Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

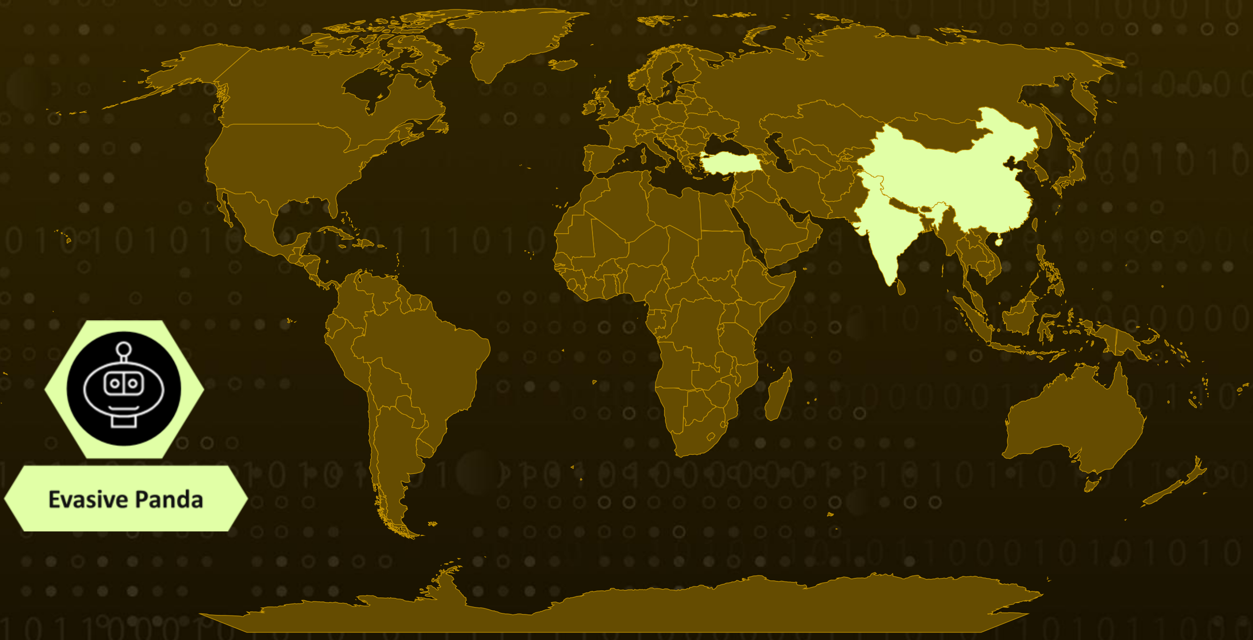
Inside Evasive Panda’s Long-Running AitM Campaign

Date of Publication	Admiralty Code	TA Number
December 29, 2025	A1	TA2025392

Summary

First Seen: November 2022
Targeted Region: Turkey, China, India
Malware: MgBot
Actor: Evasive Panda (aka Bronze Highland, Daggerfly, Storm Cloud, StormBamboo, TAG-102, TAG-112, Digging Taurus)
Affected Platform: Windows
Attack: Evasive Panda, a China-linked Advanced Persistent Threat (APT) group active since 2012, executed a sophisticated, highly-targeted cyber espionage campaign leveraging DNS poisoning techniques to deliver its signature MgBot backdoor. The threat actors performed adversary-in-the-middle (AitM) attacks on specific victims, manipulating DNS responses to redirect legitimate software update requests to attacker-controlled servers. The campaign employed multi-stage shellcode execution, hybrid encryption using DPAPI and RC5 algorithms, and DLL sideloading techniques to maintain persistent, stealthy access to compromised systems. Victims remained compromised for over a year, demonstrating the threat actor's commitment to long-term intelligence collection operations.

Attack Regions



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

Attack Details

#1 The Evasive Panda APT group, also tracked as Bronze Highland, has been active for more than a decade, steadily refining its tradecraft since at least 2012. In mid-2025 sheds light on a series of highly targeted campaigns conducted between November 2022 and November 2024, in which the group relied heavily on adversary-in-the-middle (AitM) techniques. These operations were carefully staged, with loaders deployed only to specific environments and encrypted malware components hosted on attacker-controlled infrastructure, activated selectively through crafted DNS requests.

#2 A notable evolution in these campaigns is the introduction of a new, highly evasive loader designed to minimize detection during initial infection. Evasive Panda has paired this with hybrid encryption schemes that complicate reverse engineering and produce implants uniquely tailored to each victim. Central to this approach is a custom injector that runs the MgBot malware entirely in memory, sideloading it into legitimate processes using trusted but outdated signed executables. By blending modern techniques with decade-old binaries, the group maintains a low operational footprint while preserving persistence over extended periods, underscoring a deliberate balance between innovation and proven stealth.

#3 The delivery mechanisms observed in these attacks lean heavily on deception, particularly through fake software updates for widely trusted applications. In one campaign, victims were lured with a trojanized update masquerading as a legitimate installer for SohuVA, a popular streaming application. The malicious executable closely mirrored a genuine update and redirected users to attacker-controlled resources hosted behind domains associated with the real platform. While not definitively proven, the evidence suggests DNS poisoning may have been used to silently redirect update requests, exploiting the application's normal behavior of fetching binaries from predefined directories.

#4 Once executed, the malware follows a complex, multi-stage execution flow. The primary loader, written in C++, resolves Windows APIs dynamically using hashing techniques and decrypts embedded shellcode directly in memory. It adapts its behavior based on the current user context, performs runtime permission changes to execute payloads quietly, and relies on machine-specific encryption via Windows DPAPI to ensure that secondary components can only be decrypted on the original victim system. When additional payloads are required, the malware retrieves them through poisoned DNS responses, in some cases, impersonating legitimate websites, and tailors' delivery based on the detected operating system version, suggesting deliberate differentiation between Windows and macOS implants.

#5 Further uncovered a secondary loader disguised as a legitimate Windows DLL, leveraging a signed Python executable to load additional stages covertly. This loader employs layered encryption using DPAPI combined with RC5, writes encrypted payloads to disk in a victim-specific format, and ultimately injects an MgBot variant into trusted processes such as svchost.exe. Taken together, these findings highlight Evasive Panda's sustained investment in long-term espionage operations, marked by supply-chain abuse, AitM and watering-hole techniques, and a carefully maintained command-and-control infrastructure designed to ensure resilience, persistence, and continued access to compromised environments.

Recommendations

Treat Software Updates as a Security Boundary: Do not automatically trust software updates, especially from third-party applications. Enforce signature verification, restrict automatic updates for non-critical software, and ensure update downloads occur only through secure, monitored channels.

Strengthen DNS and Network Protections: Implement DNS security controls and monitor for abnormal domain resolutions. Unexpected redirects or unusual IP mappings during update checks should be investigated immediately as potential AitM activity.

Prioritize Behavioral Detection: Relying solely on file-based detection is insufficient against in-memory threats. Monitor for abnormal DLL sideloading, misuse of signed executables, and suspicious memory permission changes that indicate stealthy execution.

Enhance Endpoint Protection: Deploy next-generation antivirus (NGAV) and endpoint detection & response (EDR) solutions to identify and block malware. Leverage behavioral analysis and machine learning-based detection to spot suspicious activity.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1195: Supply Chain Compromise	T1195.002: Compromise Software Supply Chain
Execution	T1059: Command and Scripting Interpreter	
	T1106: Native API	
Persistence	T1574: Hijack Execution Flow	T1574.001: DLL
Defense Evasion	T1140: Deobfuscate/Decode Files or Information	
	T1027: Obfuscated Files or Information	T1027.013: Encrypted/Encoded File
	T1620: Reflective Code Loading	

Tactic	Technique	Sub-technique
Defense Evasion	T1055: Process Injection	
	T1036: Masquerading	
	T1553: Subvert Trust Controls	
Credential Access	T1555: Credentials from Password Stores	
Collection	T1056: Input Capture	
	T1557: Adversary-in-the-Middle	
Command and Control	T1071: Application Layer Protocol	T1071.001: Web Protocols
	T1573: Encrypted Channel	T1573.001: Symmetric Cryptography

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	C340195696D13642ECF20FBE75461BED, 7973E0694AB6545A044A49FF101D412A, 9E72410D61EAA4F24E0719B34D7CAD19
SHA256	1E7937A73FB678AD1F261D99A505BC81AB18512DFB75A491EBC72CB9663AF3A8, CAC40C3909DBD6F096D9634F5D7F33541E55935387CAE55A8538D11E1491A06D, 7376FCB7D2BFDCD858CF0920F6B7611E263D779CDC419A246B2D3004CBA2C39F
File Paths	C:\ProgramData\Microsoft\MF, C:\ProgramData\Microsoft\eHome\status.dat, C:\ProgramData\Microsoft\eHome\perf.dat

TYPE	VALUE
IPv4	60[.]28[.]124[.]21, 123[.]139[.]57[.]103, 140[.]205[.]220[.]98, 112[.]80[.]248[.]27, 116[.]213[.]178[.]11, 60[.]29[.]226[.]181, 58[.]68[.]255[.]45, 61[.]135[.]185[.]29, 103[.]27[.]110[.]232, 117[.]121[.]133[.]33, 139[.]84[.]170[.]230, 103[.]96[.]130[.]107, 158[.]247[.]214[.]28, 106[.]126[.]3[.]78, 106[.]126[.]3[.]56

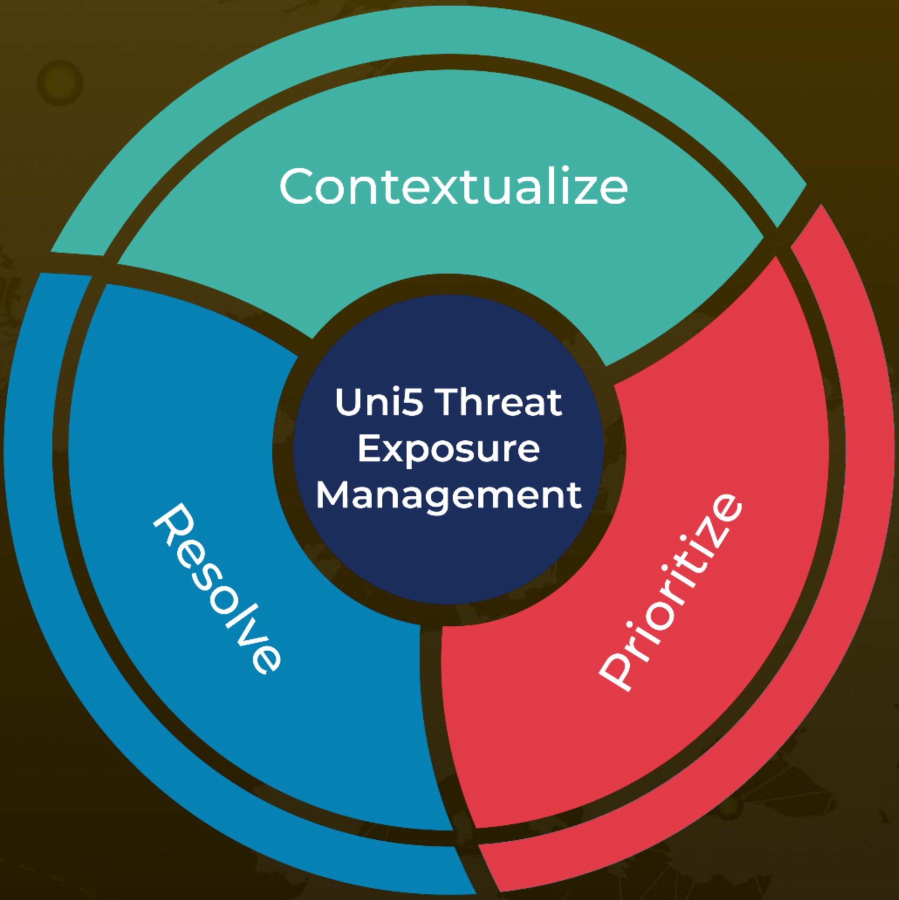
References

https://securelist.com/evasive-panda-apt/118576/

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

December 29, 2025 • 8:00 AM

More at www.hivepro.com