Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

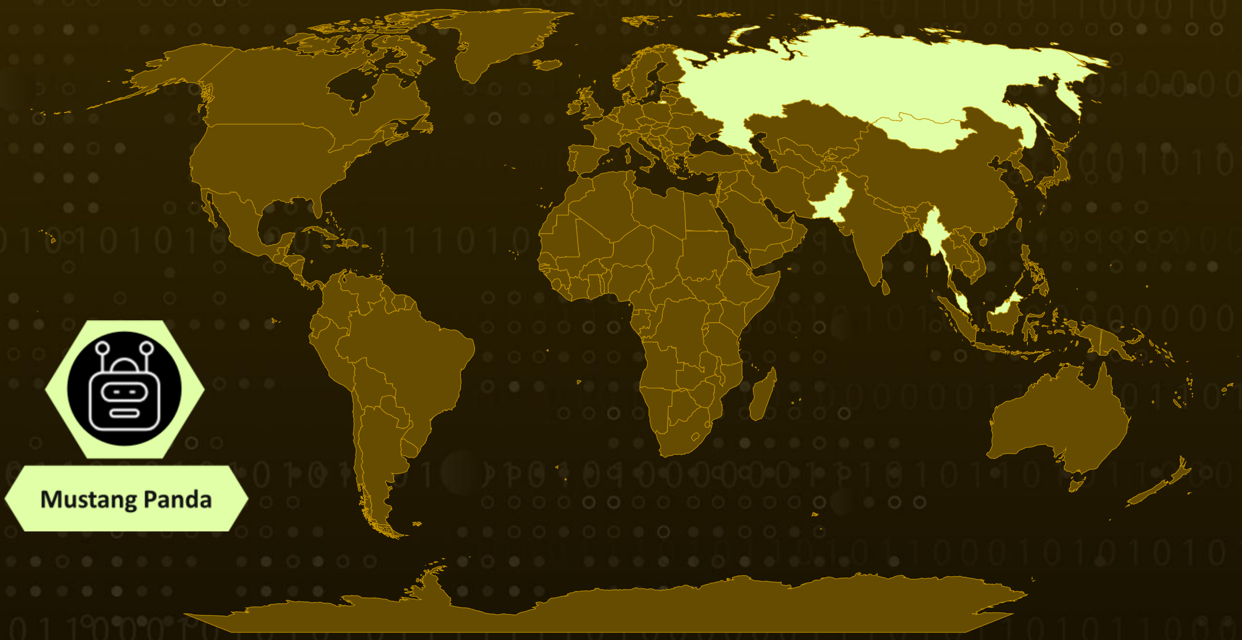
Mustang Panda Enhances CoolClient for Stealth and Surveillance

Date of Publication	Admiralty Code	TA Number
January 29, 2026	A1	TA2026028

Summary

First Seen: 2022
Targeted Regions: Myanmar, Mongolia, Malaysia, Russia, Pakistan
Affected Platform: Microsoft Windows
Targeted Industry: Government
Malware: CoolClient
Actor: Mustang Panda (aka HoneyMyte, Bronze President, TEMP.Hex, Red Lich, Earth Preta, Camaro Dragon, PKPLUG, Stately Taurus, Twill Typhoon, Hive0154)
Attack: Mustang Panda has quietly upgraded its CoolClient backdoor, transforming it from a simple foothold into a tool built for long-term, low-noise surveillance. By hiding malicious DLLs behind trusted, signed software through DLL side-loading, the group ensures its malware blends seamlessly into normal system activity. Once inside, CoolClient establishes persistence, sidesteps security controls, and escalates privileges before shifting its focus to monitoring the user's clipboard activity, active applications, and even siphoning proxy credentials from live network traffic. Paired with browser credential theft and flexible data exfiltration through FTP and cloud services, the campaign signals a clear move beyond document theft toward continuous visibility into victim environments, reinforcing Mustang Panda's reputation for patient and deeply embedded cyber espionage.

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, Overture Maps Fundation, TomTom, Zenrin

Attack Details

#1 The Chinese espionage threat group Mustang Panda has rolled out an updated variant of its CoolClient backdoor, underscoring a clear focus on stealth, persistence, and deeper user monitoring. The infection chain typically starts with CoolClient delivered alongside encrypted loader files that store configuration data, shellcode, and in-memory DLL modules. Execution relies on DLL side-loading, abusing legitimate signed executables to load malicious DLLs. Between 2021 and 2025, Mustang Panda repeatedly misused trusted binaries from software such as Bitdefender, VLC Media Player, Ulead PhotoImpact, and Sangfor, allowing the malware to blend into normal system activity.

#2 Once executed, the second-stage DLL validates parameters and injects malicious code into newly created processes. CoolClient supports several execution modes, including an installation mode that decrypts its configuration, establishes registry persistence, injects shellcode via a write.exe process, and installs a persistent service. Other modes enable routine operation or elevate privileges by bypassing UAC using techniques such as PEB spoofing, scheduled task creation, and access token duplication.

#3 The updated variant expands beyond a traditional backdoor by adding active surveillance features. It now monitors clipboard activity and active application windows, capturing copied data along with contextual metadata. CoolClient also includes an HTTP proxy credential sniffer that extracts authentication credentials from raw network traffic. All collected information is encrypted and stored locally to avoid immediate detection.

#4 For data exfiltration, Mustang Panda uses a combination of CoolClient's built-in upload functions, browser credential stealers targeting Chrome, Edge, and Firefox, and supporting batch and PowerShell scripts. These tools collect system and credential data, archive browser profiles and documents, and exfiltrate the data via FTP or cloud services such as Google Drive and Pixeldrain. Overall, HoneyMyte's campaigns reflect a shift from simple document theft toward persistent user surveillance and credential harvesting, posing a continued risk to targeted organizations.

Recommendations

Implement Application Whitelisting: Deploy application control policies to prevent unauthorized DLL side-loading by restricting execution to approved signed executables and blocking unknown or modified binaries in system directories.

Monitor for DLL Side-Loading Activity: Configure endpoint detection rules to identify legitimate applications loading unsigned or suspicious DLLs, particularly targeting processes loading unexpected modules.

Detect Malicious Scheduled Tasks and Services: Monitor for the creation of scheduled tasks named ComboxResetTask and services named media_updaten, which are indicators of CoolClient persistence mechanisms.

Audit Browser Credential Storage: Implement browser security policies that prevent credential storage or employ enterprise password management solutions to reduce the impact of credential harvesting malware.

Monitor for Clipboard and Keylogging Behavior: Deploy endpoint detection capabilities to identify processes accessing clipboard APIs (GetClipboardData) and keyboard hooks that may indicate active surveillance by CoolClient.

Restrict PowerShell and Script Execution: Implement constrained language mode for PowerShell and monitor for suspicious script execution, particularly scripts downloading tools like curl.exe and rar.exe or accessing browser data directories.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion
TA0006 Credential Access	TA0007 Discovery	TA0009 Collection	TA0010 Exfiltration
TA0011 Command and Control	TA0040 Impact	T1059 Command and Scripting Interpreter	T1059.001 PowerShell

T1059.003 Windows Command Shell	**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	**T1548** Abuse Elevation Control Mechanism
T1548.002 Bypass User Account Control	**T1574** Hijack Execution Flow	**T1574.001** DLL	**T1055** Process Injection
T1140 Deobfuscate/Decode Files or Information	**T1555** Credentials from Password Stores	**T1555.003** Credentials from Web Browsers	**T1056** Input Capture
T1056.001 Keylogging	**T1082** System Information Discovery	**T1016** System Network Configuration Discovery	**T1083** File and Directory Discovery
T1115 Clipboard Data	**T1005** Data from Local System	**T1560** Archive Collected Data	**T1071** Application Layer Protocol
T1071.001 Web Protocols	**T1041** Exfiltration Over C2 Channel	**T1567** Exfiltration Over Web Service	**T1090** Proxy
T1070 Indicator Removal	**T1070.004** File Deletion	**T1027** Obfuscated Files or Information	**T1569** System Services
T1489 Service Stop			

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	F518D8E5FE70D9090F6280C68A95998F, 1A61564841BBBB8E7774CBBEB3C68D5D, AEB25C9A286EE4C25CA55B72A42EFA2C, 6B7300A8B3F4AAC40EEECFD7BC47EE7C,

TYPE	VALUE
MD5	7AA53BA3E3F8B0453FFCFBA06347AB34, A1CD59F769E9E5F6A040429847CA6EAE, 1BC5329969E6BF8EF2E9E49AAB003F0B, 1A5A9C013CE1B65ABC75D809A25D36A7, E1B7EF0F3AC0A0A64F86E220F362B149, DA6F89F15094FD3F74BA186954BE6B05, C19BD9E6F649DF1DF385DEEF94E0E8C4, 838B591722512368F81298C313E37412, A4D7147F0B1CA737BFC133349841AABA
SHA256	FD434AC879122DEDB754BD4835822DBC185ACE3A3E75E5898FFB40C213A7C4BA, FE09953545466B29AAD35340DC2DEEA73121F3DBCD1D8E1D33F7ABBCBEEF0BB7, C41B31BEF3ACCF85EAACFCBD11ACB35AC2165AAB4064D78F37286B923EB92234, F6BA67E96316E2495E11EAB0D163C4E530581F66ECE75DD16392F9DAFE5E39C2, 558227E071DBF1A693E31CA5E37AC3FFA74C1A5349241F108CCB00ACB51246DE, 941993F885957176D75F24EF3F8935ECB589BB9B445BB0D71FB18B65E61B6EE4, 70C30A858237FB61D187DDB826AB827C246E9C2A3183A21F895F2F6A6F86B4E0, 7EA494843D8E761BB39B495F29A4C79898A60970FC2795D26BDA20DD509CB960, 81C327A872EB623F6B56945ED62CA34C1D1DBC2579E1D71E2D123C61C590168D, 1CF286285C7AC5CD14357BDE96B212B141B648F29F609F742F3817A667D2518A
Domains	account[.]hamsterxnxx[.]com, popnike-share[.]com, japan[.]Lenovoappstore[.]com
IPv4	113[.]23[.]212[.]15

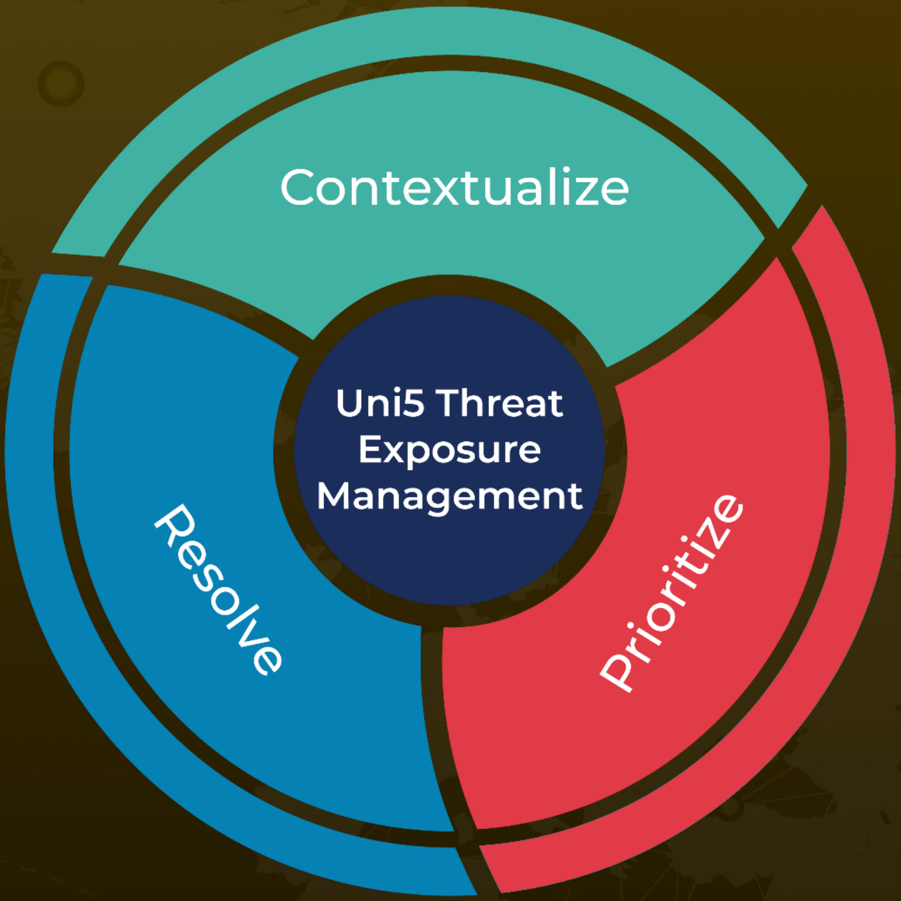
References

https://securelist.com/honeymyte-updates-coolclient-uses-browser-stealers-and-scripts/118664/

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 free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

January 29, 2026 • 9:30 AM

More at www.hivepro.com