Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

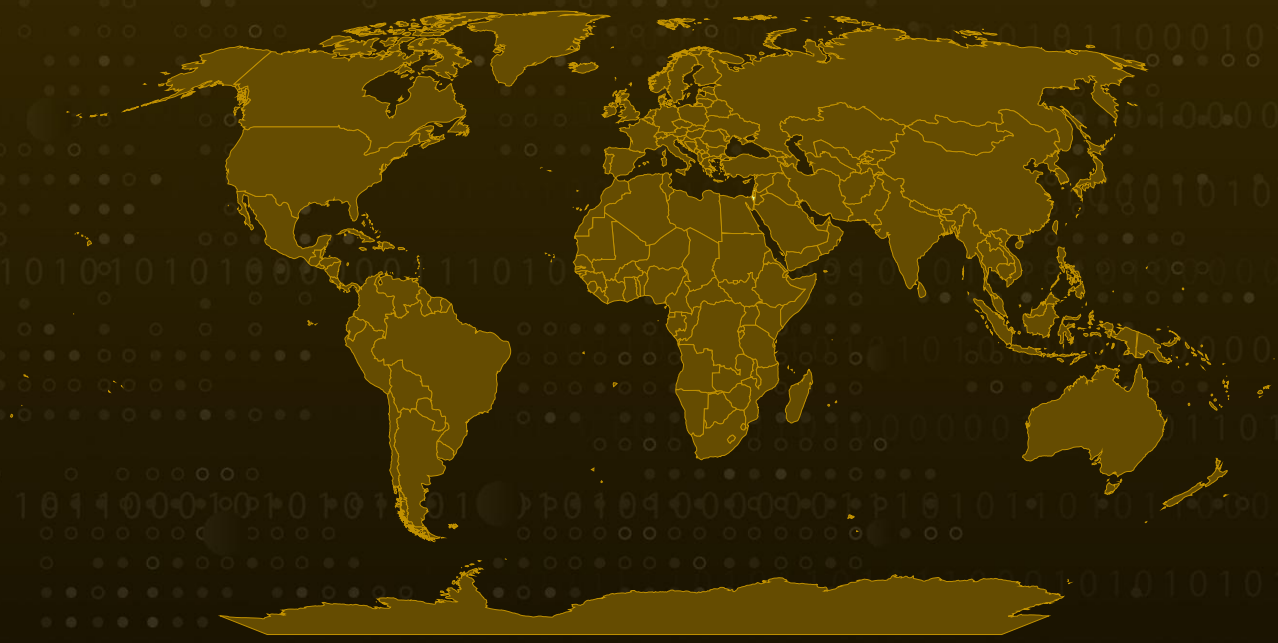
HOLLOWGRAPH Hides Its C2 in Microsoft 365 Calendars

Date of Publication	Admiralty Code	TA Number
July 22, 2026	A1	TA2026207

Summary

First Seen: June 3, 2026
Targeted Region: Israel
Targeted Platform: Windows
Targeted Products: Microsoft 365, Microsoft Graph API, Microsoft Entra ID (Azure AD)
Malware: HOLLOWGRAPH
Attack: HOLLOWGRAPH is a .NET espionage implant that turns a compromised Microsoft 365 mailbox calendar into a covert two-way command-and-control channel. Working through the trusted Microsoft Graph API, operators plant tasking as calendar events, and the implant exfiltrates stolen files as encrypted attachments on events it creates, all dated far into the future (May 13, 2050) so the mailbox owner never notices them. Payloads are protected with hybrid RSA and AES-256 encryption, using separate key pairs for incoming and outgoing traffic. A second channel uses DNS tunneling over IPv6 AAAA records to the attacker domain cloudlanecdn[.]com to refresh the Entra ID credentials the malware authenticates with. At least 12 infected systems are identified, roughly three actively communicating during analysis, with all evidence pointing to a narrow, targeted focus on Israeli entities.

Attack Regions



Attack Details

#1 HOLLOWGRAPH is a piece of espionage malware that stands out less for what it steals and more for where it hides. Instead of talking to a server the attacker owns, it borrows Microsoft's own cloud. Every command it receives and every file it steals moves through normal-looking Microsoft 365 traffic, which makes the activity extremely hard to separate from an organization's everyday cloud usage. Group-IB links the implant with high confidence to the modular Cavern backdoor framework, a toolset previously tied to Iranian-nexus activity.

#2 The malware does not need to break in on its own. It operates through an already compromised Microsoft 365 account belonging to an Israeli organization, using stored Microsoft Entra ID (Azure AD) credentials, tenant ID, client ID, client secret, and the target mailbox to authenticate with the Microsoft Graph API. How that account and the affected hosts were first compromised is not detailed in the available reporting.

#3 Technically, HOLLOWGRAPH is a .NET NativeAOT-compiled DLL that a loader runs with a structured command string. It supports only two actions, "get" and "send," and both run entirely through the Graph API. On execution, it writes its hardcoded configuration to disk as logAzure.txt, a filename chosen to blend in with ordinary log files.

#4 The clever part is the calendar. The compromised mailbox's calendar acts as a shared drop box. To pick up orders, HOLLOWGRAPH runs the "get" command, searching for an operator-planted event scheduled for May 13, 2050, and titled "Event ID: <task ID>," then downloads and decrypts the attached instructions with its private RSA key. To steal data, the "send" command reverses the flow: it encrypts the target file, creates its own far-future 2050 event, uploads the data as one or more "File{n}.txt" attachments, and renames the event to an operator-recognizable "Boss{..}ID{..}" tag. All of this is secured with a hybrid RSA-OAEP plus AES-256-GCM, using distinct key pairs so that tasking and exfiltration remain cryptographically separate.

#5 Because both tasking and exfiltration ride the same trusted Graph channel, the stolen data leaves the environment disguised as routine Microsoft 365 calendar activity rather than as recognizable outbound C2. A separate, unencrypted DNS channel keeps that access alive: the implant issues AAAA (IPv6) queries to cloudlanecdn[.]com, decodes the credential values from the returned IPv6 addresses in 14-byte chunks, and rewrites the refreshed values back into logAzure.txt. Notably, there is no Microsoft vulnerability and no patch involved here, HOLLOWGRAPH abuses a compromised account and the Graph API's legitimate functionality, which is exactly what makes it stealthy.

Recommendations

- **Hunt for HOLLOWGRAPH and Cavern Indicators:** Proactively search for the C2 domain cloudlanecdn[.]com, the on-disk configuration file logAzure.txt, and the known file hashes across your environment to identify existing infections.
- **Inspect Suspicious Calendar Artifacts:** Hunt Microsoft 365 calendars for events with the tell-tale traits of this malware, a far-future date of May 13, 2050, a bare GUID as the subject, subjects matching "Event ID:" or "Boss{..}ID{..}", and attachments named "File{n}.txt."
- **Monitor Graph API and Mailbox Audit Logs:** Review Microsoft Graph and mailbox audit activity for application-driven calendar changes, such as events created, attachments uploaded, or subjects renamed by an application rather than a human user.
- **Lock Down Client-Credential OAuth Applications:** Restrict, monitor, and audit client-credentials OAuth2 applications that can reach Graph, and alert on the creation of new client secrets or credentials that could be abused for silent cloud access.
- **Enforce Entra ID Identity Hygiene:** Apply Conditional Access policies, rotate credentials regularly, and enable anomalous-token detection across Microsoft 365 and Entra ID to limit what a stolen set of application credentials can do.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1078: Valid Accounts	T1078.004: Cloud Accounts
Execution	T1129: Shared Modules	
Defense Evasion	T1036: Masquerading	T1036.005: Match Legitimate Name or Location
Command and Control	T1102: Web Service	T1102.002: Bidirectional Communication
	T1071: Application Layer Protocol	T1071.004: DNS
	T1572: Protocol Tunneling	
	T1573: Encrypted Channel	T1573.002: Asymmetric Cryptography
Collection	T1005: Data from Local System	
Exfiltration	T1041: Exfiltration Over C2 Channel	

Indicators of Compromise (IOCs)

TYPE	VALUE
Domain	cloudlanecdn[.]com
SHA256	75e51774b8f79e5f256eaae639635f911b3e744d4774fd6068dd980255621509, f3f3006f8304788251b153d53b305322b8acab0c66ec816b8d9f101bcc851da3, b3d0f6e4e3be395fd7cf9e8101c89963d77216578cbb117a6ac9bc3564485eff

References

https://www.group-ib.com/blog/hollowgraph-microsoft-365/

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 22, 2026 • 07:30 AM

More at www.hivepro.com