Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

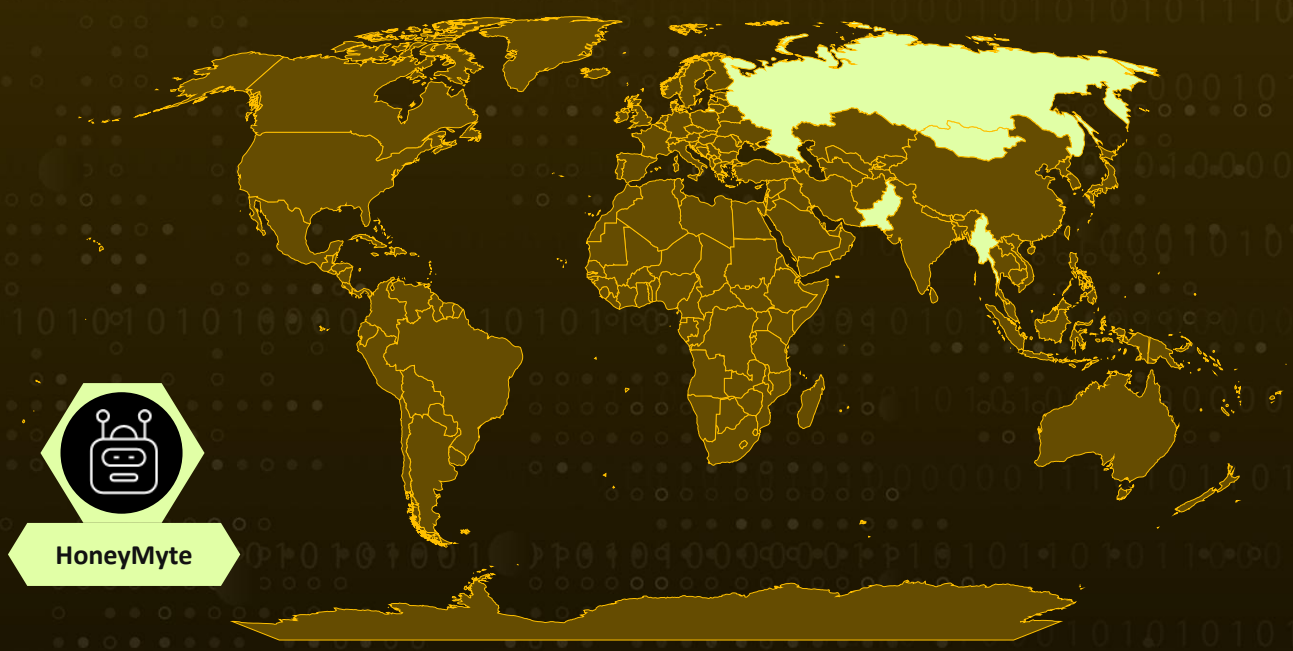
HoneyMyte Arms CoolClient with a Signed Kernel-Mode Rootkit

Date of Publication	Admiralty Code	TA Number
August 17, 2026	A1	TA2026235

Summary

First Seen: Late 2025
Targeted Countries: Myanmar, Mongolia, Pakistan, Russia
Targeted Platform: Microsoft Windows
Targeted Industry: Government
Threat Actor: HoneyMyte (aka Mustang Panda, Bronze President, TEMP.Hex, Red Lich, Earth Preta, Camaro Dragon, PKPLUG, Stately Taurus, Twill Typhoon, Hive0154)
Malware: CoolClient, PlugX
Attack: HoneyMyte has upgraded its CoolClient backdoor with a signed Windows kernel-mode rootkit, msagent.sys, that hides malicious processes, files, registry objects, and command-and-control network data from security tools and analysts. The backdoor is deployed as a secondary implant after an initial PlugX infection, using DLL side-loading of a renamed legitimate Sangfor application and impersonation of Microsoft Windows Defender to blend in. Once it gains administrative rights, CoolClient installs the driver as a Windows service and controls it via IOCTL requests, providing the espionage tool with kernel-level stealth on top of its existing keylogging, clipboard theft, and credential-harvesting features.

Attack Regions



Attack Details

#1 The threat actor known as HoneyMyte (aka Mustang Panda) has been observed deploying an updated version of the CoolClient backdoor. It is dropped only after the group first breaks in with PlugX, an older tool it favors for initial access. In the Myanmar case, the attackers told Microsoft Defender to ignore the folder they planned to use, so their files would not be scanned. They then made a fake "Microsoft\Windows Defender" folder, put the CoolClient files inside, and renamed a trusted Sangfor program (normally Sang.exe) to defender.exe. A scheduled task keeps the malware running by launching defender.exe with SYSTEM rights every time the computer starts.

#2 When defender.exe runs, it loads a malicious file called libngs.dll, which starts a chain of hidden stages. libngs.dll unlocks and runs a second file, loadcert.ini, that does most of the work. It adds more ways to stay on the machine, an AutoRun entry named goopdate and a service called media_updaten, but only after checking that security tools like 360 Total Security are not running. To gain higher access without showing a prompt, it uses a trick that makes its actions look like they came from a trusted Windows process. It then hides its code inside synchost.exe and loads the final piece, cert.ini, which runs the backdoor's real work.

#3 The big change in this version is the kernel driver. Once CoolClient has admin rights, it unpacks a driver, saves it as msagent.sys, and loads it as a service. The backdoor then talks to this driver to hide itself, protect its files and registry entries, and pass along its server address. The driver carries an old but still-valid certificate from 2014, which helps it load without warnings. From deep inside Windows, msagent.sys can hide processes, files, folders, registry keys, and even other drivers. It ships with 33 built-in commands, though this sample used only three

#4 .With the driver in place, cert.ini carries out the spying CoolClient is built for: logging keystrokes, stealing clipboard contents, grabbing saved passwords, browsing files, and collecting system details, with more features added through plugins. The stolen data is sent back to the attackers' server, while the driver quietly removes that same server address from any network view on the machine. The result is a hard problem for defenders: the connection is real, but the usual signs on the computer may never appear.

Recommendations

Block Known CoolClient Indicators: Ingest the file hashes, malicious domains, and file paths from this advisory into endpoint, DNS, and web-proxy blocklists, and alert on any historical matches uncovered during retro-hunting.

Hunt for the PlugX Foothold: Because CoolClient is only deployed after a PlugX infection, treat any PlugX detection as a trigger for a full compromise assessment rather than a simple clean-up, since a deeper secondary backdoor is likely already present.

Block Abused and Expired Signed Drivers: Enable Microsoft's vulnerable driver blocklist and use Windows Defender Application Control (WDAC) or equivalent allow-listing to stop old, third-party-signed drivers such as msagent.sys, signed with a certificate that expired in 2014, from loading into the kernel.

Watch for Defender Exclusion Tampering: Alert on programmatic changes to Microsoft Defender exclusions, especially folder or file exclusions added through wmic and MSFT_MpPreference, which the actor uses to blind Defender before staging the malware.

Monitor Suspicious Persistence Entries: Watch for the AutoRun value goopdate under the Run key, creation of services named media_updaten or msagent, and scheduled tasks that impersonate Microsoft Defender ATP and run as SYSTEM at startup.

Enforce Least Privilege and UAC Hardening: Restrict local administrator rights and monitor for the RPC-based, parent-process-spoofing elevation technique, since driver deployment proceeds only when the malware obtains administrative access and SeTcbPrivilege.

Deploy Kernel-Aware EDR and Integrity Checks: Use endpoint tooling with kernel-level visibility and periodically compare live process, driver, and network views against trusted out-of-band baselines to surface objects a rootkit may be hiding.

Segment Networks and Prioritize Government-Sector Defense: Given the focus on government entities across Asia and Russia, apply network segmentation, tighten monitoring around sensitive systems, and run proactive threat hunts aligned to HoneyMyte tradecraft.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Execution	T1569: System Services	T1569.002: Service Execution
	T1106: Native API	
Persistence	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder
	T1053: Scheduled Task/Job	T1053.005: Scheduled Task
	T1543: Create or Modify System Process	T1543.003: Windows Service
Privilege Escalation	T1548: Abuse Elevation Control Mechanism	T1548.002: Bypass User Account Control
	T1134: Access Token Manipulation	T1134.004: Parent PID Spoofing
Defense Evasion	T1574: Hijack Execution Flow	T1574.002: DLL Side-Loading
	T1562: Impair Defenses	T1562.001: Disable or Modify Tools
	T1014: Rootkit	
	T1055: Process Injection	
	T1036: Masquerading	T1036.005: Match Legitimate Name or Location
	T1553: Subvert Trust Controls	T1553.002: Code Signing
	T1140: Deobfuscate/Decode Files or Information	
	T1027: Obfuscated Files or Information	

Tactic	Technique	Sub-technique
Defense Evasion	T1112: Modify Registry	
	T1564: Hide Artifacts	
	T1070: Indicator Removal	T1070.004: File Deletion
Credential Access	T1056: Input Capture	T1056.001: Keylogging
Collection	T1115: Clipboard Data	
	T1005: Data from Local System	
Discovery	T1057: Process Discovery	
	T1082: System Information Discovery	
Command and Control	T1071: Application Layer Protocol	

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	2d7c8780e97409770a9d4f31c66c9d63, 9460E150E1981D5C165043520C5C12FE, 9717F005C5FB98E08D2AD983D88F94EE, F518D8E5FE70D9090F6280C68A95998F, EB79558B037669792652A816E2C669DE
SHA256	EE72AE4CC869AFFDDAB11647E95BAB9C5691C9FC76DCB4B31650FF504DA29156, FD434AC879122DEDB754BD4835822DBC185ACE3A3E75E5898FFB40C213A7C4BA, BF75493840862F0C9416D60A13DC92E72A7336056B2A2E22EF1D4DA44255EBAA, E0D77BCEB5EBB3FF6F31EB7B0A4671CFF8B599A0015B63FA94121B89A949F729, B35C17B889030ACED7B41158C1B6A6E8ED9C0D0290EBCEA28D1E3FE7DEEACCFC
File Path	C:\Program Files\microsoft\windows defender\, C:\Program Files\windows media player\mediares\, C:\ProgramData\symantecdir\, C:\ProgramData\virtualstore\, C:\Windows\identitycrl\production\, C:\Windows\serviceprofiles\networkservice\, C:\Users\<user>\AppData\Local\viber24.8\, C:\Users\<user>\AppData\Roaming\dsassistant\, C:\Program Files\common files\microsoft shared\office14\, C:\programdata\msdn\
Domains	cloudtroe[.]giize[.]com, employers[.]theworkpc[.]com, freeread[.]casacam[.]net, us[.]lenovoappstore[.]com, sundanish[.]freeddns[.]org, torinarlabs[.]webredirect[.]org, news[.]dursamjbataar[.]org, video[.]dursamjbataar[.]org, black-popular[.]com, whatismybestthing[.]com

References

https://securelist.com/honeymyte-coolclient-driver-rootkit/121028/

https://hivepro.com/threat-advisory/mustang-panda-enhances-coolclient-for-stealth-and-surveillance/

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

August 17, 2026 • 09:40 AM

More at www.hivepro.com