounts), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts)

Compensating: Without enterprise credential management tooling, force password resets via Active Directory PowerShell: `Set-ADAccountPassword -Identity -Reset -NewPassword (ConvertTo-SecureString -AsPlainText '' -Force)` followed by `Set-ADUser -Identity -ChangePasswordAtLogon $true`. Enumerate and remove ABCDoor/ValleyRAT scheduled tasks with `schtasks /query /fo LIST /v | findstr /i 'task\|status\|run'` and delete suspicious entries via `schtasks /delete /tn '' /f`. Remove unauthorized run key entries with `reg delete 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run' /v '' /f`. For new services installed by T1543, disable and delete via `sc stop && sc delete `. Validate file removal completeness by re-running the same YARA ruleset used in detection against cleaned endpoints before returning to production.

Evidence: Before removing artifacts, preserve SHA-256 hashes of all identified ABCDoor and ValleyRAT binaries using `certutil -hashfile SHA256` and store copies in a quarantine share for submission to threat intelligence feeds and AV vendors (ABCDoor is undocumented — vendor submissions will improve industry coverage). Capture full registry export of `HKCU\Software\Microsoft\Windows\CurrentVersion\Run`, `HKLM\Software\Microsoft\Windows\CurrentVersion\Run`, and `HKLM\SYSTEM\CurrentControlSet\Services` before deletion to document Silver Fox persistence mechanisms. Export scheduled task XML definitions from `C:\Windows\System32\Tasks` for any suspicious tasks before removal. Document all credential-bearing accounts present on compromised endpoints (via `net user` and AD query) to establish the full scope of credential exposure before revocation.

Recovery — Reimage confirmed compromised endpoints before returning them to production. Validate no lateral movement occurred by reviewing authentication logs for unusual access patterns originating from affected systems. Monitor previously infected endpoints and associated accounts for 30 days post-remediation.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST CP-10 (System Recovery and Reconstitution), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-11 (Audit Record Retention), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 6.2 (Establish an Access Revoking Process)

Compensating: Without enterprise imaging infrastructure, use a validated, centrally stored WIM image deployed via Windows Deployment Services or a bootable USB with a known-good OS image; verify image integrity via SHA-256 before deployment. For lateral movement validation without SIEM, query Windows Security Event Log (Event ID 4624 — successful logon, logon type 3 for network) on domain controllers and file servers, filtering on source IP addresses of the reimaged endpoints for the 30-day post-incident window. Deploy osquery on recovered endpoints using the `process_open_sockets` and `logged_in_users` tables to detect anomalous re-infection or residual Silver Fox activity: `SELECT pid, local_address, remote_address, remote_port FROM process_open_sockets WHERE remote_port IN (80, 443) AND remote_address NOT IN ('');`

Evidence: Before reimaging, acquire a final full forensic disk image (e.g., using FTK Imager or `dd`) and memory capture to preserve evidence of ABCDoor's full execution chain, including any data staged for exfiltration consistent with Silver Fox intelligence-collection objectives. Collect Windows Security Event Log entries for Event IDs 4624, 4625, 4648 (explicit credential use), 4768/4769 (Kerberos ticket requests), and 4776 (NTLM authentication) from domain controllers, filtered on the compromised endpoint hostnames and associated user accounts, covering the full suspected dwell time. Preserve NetFlow or proxy logs showing all outbound connections from affected endpoints during the compromise window to identify any data exfiltration to Silver Fox infrastructure before recovery closes the observation window.

Post-Incident — Assess coverage gaps for behavioral detection of undocumented malware families; signature-only endpoint controls provide insufficient coverage here. Review email gateway configuration for attachment sandboxing and link detonation. Map current detection rules to T1566.001, T1566.002, T1204.002, T1105, T1027, T1543, and T1547 to identify rule gaps. If targeting aligns with your sector or geography, evaluate threat intelligence feed coverage for Silver Fox / CL-UNK-1068 activity.

NIST Phase: Post Incident

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

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST SI-5 (Security Alerts, Advisories, and Directives), NIST SI-4 (System Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 8.2 (Collect Audit Logs)

Compensating: Without commercial TI feeds, subscribe to free OSINT sources covering Silver Fox / CL-UNK-1068: MITRE ATT&CK Group G1030 (if mapped), Unit 42 public blog indicators, and CISA Known Exploited Vulnerabilities catalog. Develop Sigma rules for the specific ATT&CK techniques in this campaign (T1566.001, T1204.002, T1547.001, T1543.003) and deploy against Windows Event Log via Chainsaw (`chainsaw hunt --sigma rules/

--directory C:\EventLogs`). For email gateway gap assessment without commercial sandboxing, configure open-source ClamAV with updated signatures plus a VirusTotal API integration (free tier, 500 req/day) for automated attachment hash lookups on inbound mail. For behavioral detection of undocumented malware like ABCDoor, author YARA rules targeting behavioral strings or PE characteristics identified during eradication and load them into periodic scans via scheduled task.

Evidence: Compile the full incident timeline including first phishing delivery timestamp (from mail server logs), first execution evidence (Sysmon Event ID 1), first C2 callback (Sysmon Event ID 3 / firewall logs), and estimated dwell time to assess whether Silver Fox achieved its intelligence-collection objectives. Document all MITRE ATT&CK technique gaps — specifically where no detection rule existed for T1566.001 (spear-phishing with attachment), T1105 (ingress tool transfer for ABCDoor staging), and T1027 (obfuscated files) — as these gaps directly enabled ABCDoor's undetected deployment. Retain all forensic artifacts, IOCs, and YARA rules developed during this incident for submission to an ISAC relevant to your sector (e.g., FS-ISAC, H-ISAC, E-ISAC) to support cross-sector defense against Silver Fox targeting of India- and Russia-operating organizations.

Detection Guidance

Detection is primarily behavioral, given ABCDoor's undocumented status and lack of published signatures. Key indicators: (1) Email gateway: filter for tax-themed lures referencing Indian or Russian regulatory bodies, with archive attachments or links to file-sharing infrastructure. (2) EDR: alert on unsigned executables launched from %TEMP%, %APPDATA%, or download directories; process injection from Office or PDF reader processes; new service registration or run key creation within minutes of email attachment open events. (3) Network: monitor for HTTP/S C2 beaconing patterns (regular interval outbound connections to newly registered or low-reputation domains); DNS queries for domains registered within 30 days. (4) SIEM: correlate T1547 registry writes and T1543 service creation events with preceding T1566/T1204 email execution events on the same host. For ValleyRAT specifically, reference published Unit 42 IOCs from the CL-UNK-1068 research. ABCDoor-specific network indicators have not been published by vendors as of the campaign date; organizations should request ABCDoor IOCs directly from Unit 42 if available under responsible disclosure, or rely on behavioral detection. MITRE ATT&CK techniques to prioritize in detection rule review: T1566.001, T1566.002, T1204.002, T1071.001, T1105, T1027, T1547, T1543.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`See Unit 42 CL-UNK-1068 report`	ValleyRAT and related Silver Fox C2 infrastructure; ABCDoor-specific IOCs not yet fully documented in open sources	MEDIUM

Framework Mappings

MITRE-ATTACK

- **T1566.002** — Spearphishing Link
- **T1059** — Command and Scripting Interpreter
- **T1071.001** — Web Protocols
- **T1071** — Application Layer Protocol

- **T1204.002** — Malicious File
- **T1105** — Ingress Tool Transfer
- **T1027** — Obfuscated Files or Information
- **T1547** — Boot or Logon Autostart Execution
- **T1566.001** — Spearphishing Attachment
- **T1543** — Create or Modify System Process

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
- **CM-7** — Least Functionality
- **SI-7** — Software, Firmware, and Information Integrity
- **CA-7** — Continuous Monitoring
- **CM-3** — Configuration Change Control

OWASP-TOP10-2021

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

CIS-V8

- **2.5** — Allowlist Authorized Software
- **2.6** — Allowlist Authorized Libraries
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks
- **8.2** — Collect Audit Logs

HIPAA-SECURITY

- **164.308(a)(5)(i)** — Security Awareness and Training

ISO-27001-2022

- **A.5.34** — Privacy and protection of personal information

NIST-CSF-2

- **DE.CM-01** — Networks and network services are monitored

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1566.002	Spearphishing Link	Initial-Access
T1059	Command and Scripting Interpreter	Execution

Technique ID	Technique Name	Tactic
T1071.001	Web Protocols	Command-And-Control
T1071	Application Layer Protocol	Command-And-Control
T1204.002	Malicious File	Execution
T1105	Ingress Tool Transfer	Command-And-Control
T1027	Obfuscated Files or Information	Defense-Evasion
T1547	Boot or Logon Autostart Execution	Persistence
T1566.001	Spearphishing Attachment	Initial-Access
T1543	Create or Modify System Process	Persistence

Sources

Source	URL	Tier
Security News	https://www.darkreading.com/endpoint-security/silver-fox-tax-themed...	T3
An Investigation Into Years of Undetected Operations Targeting High ...	https://unit42.paloaltonetworks.com/cl-unk-1068-targets-critical-se...	T3
Cyber-espionage campaign breaches 37 countries, including India	https://www.linkedin.com/posts/vikaslohchab_india-trade-security-ac...	T3
Inside Russia Credential-Based Intrusions & Cyber Risks - Cyble	https://cyble.com/blog/russia-credential-based-intrusions-cisos/	T3
Cyble warns hacktivists shift tactics, targeting critical infrastructure ...	https://industrialcyber.co/industrial-cyber-attacks/cyble-warns-hac...	T3

Generated 2026-05-05 08:18 UTC by TJS Security Command Center