INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-23 13:40 UTC

GopherWhisper APT Abuses Microsoft 365, Slack, and Discord as C2 Channels Against Mongolian Government

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0208
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Microsoft 365 Outlook (Microsoft Graph API), Slack, Discord, File.io; Mongolian government entities (at least 12 confirmed systems, additional unidentified victims)
Published	2026-04-23T08:06:18
Discovery Source	Rss

Executive Summary

A newly identified threat group, GopherWhisper, assessed by ESET Research as operating in alignment with Chinese state interests, has compromised at least 12 systems within a Mongolian government institution by routing malware communications through Microsoft 365 Outlook, Slack, and Discord - platforms most organizations trust and do not inspect deeply. ESET Research recovered extensive command-and-control message evidence confirming an active, sustained intrusion campaign. Organizations in government, defense, and diplomatic sectors that rely on these platforms face elevated risk of undetected long-term compromise.

Technical Analysis

GopherWhisper operates a custom Go-based malware toolkit that communicates exclusively through legitimate cloud services: Microsoft Outlook via the Microsoft Graph API (T1071.003, T1102.002), Slack, Discord, and the file-sharing service File.io. This technique, Living off Trusted Sites (LoTS), blends C2 traffic into normal enterprise cloud communications, bypassing network-layer detection that relies on domain reputation or TLS inspection of known-malicious endpoints. No CVEs are associated with this campaign; the attack is technique-driven. Associated CWEs include CWE-798 (hardcoded credentials potentially used in Graph API authentication) and CWE-506 (embedded malicious code). ESET confirmed infections on at least 12 systems within a Mongolian government institution, with evidence of additional unidentified victims. MITRE ATT&CK techniques include: T1078 (Valid Accounts), T1136.003 (Cloud Account creation), T1027 (Obfuscated Files),

T1102 (Web Service for C2), T1560.001 (Archive via Utility), T1583.006 (Web Services acquisition), T1059/T1059.003 (Command Scripting), T1055.012 (Process Hollowing), and T1041 (Exfiltration over C2). No patch exists; mitigation is detection- and policy-based. Attribution to Chinese state interests is ESET Research's assessment based on targeting profile and tooling characteristics, assessed with medium-to-high confidence.

Action Checklist

1. Step 1: Containment, Audit Microsoft Graph API OAuth application registrations in your Azure AD / Entra ID tenant. Revoke any unrecognized third-party app permissions to Mail.Read, Mail.Send, or Calendars scopes. Review Slack and Discord workspace integrations and remove unrecognized bots or webhook connections. Block File.io at the network perimeter if it is not a business-required service.
2. Step 2: Detection, Query Microsoft 365 Unified Audit Log for Mail.Read and Mail.Send Graph API activity from non-standard application client IDs. Search Slack and Discord audit logs for bot account creation or abnormal API call volumes from unfamiliar IP ranges. Hunt for Go-compiled binaries by examining PE/ELF section names for .gopclntab or using strings output to identify Go runtime artifacts, executing from user-writable paths. Look for process hollowing indicators (T1055.012): child processes spawned with mismatched parent image paths. Review endpoint telemetry for outbound HTTPS connections to graph.microsoft.com, slack.com, discord.com, and file.io from non-user-initiated processes.
3. Step 3: Eradication, Remove identified malicious OAuth app registrations from Entra ID. Terminate and delete attacker-created cloud accounts (T1136.003). Wipe and reimage confirmed infected endpoints; do not rely on AV-only remediation given process hollowing use. Rotate all service account credentials and Graph API tokens associated with affected tenants. Revoke and reissue any OAuth tokens linked to suspicious application registrations.
4. Step 4: Recovery, Validate Graph API application inventory against a known-good baseline post-remediation. Monitor for re-registration of similar OAuth apps using Entra ID alerts. Confirm outbound connections to File.io and anomalous API call volumes have ceased. Restore affected systems from verified clean backups taken prior to the assessed initial compromise window (late 2023 onward). Implement Conditional Access policies requiring device compliance for Graph API access.
5. Step 5: Post-Incident, This campaign exposes a gap in cloud application governance: OAuth app registration is often ungoverned and under-logged. Implement a formal OAuth app approval workflow. Enable Microsoft Purview audit logging at the maximum retention tier. Extend network monitoring to flag process-initiated (non-browser) connections to collaboration platforms. Consider implementing MITRE ATT&CK T1102 detection logic in your SIEM as a standing hunt rule.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate immediately to senior IR leadership, legal counsel, and — given confirmed compromise of Mongolian government entities and Chinese state-aligned attribution — national cybersecurity authorities (e.g., CISA for US government entities) if any of the following are met: discovery of active OAuth token issuance within the past 72 hours for the malicious App IDs, evidence that Mail.Read access exposed classified or controlled unclassified information (CUI/PII/PHI triggering breach notification obligations), identification of additional compromised systems beyond the initial 12 confirmed hosts, or any indicator that the intrusion has pivoted to on-premises Active Directory from the Entra ID tenant.
Recovery Notes	Restore affected endpoints only from backup snapshots confirmed to predate the assessed late-2023 initial compromise window; do not restore from snapshots of unknown provenance as GopherWhisper's sustained access means the intrusion dwell time may extend back further than currently confirmed. Post-recovery, maintain 30-day continuous monitoring of Entra ID OAuth consent grant events, Microsoft 365 MailItemsAccessed Graph API activity, and process-initiated outbound HTTPS to Slack, Discord, and file.io to detect any re-establishment of C2 channels via newly registered applications or re-compromised accounts. Verify integrity of restored systems using Sysinternals Autoruns and file hash comparisons against vendor-provided baseline hashes before returning endpoints to production, given GopherWhisper's use of process hollowing which may survive superficial remediation.
Forensic Artifacts	Microsoft 365 Unified Audit Log — MailItemsAccessed and Send operation records filtered on non-standard Graph API client IDs: these directly document GopherWhisper's use of Outlook/Graph API as a C2 polling channel and will show the specific AppId, ClientIP, and timestamp of each of the 9,000+ recovered C2 transactions. | Entra ID Audit Logs — Application registration events, OAuth delegated permission grant events (specifically Mail.Read, Mail.Send, Calendars scopes), and service principal creation timestamps: these establish the timeline of when GopherWhisper implanted its cloud persistence mechanism in the tenant. | Sysmon Event ID 1 (Process Create) and Event ID 3 (Network Connection) logs from infected endpoints — specifically: Go-compiled binary execution from %AppData%, %Temp%, or %LocalAppData% paths, and outbound HTTPS connections from that process to graph.microsoft.com, slack.com, discordapp.com, and file.io, confirming endpoint-side C2 beacon activity. | Windows Memory Forensics (WinPmem/Magnet RAM Capture) from hollowed processes — process hollowing (T1055.012) leaves the legitimate host process (e.g., a system binary) with a remapped memory image containing the Go malware payload; memory forensics will show a mismatched on-disk PE hash versus in-memory PE image, confirming the injection technique. | Proxy or firewall logs showing historical outbound connections to file.io — GopherWhisper used File.io for payload staging and possibly data exfiltration; URI patterns in web proxy logs (e.g., POST requests to file.io/api/v1/file with large content-length values) will establish the file transfer timeline and potentially recover staging artifact metadata.

Per-Action IR Details

Step 1: Containment — Audit Microsoft Graph API OAuth application registrations in your Azure AD / Entra ID tenant. Revoke any unrecognized third-party app permissions to Mail.Read, Mail.Send, or Calendars scopes. Review Slack and Discord workspace integrations and remove unrecognized bots or webhook connections. Block File.io at the network perimeter if it is not a business-required service.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: NIST IR-4 (Incident Handling), NIST AC-3 (Access Enforcement), NIST AC-17 (Remote Access), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 6.2 (Establish an Access Revoking Process)

Compensating: Export Entra ID OAuth app registrations via PowerShell: `Get-AzureADServicePrincipal -All $true | Select DisplayName, AppId, ReplyUrls | Export-Csv oauth_audit.csv`. Cross-reference each AppId against your known-good application list. For Slack, navigate to api.slack.com/apps and audit installed apps manually; revoke tokens for unknown entries. For Discord, use the Server Settings > Integrations panel to identify and remove unrecognized webhooks or bots. Block file.io at the perimeter firewall or proxy using a deny rule on the FQDN; on Linux endpoints use iptables: `iptables -A OUTPUT -d file.io -j DROP`.

Evidence: Before revoking any OAuth apps, export the full Entra ID audit log for the 90-day maximum retention window via the Azure Portal (Entra ID > Audit Logs > Export) or via `Get-AzureADAuditDirectoryLogs` — capture specifically: application registrations, OAuth permission grants (consent events), and service principal creation timestamps tied to Mail.Read, Mail.Send, or Calendars scopes. Screenshot or export the Entra ID App Registrations blade showing all apps with delegated Graph API permissions before removal. Capture Slack audit logs (available via Slack Admin > Audit Logs API for Enterprise Grid) for bot account creation events and webhook registration timestamps. Capture Discord server audit logs showing bot additions and webhook creation events. Preserve firewall or proxy logs showing historical outbound connections to file.io, graph.microsoft.com, slack.com, and discordapp.com from non-browser process user-agents.

Step 2: Detection — Query Microsoft 365 Unified Audit Log for Mail.Read and Mail.Send Graph API activity from non-standard application client IDs. Search Slack and Discord audit logs for bot account creation or abnormal API call volumes from unfamiliar IP ranges. Hunt for Go-compiled binaries (PE or ELF) executing from user-writable paths. Look for process hollowing indicators (T1055.012): child processes spawned with mismatched parent image paths. Review endpoint telemetry for outbound HTTPS connections to graph.microsoft.com, slack.com, discord.com, and file.io from non-user-initiated processes.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST IR-4 (Incident Handling), NIST IR-5 (Incident Monitoring), NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: Query the Microsoft 365 Unified Audit Log via the Compliance Center or PowerShell using `Search-UnifiedAuditLog -Operations 'Send','MailItemsAccessed' -StartDate (Get-Date).AddDays(-90)` and filter results for AppId values not matching known Microsoft first-party IDs (e.g., not '00000002-0000-0ff1-ce00-000000000000'). Deploy Sysmon with a configuration that captures Event ID 1 (Process Create) and Event ID 3 (Network Connection) — filter Event ID 3 for connections to graph.microsoft.com, slack.com, discordapp.com, and file.io originating from non-browser processes (exclude chrome.exe, msedge.exe, firefox.exe). Use Sysmon Event ID 8 (CreateRemoteThread) and Event ID 25 (ProcessTampering) to detect process hollowing (T1055.012). For Go binary hunting, use the Sigma rule 'Suspicious Execution from User-Writable Directory' adapted for paths: %AppData%, %Temp%, %LocalAppData%, C:\Users*\Downloads. Use YARA rule targeting Go binary PE characteristics: MZ header with '.go' section names or 'runtime.main' string present in the binary.

Evidence: Collect Microsoft 365 Unified Audit Log entries for the MailItemsAccessed, Send, and FileAccessed operations exported as CSV from the M365 Compliance Center — these will show the specific Graph API client IDs used by GopherWhisper's malware to poll Outlook for C2 instructions. Capture Sysmon Event ID 1 logs showing Go-compiled binary execution from user-writable paths (look for binaries with no digital signature, unusual ImageFileVersionInfo, or section names consistent with Go runtime). Collect Sysmon Event ID 3 network connection logs showing HTTPS (port 443) connections to graph.microsoft.com, slack.com, discordapp.com, and file.io where the initiating process is not a recognized browser or email client. Collect Windows Security Event Log Event ID 4688 (Process Creation with command line) filtering for child processes spawned by the suspected hollowed parent process. Capture memory dumps of suspicious processes showing mismatched parent-child image paths for later process hollowing validation.

Step 3: Eradication — Remove identified malicious OAuth app registrations from Entra ID. Terminate and delete attacker-created cloud accounts (T1136.003). Wipe and reimage confirmed infected endpoints; do not rely on AV-only remediation given process hollowing use. Rotate all service account credentials and Graph API tokens associated with affected tenants. Revoke and reissue any OAuth tokens linked to suspicious

application registrations.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST IR-4 (Incident Handling), NIST SI-2 (Flaw Remediation), NIST IA-4 (Identifier Management), NIST AC-2 (Account Management), CIS 5.3 (Disable Dormant Accounts), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts)

Compensating: Remove malicious OAuth app registrations via Entra ID Portal (App Registrations > select app > Delete) or PowerShell: `Remove-AzureADApplication -ObjectId `. Enumerate and delete attacker-created accounts with: `Get-AzureADUser -All $true | Where-Object {$_.CreatedDateTime -gt '2023-10-01'} | Select DisplayName, UserPrincipalName, CreatedDateTime` — review all accounts created after the assessed late-2023 initial compromise window. Revoke all active OAuth refresh tokens for the affected tenant with: `Revoke-AzureADUserAllRefreshToken -ObjectId `. For endpoint reimaging without enterprise MDM, use a verified offline installation media and restore from the last known-clean backup snapshot predating October 2023. After reimaging, use Sysinternals Autoruns to validate no persistence mechanisms survived; export results to CSV for comparison against a clean baseline.

Evidence: Before reimaging endpoints, collect a full disk image using open-source tools (e.g., `dc3dd` or FTK Imager Lite) to preserve forensic evidence of the Go-compiled malware binary, hollowed process memory, and any staging artifacts written to user-writable paths. Capture volatile memory using WinPmem or Magnet RAM Capture before shutdown to preserve in-memory indicators of process hollowing (T1055.012) and loaded malicious modules. Export the complete Entra ID application and service principal list, consent grant history, and sign-in logs for the identified malicious App IDs before deletion. Collect all OAuth token issuance records from Entra ID sign-in logs filtered on the suspicious AppId values. Preserve copies of any files downloaded from or uploaded to file.io by the malware, retrievable from endpoint download history, browser cache, or proxy logs.

Step 4: Recovery — Validate Graph API application inventory against a known-good baseline post-remediation. Monitor for re-registration of similar OAuth apps using Entra ID alerts. Confirm outbound connections to File.io and anomalous API call volumes have ceased. Restore affected systems from verified clean backups taken prior to the assessed initial compromise window (late 2023 onward). Implement Conditional Access policies requiring device compliance for Graph API access.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST SI-7 (Software, Firmware, and Information Integrity), NIST CP-9 (System Backup), NIST CM-2 (Baseline Configuration), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Establish a known-good OAuth app baseline by exporting the current Entra ID App Registrations post-remediation to CSV and storing it in version control (git). Configure Entra ID diagnostic settings to stream audit logs to a Log Analytics Workspace (free tier available) and create an alert rule on 'Add application' and 'Add delegated permission grant' operations. For continuous monitoring without SIEM, schedule a weekly PowerShell task: `Search-UnifiedAuditLog -Operations 'Add service principal.','Consent to application.' -StartDate (Get-Date).AddDays(-7)` and diff output against the baseline CSV. Verify cessation of file.io traffic using firewall deny-rule hit counters or by querying proxy logs: `grep 'file.io' /var/log/squid/access.log | tail -100`. Implement Entra ID Conditional Access by navigating to Entra ID > Security > Conditional Access > New Policy, targeting 'All cloud apps', requiring 'Compliant device' as a grant control.

Evidence: Capture a post-remediation snapshot of the Entra ID App Registrations and OAuth permission grants to serve as the new clean baseline; store with a timestamp and hash for integrity verification (sha256sum on the exported CSV). Collect firewall and proxy logs for 72 hours post-recovery to confirm no resumed outbound connections to file.io, graph.microsoft.com from non-user processes, or discordapp.com/slack.com from non-browser processes — absence of these connections is confirmatory evidence of successful eradication. Pull Microsoft 365 Unified Audit Log entries for MailItemsAccessed and Send operations filtered on any AppId matching the previously identified malicious registrations for 30 days post-recovery to confirm no continued mail exfiltration via a re-registered app.

Step 5: Post-Incident — This campaign exposes a gap in cloud application governance: OAuth app registration is often ungoverned and under-logged. Implement a formal OAuth app approval workflow. Enable Microsoft Purview audit logging at the maximum retention tier. Extend network monitoring to flag process-initiated (non-browser) connections to collaboration platforms. Consider implementing MITRE ATT&CK T1102 detection logic in your SIEM as a standing hunt rule.

NIST Phase: Post Incident

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

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST AU-11 (Audit Record Retention), NIST AU-12 (Audit Record Generation), NIST SI-4 (System Monitoring), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 8.2 (Collect Audit Logs)

Compensating: Enable Microsoft Purview Audit (Premium) log retention to 1 year via the M365 Compliance Center > Audit > Audit retention policies — this captures MailItemsAccessed events required to detect GopherWhisper-style Graph API mail polling that are absent in Audit Standard. For T1102 (Web Service C2) detection without a commercial SIEM, deploy the open-source Sigma rule 'Suspicious Process Initiated Network Connection to Collaboration Platform' using sigmac to convert to a Sysmon XML filter targeting Event ID 3 connections to slack.com, discordapp.com, and graph.microsoft.com from non-whitelisted process images. Implement an OAuth app approval workflow using Entra ID's built-in 'Admin consent required' setting (Entra ID > Enterprise Applications > User Settings > Users can consent to apps accessing company data on their behalf: No) so all new app registrations require explicit administrator approval. Document lessons learned in a structured after-action report referencing GopherWhisper TTPs mapped to MITRE ATT&CK T1102, T1055.012, T1136.003, and T1071.001.

Evidence: Compile the complete post-incident evidence package: the Entra ID audit log showing the full OAuth app registration and consent grant timeline for the malicious applications; all Sysmon Event ID 1 and Event ID 3 logs from affected endpoints showing Go binary execution and C2 beaconing to Graph API, Slack, Discord, and file.io; the Microsoft 365 Unified Audit Log export documenting the 9,000+ C2 message transactions via MailItemsAccessed and Send operations; memory and disk forensic images from all 12 confirmed compromised systems; and the Entra ID sign-in logs showing authentication events for attacker-created cloud accounts (T1136.003). Preserve this evidence package per NIST AU-11 (Audit Record Retention) for a minimum retention period consistent with your organization's incident records policy and any applicable government sector regulatory requirements.

Detection Guidance

Primary detection surface is cloud API audit logs, not endpoint AV. Query Microsoft 365 Unified Audit Log for Graph API operations (Mail.Read, Mail.Send, Files.ReadWrite) initiated by application client IDs not in your approved inventory. Flag any OAuth application granted these scopes by a non-admin user. In Entra ID, alert on new app registrations and service principal creations outside change-control windows. On endpoints, hunt for Go-compiled binaries by examining PE/ELF section names for .gopclntab or using strings output to identify Go runtime artifacts, executing from %APPDATA%, %TEMP%, or user-writable directories. Behavioral: alert on processes initiating HTTPS connections to graph.microsoft.com, discord.com, slack.com, or file.io where the initiating process image is not a recognized browser or productivity application. For process hollowing (T1055.012), look for CreateRemoteThread or NtWriteVirtualMemory calls from processes with mismatched parent-child image paths. SIEM rule suggestion: alert on any non-browser process making repeated HTTPS POST requests to graph.microsoft.com/v1.0/me/sendMail. No public IOC list (IPs, hashes, domains) has been confirmed in source reporting; treat behavioral indicators as primary detection layer.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`graph.microsoft.com`	Microsoft Graph API used as C2 channel for Outlook-based command routing — flag non-browser process connections	HIGH
DOMAIN	`file.io`	Used for file exfiltration and payload staging by GopherWhisper toolkit	HIGH
DOMAIN	`slack.com`	Slack API used as secondary C2 channel; flag process-initiated (non-Slack-client) API connections	HIGH
DOMAIN	`discord.com`	Discord API used as secondary C2 channel; flag process-initiated API connections from non-Discord executables	HIGH

Framework Mappings

MITRE-ATTACK

- **T1078** — Valid Accounts
- **T1136.003** — Cloud Account
- **T1027** — Obfuscated Files or Information
- **T1102** — Web Service
- **T1560.001** — Archive via Utility
- **T1102.002** — Bidirectional Communication
- **T1583.006** — Web Services
- **T1071.003** — Mail Protocols
- **T1059** — Command and Scripting Interpreter
- **T1059.003** — Windows Command Shell
- **T1055.012** — Process Hollowing
- **T1041** — Exfiltration Over C2 Channel

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **CM-7** — Least Functionality
- **SI-7** — Software, Firmware, and Information Integrity

- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection

OWASP-TOP10-2021

- **A07:2021** — Identification and Authentication Failures

CIS-V8

- **16.10** — Apply Secure Design Principles in Application Architectures
- **6.3** — Require MFA for Externally-Exposed Applications
- **8.2** — Collect Audit Logs

ISO-27001-2022

- **A.8.28** — Secure coding
- **A.8.8** — Management of technical vulnerabilities

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication

SOC2-TSC

- **CC6.1** — Logical access security software, infrastructure, and architectures

NIST-CSF-2

- **DE.CM-01** — Networks and network services are monitored

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1078	Valid Accounts	Defense-Evasion
T1136.003	Cloud Account	Persistence
T1027	Obfuscated Files or Information	Defense-Evasion
T1102	Web Service	Command-And-Control
T1560.001	Archive via Utility	Collection
T1102.002	Bidirectional Communication	Command-And-Control
T1583.006	Web Services	Resource-Development
T1071.003	Mail Protocols	Command-And-Control
T1059	Command and Scripting Interpreter	Execution
T1059.003	Windows Command Shell	Execution
T1055.012	Process Hollowing	Defense-Evasion

Technique ID	Technique Name	Tactic
T1041	Exfiltration Over C2 Channel	Exfiltration

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/new-gopherwhisper-ap...	T3
China-Linked GopherWhisper Infects 12 Mongolian Government ...	https://thehackernews.com/2026/04/china-linked-gopherwhisper-infect...	T3
ESET Research discovers new China-aligned group, GopherWhisper	https://www.mycarrollcountynews.com/online_features/press_releases/...	T3
ESET Research discovers new China-aligned group, GopherWhisper	https://www.bakersfield.com/ap/news/eset-research-discovers-new-chi...	T3
APT Group GopherWhisper Leverages Outlook, Slack, and Discord ...	https://www.livethreat.ai/intelligence/new-gopherwhisper-apt-group-...	T3

Generated 2026-04-23 13:40 UTC by TJS Security Command Center