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

Chinese APT Routes C2 Through Outlook, Slack, Discord, and file.io in Targeted Mongolia Espionage Campaign

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0209
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Microsoft Outlook, Slack, Discord, file.io, organizations using these SaaS platforms in government and enterprise environments
Published	2026-04-23T21:00:00
Discovery Source	Rss

Executive Summary

ESET Research has identified GopherWhisper, a China-aligned threat actor, conducting espionage against Mongolian government systems by routing all malicious communications through Microsoft Outlook, Slack, Discord, and file.io. The campaign exploits no software vulnerabilities; instead, it abuses legitimate API access to these widely trusted SaaS platforms, making traffic appear indistinguishable from normal business operations. Organizations without SaaS API monitoring or behavioral detection capabilities face significant blind spots against this technique; conventional network controls, domain blocklists, and TLS inspection policies alone will not detect this activity.

Technical Analysis

GopherWhisper conducts targeted espionage using a Living Off Trusted Sites (LOTS) technique, tunneling all C2 communications through legitimate SaaS APIs: Microsoft Outlook (email API abuse, T1114), Slack (T1102.002 bidirectional C2), Discord (T1102.003), and file.io (T1567.002 exfiltration to cloud storage). Campaign exploits no documented CVEs; exploitation relies entirely on abuse of platform authentication and API mechanisms, not software flaws. Relevant CWEs: CWE-693 (Protection Mechanism Failure) and CWE-441 (Unintended Proxy/Intermediary). MITRE techniques include T1071.001, T1071.003, T1071.004, T1102, T1102.002, T1102.003, T1105, T1027, T1567, T1567.002, and T1114. Attribution is China-aligned per ESET TTP and infrastructure analysis. No patch exists; mitigation requires behavioral detection and SaaS API monitoring. Source: ESET Research via BleepingComputer, Dark Reading, Help Net Security (all T2/T3, source

quality score 0.54; primary ESET research report should be consulted for full IOC and technical detail).

Action Checklist

1. Step 1: Containment, audit OAuth tokens and API integrations granted to Outlook, Slack, Discord, and file.io across your environment; revoke unrecognized or unauthorized application registrations immediately, particularly in government or sensitive enterprise tenants.
2. Step 2: Detection, query email gateway and Microsoft 365 audit logs for unusual Outlook API call patterns (automated send/receive outside business hours, non-human user-agents, large attachment transfers via Graph API); review Slack and Discord audit logs for bot or webhook activity not tied to approved integrations; flag outbound connections to file.io from endpoints that do not have a documented business need.
3. Step 3: Eradication, remove unauthorized API registrations and OAuth grants from all four platforms; rotate credentials for any service accounts with delegated API access; block file.io at the proxy or firewall after confirming no documented business need exists in your organization; enforce application allowlisting for approved SaaS integrations via your IdP.
4. Step 4: Recovery, validate that all removed integrations have not re-registered; monitor SIEM for resumed LOTS-pattern traffic (SaaS API calls with anomalous timing or data volume) for a minimum of 30 days post-remediation; confirm endpoint integrity on systems that accessed the flagged SaaS channels.
5. Step 5: Post-Incident, review gaps in SaaS API visibility; implement Cloud Access Security Broker (CASB) controls if not already in place to inspect and alert on anomalous API usage across sanctioned SaaS platforms; update detection rules to baseline and alert on deviations from normal SaaS communication patterns (MITRE T1102, T1567 detection coverage).

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to senior IR leadership and legal counsel if forensic evidence confirms exfiltration of government-classified, PII, or strategically sensitive data via file.io or Discord webhooks — confirmed data egress from a government or regulated enterprise tenant triggers breach notification obligations under applicable frameworks (FISMA, GDPR, sector-specific) and may require CISA notification under 6 CFR Part 26 if a federal civilian agency is involved.
Recovery Notes	Post-containment, enforce a minimum 30-day heightened monitoring window specifically for new OAuth app registrations and Graph API token issuances in the affected M365 tenant, as GopherWhisper's LOTS tradecraft makes re-entry via a freshly registered app indistinguishable from legitimate SaaS adoption without active consent-policy controls. Validate endpoint integrity on all systems with confirmed or suspected contact with the C2 channels before returning them to production, prioritizing memory forensics over disk forensics given the likelihood of in-memory or Electron-process-injected implants. Coordinate with Microsoft, Slack, and Discord trust-and-safety teams to report the malicious app registrations — platform-side revocation and AppId blocklisting prevents reuse of the same registration against other victim organizations.

Forensic Artifacts	Microsoft 365 Unified Audit Log — MailItemsAccessed and OAuth2:Token records: GopherWhisper's Outlook C2 generates programmatic Graph API token issuances with non-interactive sign-in type and non-Outlook UserAgent strings (e.g., python-requests, Go-http-client); these records are the primary artifact distinguishing automated C2 polling from legitimate user mail access. | Microsoft Entra ID Enterprise Applications audit log — App Registration and OAuth grant creation events: the malicious app registration used by GopherWhisper to gain delegated Mail.ReadWrite or Mail.Send access appears here with creation timestamp, consenting user UPN, and granted permission scopes; this is the key containment and attribution artifact. | Sysmon EventID 22 (DNS Query) and EventID 3 (Network Connection) logs from affected endpoints: captures DNS resolutions and outbound TCP connections to file.io, discord.com/api/webhooks/, and slack.com/api/ initiated by non-browser parent processes, distinguishing GopherWhisper's implant-driven API calls from user-initiated browser traffic. | Slack Audit Logs API (GET /audit/v1/logs) — app_installed and webhook_added action records: documents the timestamp and installing user identity for any Slack app or incoming webhook added during the compromise window that served as a C2 channel; available to Slack Enterprise Grid admins and is the definitive record of unauthorized bot registration on the platform. | Proxy or next-gen firewall egress logs filtered for file.io destinations: captures POST and PUT requests to file.io with source IP, byte count, and timestamp, providing exfiltration volume and timing data specific to GopherWhisper's use of file.io as a dead-drop exfiltration point; byte counts exceeding normal browser-initiated file.io traffic (typically small, infrequent uploads) indicate staged data exfiltration.

Per-Action IR Details

Step 1: Containment — audit OAuth tokens and API integrations granted to Outlook, Slack, Discord, and file.io across your environment; revoke unrecognized or unauthorized application registrations immediately, particularly in government or sensitive enterprise tenants.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy: isolate affected assets and cut off adversary communication channels without destroying evidence

Controls: NIST IR-4 (Incident Handling), NIST AC-2 (Account Management), NIST AC-17 (Remote Access), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 6.2 (Establish an Access Revoking Process)

Compensating: For teams without a CASB or identity governance platform: run Microsoft Graph PowerShell 'Get-MgServicePrincipal | Select DisplayName, AppId, OAuth2PermissionGrants' to enumerate all app registrations in the M365 tenant; export Slack's App Management page (admin.slack.com/apps) and compare against an approved integration list maintained in a spreadsheet; for Discord, audit server integrations via Server Settings > Integrations and document all webhooks. Flag any app with 'Mail.ReadWrite', 'Mail.Send', 'files:read', or 'channels:history' scopes not tied to a named business owner.

Evidence: Before revoking any token, export the full OAuth grant list with timestamps from the Microsoft Entra ID (Azure AD) portal under Enterprise Applications > App Registrations — capture AppId, consentType, principalId, and scope fields. Preserve Slack audit log export (JSON) for the 90-day window covering bot/webhook creation events (action: 'app_installed', 'webhook_added'). Screenshot Discord server integration panel before removal. These records establish the initial access timeline for GopherWhisper's C2 registration and are required for legal hold if espionage is confirmed.

Step 2: Detection — query email gateway and Microsoft 365 audit logs for unusual Outlook API call patterns (automated send/receive outside business hours, non-human user-agents, large attachment transfers via Graph API); review Slack and Discord audit logs for bot or webhook activity not tied to approved integrations; flag outbound connections to file.io from endpoints that do not have a documented business need.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: correlate indicators across multiple log sources to characterize adversary activity and scope

Controls: NIST SI-4 (System Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-2 (Event Logging), CIS 8.2 (Collect Audit Logs), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Without a SIEM: query Microsoft 365 Unified Audit Log via PowerShell — 'Search-UnifiedAuditLog -StartDate -EndDate -RecordType ExchangeItemGroup -Operations SendAs,Send,MailItemsAccessed' and filter for UserAgent strings containing 'python-requests', 'curl', 'axios', or other non-Outlook clients indicative of Graph API programmatic access. For file.io detection on endpoints without EDR, deploy Sysmon with EventID 22 (DNS query) logging and grep Sysmon operational log for queries to 'file.io' or 'files.io'; on Linux endpoints use auditd with '-a always,exit -F arch=b64 -S connect' and parse for connections to file.io's IP ranges. Apply the public Sigma rule 'proc_creation_win_lolbin_susp_web_request_cmd_and_target.yml' to Windows Event Log 4688 captures to catch staging activity.

Evidence: Preserve M365 Unified Audit Log entries (JSON export) for MailItemsAccessed, FileAccessed, and OAuth2:Token operations scoped to the suspected compromise window — GopherWhisper's Outlook C2 leaves MailItemsAccessed records with a non-interactive logon type and programmatic UserAgent. Capture DNS query logs from your recursive resolver or endpoint Sysmon EventID 22 for resolutions to 'file.io', 'discord.com/api/webhooks/', and 'slack.com/api/' from non-browser processes. Export Microsoft Entra ID Sign-In Logs filtering for 'Application' token issuances (TokenIssuanceSuccess) to the affected service principal AppIds identified in Step 1.

Step 3: Eradication — remove unauthorized API registrations and OAuth grants from all four platforms; rotate credentials for any service accounts or user accounts with delegated API access; block file.io at the proxy or firewall if no legitimate business use exists; enforce application allowlisting for approved SaaS integrations via your IdP.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication: eliminate all components of the incident from the environment and close the access vectors used by the adversary

Controls: NIST IR-4 (Incident Handling), NIST AC-2 (Account Management), NIST CM-7 (Least Functionality), NIST SI-2 (Flaw Remediation), CIS 4.7 (Manage Default Accounts on Enterprise Assets and Software), CIS 6.2 (Establish an Access Revoking Process)

Compensating: For IdP allowlisting without an enterprise CASB: in Microsoft Entra ID, enable the 'User consent settings' policy to block all user-initiated OAuth consent and require admin approval for all third-party app registrations — this closes the self-service OAuth grant path GopherWhisper uses for persistence. For file.io blocking without a next-gen proxy, add a DNS sinkhole entry for 'file.io' on your internal resolver (bind9: 'file.io A 0.0.0.0'; Windows DNS: add a stub zone for file.io pointing to 127.0.0.1) and validate with a test curl from an endpoint. Document all removed registrations with their AppId, creation timestamp, and granted scopes in an incident evidence log before deletion.

Evidence: Before rotating credentials, export Azure AD sign-in logs for the compromised service account/user showing all token issuance events tied to the malicious app registration — this captures the full C2 session history. Preserve a timestamped screenshot and JSON export of the malicious app registration detail page (permissions granted, admin consent state, credential certificates/secrets with expiry dates) from Entra ID before deletion, as this is primary attribution evidence linking the registration to GopherWhisper infrastructure. Capture proxy or firewall logs showing historical outbound traffic volume to file.io per source IP to establish data exfiltration volume estimates.

Step 4: Recovery — validate that all removed integrations have not re-registered; monitor SIEM for resumed LOTS-pattern traffic (SaaS API calls with anomalous timing or data volume) for a minimum of 30 days post-remediation; confirm endpoint integrity on systems that accessed the flagged SaaS channels.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery: restore systems to normal operation and verify that threat actor access has been fully removed and has not resumed

Controls: NIST IR-4 (Incident Handling), NIST SI-7 (Software, Firmware, and Information Integrity), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory)

Compensating: Without a SIEM for 30-day monitoring: configure a recurring daily PowerShell task on a jump host — 'Search-UnifiedAuditLog -Operations Add service principal credentials, Add OAuth2PermissionGrant' — and email output to the IR team for manual review; this catches re-registration attempts. For endpoint integrity validation on systems that communicated with GopherWhisper's C2 channels, run Sysinternals Autoruns against those hosts and export to CSV; diff against a known-good baseline to identify persistence mechanisms (scheduled tasks, registry run keys, WMI subscriptions) that a LOTS-enabled implant may have planted during the access window. Use YARA rule scanning (open-source 'yara' binary) against the endpoint file system targeting known GopherWhisper or related China-nexus implant signatures published by ESET.

Evidence: Before declaring recovery complete, collect a full memory image from highest-risk endpoints (those with evidence of file.io or Discord webhook C2 contact) using WinPmem or LiME — LOTS-based implants that communicated via Graph API or webhook may reside only in memory or inject into legitimate browser/Electron processes and leave minimal disk artifacts. Verify M365 Unified Audit Log continuity — confirm no gaps in MailItemsAccessed logging for the affected mailboxes that could indicate log tampering or a secondary access path not yet identified.

Step 5: Post-Incident — review gaps in SaaS API visibility; implement Cloud Access Security Broker (CASB) controls if not already in place to inspect and alert on anomalous API usage across sanctioned SaaS platforms; update detection rules to baseline and alert on deviations from normal SaaS communication patterns (MITRE T1102, T1567 detection coverage).

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: conduct lessons learned, update detection capabilities, and share intelligence to prevent recurrence

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST SI-4 (System Monitoring), NIST AU-2 (Event Logging), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 8.2 (Collect Audit Logs)

Compensating: Without a commercial CASB: implement open-source detection coverage for MITRE T1102 (Web Service C2) and T1567 (Exfiltration to Web Service) using Sigma rules — specifically adapt 'net_connection_win_discord_api.yml' and create a custom rule firing on Sysmon EventID 3 (Network Connection) where Image is not a browser process and DestinationHostname matches 'discord.com', 'slack.com', or 'file.io'; submit rules to the SigmaHQ community repository for peer review. For CASB-equivalent API baselining without budget, enable Microsoft Defender for Cloud Apps (included in M365 E5/A5 or as a standalone trial) and configure an anomaly detection policy scoped to OAuth app activity — this provides GopherWhisper-relevant alerts on impossible travel, mass download, and API call rate anomalies at no incremental cost for eligible tenants.

Evidence: For the lessons-learned record, compile the full timeline from Entra ID and M365 audit logs showing first malicious app registration date versus first detection date — this gap quantifies dwell time and is the primary metric for assessing detection program effectiveness against LOTS-based campaigns. Contribute sanitized IOCs (malicious AppIds, OAuth scope combinations, UserAgent strings) to your sector ISAC and to ESET's public threat intelligence channels to support broader detection of GopherWhisper infrastructure reuse across other targeted organizations.

Detection Guidance

Detection must focus on behavioral anomalies in SaaS API usage rather than network destination blocking. Key signals: (1) Microsoft 365 / Outlook, audit logs (UnifiedAuditLog) showing Graph API calls from non-interactive sign-ins, automated mail send/receive at unusual intervals, or mail rule creation (T1114); query for MailItemsAccessed and Send operations outside expected user behavior baselines. (2) Slack, audit logs showing new bot or webhook creation, high-frequency automated message activity, or OAuth app grants not in your approved list. (3) Discord, outbound HTTPS to discord.com or discordapp.com from endpoints with no documented business need; webhook POST activity. (4) file.io, outbound HTTPS to file.io from corporate endpoints; flag any upload (POST) or download (GET) from this service on networks where it has not been

approved. Behavioral indicators: C2 beaconing presents as low-volume, periodic API calls blending with legitimate SaaS traffic. UEBA tools tuned to SaaS API call frequency and volume deviations are the most effective detection layer. MITRE coverage gaps to close: T1102, T1102.002, T1102.003, T1567, T1567.002.

Note on IOCs: As of current sourcing, ESET has not publicly released specific IOC hashes or IPs for GopherWhisper. Consult the ESET Research blog directly for updated indicator releases. Detection should prioritize behavioral anomalies over hash or IP-based indicators.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`file.io`	Cloud file transfer service abused by GopherWhisper for data exfiltration (T1567.002); flag outbound connections from enterprise endpoints with no approved business use	MEDIUM
DOMAIN	`discord.com`	Legitimate Discord infrastructure abused for C2 bidirectional communication (T1102.003); flag from endpoints without documented business need	MEDIUM
DOMAIN	`discordapp.com`	Alternate Discord domain used for webhook and API communications; same detection context as discord.com	MEDIUM
DOMAIN	`slack.com`	Legitimate Slack infrastructure abused for bidirectional C2 (T1102.002); anomalous API or webhook activity should be correlated against approved integrations	MEDIUM
URL	`https://graph.microsoft.com`	Microsoft Graph API endpoint abused via Outlook for C2 and possible email collection (T1114, T1102); monitor for non-interactive or automated access patterns deviating from user baselines	MEDIUM

Framework Mappings

MITRE-ATTACK

- **T1567.002** — Exfiltration to Cloud Storage
- **T1102.002** — Bidirectional Communication
- **T1567** — Exfiltration Over Web Service
- **T1105** — Ingress Tool Transfer
- **T1102** — Web Service
- **T1102.003** — One-Way Communication

- **T1027** — Obfuscated Files or Information
- **T1071.004** — DNS
- **T1071.003** — Mail Protocols
- **T1071.001** — Web Protocols
- **T1114** — Email Collection

NIST-800-53R5

- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SC-13** — Cryptographic Protection

HIPAA-SECURITY

- **164.312(e)(1)** — Transmission Security

CIS-V8

- **8.2** — Collect Audit Logs

NIST-CSF-2

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

ISO-27001-2022

- **A.5.23** — Information security for use of cloud services

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1567.002	Exfiltration to Cloud Storage	Exfiltration
T1102.002	Bidirectional Communication	Command-And-Control
T1567	Exfiltration Over Web Service	Exfiltration
T1105	Ingress Tool Transfer	Command-And-Control
T1102	Web Service	Command-And-Control
T1102.003	One-Way Communication	Command-And-Control
T1027	Obfuscated Files or Information	Defense-Evasion
T1071.004	DNS	Command-And-Control
T1071.003	Mail Protocols	Command-And-Control
T1071.001	Web Protocols	Command-And-Control

Technique ID	Technique Name	Tactic
T1114	Email Collection	Collection

Sources

Source	URL	Tier
Security News	https://www.darkreading.com/cyberattacks-data-breaches/chinese-apt-...	T3
New GopherWhisper APT group abuses Outlook, Slack, Discord for ...	https://www.bleepingcomputer.com/news/security/new-gopherwhisper-ap...	T3
GopherWhisper APT group hides command and control traffic in ...	https://www.helpnetsecurity.com/2026/04/23/gopherwhisper-apt-group/	T3
ESET Research discovers new China-aligned group, GopherWhisper	https://www.mycarrollcountynews.com/online_features/press_releases/...	T3
A China-aligned APT, GopherWhisper, targeted Mongolian ...	https://www.facebook.com/thehackernews/posts/%EF%B8%8F-a-china-alig...	T3

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