Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

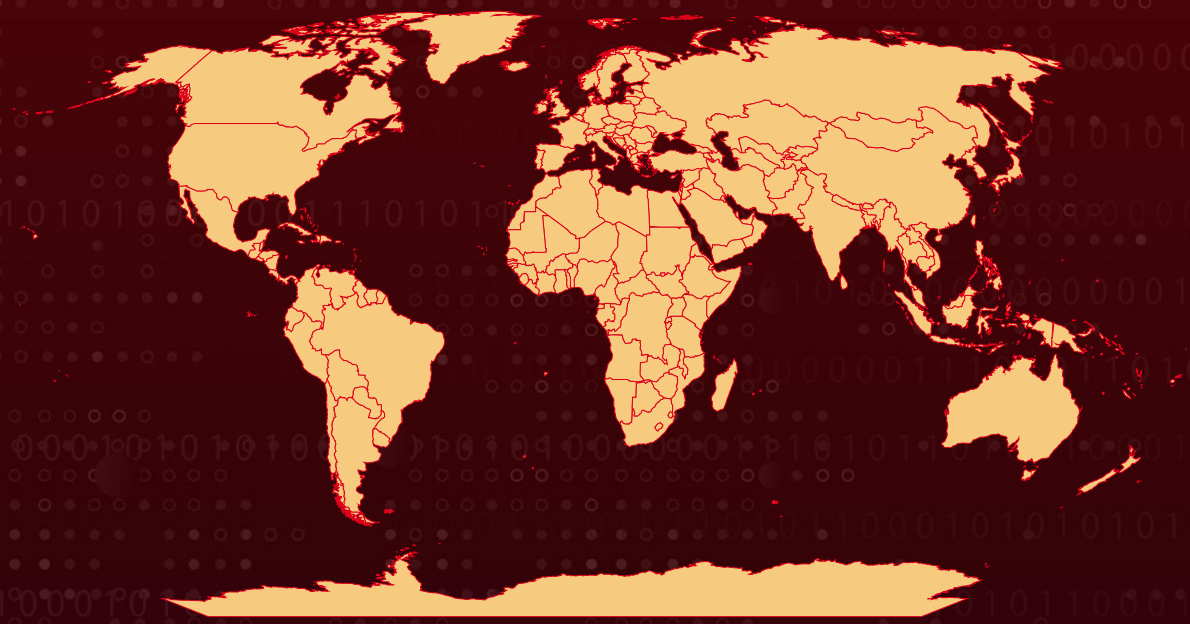
Edgecution: Malicious Edge Extension Opens the Door to Host Compromise

Date of Publication	Admiralty Code	TA Number
June 25, 2026	A1	TA2026178

Summary

First Seen: June 2026
Targeted Regions: Worldwide
Targeted Platforms: Windows
Targeted Products: Microsoft Edge, Microsoft Teams, Microsoft Outlook
Malware: Edgecution
Attack: The Edgecution malware campaign uses social engineering and stealthy persistence to gain deep access into victim environments. By impersonating IT support via Microsoft Teams, threat actors lure users to a fake Outlook update portal that deploys a malicious browser extension that is backed by a Python-based native host. Operating through AWS CloudFront infrastructure and encrypted WebSocket communications, the malware blends into legitimate traffic while enabling shell execution, file manipulation, process monitoring, and arbitrary code execution. Its ability to maintain a covert foothold and extend access to both local systems and cloud identities makes Edgecution a highly flexible initial access operation that can pave the way for broader post-compromise activities, including ransomware attacks.

Attack Regions



Targeted Non-Targeted

Attack Details

#1

The Edgecution attack chain begins with a convincing social engineering campaign conducted through Microsoft Teams, where threat actors pose as internal IT personnel and claim that a critical spam filter update must be installed. Victims are then redirected to a fake Microsoft-branded portal, presented as an "Outlook Updates Management Console," which offers multiple installation methods, including an obfuscated AutoHotKey script, a clipboard-delivered batch file, and a PowerShell-based installer.

#2

Once executed, the deployment scripts establish a staging environment within %LOCALAPPDATA%\Microsoft\Edge\User Data\test1. At this stage, the malformed archive is repaired and unpacked, revealing an embedded Python 3.13.3 runtime along with supporting extension and native components. The installer creates a Chrome native messaging manifest and a launcher script named native_host.bat, while storing a campaign-specific hexadecimal key in HKCU\SOFTWARE\Microsoft\Edge as AppKey. This key is required to decrypt strings embedded within the Python backdoor, significantly complicating independent analysis and reverse engineering efforts.

#3

To maintain persistence, the malware creates a scheduled task that launches Microsoft Edge in headless mode using a dedicated user data directory and silently loads the malicious extension without displaying a visible browser window. Disguised as an "Edge Monitoring Agent" within the browser's extension manager, the extension establishes secure WebSocket (WSS) communications with attacker-controlled CloudFront domains. It continuously exchanges heartbeat signals, subscription requests, and operational commands, allowing the threat actor to maintain a reliable foothold while blending malicious traffic with legitimate cloud services.

#4

Whenever actions exceed the browser's native permissions, the extension leverages chrome.runtime.sendNativeMessage to communicate with the Python backdoor. The native host executes attacker instructions encapsulated in JSON messages containing command identifiers, parameters, and request tokens. This mechanism enables a broad range of capabilities, including system reconnaissance, shell and PowerShell execution, arbitrary file creation, process enumeration, and even the execution of attacker-supplied Python code. To reduce its forensic footprint, the Python process terminates immediately after responding to each request, minimizing its time in memory.

#5

Although no explicit lateral movement techniques have been publicly documented, the extensive privileges granted by the backdoor provide the level of host control commonly associated with initial access brokers preparing environments for ransomware deployment. Its exclusive use of AWS CloudFront infrastructure further obscures malicious activity by blending command-and-control traffic with legitimate CDN communications. Additionally, the malware removes the original configuration file after storing the C2 address in local browser storage, leaving fewer artifacts behind while retaining flexible mechanisms for data collection and exfiltration through file access, command execution, and JSON-based WSS responses.

Recommendations

Block Edgecution C2 Infrastructure: Block the four observed CloudFront WSS endpoints listed in the IoC section at the proxy, secure web gateway, and DNS layer, and add the two SHA256 hashes to EDR and AV blocklists. Track additional `.cloudfront.net` WSS callbacks from endpoints that do not normally use cloud CDN WebSocket traffic.

Restrict Edge Extension Installation: Enforce the `ExtensionInstallAllowlist` and `ExtensionInstallBlocklist` Group Policy settings for Microsoft Edge so that only IT-approved extensions can load, and audit any extension running from `%LOCALAPPDATA%\Microsoft\Edge\User Data` paths outside the default profile directory.

Detect Headless Edge with Side-Loaded Extensions: Build EDR detections for `msedge.exe` invocations that combine `--headless`, `--load-extension`, `--disable-sync`, and `--no-first-run` flags, particularly when launched by a scheduled task or non-interactive parent process.

Monitor Native Messaging Host Manifests: Alert on the creation or modification of Chrome/Edge native messaging manifest files and on registry keys under `HKCU\Software\Microsoft\Edge\NativeMessagingHosts` and the corresponding Chrome paths, and review any host pointing at a batch file or scripting interpreter in a user-writable directory.

Harden Microsoft 365 Against Credential Theft: Enforce phishing-resistant MFA for all Microsoft 365 accounts, deploy Conditional Access policies that block legacy authentication and require compliant devices, and monitor sign-in logs for anomalous OAuth token issuance following the timing of any reported Teams-based impersonation attempt.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Resource Development	T1583: Acquire Infrastructure	T1583.006: Web Services
Initial Access	T1566: Phishing	T1566.003: Spearphishing via Service
Execution	T1204: User Execution	T1204.001: Malicious Link
		T1204.002: Malicious File
	T1059: Command and Scripting Interpreter	T1059.001: PowerShell
		T1059.006: Python
		T1059.010: AutoHotKey & AutoIT
Persistence	T1053: Scheduled Task/Job	T1053.005: Scheduled Task
	T1176: Browser Extensions	
Defense Evasion	T1027: Obfuscated Files or Information	T1027.013: Encrypted/Encoded File
	T1140: Deobfuscate/Decode Files or Information	
	T1564: Hide Artifacts	T1564.003: Hidden Window

Tactic	Technique	Sub-technique
Defense Evasion	T1112: Modify Registry	
	T1036: Masquerading	T1036.005: Match Legitimate Name or Location
Discovery	T1057: Process Discovery	
	T1082: System Information Discovery	
Command and Control	T1071: Application Layer Protocol	T1071.001: Web Protocols
	T1102: Web Service	

Indicators of Compromise (IOCs)

TYPE	VALUE
URLs	wss[:]//d3nh8sl98s2554[.]cloudfront[.]net/ws, wss[:]//d2g6dl71gua1qa[.]cloudfront[.]net/ws, wss[:]//d1jp293q9tvi92[.]cloudfront[.]net/ws, wss[:]//d23l50n6ubud7p[.]cloudfront[.]net/ws
SHA256	a08d8e63b0cd3638fb40b8e6da546e26da69439597565827f9cec87915f78568, 3d1158884fb339b3328bd330fcc27598e1f1c94bcac39e75d1a272afa4deee1a

References

https://www.zscaler.com/blogs/security-research/payouts-king-ransomware-initial-access-broker-deploys-new-edgecution

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 25, 2026 • 10:00 AM

More at www.hivepro.com