Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

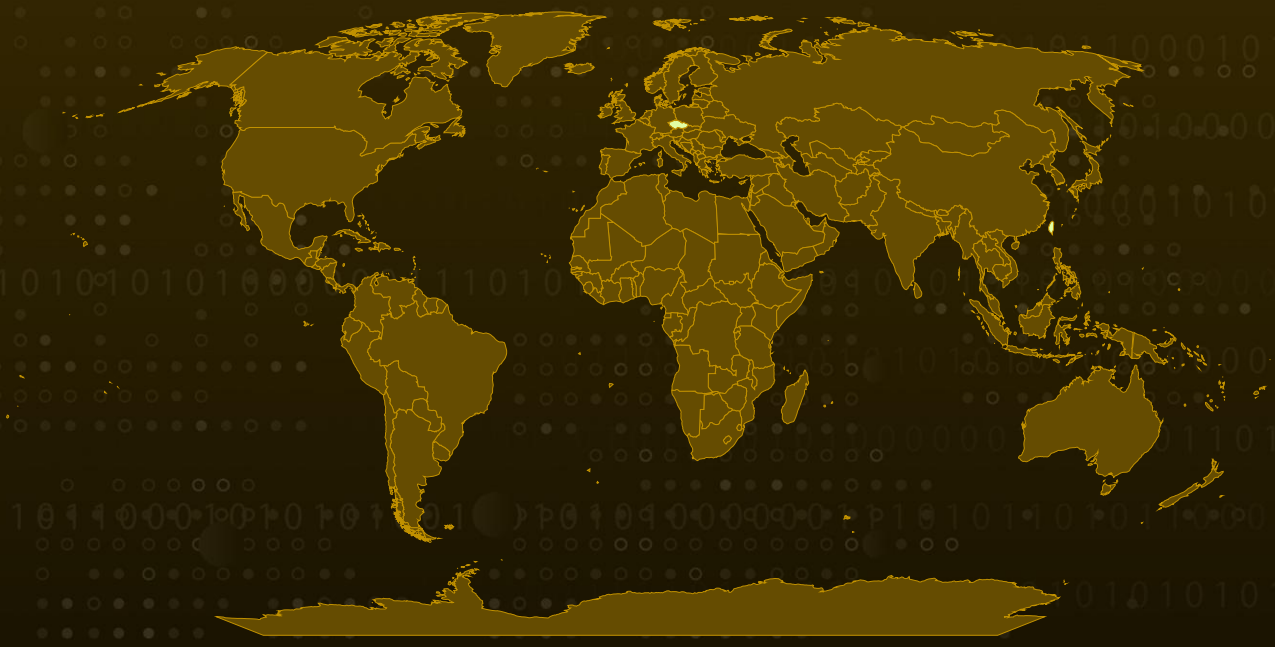
Operation Dragon Weave Spins a Web of Espionage Through Microsoft Azure

Date of Publication	Admiralty Code	TA Number
June 03, 2026	A1	TA2026152

Summary

First Seen: March 2026
Targeted Regions: Czech Republic, Taiwan
Targeted Platform: Windows
Targeted Industries: Government & Public Sector, Research & Academia, Technology & Software, Financial Services
Malware: AZUREVEIL, RUSTCLOAK
Campaign: Operation Dragon Weave
Attack: Operation Dragon Weave is a targeted cyber-espionage campaign aimed at officials and citizens in the Czech Republic and Taiwan. It begins with a spearphishing email carrying a ZIP attachment whose contents masquerade as official government correspondence. The archive offers two interchangeable infection paths, a malicious LNK shortcut and a self-contained Rust-based executable dropper, that both converge on DLL sideloading of a malicious UnityPlayer.dll. That DLL is a Rust loader (RUSTCLOAK) which decrypts and runs the final payload, AZUREVEIL, a 64-bit Adaptix C2 agent. AZUREVEIL is notable for using Microsoft Azure Blob Storage as a dead-drop command-and-control channel, blending its traffic with legitimate cloud activity, and for supporting 36 post-exploitation commands, including in-memory Beacon Object File (BOF) execution.

Attack Regions



Attack Details

#1

A newly identified cyber espionage campaign, dubbed Operation Dragon Weave, has been targeting government officials and citizens in Taiwan and the Czech Republic using an AdaptixC2 agent. The operation begins with spear-phishing emails disguised as legitimate government communications, such as project review notices or appointment notifications. Victims receive a ZIP archive that delivers malware through one of two methods: a malicious Windows shortcut disguised as a PDF document or a Rust-based dropper that extracts the required components onto the system. The use of Traditional Chinese filenames and Czech-language decoy documents highlights the campaign's targeted nature. The earliest known sample linked to the operation was uploaded from Taiwan in March 2026.

#2

In the script-based infection chain, a VBScript launches a hidden PowerShell script that decrypts and reconstructs a malicious executable named RuntimeBroker_update.exe while displaying a decoy document to distract the victim. Both infection methods ultimately execute RuntimeBroker_update.exe, which uses DLL sideloading to load a malicious library called UnityPlayer.dll, also known as RUSTCLOAK. Before running its payload, RUSTCLOAK performs checks to detect sandbox and analysis environments. Researchers also discovered a developer oversight that exposed a Rust build path and the username "dell2" within the malware.

#3

RUSTCLOAK decrypts and launches its final payload, AZUREVEIL, using multiple encryption and evasion techniques. AZUREVEIL is a fully featured AdaptixC2 agent that supports file operations, command execution, shell access, network tunneling, and in-memory execution of additional tools. These capabilities give attackers flexibility for espionage, lateral movement, and maintaining access within compromised environments.

#4

Rather than using traditional command-and-control servers, AZUREVEIL relies on Microsoft Azure Blob Storage for communications. Using HTTPS traffic helps the malware blend in with legitimate cloud activity. The malware periodically uploads encrypted beacons, retrieves encrypted commands, and returns encrypted results through the same storage container. Researchers also identified a hardcoded Shared Access Signature (SAS) token with broad permissions to the Azure storage account. The token remains valid from March 2026 through March 2027, suggesting the infrastructure was designed to support long-term espionage operations and persistent access to victim networks.

Recommendations

Block the Azure Blob Storage C2 Endpoint: Block and alert on outbound connections to the identified dead-drop storage account (note1ggbbhggdwa1[.]blob[.]core[.]windows[.]net) and treat the listed file hashes as high-priority detections across endpoint and network tooling.

Restrict LNK and Script Execution: Block execution of unexpected LNK shortcut files and unsigned binaries delivered via email, and constrain wscript.exe and PowerShell so that script-based dropper chains cannot run silently from user-writable directories.

Constrain PowerShell Execution-Policy Bypass: Restrict or closely monitor PowerShell invocations that use execution-policy bypass and hidden-window flags, since the campaign relies on this pattern to run its decryption stage without user visibility.

Hunt for DLL Sideloading of UnityPlayer.dll: Hunt for RuntimeBroker_update.exe and BrowserViewUtility.exe loading a UnityPlayer.dll from non-standard, user-writable paths, which is the convergence point for both infection paths.

Monitor Suspicious File Creation in %LOCALAPPDATA% and %TEMP%: Detect creation of the campaign's staged artifacts (1.dat, Com.dat, RuntimeBroker_update.exe, and related components) in %LOCALAPPDATA%\WebViewFixUtility and %TEMP%, and isolate hosts where these patterns appear.

Strengthen Spearphishing Defenses: Reinforce email filtering for ZIP attachments containing LNK or executable files, and deliver targeted user-awareness training for government, research, technology, and financial-services staff in the affected regions on double-extension lures and fake official-document themes.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1566: Phishing	T1566.001: Spearphishing Attachment
Execution	T1204: User Execution	T1204.002: Malicious File
	T1059: Command and Scripting Interpreter	T1059.001: PowerShell
		T1059.005: Visual Basic
Defense Evasion	T1574: Hijack Execution Flow	T1574.001: DLL
	T1027: Obfuscated Files or Information	
	T1497: Virtualization/Sandbox Evasion	T1497.001: System Checks
	T1620: Reflective Code Loading	
	T1055: Process Injection	
Discovery	T1083: File and Directory Discovery	
	T1057: Process Discovery	
	T1016: System Network Configuration Discovery	
	T1082: System Information Discovery	

Tactic	Technique	Sub-technique
Command and Control	T1102: Web Service	T1102.001: Dead Drop Resolver
	T1573: Encrypted Channel	
	T1090: Proxy	
	T1105: Ingress Tool Transfer	
Exfiltration	T1041: Exfiltration Over C2 Channel	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	096372d19b4787e989f44e04c5ecc29885aa927c34ae8666628d6c0eb20bb447, 1c56228cbd1bdebb9e5ea55c2749150fee06c865ede4a3754e8bd6843e51d2d4, 080ab9bc2893ba7bad354551604a667af40ed2ae2d042d2323c2bd9ad3122192, 5ed14c2b7f7433a1a72dd6b668413f935a217ba10b69d89b774a82990fa12fe1, 61f7d9cd2d8ce7df950639b23ce90085b300b0c6dd0d8d934bba8fdecb670f15, 24aa4e780ccd66cef13da9ef98c32954105cf2a32ec643efab0ba1aa2d6352f4, 02542a49b3bd6bd2795afb67840acb4557b17e017f7503dd03ebe3aeeb28720e, 8ae7c82a3e4f742777e590b25a1c563d19bd9bcba2a387d004aae72c4b2828f9, 0476875486057343487 92e2a9d771b6cba42facd0d0d7d44d778290a25848574, a4e9f9919d62589b57cfa08c9ccb89e386b09f683271373413cd8e8c8c7d1c5a, 823d5969db3f3b72ebbdce1b78752717ea849884a0fb40d86146416c38e128de, 783661d0f7edb338d2d50be087764d82dbbc9ee7989ddc57db1801e4ec9045b0
Domain	note1ggbbhggdwa1[.]blob[.]core[.]windows[.]net

References

https://www.seqrite.com/blog/operation-dragon-weave-uncovering-a-china-linked-campaign-targeting-czech-republic-and-taiwan-using-azure-cloud-c2/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a Demo of **HivePro**.

REPORT GENERATED ON

June 03, 2026 • 7:30 AM

More at www.hivepro.com