ET CISO.in
From The Economic Times

China-linked cyber-espionage campaign abuses Azure for covert operations

Operation Dragon Weave is a cyber-espionage campaign tied to a China-based threat actor targeting officials in Czech Republic and Taiwan. Researchers uncovered the operation's methods of using spear-phishing tactics and region-specific decoy documents. The malware employs a cloud-based command-and-control mechanism utilizing Microsoft Azure services for communication. Attackers leverage sophisticated techniques, including multi-layer encryption and sandbox evasion, to achieve their goals.

A targeted cyber-espionage campaign, identified as Operation Dragon Weave, has been assessed with moderate confidence to be linked to a China-based threat actor. The operation targets officials and citizens in the Czech Republic and Taiwan through spear-phishing archives carrying region-specific decoy documents, encrypted malware components and a cloud-hosted command-and-control mechanism designed to blend into legitimate Microsoft Azure activity.

Researchers identified the campaign while monitoring global threat activity after a suspicious ZIP archive was first submitted from Taiwan earlier this year. The archive contained malicious files masquerading as a Traditional Chinese "Project Application Review Result Notification," suggesting targeted delivery to Taiwan-based users. The same operation also used a Czech-language decoy appointment notice impersonating the Czech Social Security Administration, indicating a parallel focus on Czech officials and residents.

The campaign uses two distinct infection paths to reach the same final payload. In the first, a malicious Windows shortcut file disguised as a PDF launches a hidden VBScript and PowerShell sequence. This decrypts a payload container and executes a malicious file. In the second, a Rust-based executable dropper deploys all required components directly, including a decoy PDF, encrypted configuration material and a malicious DLL.

Both paths converge on a DLL sideloading stage. Researchers have named this Rust-based loader RUSTCLOAK. The loader is designed to evade analysis by checking the victim machine name against a list of more than 100 sandbox and researcher-system identifiers.

It then decrypts its final payload through a three-layer routine. Rather than creating a conventional process or writing its final payload visibly to disk, RUSTCLOAK executes the decrypted malware in memory using Windows fibers. This technique enables the campaign to reduce its on-disk footprint and avoid some behavioural patterns commonly monitored by security products.

The final payload, named AZUREVEIL, is a 64-bit Adaptix command-and-control agent capable of remote command execution, file operations, data exfiltration, process discovery, network enumeration, proxying and in-memory execution of Beacon Object Files. Analysis identified 36 post-exploitation commands

supported by the agent, providing attackers with broad capabilities to control infected systems and move through targeted environments.

A key feature of Operation Dragon Weave is its abuse of Microsoft Azure Blob Storage as a dead-drop command-and-control channel. Instead of communicating directly with a traditional attacker-operated server, AZUREVEIL exchanges encrypted tasking and results through an Azure storage container.

The infected device uploads an encrypted beacon, operators place commands in the storage account, and the malware retrieves, executes and returns the results as encrypted blobs.
This cloud-based method helps malicious traffic resemble normal HTTPS activity to a widely used enterprise service. Researchers also identified a hardcoded Shared Access Signature token in the malware configuration that was valid for a full year and granted extensive read, write, delete and upload permissions to the associated storage container.

Operation Dragon Weave highlights how sophisticated threat actors are increasingly abusing legitimate cloud services, familiar file formats and trusted Windows processes to conceal their operations. The use of targeted decoys in Traditional Chinese and Czech, multi-layer encryption, sandbox evasion and Azure-based dead-drop infrastructure indicates a planned espionage operation rather than opportunistic malware distribution.

Organisations, particularly government bodies, research organisations, financial institutions and technology companies, should exercise caution with unexpected archives and files that use double extensions, such as .pdf.lnk, or present executables as documents.

Security teams should monitor unusual PowerShell and VBScript activity, investigate DLL sideloading behaviour, inspect unexpected use of cloud-storage services, and ensure that security controls can detect encrypted or fileless execution chains.