Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

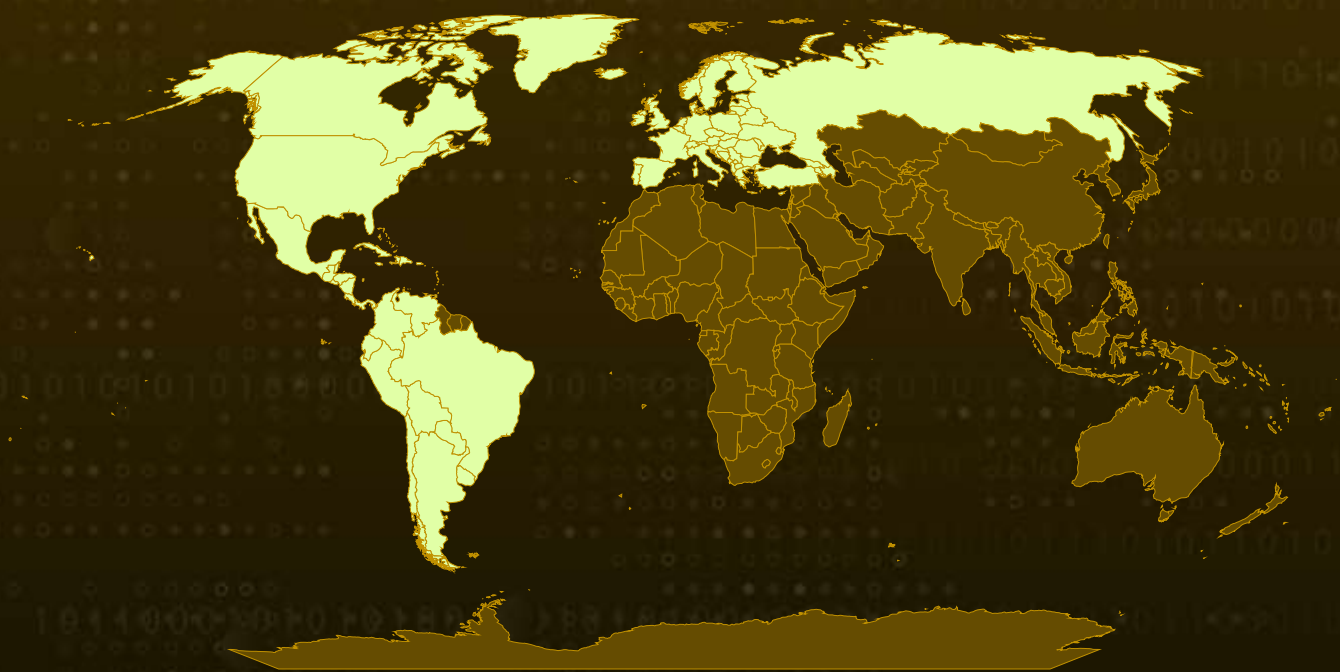
Grandoreiro Outlives Its Own Takedown

Date of Publication	Admiralty Code	TA Number
August 21, 2026	A1	TA2026242

Summary

First Seen: 2016
Targeted Regions: Mexico, Spain, wider Latin America, Europe, and North America
Targeted Platform: Microsoft Windows
Targeted Industries: Banking and Financial Services (financial institutions and their retail customers)
Malware: Grandoreiro
Attack: Grandoreiro operators have resumed activity more than two years after the 2024 law enforcement disruption, running a Mexico-focused campaign built around DLL sideloading. Victims receive a ZIP archive with an invoice-themed filename, assessed with moderate confidence to be delivered via spam.

Attack Regions



Targeted Non-Targeted

Attack Details

#1

Grandoreiro operators are active again more than two years after the 2024 law enforcement disruption, with a Mexico-focused campaign built on DLL sideloading. Delivery is a ZIP archive named like a commercial invoice, assessed with moderate confidence to arrive via spam. It holds a hidden folder of decoy PDF and XML files to make the archive look benign, plus a copy of Duplicate Files Finder, a legitimate cleanup utility renamed to a random string.

#2

Execution runs through a three-link sideloading chain: the renamed executable loads legitimate dupfdll.dll, which pulls in mingwm10.dll, a malicious replacement dropped alongside the trusted binaries. The payload therefore executes inside a process the operating system and most monitoring tools treat as trusted. Compilation timestamps across the chain are inconsistent, with the parent binary dated 2008 and the malicious library 2026. Timestamps are trivially forged, but combined with the dependency mismatch they support high confidence that a benign binary is being abused as a loader. Since Duplicate Files Finder has a GUI, the implant hides the window immediately so nothing appears on the victim's desktop.

#3

The loader then runs an unusually deep anti-analysis sequence before contacting any infrastructure. A geolocation lookup terminates execution on hosts in the Czech Republic, Russia, or the Netherlands, a choice assessed as operational rather than ideological since traffic from those countries skews toward researchers and automated analysis. Flagged systems get a Spanish-language error claiming the document failed to display, and execution stops.

#4

Surviving hosts proceed to command-and-control. The loader resolves its hardcoded C2 domain over Google's DNS-over-HTTPS service rather than the system resolver, hiding the lookup from conventional DNS monitoring, then issues an encrypted HTTP GET over TCP port 6432 for the second stage. The request opens with the token CLIENT_SOLICITA_DDS_MDL and carries geolocation, hostname, username, OS version, and installed antivirus, profiling the victim at first contact. Runtime strings are protected by a custom XOR and unpadded Base64 scheme with no public decoder.

#5

The C2 was offline during analysis, so the second stage was never recovered and no credential harvesting, network enumeration, or lateral movement was observed. The payload is documented to support keylogging, screen sharing, and remote device control, aimed at banking credentials and account access. Splitting a heavily armored loader from the full-capability payload protects the operators' long-term tooling, and points the threat at individual banking customers rather than enterprise networks.

Recommendations

Hunt for the Duplicate Files Finder Sideload Chain: Search endpoint telemetry for any process loading mingwm10.dll from the same directory as its parent executable, particularly where the parent is a renamed copy of Duplicate Files Finder. Load events for dupfdll.dll followed by mingwm10.dll from a user-writable directory such as Downloads, Temp, or a desktop folder are high-signal indicators.

Monitor for DNS-over-HTTPS Resolution Followed by Unusual Egress: Flag endpoint processes that query a public DoH endpoint directly and then immediately open an outbound connection to a non-standard port. Where policy permits, force all endpoint name resolution through enterprise resolvers and block direct DoH access from workstations so that C2 domain lookups remain visible to DNS logging.

Deploy Network Signatures for the C2 Protocol Tokens: The uppercase command strings used by this implant, beginning with CLIENT_SOLICITA_DDS_MDL, are distinctive enough to serve as network and memory hunting signatures. Deploy detection content covering these tokens across egress inspection points and endpoint memory scanning.

Enforce Application Allowlisting on Endpoint Executables: Renaming a legitimate signed utility to a random string defeats name-based controls but not hash-based or publisher-based allowlisting. Restrict execution from user-writable directories entirely, which breaks this attack chain at the point of first execution regardless of how convincingly the loader is disguised.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1566: Phishing	T1566.001: Spearphishing Attachment
Execution	T1204: User Execution	T1204.002: Malicious File
Defense Evasion	T1574: Hijack Execution Flow	T1574.001: DLL
	T1036: Masquerading	T1036.005: Match Legitimate Name or Location
	T1564: Hide Artifacts	T1564.003: Hidden Window
		T1564.001: Hidden Files and Directories
	T1497: Virtualization/Sandbox Evasion	T1497.001: System Checks
		T1497.003: Time Based Evasion
	T1622: Debugger Evasion	
	T1140: Deobfuscate/Decode Files or Information	
	T1027: Obfuscated Files or Information	
Discovery	T1082: System Information Discovery	
	T1016: System Network Configuration Discovery	
	T1614: System Location Discovery	
	T1057: Process Discovery	
	T1518: Software Discovery	T1518.001: Security Software Discovery
	T1012: Query Registry	

Tactic	Technique	Sub-technique
Discovery	T1083: File and Directory Discovery	
Command and Control	T1071: Application Layer Protocol	T1071.001: Web Protocols
		T1071.004: DNS
	T1571: Non-Standard Port	
	T1573: Encrypted Channel	
	T1105: Ingress Tool Transfer	
	T1219: Remote Access Tools	
Collection	T1056: Input Capture	T1056.001: Keylogging
	T1113: Screen Capture	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	1b2fe30c5bf57f9623efb34688580fe5bbb2c55351c5a07a6c4313bb6faa29f1, 1fe5a72aefc38afeeee72d8a939f9db50800a447b7313f4d8c504771bb7fa2de, 2820a2e36f1cb537a7853fde2313a5158d1e3696ff81c3066ec8fe274358c22d, 368246eb503585f26e0151431909792b8d9be0edc229bb207be882bfb374c005, 37492ecd9deb8591ea7e179ebb8e13c6b486cdacae18a6a482d9dd18f08453a3, 47d5a73b220813299f753ef0a96582a8d08b853391864128a1f15271dbb42e65, 609755a8c73e53f332428786c366323b3979850aaa0e075d946e6c05aa62f867, 65db035f79db85ad66fb3e0365e478f95f8f648545b18360d850a7ed179c9dab, 684f5eb157ef2ba3ea17335d6c8c9c801f93e6eb3aa08ecbfaf5806a4b5e3b80, a91c7cb932301454df4b0feed58082cae7f2d0e4078d7e6df3f53d806ed04f1d, ac35843c81381107d4f816681477d706c43fa75f064f2c3d99237c7282f0b798,

TYPE	VALUE
SHA256	ad5762fa98da2aff24d9d6b55be5dae21d07c54679ead67252a19c2521162a87, c019cfa9b50a69ff07e98bd78b3a6fc489110e5db1c0d79ada716605a2320951, ca33f5608b72ecca64a002074a4103c7cb83de902ecf5c69949eecb7eef03b5a, cc238813ab277cbb4324d37875c37985ca5baeaf8c412b4c85aa8ec5faec7096, e0491eddb45425a674e479b2590517ffef2f108add431761bb89791fc208b6e9, e99416ff71e4574de4fceebdc34f3b9a6e0610f36b77b735b231bd39edb7a0a1
MD5	82f771c3ec4fe979c3ae00372e8c3ac8, cfbd8d062e9baa98737a0260996f48c6, e882ee4a643b00871c98bcfe4b4d7cd1, f1aed8cf2adafa86927fc58d5f24073e
Domains	445675885304004[.]pointto[.]us, b744156103040828396040[.]nhlfan[.]net, beeges[.]health-carereform[.]com, smartpdfhub-7q2m[.]read-books[.]org, streamlinepdf-8m2x[.]workisboring[.]com, voyage[.]mydissent[.]net
Filename	Fac-BH22DC0608_RevMQKSAC.zip, _2IH4ENJIRRNCobran_03732qyykae214BKXXN6180-Dt.exe, dupfdll.dll, mingwm10.dll

References

https://www.acronis.com/en/tru/posts/grandoreiro-goes-north-from-brazil-to-mexico-with-a-new-dll-sideloading-campaign/

https://www.hivepro.com/threat-advisory/grandoreiro-trojan-an-evolving-threat-to-global-banking

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

August 21, 2026 • 07:00 AM

More at www.hivepro.com