ultraviolet

THREAT ADVISORY

HOLLOWGRAPH Malware

Services Performed By:
UltraViolet Cyber TIDE Team
tide@uvcyber.com

Published Date:
July 22, 2026
TLP:GREEN

Executive Snapshot

HOLLOWGRAPH is a newly identified .NET malware that is attributed with high confidence to the Iranian-nexus Cavern backdoor framework. It abuses the Microsoft Graph API to turn a compromised Microsoft 365 mailbox calendar into a covert, two-way, command-and-control channel. This channel hides tasking and stolen data inside encrypted calendar event attachments dated to the year 2050 while using DNS tunneling over IPv6 to refresh the Entra ID credentials it depends on. Current evidence points to a small, disciplined, espionage campaign focused on Israeli entities rather than broad opportunistic targeting.

- **Monitor Graph API and mailbox activity.** Audit Microsoft 365 mailbox logs for anomalous calendar operations, including event creation, attachment uploads, and subject renames performed by an application identity rather than a human user.
- **Hunt for known artifacts.** Search for calendar events dated “2050-05-13", GUID-only or placeholder subjects, subject patterns such as "Event ID:" or "Boss{..}ID{..}", and attachments named File{n}.txt.
- **Restrict and audit application access.** Review OAuth2 client-credential app registrations in Entra ID, alert on newly created client secrets, and flag applications with broader Graph permissions than their function requires.
- **Strengthen DNS monitoring.** Deploy detection for tunneling behavior, such as unusually frequent AAAA record queries or high-entropy subdomains, and route outbound DNS through controlled, filterable resolvers capable of sinkholing known malicious infrastructure.

TIDE Team Analysis

The Group-IB Threat Intelligence team has identified HOLLOWGRAPH, a new malware sample attributed with high confidence to the Cavern backdoor framework. HOLLOWGRAPH is one component of a larger toolkit and uses the Microsoft Graph API through a compromised Microsoft 365 account, observed in Israel, to communicate with its operators, a technique that conceals command-and-control traffic within legitimate Microsoft 365 communications. Given the widespread enterprise reliance on Microsoft 365 and Entra ID, this technique warrants immediate attention from security leadership.

HOLLOWGRAPH is a .NET NativeAOT-compiled DLL that supports just two commands, get and send, executed exclusively through trusted Microsoft cloud infrastructure. Using the Graph API, it treats the compromised mailbox's calendar as a two-way dead-drop: operators plant tasking as calendar events, and the implant exfiltrates stolen files by creating its own events with encrypted data attached. Every event is dated far into the future, 13 May 2050, with payloads attached as files, specifically to avoid drawing the mailbox owner's attention.

A second channel handles credential renewal. HOLLOWGRAPH performs DNS tunneling, using IPv6 AAAA record queries against the attacker-controlled domain cloudlanecdn[.]com, to refresh the Microsoft Entra ID (Azure AD) credentials it authenticates with, writing the updated values to an on-disk configuration file named logAzure.txt and disguised as an ordinary log. This channel is not encrypted and operates independently of the Graph API communication channel.

MALWARE PROFILE

HOLLOWGRAPH

Microsoft 365 Calendar-Based C2 Backdoor

ALSO Cavern Framework Component

FUNCTIONALITY	**Backdoor** **Data Exfiltration** **Cyber Espionage**
ACTIVE SINCE	At least June 2026
OPERATORS	Unattributed; linked with high confidence to the Cavern backdoor framework, with a low-confidence possible connection to the Iranian-nexus actor Lyceum (OilRig sub-group)
TARGETING	Highly targeted espionage focused on Israeli entities; 12 confirmed infections identified, with approximately 3 actively communicating with attacker infrastructure

NOTABLE TTPs

01	Abuses Microsoft Graph API to use a compromised Microsoft 365 mailbox calendar as a two-way command-and-control dead-drop
02	Plants and retrieves tasking/exfiltrated data as encrypted attachments on calendar events dated far in the future (2050-05-13)
03	Uses DNS tunneling over IPv6 AAAA records to an attacker-controlled domain (cloudlanecdn[.]com) to refresh Microsoft Entra ID credentials
04	Secures all Graph API payloads with hybrid RSA-OAEP and AES-256-GCM encryption using separate key pairs per communication direction
05	Stores credentials and configuration in an on-disk file (logAzure.txt) disguised as an ordinary log
06	Compiled as a .NET NativeAOT DLL, invoked with a structured two-command syntax (get / send) matching the Cavern framework's command format
07	Blends malicious traffic into legitimate Microsoft 365 activity, evading conventional network and perimeter-based defenses
08	Selectively engages a small subset of infected hosts, reflecting disciplined, narrowly scoped operational tradecraft

All Graph payloads are secured with hybrid RSA-OAEP and AES-256-GCM encryption, using two separate key pairs so that inbound tasking and outbound exfiltration remain cryptographically independent of one another. Several technical characteristics, including the command syntax and command codes observed in tasking, strongly suggest HOLLOWGRAPH is a variant of the Cavern framework, which itself shares tradecraft with a .NET backdoor previously attributed to the Iranian-nexus actor Lyceum, a sub-group of OilRig.

The organizational impact of this technique is significant precisely because it does not rely on a vulnerability in

Microsoft 365 or Entra ID. It relies on an already-compromised account and a legitimate, sanctioned API used in an unexpected way. Traditional network monitoring, built to flag connections to unfamiliar external infrastructure, will not surface this activity, since the "C2 server" is Microsoft's own cloud. Detection must shift toward behavioral analysis of application and identity activity inside Microsoft 365 rather than relying solely on where network traffic is going.

Group-IB identified 12 systems infected with HOLLOWGRAPH, of which only approximately three were actively communicating with the attacker at the time of analysis. The earliest observed communication occurred on 3 June 2026, with the most recent on 9 July 2026. The recovered indicators, an Israeli mailbox used for exfiltration and malware samples uploaded from Israel, indicate a focused interest in Israeli entities and a disciplined, narrowly scoped operational approach rather than broad opportunistic compromise.

Security leadership should prioritize the following actions. First, monitor Microsoft Graph API activity and mailbox audit logs for anomalous calendar operations performed by an application identity. Second, hunt for the specific artifacts described in this report, including far-future calendar events dated 2050-05-13 and File{n}.txt attachments. Third, audit and restrict OAuth2 client-credential application registrations in Entra ID, alerting on newly created client secrets. Fourth, deploy DNS monitoring capable of detecting tunneling behavior, such as unusually frequent AAAA queries or high-entropy subdomains.

This campaign reinforces the need for continuous visibility into cloud identity and application behavior, not just network and endpoint telemetry. The combination of trusted-service abuse, hybrid encryption, and a secondary DNS-based credential channel makes HOLLOWGRAPH one of the more sophisticated Microsoft 365 abuse techniques observed to date. Organizations that lack cloud application governance and Graph API monitoring accept material risk of undetected espionage activity within their environment.

Why It Matters

The use of trusted cloud services as covert command-and-control infrastructure is not a new idea, but HOLLOWGRAPH reflects a steady maturation of a technique that has been evolving for years. Early examples of this approach used services like Twitter, Dropbox, and Google Docs as simple beacon or dead-drop channels, largely because free-tier APIs were easy to abuse and rarely monitored. As enterprises consolidated around Microsoft 365 and Google Workspace for daily business operations, threat actors followed that shift, recognizing that traffic to Graph API endpoints, SharePoint, or Gmail is functionally invisible against the baseline of ordinary corporate activity.

Nation-state groups, including Iranian-nexus actors like OilRig and its sub-groups, have progressively refined this model, moving from single-purpose beaconing toward fully modular frameworks such as Cavern that support multiple communication channels, credential lifecycle management, and encryption schemes independent of the transport layer itself. HOLLOWGRAPH's dead-drop calendar model, layered DNS-based credential refresh, and per-direction key separation represent the current state of that evolution: an implant designed from the ground up to have no direct, visible relationship to attacker infrastructure during its primary function.

Looking forward, this trajectory is likely to accelerate rather than plateau. As organizations harden traditional network perimeters and endpoint defenses, adversaries have a clear incentive to keep pushing C2 logic into the identity and SaaS layer, where detection tooling is comparatively immature and where an attacker only needs one compromised account or one over-permissioned application to persist indefinitely. CTOs and CISOs should expect more variants that blend legitimate SaaS platforms, secondary side channels like DNS or messaging APIs, and strong per-channel

encryption, which means identity governance, application permission audits, and behavioral analytics on cloud API usage are shifting from a defense-in-depth nicety to a core requirement of enterprise security architecture.

How to Respond

- Strictly adhere to cybersecurity fundamentals and ensure all personnel undergo annual phishing and social engineering training. Speak with your UltraViolet Cyber TAM Representative to schedule a live phishing engagement.
- Review OAuth2 client-credential app registrations in Entra ID, alert on newly created client secrets, and flag applications with broader Graph permissions than their function requires.
- Perform annual tech refresh reviews to gain a holistic understanding of your infrastructure. Speak with your UltraViolet Cyber TAM Representative to schedule a Red Team or Purple Team engagement to gain insight into the vulnerabilities in your environment.

What UltraViolet Cyber is Doing

- Tracking new CVEs and high impact vulnerabilities, analyzing and deploying public Proof-Of-Concept code against custom built targets.
- Proactively enabling custom detections based on the collected artifacts, tactics, techniques, and procedures identified in this activity.
- Performing hypothesis driven threat hunts based on threat actor behavior and artifacts. UVCyber customers will be informed of the results through secure channels.
- Parsing available victim dump data for any social, financial, business, or technical relations to UVCyber Clients and partner organizations.
- Aggregating threat intelligence from myriad sources and applying the most up-to-date knowledge to proactive threat hunting and response.

About UltraViolet Cyber

UltraViolet Cyber is a leading tech-enabled managed security services provider, delivering unparalleled cybersecurity expertise that fills technology and talent gaps across Global 2000 and Federal Government customers. Founded and operated by security practitioners from the national intelligence community, UltraViolet Cyber connects offensive security, application security, detection and response, and security engineering to deliver a differentiated approach to cybersecurity operations. Transforming customers' security programs, UltraViolet Cyber's flagship security-as-a-service solution, UV Lens, removes complex operational silos, replacing them with integrated security capabilities. UltraViolet is headquartered in McLean, Virginia with technology centers across the world.

443.351.7630 / info@uvcyber.com | UltraViolet Cyber | @uv_cyber

---