Chinese APT LongNosedGoblin Targets Government Networks in Southeast Asia and Japan

By Written by

Published: 2025-12-19 · Archived: 2026-04-05 15:55:51 UTC

The Chinese APT tracked as LongNosedGoblin represents a highly structured cyberespionage operation focused on government networks in Southeast Asia and Japan. The activity was uncovered during forensic analysis of a compromised government environment, where investigators identified a collection of previously undocumented malware families operating under centralized control. The tooling, delivery mechanisms, and operational pacing observed throughout the campaign indicate a deliberate intelligence collection mission rather than a short-term intrusion or financially motivated attack.

What sets this Chinese APT apart is not a single novel exploit, but the way it combines trusted enterprise mechanisms, selective deployment logic, and a modular malware ecosystem to quietly persist inside sensitive networks. LongNosedGoblin does not rely on loud exploitation frameworks or mass deployment. Instead, it uses reconnaissance-driven decision making to determine which systems warrant deeper compromise, significantly reducing exposure and detection risk.

Initial Discovery and Scope of the Campaign

The campaign was first identified in early 2024 after analysts discovered an unfamiliar backdoor on a workstation belonging to a Southeast Asian governmental entity. Further investigation revealed that this was not an isolated infection. Multiple systems within the same domain had received different malicious payloads, all distributed through Active Directory Group Policy. This immediately suggested that the attackers had already obtained elevated privileges within the domain and were operating with administrator-level access.

Timeline analysis later showed that some components of the operation had been active since at least September 2023. Telemetry collected throughout 2024 and into 2025 indicates multiple waves of activity, including renewed deployments and updated tooling. While most confirmed victims were located in Southeast Asia, at least one later campaign targeted an organization in Japan, demonstrating a geographically consistent but expanding operational focus.

Abuse of Group Policy as a Primary Deployment Mechanism

A defining characteristic of this Chinese APT campaign is its reliance on Group Policy Objects as a malware distribution channel. Group Policy is a core administrative feature in Windows enterprise environments and is implicitly trusted by most organizations. Once domain administrator privileges are obtained, Group Policy provides a powerful and stealthy method to push executables, configuration files, and scripts across a network.

LongNosedGoblin used this mechanism to deploy multiple malware families under filenames designed to blend into the Group Policy cache. Executables were frequently disguised as configuration files, registry policy artifacts,

or system utilities. Because Group Policy updates occur routinely, malicious payloads delivered in this manner are less likely to trigger alarms or attract administrator scrutiny.

This technique also provides built-in persistence. As systems refresh policy settings, malicious components can be redeployed automatically, allowing attackers to maintain access even if individual files are removed.

Reconnaissance-Driven Target Selection

One of the earliest tools deployed across compromised environments was a reconnaissance utility designed to collect browser history from all local user profiles. This component, referred to by researchers as NosyHistorian, was not a backdoor and did not provide interactive control. Instead, its sole purpose was to gather contextual information about how each system was used.

By harvesting browser history from Google Chrome, Microsoft Edge, and Mozilla Firefox, the attackers were able to identify systems associated with sensitive workflows, internal portals, government services, or policy-related research. Collected data was staged internally on network shares rather than immediately exfiltrated to the internet, reducing the likelihood of detection during the reconnaissance phase.

Only a small subset of systems identified through this process were selected for further compromise. This selective escalation strongly suggests that the Chinese APT prioritized intelligence value over coverage, a tradecraft decision typical of long-term espionage operations.

NosyDoor Backdoor Architecture and Execution Flow

Systems selected for deeper access received a custom backdoor known as NosyDoor. This backdoor operates through a multi-stage execution chain designed to evade security controls and blend into normal system activity.

The initial stage is a dropper deployed via Group Policy under filenames that mimic legitimate policy artifacts. This dropper decrypts embedded components and installs them into directories that normally contain Microsoft .NET framework files. Filenames are deliberately chosen to closely resemble legitimate system binaries, increasing the chance they will be overlooked during routine inspection.

The second stage abuses a legitimate Microsoft .NET executable through AppDomainManager injection. By supplying a crafted configuration file, the attackers force the legitimate binary to load a malicious library during initialization. This approach allows malicious code execution without introducing a suspicious process into memory.

During this stage, event tracing and antimalware scanning interfaces are deliberately disabled or bypassed. This prevents script inspection and reduces the visibility of subsequent payload execution.

The final stage is the NosyDoor backdoor itself, a C# application that establishes persistent command and control communication using cloud storage services.

Cloud-Based Command and Control Infrastructure

Rather than operating dedicated command servers, this Chinese APT relies heavily on legitimate cloud platforms for command and control. Observed campaigns used services such as Microsoft OneDrive, Google Drive, and Google Docs to exchange commands, upload stolen data, and maintain task queues.

From a network monitoring perspective, this traffic appears indistinguishable from legitimate user activity. Authentication occurs through valid OAuth tokens, and data transfers use HTTPS connections to well-known cloud providers. This significantly complicates detection, particularly in government environments where cloud services are widely used.

Data Protection Services

NosyDoor encrypts collected system metadata using asymmetric cryptography before uploading it to cloud storage. Commands are delivered in encrypted task files, which are periodically polled and processed by the backdoor. Results are encrypted again before being uploaded as response files, maintaining confidentiality even if cloud storage is inspected.

Capabilities of the NosyDoor Backdoor

Once active, NosyDoor provides full remote control over compromised systems. Supported functionality includes file upload and download, directory enumeration, command execution, assembly loading, and configuration updates. The backdoor also collects detailed system metadata such as operating system version, process architecture, network configuration, and local timestamps.

Operational hours can be configured, allowing the backdoor to remain dormant outside defined time windows. This reduces the chance of detection during off-hours monitoring while still allowing queued commands to be processed when the backdoor resumes activity.

Error handling is implemented locally, with logs written to disk in locations that blend into existing directory structures. These logs can provide operators with feedback on failed operations without generating network noise.

Credential Theft and Data Collection Tooling

In addition to the primary backdoor, LongNosedGoblin deployed several specialized data collection tools. These include browser data stealers, keyloggers, and utilities designed to capture clipboard content, screen activity, and audio recordings.

The browser stealer component targets Chromium-based browsers and extracts stored credentials, cookies, and profile data. Stolen data is archived, encrypted, and exfiltrated using cloud storage APIs. In some cases, data exfiltration is gated by configuration files retrieved from cloud documents, allowing operators to dynamically enable or disable collection on a per-victim basis.

The keylogger component operates in memory and stores encrypted keystroke logs locally. Data is periodically flushed to disk in encrypted form, reducing the risk of detection by real-time monitoring tools.

Additional tooling observed in the environment includes an argument runner used to execute multimedia recording software. This allowed attackers to capture audio and video output from selected systems, indicating an

interest in monitoring internal meetings or restricted workflows.

Use of Downloaders and Secondary Payloads

LongNosedGoblin also deployed a PowerShell-based downloader that executed multi-stage payloads entirely in memory. Each stage is encoded, compressed, and decrypted at runtime, minimizing on-disk artifacts. Antimalware scanning interfaces are explicitly bypassed during execution.

This downloader was used to deploy additional components, including a reverse SOCKS5 proxy that provided interactive network access from within the compromised environment. By tunneling traffic through internal systems, the attackers could reach services not directly exposed to the internet.

Attribution and Malware Sharing Indicators

While the campaign is attributed to a Chinese APT based on targeting, tradecraft, and infrastructure patterns, some components of the toolset appear to be shared across multiple China-aligned operations. Variants of the NosyDoor backdoor have been observed in unrelated incidents using different cloud providers and targeting different regions.

Debugging paths and internal markers suggest that some malware may be developed or distributed commercially within a broader ecosystem. This indicates that certain tools are likely reused, licensed, or sold between operators rather than being exclusive to a single group.

Despite this overlap, the consistent abuse of Group Policy for lateral movement remains a distinguishing characteristic of LongNosedGoblin activity.

Implications for Government Network Defenders

The LongNosedGoblin campaign demonstrates how trusted administrative features can be turned into stealthy attack vectors once domain-level access is achieved. Traditional defenses focused on exploit detection or perimeter monitoring are insufficient against this type of operation.

Defenders should closely audit Group Policy changes, monitor scheduled task creation, and treat cloud service authentication events as potential command and control activity. Domain administrator access must be rigorously protected, as compromise at this level effectively grants attackers full control over deployment mechanisms.

The campaign also highlights the growing role of cloud platforms in modern espionage operations. Visibility into cloud API usage and abnormal access patterns is now as critical as monitoring traditional network traffic.

Closing Analysis

The Chinese APT known as LongNosedGoblin illustrates a mature and disciplined approach to cyberespionage. By combining reconnaissance-driven targeting, abuse of trusted enterprise mechanisms, and cloud-based command infrastructure, the group achieves long-term access with minimal visibility.

This operation reinforces a broader trend in state-aligned threat activity, where success is measured not by rapid exploitation, but by persistence, discretion, and sustained intelligence collection. Organizations responsible for

sensitive government data must assume that administrative tooling and cloud services are potential attack surfaces and adapt their defensive strategies accordingly.
