Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

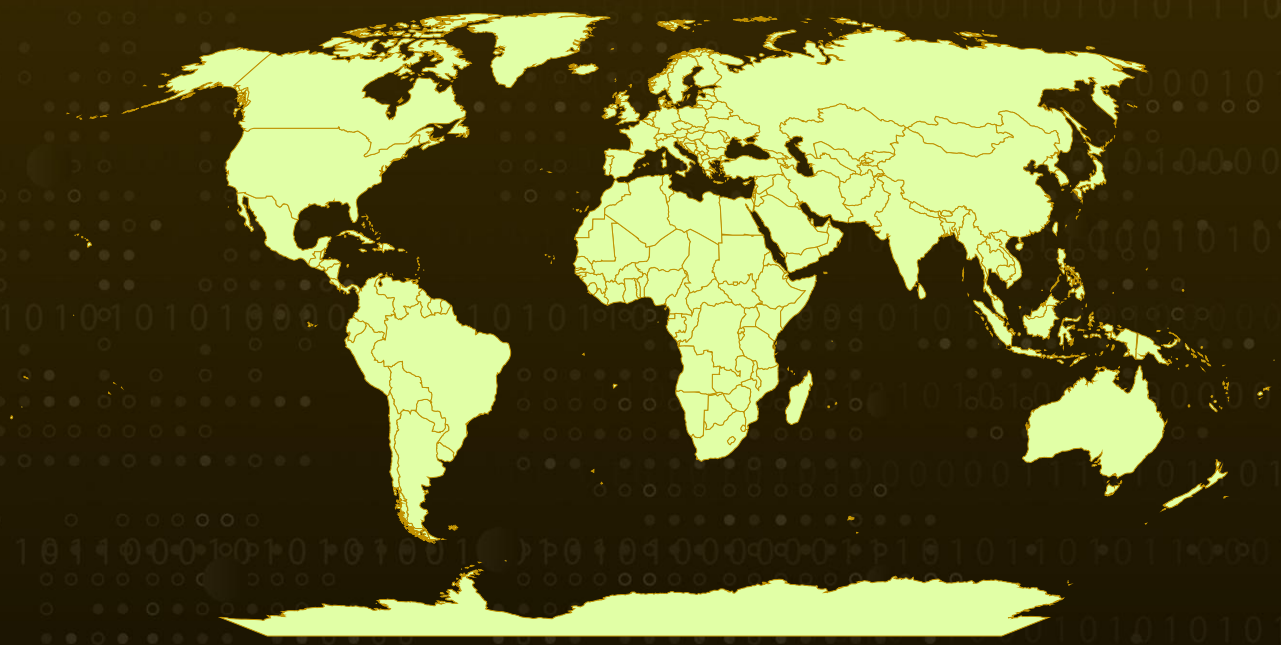
GigaWiper: The All-in-One Destruction Kit

Date of Publication	Admiralty Code	TA Number
July 13, 2026	A1	TA2026197

Summary

First Seen: October 2025
Targeted Regions: Worldwide
Targeted Platform: Windows
Targeted Product: Microsoft Windows
Malware: GigaWiper (aka BLUERABBIT)
Attack: GigaWiper is a Go-based backdoor that packs several destructive tools into a single implant. Researchers first spotted it wiping compromised environments in October 2025. Instead of being one purpose-built tool, it stitches together code from at least three older malware families and exposes them as on-demand commands. Operators can quietly gather intelligence, then flip to destruction on command: overwriting physical disks, encrypting files with keys that are never saved (fake ransomware with no recovery path), or forcing an unbootable Blue Screen of Death. It maintains persistence, communicates over RabbitMQ and Redis, and offers a broad remote-control toolkit.

Attack Regions



Targeted Non-Targeted

Attack Details

#1

GigaWiper also tracked as BLUERABBIT, is a newly identified Windows threat built to do more than steal information or lock a screen. It is a Go-based implant that pairs a full command-and-control backdoor with several built-in destruction routines, and it appears in two closely related forms: standalone wiper binaries and a larger backdoor. Both are unstripped Go portable executables, and the standalone wiper's code is embedded wholesale inside the backdoor as one of its on-demand commands, letting an operator move from a quiet presence to irreversible damage whenever they choose.

#2

Once running, GigaWiper establishes persistence by creating a registry key at HKCU\SOFTWARE\OneDrive\Environment that tracks how many times it has executed. On first run it creates a scheduled task named "OneDrive Update" set to fire every minute and again at system startup, then exits; on later runs it recognizes it is executing as that task and continues. It decrypts a hard-coded configuration using AES with a hard-coded key to recover its command-and-control details, then receives operator commands over RabbitMQ (AMQP) and reports status and output back through a Redis server. Its commands are numbered 1 through 20 and span destruction, surveillance, and system management, with a fanout exchange named "All" broadcasting a command to every infected host at once and a topic exchange named "Topic" letting operators target specific machines.

#3

Beyond persistence and communication, the backdoor gives operators a broad remote-control toolkit. Command 20 stands up a VNC-style server with keyboard, mouse, and live screen streaming over a chosen TCP port, disguising the firewall rules it needs with names borrowed from legitimate Windows components. Interactive managers for processes (command 16), services (command 17), and the registry (command 18, which keeps session state between requests like an interactive browser) provide hands-on control of a compromised host.

#4

For data handling, command 4 uses the MinIO Client to upload files to remote S3-compatible storage, while command 15 gathers extensive system information such as IP address, machine GUID, CPU, OS, network configuration, firmware, user details, and installed antivirus products, and returns it through the C2 channel. Screenshots (command 9) and continuous screen recording while the user is active (command 10) round out its collection capability. The operation ends in destruction: command 1 overwrites raw disk content and removes partition metadata before rebooting, command 12 performs a multi-pass secure wipe of the Windows drive, command 3 encrypts files with an unsaved key and renames them with a .candy extension while dropping a threatening wallpaper, and command 2 disables recovery and deletes boot and kernel files to leave the machine unbootable. Command 19 then clears Windows event logs to frustrate incident response.

#5 Taken together, these capabilities make GigaWiper less a single tool than a destruction platform: at least three previously separate malware families are folded into one backdoor that can switch from quiet surveillance to irreversible sabotage on demand, all while masquerading as routine OneDrive activity.

Recommendations

Enable Tamper Protection Tenant-Wide: Turn on tamper protection so attackers cannot disable security services or add antivirus exclusions before deploying destructive commands. Where supported, enable DisableLocalAdminMerge to stop local modification of exclusions via GPO.

Block the Known C2 Infrastructure: Block outbound access to the reported command-and-control addresses (185.182.193[.]21 and 212.8.248[.]104), including the RabbitMQ and Redis service ports observed in samples, and feed these indicators into perimeter and DNS controls.

Hunt for the Persistence Artifacts: Search for the scheduled task named "OneDrive Update" that runs every minute, and for the registry key HKCU\SOFTWARE\OneDrive\Environment. Both impersonate legitimate OneDrive naming and are strong signals of a GigaWiper foothold.

Isolate and Preserve Suspected Hosts Immediately: Treat a suspected GigaWiper infection as a business-continuity emergency, not routine malware cleanup. Isolate affected devices from the network to cut them off from broadcast C2 commands, and preserve forensic evidence before destructive commands can spread.

Maintain Tested Offline Backups: Keep offline or otherwise protected backups, since a disk wiper can destroy the operating system and any data stored beside it. Rehearse recovery under realistic failure conditions, including unbootable systems and unavailable network services.

Monitor Scheduled Tasks and Registry Changes: Continuously monitor for new scheduled tasks and registry modifications that masquerade as trusted software, and for firewall rules created under names that mimic legitimate Windows components.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Execution	T1059: Command and Scripting Interpreter	T1059.001: PowerShell
Persistence	T1053: Scheduled Task/Job	T1053.005: Scheduled Task
Defense Evasion	T1036: Masquerading	T1036.004: Masquerade Task or Service
		T1036.005: Match Legitimate Resource Name or Location
	T1070: Indicator Removal	T1070.001: Clear Windows Event Logs
	T1112: Modify Registry	
	T1140: Deobfuscate/Decode Files or Information	
	T1562: Impair Defenses	T1562.004: Disable or Modify System Firewall
Discovery	T1082: System Information Discovery	
	T1518: Software Discovery	T1518.001: Security Software Discovery
Collection	T1113: Screen Capture	
Command and Control	T1071: Application Layer Protocol	
	T1219: Remote Access Software	

Tactic	Technique	Sub-technique
Exfiltration	T1567: Exfiltration Over Web Service	T1567.002: Exfiltration to Cloud Storage
Impact	T1485: Data Destruction	
	T1486: Data Encrypted for Impact	
	T1561: Disk Wipe	T1561.002: Disk Structure Wipe
		T1561.001: Disk Content Wipe
	T1490: Inhibit System Recovery	
	T1529: System Shutdown/Reboot	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	633d4cbd496b1094495da89a64f5e6c31a0f6d4d1488411db5b0cba1cfe42001, ce9ad5f6c12019f4aae5b189bd8ddf5bb09e75b06a0a587b25a855c65948c913, f622ed85ef31ad4ab973f4e74524866fe1bb44f0965ad2b2ad796cd657a05bfd, 9706a192e2c1a1faaf0a521daf31c2af60ff4590e3f47bbb4abc227f42af0683, 3c30deb6556a94cfb84ae51798f4aecfae8c7358e55fdb321c5f2376579631cd, 440b5385d3838e3f6bc21220caa83b65cd5f3618daea676f271c3671650ce9a3, 12c39f052f030a77c0cd531df86ad3477f46d1287b8b98b625d1dcf89385d721, db41e0da7ab3305be8d9720769c6950b4dc1c1984ef857d3310eb873a0fc7674
IPv4	185[.]182[.]193[.]21, 212[.]8[.]248[.]104
IPv4:Port	185[.]182[.]193[.]21[:]5544, 185[.]182[.]193[.]21[:]7542

References

https://www.microsoft.com/en-us/security/blog/2026/07/09/gigawiper-anatomy-of-a-destructive-backdoor-assembled-from-multiple-malware/

https://binarydefense.com/resources/blog/bluerabbit-a-golang-based-backdoor-with-ransomware-and-destructive-capabilities

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

July 13, 2026 • 08:00 AM

More at www.hivepro.com