INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-22 06:44 UTC

Lotus Wiper Targets Venezuelan Energy Infrastructure in Geopolitically Timed Destructive Campaign

THREAT CAMPAIGN | **CRITICAL** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0196
Type	Threat Campaign
Severity	CRITICAL
CVSS Base Score	7.5
Affected Products	Windows systems in Venezuelan energy and utilities sector; abuses Windows System Restore API, diskpart, robocopy, fsutil, UI0Detect service; PDVSA referenced as adjacent incident
Published	2026-04-21T14:38:40
Discovery Source	Rss

Executive Summary

A previously undocumented destructive malware called Lotus was deployed against Venezuelan energy and utility organizations in late 2025, overwriting physical drives and eliminating all Windows recovery paths to render systems permanently unrecoverable. The campaign coincides with a separate December 2025 cyberattack on state oil company PDVSA, though no confirmed technical link between the two incidents exists. For organizations operating critical infrastructure in politically volatile regions, this campaign signals an active, sophisticated threat prioritizing destruction over espionage, with near-zero recovery options once deployed.

Technical Analysis

Lotus is a multi-stage destructive wiper targeting Windows systems in Venezuela's energy and utilities sector. Its execution chain abuses native Windows utilities: diskpart for physical drive overwriting, robocopy and fsutil for file and volume operations, and the UI0Detect service as part of its deployment mechanism. The malware systematically eliminates all standard recovery paths by deleting Volume Shadow Copies (VSS), removing System Restore points, and disabling network access to block remote remediation or backup retrieval. No CVE identifier is associated with this campaign; exploitation relies on living-off-the-land (LotL) techniques rather than a specific software vulnerability. The primary CWE classification is CWE-693 (Protection Mechanism Failure), reflecting the malware's strategy of disabling defensive and recovery controls before executing destructive

payloads. MITRE ATT&CK techniques observed include T1561.001 (Disk Content Wipe), T1490 (Inhibit System Recovery), T1485 (Data Destruction), T1489 (Service Stop), T1531 (Account Access Removal), T1059.003 (Windows Command Shell), T1070.004 (File Deletion), T1021.002 (SMB/Windows Admin Shares), T1562.001 (Disable or Modify Tools), and T1036.003 (Rename System Utilities). Attribution remains unconfirmed. The PDVSA cyberattack of December 2025 is a temporally adjacent incident with no established technical overlap. Source: BleepingComputer (T3), Reuters (T2), The Record (T3), Dark Reading (T3).

Action Checklist

1. Step 1: Containment, Isolate Windows endpoints in energy, utilities, and OT-adjacent environments from lateral movement paths immediately. Disable SMB shares (T1021.002) and restrict Windows Admin Share access. Block outbound connections from operational systems that have no business requirement for external network access. If Lotus artifacts are suspected, take the system offline before attempting any analysis.
2. Step 2: Detection, Query Windows Event Logs for diskpart execution (Event ID 4688, process name diskpart.exe), vssadmin delete shadows commands, fsutil usn deletejournal calls, and UI0Detect service state changes. Alert on robocopy executing at unusual hours or from non-standard parent processes. Review PowerShell and cmd.exe logs for chained execution of multiple LotL utilities within short time windows. No confirmed Lotus-specific file hashes or network IOCs are publicly available at this time.
3. Step 3: Eradication, Lotus exploits no CVE and requires no patching; eradication requires full reimaging of affected systems from known-good, offline backups predating any suspected compromise window. Do not attempt in-place recovery on wiped systems. Remove UI0Detect service modifications and audit service configurations across the environment. Harden diskpart, fsutil, and robocopy execution via Windows Defender Application Control (WDAC) or AppLocker policies restricting their use to authorized administrative accounts only.
4. Step 4: Recovery, Restore from immutable, offline backups only. Validate backup integrity before restoration; confirm backups predate the suspected intrusion window. After restoration, verify VSS and System Restore are functional, network segmentation is intact, and no persistence mechanisms remain. Monitor restored systems for recurrence of LotL tool execution patterns for a minimum of 30 days post-recovery.
5. Step 5: Post-Incident, Audit VSS and backup configurations across all critical infrastructure systems; ensure at least one backup copy is air-gapped or immutable and inaccessible from production networks. Review and enforce least-privilege controls on accounts with access to diskpart, vssadmin, and fsutil. Develop or update destructive malware response playbooks covering wiper-class threats. Map control gaps to NIST SP 800-53 controls CP-9 (Information System Backup), CP-10 (Information System Recovery), and SI-3 (Malicious Code Protection).

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate to senior IR leadership, legal, and executive stakeholders immediately if Lotus artifacts or LotL tool chain execution is confirmed on any OT-adjacent or SCADA-connected Windows system, if PDVSA-linked infrastructure or shared network segments are identified in scope, or if backup validation reveals all recovery paths have been eliminated — indicating the organization faces permanent data loss without offline restore capability.
Recovery Notes	Recovery from Lotus is binary — systems where physical drive overwrite completed cannot be recovered in place and must be fully reimaged from offline backups that demonstrably predate the intrusion window; any backup accessible from the production network during the attack window must be treated as potentially compromised and integrity-verified before use. Post-restoration, monitor all recovered systems for a minimum of 30 days using Sysmon Event ID 1 alerts on diskpart.exe, vssadmin.exe, fsutil.exe, and robocopy.exe execution chains, as Lotus-class campaigns in geopolitically volatile regions frequently involve staged redeployment after initial triage closes. Verify that VSS, System Restore, and Windows Recovery Environment (WinRE) are fully functional on all restored systems before returning them to production, and confirm at least one backup copy for each restored system has been moved to an air-gapped or immutable store before the 30-day monitoring window closes.
Forensic Artifacts	Windows Security Event Log (Event ID 4688 with command-line auditing enabled): primary source for confirming Lotus LotL execution chain — filter for diskpart.exe, vssadmin.exe with 'delete shadows', fsutil.exe with 'usn deletejournal', and robocopy.exe with non-standard parent processes, all within compressed time windows indicative of scripted wiper orchestration | $MFT and $UsnJrnl (C:\$Extend\$UsnJrnl:$J): the absence or truncation of the USN journal is itself a Lotus indicator — fsutil usn deletejournal removes this artifact; extract $MFT using MFTECmd or Velociraptor before any further disk operations to capture file creation/modification timestamps from the wiper deployment window | Windows Prefetch files (C:\Windows\Prefetch\): DISKPART.EXE-*.pf, ROBOCOPY.EXE-*.pf, FSUTIL.EXE-*.pf, and VSSADMIN.EXE-*.pf establish first and last execution timestamps for Lotus LotL tools even when event logs have been cleared; parse with PECmd (Eric Zimmerman) to extract run counts and timestamps | SYSTEM registry hive (HKLM\SYSTEM\CurrentControlSet\Services\UI0Detect): Lotus modifies the UI0Detect service to interact with the desktop session during wiper execution — the service configuration key will show anomalous start type, binary path, or account changes compared to the Windows default; export and diff against a known-good baseline from an unaffected system of the same OS version | Physical disk raw image (MBR and VBR sectors via dd or FTK Imager): Lotus overwrites physical drive structures — the overwrite pattern in the MBR/VBR sectors (first 512 bytes of PhysicalDrive0 and volume boot records) is a wiper-class signature that can be compared against known Lotus samples if public research develops confirmed indicators, and documents the extent of physical overwrite for insurance and regulatory reporting purposes

Per-Action IR Details

Step 1: Containment — Isolate Windows endpoints in energy, utilities, and OT-adjacent environments from lateral movement paths immediately. Disable SMB shares (T1021.002) and restrict Windows Admin Share access. Block outbound connections from operational systems that have no business requirement for external network access. If Lotus artifacts are suspected, take the system offline before attempting any analysis.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST SC-7 (Boundary Protection), NIST AC-3 (Access Enforcement), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices)

Compensating: On each suspected host, run: 'netsh advfirewall set allprofiles state on' and 'netsh advfirewall firewall add rule name=BlockSMB dir=out protocol=TCP localport=445 action=block'. Disable Admin Shares via registry: 'reg add HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters /v AutoShareWks /t REG_DWORD /d 0 /f'. For OT-adjacent network isolation, use managed switch VLAN reassignment to quarantine segments without requiring host-level access on potentially wiped systems. If the system is already exhibiting wiper behavior (disk I/O spike, recovery service failures), pull the network cable — do not rely on software-based isolation on a host under active destructive attack.

Evidence: Before isolating, capture: (1) running process list via 'tasklist /v /fo csv > C:\evidence\proc_$(Get-Date -f yyyyMMddHHmm).csv' — specifically look for diskpart.exe, robocopy.exe, fsutil.exe, or cmd.exe/powershell.exe with anomalous parent PIDs; (2) active network connections via 'netstat -ano > C:\evidence\netstat_$(Get-Date -f yyyyMMddHHmm).txt' to identify C2 or lateral movement staging connections before isolation severs them; (3) Windows Security Event Log filtered for Event ID 4648 (explicit credential logon) and Event ID 4624 Type 3 (network logon) to identify accounts used for SMB-based lateral movement into this host; (4) VSS snapshot enumeration via 'vssadmin list shadows' — Lotus destroys these, so documenting their absence or partial deletion state establishes the attack timeline.

Step 2: Detection — Query Windows Event Logs for diskpart execution (Event ID 4688, process name diskpart.exe), vssadmin delete shadows commands, fsutil usn deletejournal calls, and UI0Detect service state changes. Alert on robocopy executing at unusual hours or from non-standard parent processes. Review PowerShell and cmd.exe logs for chained execution of multiple LotL utilities within short time windows. No confirmed Lotus-specific file hashes or network IOCs are publicly available at this time.

NIST Phase: Detection Analysis

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

Controls: NIST SI-4 (System Monitoring), NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-12 (Audit Record Generation), CIS 8.2 (Collect Audit Logs)

Compensating: Deploy Sysmon with SwiftOnSecurity or Olaf Hartong's modular config to capture Event ID 1 (Process Create) with full command-line logging — this will catch diskpart.exe, fsutil.exe with 'usn deletejournal', and robocopy chains that Windows native 4688 logging may miss without enhanced auditing. Write a Sigma rule targeting: parent_image not in ('explorer.exe','mmc.exe','services.exe') AND image endswith ('\diskpart.exe' OR '\fsutil.exe' OR '\vssadmin.exe') within a 300-second sliding window across the same host. Use 'wevtutil qe Security /q:"*[System[(EventID=4688)]]" /f:text /rd:true' locally on each host if no central log collector exists. For UI0Detect detection: 'sc query UI0Detect' and compare against baseline — Lotus modifies this service to interact with the desktop session during wiper execution.

Evidence: Capture before any remediation action: (1) Windows Security Event Log (Event ID 4688 with process creation auditing enabled) filtered for diskpart.exe, vssadmin.exe, fsutil.exe, robocopy.exe — export via 'wevtutil epl Security C:\evidence\security.evtx'; (2) PowerShell Operational Log (Microsoft-Windows-PowerShell/Operational, Event ID 4103/4104) for script block logging of cmdlets chaining these LotL utilities; (3) System Event Log for Service Control Manager Event ID 7045 (new service installed) and 7036 (service state change) tied to UI0Detect modifications; (4) $MFT and $UsnJrnl — if fsutil usn deletejournal was executed, the journal will be absent or truncated, which is itself forensic evidence; extract $MFT using a tool like MFTECmd before further disk operations; (5) Prefetch files at C:\Windows\Prefetch\ for DISKPART.EXE-*.pf, ROBOCOPY.EXE-*.pf, FSUTIL.EXE-*.pf — these survive in memory even if the disk has begun to be overwritten and establish execution timestamps.

Step 3: Eradication — No patch applies; Lotus exploits no CVE. Eradication requires full reimaging of affected systems from known-good, offline backups predating any suspected compromise window. Do not attempt in-place recovery on wiped systems. Remove UI0Detect service modifications and audit service configurations across the environment. Harden diskpart, fsutil, and robocopy execution via Windows Defender Application Control (WDAC) or AppLocker policies restricting their use to authorized administrative accounts only.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST IR-4 (Incident Handling), NIST SI-2 (Flaw Remediation), NIST SI-3 (Malicious Code Protection), NIST CM-7 (Least Functionality), CIS 2.3 (Address Unauthorized Software), CIS 4.6 (Securely Manage Enterprise Assets and Software)

Compensating: Since Lotus is wiper-class with no patch, eradication IS reimaging — there is no partial remediation path. For teams without enterprise deployment tools, use a hardened WinPE USB to boot affected systems and validate drive state before reimaging. To harden LotL utility access without WDAC licensing: use AppLocker (available on Windows 10/11 Enterprise and Education) with deny rules scoped to diskpart.exe, fsutil.exe, and robocopy.exe for all non-Administrator accounts — deploy via GPO: 'Computer Configuration > Windows Settings > Security Settings > Application Control Policies > AppLocker'. For UI0Detect hardening on unaffected systems: 'sc config UI0Detect start= disabled && sc stop UI0Detect' and document the baseline state via 'sc qc UI0Detect > C:\evidence\ui0detect_baseline.txt'. Audit all services with SYSTEM-level privileges using Autoruns (Sysinternals) before reimaging adjacent systems.

Evidence: Before wiping and reimaging affected systems, capture forensic images using a write-blocker: (1) Full physical disk image (dd or FTK Imager) even if the drive appears overwritten — partial forensic recovery may be possible from sectors Lotus did not reach, and the overwrite pattern itself is intelligence for attribution; (2) Windows Registry hive exports (SYSTEM, SOFTWARE, SECURITY, SAM) from C:\Windows\System32\config\ — the SYSTEM hive will contain UI0Detect service configuration modifications; (3) Service registry key: 'HKLM\SYSTEM\CurrentControlSet\Services\UI0Detect' — export before reimaging to document Lotus's service manipulation; (4) Event ID 7040 (Service start type changed) and 7045 (Service installed) from System Event Log; (5) Volume boot record and master boot record — Lotus targets physical drive structures, so capture raw MBR/VBR using 'dd if=\\.\PhysicalDrive0 of=C:\evidence\mbr.bin bs=512 count=1' before any write operations.

Step 4: Recovery — Restore from immutable, offline backups only. Validate backup integrity before restoration; confirm backups predate the suspected intrusion window. After restoration, verify VSS and System Restore are functional, network segmentation is intact, and no persistence mechanisms remain. Monitor restored systems for recurrence of LotL tool execution patterns for a minimum of 30 days post-recovery.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST CP-9 (Information System Backup), NIST CP-10 (System Recovery and Reconstitution), NIST IR-4 (Incident Handling), NIST SI-7 (Software, Firmware, and Information Integrity), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 4.4 (Implement and Manage a Firewall on Servers)

Compensating: Validate backup integrity before restoration using hash verification — compute SHA-256 of backup archives offline and compare against recorded values from backup creation time: 'certutil -hashfile SHA256'. Verify VSS functionality post-restoration: 'vssadmin list shadowstorage' should show allocated storage, and 'wmic shadowcopy list brief' should return at least one restore point. For 30-day LotL monitoring without SIEM, deploy Sysmon and configure a scheduled task to run a daily PowerShell query: 'Get-WinEvent -FilterHashtable @{LogName="Security"; Id=4688} | Where-Object {$_.Message -match "diskpart|fsutil|vssadmin|robocopy"} | Export-Csv C:\monitoring\lol_daily_$(Get-Date -f yyyyMMdd).csv'. Verify network segmentation by running 'Test-NetConnection -ComputerName -Port 445' from restored systems — SMB reachability to OT segments should fail if segmentation is intact.

Evidence: Before declaring recovery complete, document: (1) VSS snapshot inventory post-restoration ('vssadmin list shadows') to confirm recovery paths are re-established and functional; (2) Baseline Sysmon Event ID 1 logs from the first 24 hours post-restoration to establish a clean execution baseline for comparison during the 30-day monitoring window; (3) Network flow logs or firewall logs confirming no outbound connections to IP ranges or ASNs observed during the original Lotus intrusion (if any C2 infrastructure was identified); (4) Registry export of 'HKLM\SYSTEM\CurrentControlSet\Services' on restored systems to confirm UI0Detect and other services match known-good baseline; (5) Integrity verification of restored system binaries using 'sfc /scannow' and compare results — any corruption suggests the backup itself predates complete drive overwrite and may require a cleaner restore point.

Step 5: Post-Incident — Audit VSS and backup configurations across all critical infrastructure systems; ensure at least one backup copy is air-gapped or immutable and inaccessible from production networks.

Review and enforce least-privilege controls on accounts with access to diskpart, vssadmin, and fsutil. Develop or update destructive malware response playbooks covering wiper-class threats. Map control gaps to NIST SP 800-53 controls CP-9 (Information System Backup), CP-10 (Information System Recovery), and SI-3 (Malicious Code Protection).

NIST Phase: Post Incident

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

Controls: NIST CP-9 (Information System Backup), NIST CP-10 (System Recovery and Reconstitution), NIST SI-3 (Malicious Code Protection), NIST IR-8 (Incident Response Plan), NIST AU-11 (Audit Record Retention), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts)

Compensating: Audit VSS storage allocation across all critical hosts with: 'vssadmin list shadowstorage' — flag any host where MaxSize is set to 'unbounded' or below 10% of volume size, as Lotus exploits inadequate VSS capacity limits. For least-privilege enforcement on LotL utilities without PAM tooling, create a dedicated restricted-use GPO: deny 'diskpart.exe', 'fsutil.exe', and 'vssadmin.exe' execution via AppLocker for all accounts except a named break-glass admin account, and log all exceptions via Event ID 8004. For wiper-class playbook development, reference the CISA Wiper Malware Guidance (published post-2022 Ukraine incidents) as a structural template — adapt specifically for Lotus's Windows System Restore API abuse and diskpart physical overwrite sequence. Share Lotus behavioral indicators (LotL tool chains, UI0Detect service manipulation, VSS deletion sequence) with sector peers via ISACs relevant to energy and utilities (E-ISAC or equivalent) under TLP:AMBER.

Evidence: Post-incident documentation must include: (1) Lessons-learned report documenting the specific Lotus execution chain — diskpart physical overwrite sequence, vssadmin shadow deletion, fsutil USN journal deletion, and UI0Detect service interaction — as a reference artifact for future wiper detections; (2) Account privilege audit report showing which accounts held rights to execute diskpart, vssadmin, and fsutil, and whether those accounts show anomalous logon activity during the intrusion window (Event ID 4624/4648 correlation); (3) Backup integrity audit results documenting which backup copies predated the intrusion window and which were rendered inaccessible by Lotus's recovery path elimination; (4) Updated threat model documenting Lotus as a geopolitically-timed wiper campaign targeting Venezuelan energy sector Windows infrastructure, with MITRE ATT&CK technique mappings: T1561.002 (Disk Structure Wipe), T1490 (Inhibit System Recovery), T1021.002 (SMB/Windows Admin Shares), T1059.003 (Windows Command Shell); (5) Gap analysis against NIST CP-9 and CP-10 showing backup frequency, air-gap status, and recovery time objectives for each critical system, with remediation owners and target dates assigned.

Detection Guidance

No confirmed public IOCs (file hashes, IPs, domains) for Lotus are available at time of writing. Detection must rely on behavioral indicators. Key signals: (1) diskpart.exe executing from a non-interactive parent process or outside a maintenance window; (2) vssadmin.exe delete shadows /all /quiet executed via script or command shell; (3) fsutil usn deletejournal or fsutil behavior set commands; (4) robocopy executing in bulk file operations from an unusual parent or account context; (5) UI0Detect service being started, modified, or used outside normal system behavior; (6) rapid sequential execution of multiple native Windows utilities (chained LotL pattern) within a single session. SIEM correlation rule: alert on any combination of three or more of diskpart, vssadmin, fsutil, robocopy, and net stop within a 10-minute window on the same host. Windows Event IDs to monitor: 4688 (process creation with command-line logging enabled), 7036 (service state change for UI0Detect), 7040 (service start type change). Endpoint detection platforms should flag shadow copy deletion as a high-confidence wiper precursor. No CISA KEV entry exists for this campaign.

Indicators of Compromise

Type	Value	Context	Confidence
HASH	`Not publicly available`	No confirmed Lotus malware file hashes have been published in available sources at time of writing	LOW
DOMAIN	`Not publicly available`	No confirmed command-and-control domains or network IOCs for Lotus have been published in available sources	LOW

Framework Mappings

MITRE-ATTACK

- **T1531** — Account Access Removal
- **T1561.001** — Disk Content Wipe
- **T1489** — Service Stop
- **T1485** — Data Destruction
- **T1059.003** — Windows Command Shell
- **T1070.004** — File Deletion
- **T1021.002** — SMB/Windows Admin Shares
- **T1490** — Inhibit System Recovery
- **T1562.001** — Disable or Modify Tools
- **T1036.003** — Rename Legitimate Utilities

NIST-800-53R5

- **CM-6** — Configuration Settings
- **SI-4** — System Monitoring
- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution

HIPAA-SECURITY

- **164.308(a)(6)(ii)** — Response and Reporting

SOC2-TSC

- **CC7.4** — Responds to identified security incidents

ISO-27001-2022

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

CIS-V8

- **8.2** — Collect Audit Logs

NIST-CSF-2

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1531	Account Access Removal	Impact
T1561.001	Disk Content Wipe	Impact
T1489	Service Stop	Impact
T1485	Data Destruction	Impact
T1059.003	Windows Command Shell	Execution
T1070.004	File Deletion	Defense-Evasion
T1021.002	SMB/Windows Admin Shares	Lateral-Movement
T1490	Inhibit System Recovery	Impact
T1562.001	Disable or Modify Tools	Defense-Evasion
T1036.003	Rename Legitimate Utilities	Defense-Evasion

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/new-lotus-data-wiper...	T3
Venezuela's PDVSA suffers cyberattack, tankers make u-turns amid ...	https://www.reuters.com/world/americas/venezuelas-pdvsa-says-operat...	T2
Venezuela state oil company blames cyberattack on US after tanker ...	https://therecord.media/venezuela-state-oil-company-blames-cyberatt...	T3
Cyberattack disrupts Venezuelan oil giant PDVSA's operations	https://www.bleepingcomputer.com/news/security/cyberattack-disrupts...	T3
Venezuelan Oil Company Downplays Alleged US Cyberattack	https://www.darkreading.com/cyber-risk/venezuela-oil-company-downpl...	T3

DISCLAIMER

This intelligence report is produced by Tech Jacks Solutions Security Command Center (SCC) for informational purposes only. It does not constitute professional security advice, legal counsel, or an incident response engagement. The information herein is derived from publicly available sources and AI-assisted analysis; while every effort is made to ensure accuracy, Tech Jacks Solutions makes no warranties regarding completeness or timeliness. Organizations should conduct their own validation and consult qualified security professionals before taking action based on this report. Tech Jacks Solutions is not liable for any damages resulting from the use of this information.

Generated 2026-04-22 06:44 UTC by TJS Security Command Center