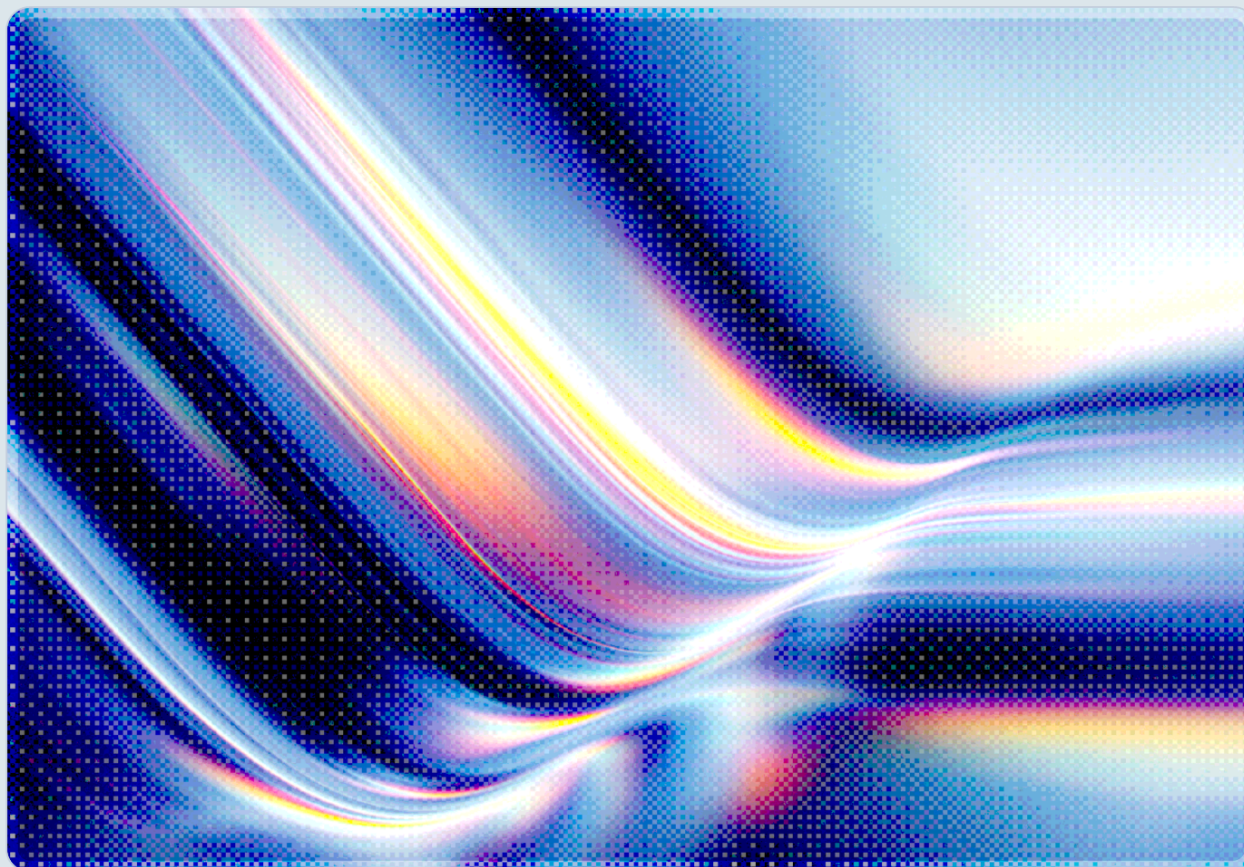


Antino Backdoor: China-Nexus Espionage Through Microsoft 365 C2

Security Implications and Guidance

2026-10-04

 AI-assisted Rapid Research



© 2026 Cloud Security Alliance. Some rights reserved.

You may download, store, display, view, print, redistribute, and link to this document in its original, unmodified form, provided that attribution to the Cloud Security Alliance is maintained and all trademark and copyright notices remain intact.

This document may not be modified or altered. You may quote portions of the document as permitted by the Fair Use provisions of the United States Copyright Act, provided that attribution is given to the Cloud Security Alliance.

This document may be shared on professional and social media platforms in its original form with attribution.

This document was generated with AI assistance and has not undergone official CSA review and approval processes.

Key Takeaways

Cisco Talos reported on September 30, 2026 that a China-nexus actor it tracks as UAT-11587 has run an espionage campaign against government and policy organizations in eight Asian countries since September 2025 [1]. The actor's custom Rust backdoor, Antino, uses no dedicated command-and-control (C2) server after installation. It sends commands through an Outlook mailbox and exchanges heartbeats, tools, and stolen files through OneDrive, using the Microsoft Graph API [1][2].

The main defensive lesson is that this traffic ends at `graph.microsoft.com` and `login.microsoftonline.com`, domains that enterprise networks routinely allow [1]. Domain reputation, egress allow-listing, and IP blocklists therefore give limited help against the post-installation C2 channel. Detection is most likely to succeed at the endpoint: the process that is talking to Microsoft, and the execution chain that put it there.

Talos's report does not say how the actor obtained the Microsoft 365 accounts used for C2 [1]. It does say that the Antino Gen2 implant authenticates with the OAuth 2.0 client-credentials flow, using an Entra ID application registered by the actor [1]. Our analysis, which is an inference and not a Talos finding, is that because those resources sit in the attacker's tenant, a victim organization's own Microsoft Graph activity logs would likely not record the C2 requests (see Security Analysis). Defenders should therefore plan to hunt on endpoint and network telemetry rather than on tenant audit logs.

Antino is not an AI-specific threat. We cover it because it is a current example of the broader pattern of attackers using trusted SaaS and cloud APIs as C2, a pattern that also applies to AI agents and automation holding Graph credentials.

Background

Talos describes UAT-11587 as a China-nexus intrusion set first observed in September 2025, in a spear-phishing campaign aimed at Taiwan's academic, think-tank, and civil-society policy community [1][3]. According to the Talos report, activity ran through July 2026 and affected 15 institutional environments (10 confirmed, 5 probable) and approximately 350 endpoints across Taiwan, India, the Philippines, Cambodia, Pakistan, Thailand, Myanmar, and Syria [1]. Secondary coverage reports that victims included

organizations in defense, national security, diplomacy, law enforcement, legislatures, universities, and think tanks [2]. Other coverage of the same campaign counts victims differently, so this note uses the Talos figures.

Talos attributes the activity to a China-nexus actor with high confidence. The evidence it cites includes Simplified Chinese language metadata, UTC+8 timestamps in phishing headers, build artifacts that reference the Chinese `rsproxy.cn` Rust package mirror, and a focus on Taiwan policy audiences [1] [2]. Talos notes an infrastructure overlap with UNC6384 but tracks the activity separately, and it reports that it could not independently verify a connection to the financially motivated activity of the Jewelbug cluster [1]. Attribution beyond "China-nexus" is therefore unresolved.

The Microsoft Graph API is a legitimate interface that gives applications programmatic access to Outlook mail, OneDrive files, and other Microsoft 365 data. Other malware families have used Microsoft cloud services for C2 before, and Antino extends that broader pattern. The Talos report documents the delivery chain in detail, which shows how the actor combines the C2 channel with a layered, mostly script-based intrusion path.

Security Analysis

Delivery and execution chain

Talos describes a five-stage chain that begins with spear-phishing [1]. The lures are tailored to foreign-affairs, security, and policy audiences, use spoofed sender identities, and embed a replica of a Gmail attachment preview widget built from Base64-encoded images [3]. The attachment retrieves an HTA or WSF stager from Cloudflare Pages, which also hosts an execution-tracking endpoint. Encoded loader stages and decoy documents come from Cloudflare R2, and additional scripts from Amazon CloudFront [2].

The next stages abuse built-in and signed components. A JScript orchestrator decodes and decrypts (Base64 and RC4) .NET gadget resources, then abuses unsafe `BinaryFormatter` deserialization to load a .NET assembly, `TestAssembly.dll`, into the memory of `mshta.exe` [2]. That assembly fetches a decoy document and a three-file payload bundle and launches `GatherOsState.exe`, a Microsoft-signed binary from the Windows Assessment and Deployment Kit. A malicious `slc.dll` placed beside it is loaded through DLL sideloading and runs Antino [2][3]. Because the sideloading host is legitimately signed, signature-based allow-listing alone may not flag it.

Antino capabilities and persistence

Antino is a Rust-compiled Windows backdoor, seen as 32-bit and 64-bit builds in both executable and DLL forms [2]. Its command set covers host reconnaissance, command execution through `cmd.exe` and PowerShell, directory enumeration, file upload and download, process enumeration, in-memory shellcode loading, persistence, and self-termination [2][3]. Some builds include a sleep-masking technique intended to reduce the exposure of recognizable code in memory while secondary payloads are idle [2].

Persistence uses an `HKCU` Run registry value, file staging under `%LOCALAPPDATA%\Windows GatherOSStateKit\`, and abuse of the Windows Scripted Diagnostics framework to run attacker-controlled PowerShell through legitimate Windows components, which obscures the parent process [2] [3].

The Microsoft 365 C2 channel

The channel's design is the campaign's most distinctive feature. The Antino Gen2 implant authenticates to Microsoft Graph using the OAuth 2.0 client-credentials flow, which lets the actor's registered Entra ID application reach the configured Outlook mailbox and OneDrive without an interactive sign-in [1]. Talos reports that the mailbox and OneDrive belong to the threat actor, but it does not explain how those accounts were obtained [1]. The division of labor between the two services is summarized below.

Service	Role	Reported details
Outlook	Commands and responses	Implant polls the mailbox every 10 seconds; command messages use the subject prefix <code>command_req_[session_id]</code> and responses use <code>command_res_[session_id]</code> [1]
OneDrive	Registration, heartbeat, tool delivery, exfiltration	Heartbeat JSON with system telemetry uploaded every minute to <code>/antino/heartbeats/{id}.json</code> ; stolen files to <code>/antino_downloads/</code> ; staged tools in <code>/antino_uploads/</code> [1]

For a victim, this means the post-installation network footprint is limited to TLS connections to Microsoft endpoints. Talos recommends monitoring the Cloudflare Pages, R2, and CloudFront delivery infrastructure and blocking the domains `osc-cdn.com`, `microsoft-flash.com`, and `wps-`

cn.com . It also published hashes, ClamAV signatures, and Snort rules (1:66880–66882) [1]. Those controls address delivery rather than C2, which is the reason endpoint behavior matters more.

Visibility limits for defenders

Microsoft Graph activity logs record HTTP requests that Microsoft Graph processes for a tenant, but they are collected for the resource tenant only and do not show a multitenant application's activity in another tenant [4]. This is our inference from the Talos description, not a finding in the report: because Antino's mailbox, OneDrive, and application registration reside with the actor, the C2 requests would be logged in the actor's tenant and not the victim's. Defenders should assume that tenant-side logging will not reveal this activity and plan accordingly.

Relevance to AI systems

We found no public report that Antino targets or manipulates AI systems. The relevance to AI security is indirect. Agents, copilots, and automation increasingly hold Graph credentials and make frequent calls to Microsoft 365 endpoints, so their traffic is a ready source of cover for malicious use of the same APIs. Organizations that treat "Graph traffic from a process" as inherently benign are exposed to this class of technique and, in addition, will have a harder time baselining legitimate agent behavior.

Indicators for hunting

The behaviors below are CSA's synthesis of details in the Talos report [1] and secondary coverage [2][3]. They are suggested hunting hypotheses, not detections published by Talos.

Behavior	Why it matters
<code>mshta.exe</code> or Windows Script Host retrieving content from Cloudflare Pages, R2, or CloudFront	Stage 1 and 2 delivery [2]
<code>GatherOsState.exe</code> running from a user-writable path next to <code>slc.dll</code>	DLL sideloading of Antino [2][3]
<code>sdiagnhost.exe</code> activity followed by PowerShell or <code>HKCU</code> Run changes	Scripted Diagnostics abuse and persistence [2][3]

Behavior	Why it matters
Non-browser, non-Office processes not on your baselined allow-list connecting to <code>graph.microsoft.com</code> or <code>login.microsoftonline.com</code>	Antino C2 polling at 10-second and one-minute intervals [1]

Recommendations

Immediate Actions

Load the Talos hashes, domains, URLs, ClamAV signatures, and Snort rules into detection tooling and search historical telemetry from September 2025 through July 2026, the period Talos reports for the campaign [1]. Hunt for the process-tree behaviors in the table above, with particular attention to `GatherOsState.exe` outside its expected installation location. Review mail gateway logs for HTA and WSF attachments and for links to Cloudflare Pages and R2 hosts, and consider quarantining those file types at the gateway, as they have few legitimate uses in email in most environments. Organizations in the affected countries and sectors, particularly those serving Taiwan policy, foreign affairs, and defense audiences, should treat this as a priority threat.

Short-Term Mitigations

Constrain script-host execution: block or tightly scope `mshta.exe` and `wscript.exe` for standard users through application control or attack surface reduction rules. Alert on signed Microsoft binaries executing from user-writable directories. Build endpoint detections that flag unexpected processes making sustained, periodic connections to Microsoft Graph and login endpoints, and baseline which sanctioned applications, including AI agents and automation, legitimately do this. Where proxy or EDR telemetry exposes the calling process and its request pattern, use it for hunting, since tenant logs are collected for the resource tenant only and would not cover the actor's tenant [4].

For your own tenant, review Entra application registrations and consented permissions for the same pattern. Application-only Graph permissions that grant access to all mailboxes should be scoped. Microsoft documents Role Based Access Control for Applications in Exchange Online as the mechanism for limiting which mailboxes an application can access [5]. Enable Microsoft Graph activity log collection so that abuse of your own tenant's Graph surface is investigable [4].

Strategic Considerations

The campaign illustrates a structural gap: many programs treat trusted SaaS domains as low risk, yet the same trust is what makes them useful to attackers. Plan detection around identity, process, and behavior, not destination. Document which workloads need Graph access, enforce least-privilege application permissions with periodic review, and treat AI agents and automation service principals as non-human identities subject to the same controls. Also consider that state-sponsored actors may adapt the technique to other SaaS APIs with similar properties, so the behavioral detections above should be written generically (periodic API polling by unexpected processes) instead of Antino-specific.

CSA Resource Alignment

CSA's research note on UNC6508 is the closest prior work in our catalog [6]. It describes a multiyear China-nexus campaign against North American medical research networks in which the actor abused legitimate Google Workspace compliance features to exfiltrate data. The shared theme with Antino is the abuse of trusted SaaS functionality for covert collection and C2, which suggests defenders may want to extend SaaS-abuse hunting beyond a single vendor's platform.

CSA's note on ACR Stealer's ClickFix campaigns addresses a different intrusion path into Microsoft 365, in which stolen browser session tokens give access to document stores [7]. It complements this note: Antino uses attacker-owned Microsoft 365 resources for C2 and does not compromise the victim's, so the two notes together illustrate two contrasting forms of Microsoft 365 abuse, with the attacker inside a victim's tenant and the attacker hiding in plain sight on Microsoft's infrastructure.

As a standing control reference, the AI Controls Matrix (AICM v1.1) offers control objectives in its identity and access management and threat and vulnerability management domains that map to the least-privilege application permissions, non-human identity governance, and monitoring practices recommended above [8].

References

- [1] Cisco Talos (Ashley Shen). "[China-nexus UAT-11587 targets government and policy organizations across Asia with Antino backdoor](#)." Cisco Talos Blog, September 30, 2026.
- [2] eSecurity Planet. "[China-Linked Hackers Use Antino Backdoor in Asia](#)." eSecurity Planet, October 2026.
- [3] The Hacker News. "[Antino Backdoor Uses Outlook and OneDrive for C2 in China-Nexus Espionage Campaign](#)." The Hacker News, October 2, 2026.
- [4] Microsoft. "[Access Microsoft Graph activity logs for tenant monitoring](#)." Microsoft Learn, accessed October 4, 2026.
- [5] Microsoft. "[Role Based Access Control for Applications in Exchange Online](#)." Microsoft Learn, accessed October 4, 2026.
- [6] Cloud Security Alliance. "[UNC6508: A Multiyear China-Nexus Campaign in Medical Research](#)." CSA Labs, 2026.
- [7] Cloud Security Alliance. "[ACR Stealer's ClickFix Campaigns Drain M365 Tokens](#)." CSA Labs, July 2026.
- [8] Cloud Security Alliance. "[AI Controls Matrix \(AICM\) v1.1](#)." Cloud Security Alliance, 2026.