Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

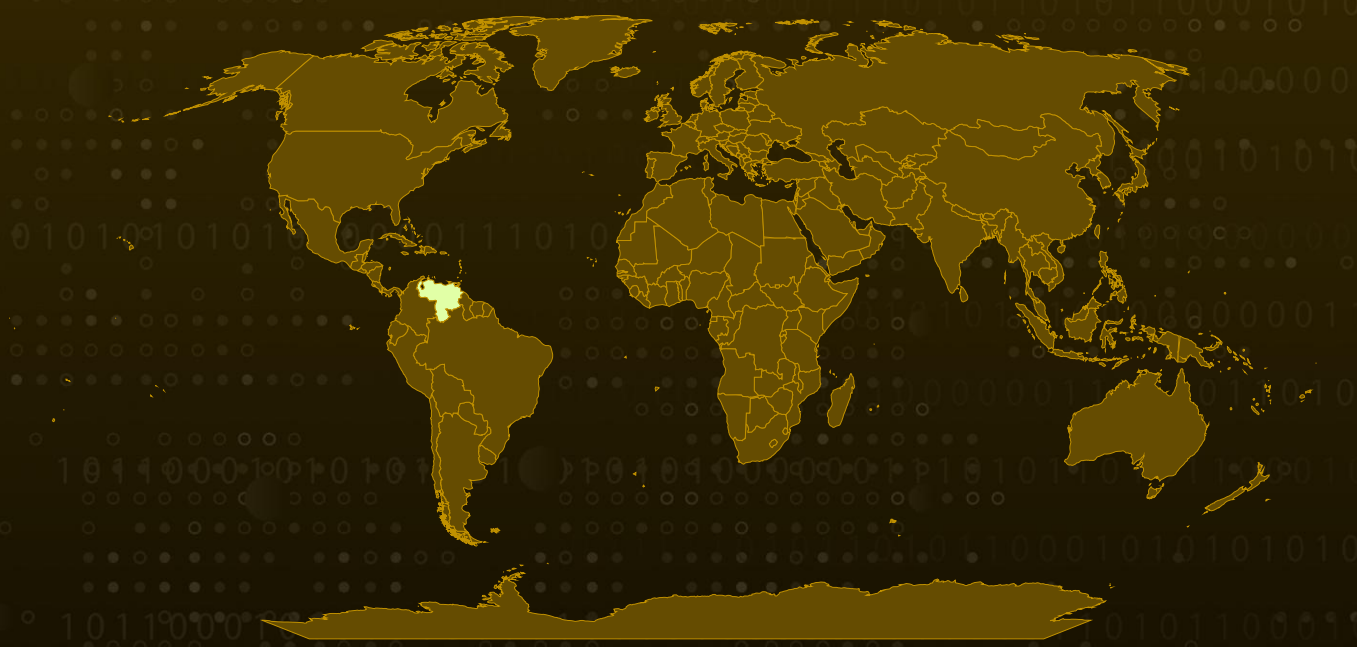
Lotus Wiper: Silent Sabotage Targeting Venezuela's Energy Sector

Date of Publication	Admiralty Code	TA Number
April 22, 2026	A1	TA2026109

Summary

First Seen: Mid-December 2025 (uploaded to publicly available resource); compiled late September 2025
Targeted Regions: Venezuela
Targeted Platforms: Windows
Targeted Industries: Energy and Utilities
Malware: Lotus Wiper
Attack: A destructive wiper campaign leveraging batch scripts and a previously unknown wiper dubbed Lotus Wiper was deployed against energy and utilities organizations in Venezuela amid geopolitical tensions in the Caribbean region during late 2025 and early 2026. The attack chain employs two batch scripts to weaken system defenses, disable user accounts, destroy disk contents, and ultimately decrypt and execute the Lotus Wiper payload, which removes recovery mechanisms, overwrites physical drives with zeroes, clears USN journals, and systematically deletes all files, rendering targeted systems permanently unrecoverable. No ransomware or extortion mechanisms were observed, confirming the campaign is purely destructive with no financial motivation.

Attack Regions



Attack Details

#1

A previously undocumented data-wiping malware, dubbed Lotus, was deployed last year in highly targeted attacks against energy and utilities organizations in Venezuela. The operation begins with a batch script named OhSyncNow.bat, which acts as the initial trigger for the destructive chain. This script identifies a local working directory at C:\lotus and attempts to disable the Interactive Services Detection (UI0Detect) service, effectively suppressing any visible alerts that could expose the ongoing activity. It then checks for the presence of an XML flag file (OHSync.xml) hosted on a NETLOGON share, using a hardcoded organization name to construct the network path. This external file functions as a covert control signal; once detected, it triggers execution across domain-joined systems, resembling a backdoor mechanism dependent on network-accessible resources. If the file is absent, execution halts; if the share is temporarily unreachable, the script introduces a randomized delay of up to 20 minutes before retrying, adding resilience and stealth to the operation.

#2

Once activated, a secondary script, notesreg.bat, is executed to carry out a one-time destructive routine. It first checks for a marker file to avoid re-execution, deleting itself if the operation has already been performed. The script then systematically targets user accounts, excluding specific predefined names, likely tied to IT personnel, by resetting passwords to random values, disabling accounts, and restricting login hours. It further disrupts access by disabling cached credentials through registry modification and forcibly logging off all active sessions using qwinsta. Network isolation is achieved by disabling all interfaces via netsh, effectively cutting off external communication. From there, the script escalates into full-scale destruction: it enumerates all logical drives and leverages diskpart clean all to overwrite disks with zeros, recursively overwrites directory contents using robocopy, and exhausts remaining disk space with fsutil, ensuring complete system inoperability.

#3

The final stage introduces a binary named nstats.exe, which masquerades as a legitimate HCL Domino server component. This executable accepts two arguments: nevent.exe, an XOR-encrypted payload, and ndesign.exe, the output file, and decrypts the payload to produce the actual Lotus Wiper binary. The requirement to pre-stage these components strongly indicates that the attackers had already established a foothold within the environment before detonation. Additionally, the deliberate targeting of legacy Windows features, such as UI0Detect, suggests a detailed understanding of the victim's infrastructure. Timeline analysis reveals that the wiper was compiled in late September 2025 and only deployed months later, pointing to a carefully planned and staged intrusion.

#4

Once executed, the Lotus Wiper escalates its privileges to gain full administrative control and begins a multi-phase destruction process. It first removes all system restore points by dynamically loading srclient.dll and invoking the System Restore API, ensuring that recovery options are eliminated. It then wipes physical drives by querying disk geometry via IOCTL_DISK_GET_DRIVE_GEOMETRY_EX and overwriting all sectors with zeros. Between these wipe cycles, the malware enumerates mounted volumes and spawns' parallel threads to erase USN journal entries and delete files at scale. Individual file destruction involves zeroing data regions, renaming files to random hexadecimal strings to obscure their identity, and deleting them using native Windows APIs. In cases where files are locked, deletion is deferred until reboot using MoveFileExW. This process is repeated in multiple passes, with additional restore point removal after each cycle, ensuring irrecoverable damage. The operation concludes with a system-level update call to reflect disk changes, leaving the compromised machine effectively unusable.

Recommendations

- **Audit NETLOGON and Domain Shares:** Review permissions and file activity on domain shares, specifically monitoring the NETLOGON share for unauthorized file additions or modifications, as the attack chain uses shared XML files as trigger mechanisms to coordinate wiper execution across domain-joined hosts.
- **Monitor for Unauthorized Service Manipulation:** Deploy detection rules for attempts to query, stop, or disable system services such as UI0Detect using sc.exe, as this behavior was used to suppress visible warnings during the initial attack phase.
- **Detect Mass Account Manipulation:** Alert on bulk password changes and account deactivation events (Windows Event 4724) across local user accounts, particularly when performed in rapid succession by scripted processes rather than administrative workflows.
- **Block Living-off-the-Land Abuse:** Monitor and restrict unusual use of built-in system utilities including fsutil, robocopy, diskpart, netsh, and qwinsta, especially when invoked from non-standard directories or batch scripts, as the attackers relied on these legitimate tools for disk destruction and network isolation.

Restrict Network Interface Changes: Implement controls to alert on or prevent unauthorized disabling of network interfaces via netsh, which was used to isolate compromised systems from external communication and impede incident response.

Harden Cached Credential Policy: Enforce group policy settings for CachedLogonsCount and monitor for unauthorized registry modifications to the Winlogon key, as the attack manipulated this value to prevent domain users from logging in without network connectivity.

Implement Immutable and Offline Backups: Maintain air-gapped or immutable backup copies of critical systems and data, and regularly test restoration procedures. Wiper attacks like Lotus Wiper are specifically designed to render systems permanently unrecoverable, making resilient backup strategies the primary recovery mechanism.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Execution	T1059: Command and Scripting Interpreter	T1059.003: Windows Command Shell
Persistence	T1078: Valid Accounts	T1078.002: Domain Accounts
Defense Evasion	T1036: Masquerading	T1036.005: Match Legitimate Name or Location
	T1140: Deobfuscate/Decode Files or Information	
	T1562: Impair Defenses	T1562.001: Disable or Modify Tools
Discovery	T1082: System Information Discovery	
	T1083: File and Directory Discovery	
	T1049: System Network Connections Discovery	
Lateral Movement	T1080: Taint Shared Content	

Tactic	Technique	Sub-technique
Credential Access	T1098: Account Manipulation	
Impact	T1561: Disk Wipe	T1561.001: Disk Content Wipe
		T1561.002: Disk Structure Wipe
	T1485: Data Destruction	
	T1490: Inhibit System Recovery	
	T1489: Service Stop	
	T1531: Account Access Removal	

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	0b83ce69d16f5ecd00f4642deb3c5895, c6d0f67db6a7dbf1f9394d98c1e13670, b41d0cd22d5b3e3bdb795f81421a11cb
SHA256	405177294F6F9268432A43998049AD0D4A61C6909216533B8713C911BC430755, 9D05854C95C6AFA68911BD28AF12282185E0FE34F2E58FDDBC503AB22D1508D7, 1D6F374087087738B7699EBF91F1CFDB3B2A65C2E9BE72E106EE7C9814BE3274

References

https://securelist.com/tr/lotus-wiper/119472/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a demo of **HivePro.**

REPORT GENERATED ON

April 22, 2026 • 9:00 AM

More at www.hivepro.com