INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-07-11 14:56 UTC

GigaWiper: Go-Based Multi-Capability Destructive Backdoor Targeting Windows Systems

THREAT CAMPAIGN | **CRITICAL** | CVSS 8.4

SCC Item ID	SCC-CAM-2026-0648
Type	Threat Campaign
Severity	CRITICAL
CVSS Base Score	8.4
Affected Products	Microsoft Windows (specific versions not confirmed in available source material)
Published	2026-07-10
Discovery Source	Gemini

Executive Summary

A Go-based malware family called GigaWiper has been reported to combine disk wiping, ransomware-style encryption, and spyware capabilities in a single backdoor, reportedly active for over eight months on Windows systems. Organizations running Windows face potential for irreversible data destruction, operational shutdown, or covert exfiltration depending on how threat actors deploy the malware's modular capabilities. This report is based on a single unconfirmed discovery; Microsoft Threat Intelligence has not yet published independent confirmation, and the full technical picture and attribution remain unverified pending direct confirmation from Microsoft Threat Intelligence publications.

Technical Analysis

GigaWiper is reported as a Go-compiled backdoor targeting Microsoft Windows systems, active for over eight months based on the single source discovery. The malware is described as multi-capability: it combines disk wiping (T1485, Data Destruction), ransomware-style encryption (T1486, Data Encrypted for Impact), and spyware functions, with operators selecting operational mode based on mission objectives. Additional mapped techniques include T1560 (Archive Collected Data), T1071 (Application Layer Protocol for C2 communication), T1059.001 (Command and Scripting Interpreter, PowerShell), and T1027 (Obfuscated Files or Information). Relevant CWEs include CWE-693 (Protection Mechanism Failure), CWE-506 (Embedded Malicious Code), and CWE-400 (Uncontrolled Resource Consumption). No CVE ID is assigned. Specific affected Windows versions are not confirmed in available source material. No patch or vendor mitigation advisory has been confirmed at this time. Source quality is single-sourced via a Gemini-grounded discovery; no corroborating independent

reporting has been identified. Technical details should be treated as unverified pending direct confirmation from Microsoft Threat Intelligence (MSTIC) or the Microsoft Security Blog. CVSS base score of 8.4 is noted in item data but no associated vector string is provided; treat this figure as provisional.

Action Checklist

1. Step 1: Containment. Identify Windows hosts exhibiting anomalous Go-runtime process execution, unexpected disk I/O spikes, or outbound C2 communication patterns consistent with T1071 (Application Layer Protocol for C2 communication). Isolate any suspected hosts from the network immediately. Specific Windows versions affected are not confirmed in source material; treat all production Windows endpoints as potentially in scope until scoping is refined against confirmed MSTIC guidance.
2. Step 2: Detection. Query endpoint detection logs for execution of unsigned Go binaries, mass file modification or deletion events (T1485), and bulk encryption activity (T1486). Review Windows Event Logs for scripting-layer execution anomalies (T1059) and obfuscated payload launches (T1027). Monitor for archive creation activity (T1560) on sensitive data directories. See detection_guidance field for additional behavioral indicators. Cross-reference with MSTIC advisories when published for confirmed IOC hashes and C2 indicators.
3. Step 3: Eradication. No vendor-confirmed patch or removal tool is available in current source material. If infection is confirmed, rebuild affected hosts from known-good images rather than attempting in-place remediation, given the destructive wiper capability. Remove and rotate all credentials stored on or accessible from affected systems per NIST AC-2 (Account Management) and IA-4 (Identifier Management). Apply NIST SI-3 (malicious code protection) controls to block re-infection vectors pending confirmed MSTIC remediation guidance.
4. Step 4: Recovery. Restore from offline, integrity-verified backups only; verify backup integrity before restoration given the wiper component's potential to corrupt or encrypt data prior to detection. Post-restoration, validate system file integrity using NIST SI-7 (Software, Firmware, and Information Integrity) monitoring against known-good baselines. Monitor restored hosts for recurrence of behavioral indicators for a minimum of 30 days. Enable enhanced audit logging per NIST AU-2 and AU-12 across recovered systems.
5. Step 5: Post-Incident. Review detection gaps that allowed an eight-month-active backdoor to persist undetected. Assess coverage against T1485, T1486, and T1027 in your current detection ruleset. Strengthen endpoint behavioral monitoring per CIS 8.2 (Collect Audit Logs) and enforce least-privilege access per NIST AC-6 to limit lateral movement opportunity. Subscribe to MSTIC and CISA advisories for updated attribution, IOCs, and confirmed mitigations as this campaign report matures.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to senior IR leadership, legal counsel, and executive stakeholders if GigaWiper infection is confirmed on any host containing PII, PHI, or regulated financial data, or if wiper module activity is detected indicating active data destruction that may trigger breach notification obligations under HIPAA, GDPR, or state data protection statutes.

Recovery Notes	Restoration must use only offline, air-gapped backups whose integrity has been cryptographically verified against pre-incident checksums, as GigaWiper's encryption module may have silently corrupted or encrypted data stores weeks before detection given the eight-month reported dwell time. All restored hosts must be monitored with off-host logging (remote syslog or forwarded Windows Event Log) for a minimum of 30 days, with specific alerting on unsigned Go binary execution, bulk file modification events (Sysmon Event ID 11 volume spikes), and outbound connections to newly registered or uncategorized domains. Do not return any host to production until MSTIC publishes confirmed IOC hashes and C2 infrastructure indicators, which should be used to retrospectively validate that restored systems show no matching artifacts.
Forensic Artifacts	USN Change Journal (fsutil usn readjournal): Reconstructs the sequence and timestamps of mass file deletion, overwrite, or rename operations produced by GigaWiper's wiper module even after the targeted files have been destroyed — critical for establishing scope and dwell-period activity. | Windows Prefetch files (C:\Windows\Prefetch\): Preserve execution history of Go runtime binaries including last eight execution timestamps and files accessed, providing evidence of GigaWiper execution even if the malware binary was self-deleted by the wiper's cleanup routine. | LSASS process memory dump: Captures credential material harvested by GigaWiper's spyware module from LSASS, browser credential stores, and Windows Credential Manager — essential for scoping the credential exposure radius across the environment. | Windows Registry auto-start hive exports (HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run, HKCU\Software\Microsoft\Windows\CurrentVersion\Run, HKLM\SYSTEM\CurrentControlSet\Services): Documents GigaWiper persistence mechanisms (registry run keys, malicious service registration) that enabled eight-month dwell before detection. | Sysmon Operational Event Log (Microsoft-Windows-Sysmon/Operational), specifically Event IDs 1, 3, 11, and 23: Captures GigaWiper process creation with command-line arguments, outbound C2 network connections with destination IP and port, bulk file creation by the encryptor module, and file deletion sequences by the wiper module — the most threat-specific behavioral evidence source for this malware family.

Per-Action IR Details

Step 1: Containment — Identify Windows hosts exhibiting anomalous Go-runtime process execution, unexpected disk I/O spikes, or outbound C2 communication patterns consistent with T1071 (application-layer protocol abuse). Isolate any suspected hosts from the network immediately. Specific Windows versions affected are not confirmed in source material; treat all production Windows endpoints as potentially in scope until scoping is refined against confirmed MSTIC guidance.

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: Deploy Sysmon with a configuration that logs Event ID 1 (Process Create) to catch Go runtime binaries (identifiable by the goroutine scheduler thread pattern and statically linked Go standard library imports visible in the image path or PE header). Use Wireshark or Windows built-in `netstat -ano` to capture active outbound connections before isolation. Run `Get-Process | Where-Object {$_.Path -like '*.exe'} | Select-Object Name, Id, Path, Company | Export-Csv procs.csv` to snapshot running processes. Isolate via managed switch VLAN reassignment or Windows Firewall emergency block-all rule: `New-NetFirewallRule -DisplayName 'GIGAWIPER-ISOLATION' -Direction Outbound -Action Block -Enabled True`.

Evidence: BEFORE network isolation, capture: (1) full RAM image using WinPmem or Magnet RAM Capture to preserve in-memory GigaWiper payload, Go runtime goroutine stacks, and any decrypted configuration blobs; (2) live

network state via `netstat -ano > netstat_snapshot.txt` and `Get-NetTCPConnection | Export-Csv connections.csv` to preserve active C2 socket tuples; (3) running process list with parent-child relationships via `Get-CimInstance Win32_Process | Select-Object ProcessId, ParentProcessId, Name, CommandLine | Export-Csv processes.csv`; (4) Windows Security Event Log Event ID 4688 (Process Creation) entries filtered on unsigned Go binaries spawned from unexpected parent processes (e.g., Office applications, browser processes, or scheduled task hosts).

Step 2: Detection — Query endpoint detection logs for execution of unsigned Go binaries, mass file modification or deletion events (T1485), and bulk encryption activity (T1486). Review Windows Event Logs for scripting-layer execution anomalies (T1059) and obfuscated payload launches (T1027). Monitor for archive creation activity (T1560) on sensitive data directories. See detection_guidance field for additional behavioral indicators. Cross-reference with MSTIC advisories when published for confirmed IOC hashes and C2 indicators.

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: Enable Sysmon Event ID 11 (FileCreate) and Event ID 23 (FileDelete) to detect mass file destruction or encryption rename patterns (e.g., extensions changed in bulk). Use the Sigma rule framework to write host-based detection: alert on any process with no valid Authenticode signature (Sysmon Event ID 1, `Signed: false`) performing more than 50 file write or rename operations within a 60-second window — a behavioral signature consistent with GigaWiper's wiper and encryption modules. Query Windows Event Log via: `Get-WinEvent -LogName Security | Where-Object {$_.Id -eq 4688} | Where-Object {$_.Message -like '*go*.exe*' -or $_.Message -like '*.tmp*'} | Format-List`. For archive/exfil detection, monitor `%TEMP%` and `%APPDATA%` directories for unexpected `.zip`, `.7z`, or `.rar` creation using Sysmon Event ID 11.

Evidence: Before any log-clearing or host action, preserve: (1) Windows Security Event Log (`C:\Windows\System32\winevt\Logs\Security.evtx`) and System Event Log for Event IDs 4688, 4663 (file access auditing), and 7045 (new service installation); (2) Sysmon operational log (`Microsoft-Windows-Sysmon/Operational`) for process creation, network connection, and file creation events tied to the suspected GigaWiper binary; (3) USN Change Journal (`fsutil usn readjournal C: csv > usnjournal.csv`) to reconstruct mass file deletion or overwrite sequences produced by the wiper module even if files are already destroyed; (4) Windows Prefetch files (`C:\Windows\Prefetch\`) to establish execution history of Go binaries that may have since been deleted by the wiper's self-cleanup routine.

Step 3: Eradication — No vendor-confirmed patch or removal tool is available in current source material. If infection is confirmed, rebuild affected hosts from known-good images rather than attempting in-place remediation, given the destructive wiper capability. Remove and rotate all credentials stored on or accessible from affected systems per D3-CRO (Credential Rotation). Apply NIST SI-3 (malicious code protection) controls to block re-infection vectors pending confirmed MSTIC remediation guidance.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication and Recovery

Controls: CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 5.2 (Use Unique Passwords), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts)

Compensating: Because GigaWiper's spyware module may have harvested credentials stored in LSASS, browser credential stores, and Windows Credential Manager, enumerate all credentials accessible from affected hosts using `cmdkey /list` and `vaultcmd /listcreds:'Windows Credentials'` before rebuilding. Document all service accounts, API keys, and domain credentials with logon history on the host (query `net use`, `Get-StoredCredential`). Rotate all identified credentials through a clean, uncompromised management workstation. For re-infection blocking pending MSTIC guidance, create YARA rules targeting Go runtime binary characteristics (e.g., `go build` metadata strings, goroutine scheduler signatures) and deploy via ClamAV or Windows Defender custom scan.

Evidence: BEFORE reimaging: (1) acquire full disk image using `dd` or FTK Imager to preserve the GigaWiper binary, any dropped payloads in `%TEMP%`, `%APPDATA%\Roaming`, `%PROGRAMDATA%`, or auto-start locations

(`HKCU\Software\Microsoft\Windows\CurrentVersion\Run`, `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`) for later malware analysis; (2) export LSASS memory using Task Manager (protected process) or `procdump -ma lsass.exe lsass.dmp` to assess credential exposure scope from the spyware module; (3) collect Windows Registry hive exports (`HKLM\SYSTEM`, `HKLM\SOFTWARE`, `HKCU`) to document persistence mechanisms; (4) capture all scheduled tasks via `schtasks /query /fo CSV /v > tasks.csv` and Windows services via `sc query type= all > services.txt` before the rebuild destroys evidence of GigaWiper's persistence method.

Step 4: Recovery — Restore from offline, integrity-verified backups only; verify backup integrity before restoration given the wiper component's potential to corrupt or encrypt data prior to detection. Post-restoration, validate system file integrity using D3-SFA (System File Analysis) against known-good baselines. Monitor restored hosts for recurrence of behavioral indicators for a minimum of 30 days. Enable enhanced audit logging per NIST AU-2 and AU-12 across recovered systems.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-2 (Event Logging), NIST AU-12 (Audit Record Generation), NIST AU-11 (Audit Record Retention), CIS 8.2 (Collect Audit Logs)

Compensating: Before restoring from backup, hash-verify backup archives against stored checksums to confirm the wiper or encryption module did not reach backup storage (compare SHA-256 of backup files against pre-incident manifest). Use `sfc /scannow` and `DISM /Online /Cleanup-Image /RestoreHealth` post-restoration to validate Windows system file integrity against Microsoft's known-good catalog. Deploy Sysmon immediately on restored hosts with logging to a remote, isolated syslog server so that any GigaWiper reinfection (e.g., via a re-activated persistence mechanism or reintroduced infected media) is captured off-host within the 30-day monitoring window. Configure Windows Audit Policy to log Object Access (file system) and Process Tracking at minimum.

Evidence: Before completing restoration and returning the host to production: (1) verify that backup media or backup server logs show no GigaWiper-consistent file modification timestamps (bulk renames, mass deletions) during the active infection window, confirming backup integrity; (2) run a YARA scan of the restored system image against Go runtime signatures and any GigaWiper behavioral indicators published in MSTIC advisories before the host goes live; (3) establish a baseline hash inventory of all executables in `C:\Windows\System32`, `C:\Program Files`, and auto-start directories on the freshly restored system using `Get-FileHash -Path 'C:\Windows\System32\*' -Algorithm SHA256 | Export-Csv baseline_hashes.csv` for drift detection during the 30-day monitoring period.

Step 5: Post-Incident — Review detection gaps that allowed an eight-month-active backdoor to persist undetected. Assess coverage against T1485, T1486, and T1027 in your current detection ruleset. Strengthen endpoint behavioral monitoring per CIS 8.2 (Collect Audit Logs) and enforce least-privilege access per NIST AC-6 to limit lateral movement opportunity. Subscribe to MSTIC and CISA advisories for updated attribution, IOCs, and confirmed mitigations as this campaign report matures.

NIST Phase: Post Incident

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

Controls: NIST AC-6 (Least Privilege), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 8.2 (Collect Audit Logs), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts)

Compensating: Conduct a structured detection gap analysis using the MITRE ATT&CK Navigator: map current Sysmon rules and Windows Audit Policy coverage against the GigaWiper technique set (wiper, encryptor, spyware, C2 beacon) and identify blind spots. For a 2-person team, prioritize free Sigma rule repositories (SigmaHQ) for mass file deletion and bulk encryption behavioral patterns. Enforce least privilege by auditing local Administrator group membership on all Windows endpoints via `net localgroup administrators` and removing non-essential accounts. Subscribe to MSTIC GitHub and CISA Known Exploited Vulnerabilities catalog RSS feeds for GigaWiper IOC updates without requiring enterprise tooling.

Evidence: For lessons-learned documentation: (1) reconstruct the GigaWiper dwell timeline (estimated 8+ months) using USN Change Journal exports, Windows Event Log oldest records, and Prefetch file creation timestamps to

identify the earliest evidence of execution; (2) review historical Windows Event ID 4625 (failed logon) and 4624 (successful logon) records retained in SIEM or archived `.evtx` files to assess whether the spyware module's credential harvesting enabled lateral movement across the environment during the dwell period; (3) document all hosts where GigaWiper artifacts (binary hashes, auto-start registry keys, scheduled tasks) were found to produce a complete scope assessment for regulatory breach notification decisions.

Detection Guidance

Detection guidance is limited by the absence of confirmed IOCs, hash values, C2 infrastructure details, or a vendor advisory in the provided source material. The following behavioral indicators are consistent with the mapped MITRE techniques and should be used as hunting hypotheses until MSTIC publishes confirmed indicators. Monitor for: unsigned or anomalously named Go-runtime processes (look for Go-compiled binary signatures in process telemetry); mass file modification, overwrite, or deletion events in short time windows indicative of T1485 wiper activity; bulk file encryption events with renamed or extension-changed files consistent with T1486; outbound connections to low-reputation or newly registered domains using common application-layer protocols (T1071); scripting-interpreter invocations (T1059) spawned from unusual parent processes; and archive creation (T1560) targeting sensitive directories. Apply NIST SI-7 (Software, Firmware, and Information Integrity) monitoring to detect modification of system executables or configuration files. Enable NIST AC-2 (Account Management) and AU-12 (Audit Generation) monitoring to surface privilege escalation or lateral movement associated with credential access. Note: without confirmed IOC data from MSTIC or a corroborating independent source, these behavioral hunts carry elevated false-positive risk and require analyst triage. Treat all detections as unconfirmed pending primary source validation.

Framework Mappings

MITRE-ATTACK

- **T1560** — Archive Collected Data
- **T1486** — Data Encrypted for Impact
- **T1071** — Application Layer Protocol
- **T1059.002** — AppleScript
- **T1485** — Data Destruction
- **T1027** — Obfuscated Files or Information

NIST-800-53R5

- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-4** — System Monitoring
- **SI-3** — Malicious Code Protection
- **SC-5** — Denial-of-Service Protection
- **IR-4** — Incident Handling
- **SC-13** — Cryptographic Protection

CIS-V8

- **13.8** — Deploy a Network Intrusion Prevention Solution

NIST-CSF-2

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

HIPAA-SECURITY

- **164.308(a)(7)(ii)(A)** — Data Backup Plan
- **164.312(e)(1)** — Transmission Security

ISO-27001-2022

- **A.5.29** — Information security during disruption
- **A.5.34** — Privacy and protection of personal information
- **A.8.24** — Use of cryptography

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1560	Archive Collected Data	Collection
T1486	Data Encrypted for Impact	Impact
T1071	Application Layer Protocol	Command-And-Control
T1059.002	AppleScript	Execution
T1485	Data Destruction	Impact
T1027	Obfuscated Files or Information	Defense-Evasion

Sources

Source	URL	Tier
Critical Vulnerabilities in Microsoft Windows Operating Systems - CISA	https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-014a	T1
Vulnerabilities - Security Update Guide - Microsoft	https://msrc.microsoft.com/update-guide/vulnerability	T1
[PDF] “Windows System Security Vulnerabilities” CYSE 280	https://sites.wp.odu.edu/hbramow/wp-content/uploads/sites/33714/202...	T1

Source	URL	Tier
Microsoft Windows security vulnerability - BOXX Insurance USA	https://boxxinsurance.com/us/en/resources/microsoft-windows-securit...	T3

Generated 2026-07-11 14:56 UTC by TJS Security Command Center