Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

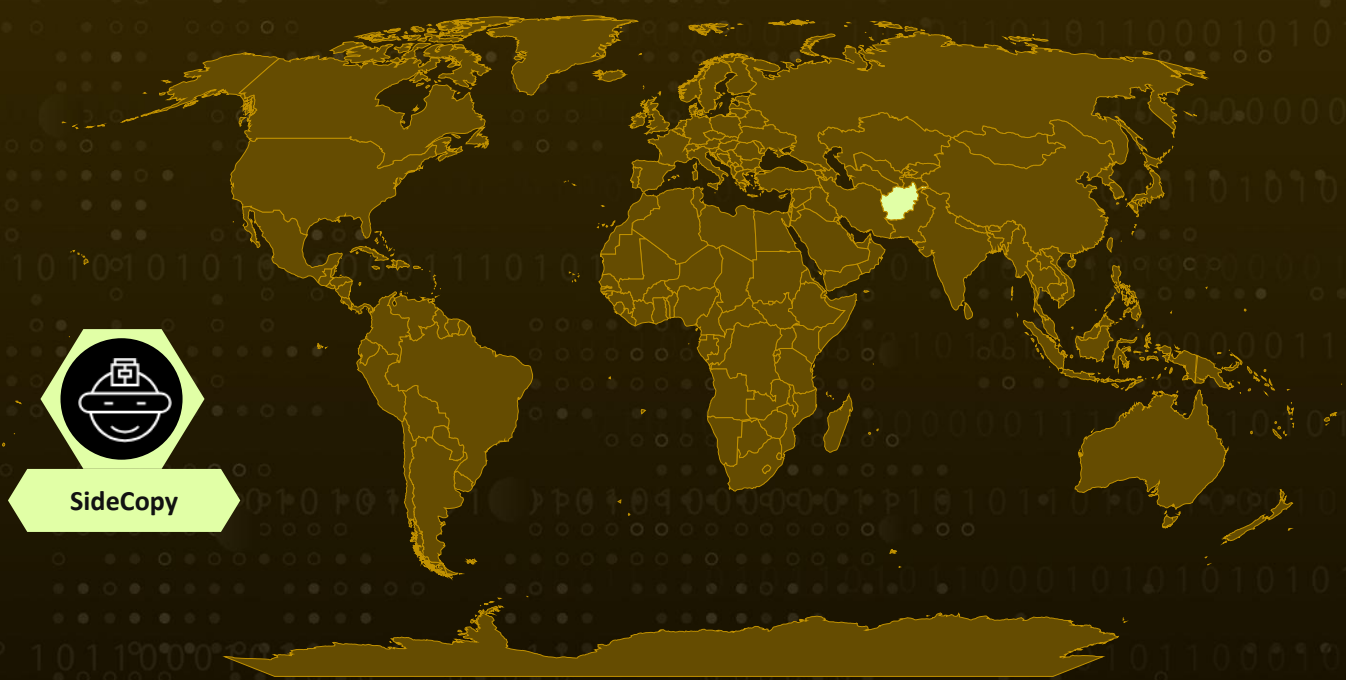
Operation XENOFISCAL: SideCopy Adopts XenoRAT to Target Afghan Finance

Date of Publication	Admiralty Code	TA Number
June 02, 2026	A1	TA2026150

Summary

First Seen: 2019
Targeted Region: Afghanistan
Targeted Platform: Windows
Targeted Industries: Government, Finance, and public administration
Threat Actor: SideCopy (alias UNC2269, White Dev 55, Mocking Draco, TAG-140)
Malware: XenoRAT
Campaign: Operation XENOFISCAL
Attack: SideCopy launched a spear-phishing campaign against the Ministry of Finance of Afghanistan and its provincial revenue and finance directorates, using a ZIP archive containing a malicious LNK file themed around an intellectual and psychological warfare seminar. Execution of the shortcut abuses the legitimate Windows binary, kicking off a multi-stage, largely fileless loader chain that ultimately deploys the open-source XenoRAT implant. The implant beacons to bulletproof European hosting infrastructure kept entirely separate from the Afghan-hosted delivery layer, providing the actor with encrypted command-and-control, surveillance, and long-term access to the compromised hosts.

Attack Regions



Attack Details

#1

The SideCopy APT cluster a Pakistan-linked threat group led a targeted campaign, Operation XENOFISCAL, directed at the Ministry of Finance, Afghanistan. The campaign begins with a spear-phishing message delivering a ZIP archive that contains a malicious Windows shortcut (LNK) file. The shortcut is disguised with a PDF icon and a carefully crafted Pashto-language filename referencing a list of employees introduced to an intellectual and psychological warfare seminar a lure tailored to provincial finance officials across all 34 Afghan Mustoufiats and reflecting precise knowledge of the targets' administrative context.

#2

When opened, the LNK silently launches mshta.exe from the System32 directory and points it at a remote PHP resource hosted on a compromised Afghan education domain. This living-off-the-land technique executes externally hosted script content directly in memory without dropping an executable to disk, and the URL is padded with excessive comma obfuscation to hinder static and signature-based detection. While the chain proceeds in the background, the victim is shown a decoy document an Afghan Ministry of Finance provincial staff directory spanning all 34 provinces, written in Dari and Pashto, whose level of organisational detail suggests prior intelligence gathering by the actor.

#3

The final payload is XenoRAT v1.8.7, an open-source remote access trojan. On execution it establishes an encrypted TCP command-and-control channel to a hard-coded IP address, and enforces single-instance execution through a mutex named "clouda." The implant supports SOCKS5 proxy tunnelling and the dynamic in-memory loading of additional DLL modules through Assembly.Load. XenoRAT reinforces its persistence by creating a scheduled task named "XenoUpdateManager" that runs with the highest available privileges, with a non-admin fallback that writes to the HKCU Run key, and it can cleanly remove these entries and self-delete via a hidden cmd.exe routine when instructed.

#4

Its post-exploitation capability set centres on surveillance and host reconnaissance: keylogging, screen capture, clipboard monitoring, webcam and microphone capture, file upload/download/deletion, antivirus enumeration via WMI, and arbitrary command execution. Taken together, the campaign reflects a deliberate, intelligence-led operation:a stealthy fileless delivery path, a surveillance-capable implant engineered for quiet, and long-term access.

Recommendations

Eradicate the Persistence Footprint: On suspected hosts, remove the HKCU\Software\Microsoft\Windows\CurrentVersion\Run value named "Edgre" and delete the scheduled task "XenoUpdateManager." Inspect and clear the staging directories C:\Users\Public\USOShared-1de48789-1285 and C:\Users\Public\firefx-1de87eec8-1241, and remove residual artifacts such as zuidrt.hta, noway.bat, ayui.vmxx, and ayhui.vmxx.

Detect mshta.exe Fetching Remote Content: Alert on mshta.exe executing with HTTP or HTTPS URL arguments, particularly remote index.php endpoints — and on mshta.exe being spawned by explorer.exe or as a child of an LNK execution. This pattern is the campaign's earliest reliable detection point.

Hunt for Fileless .NET Loader Behaviour: Build detection content for the loader tradecraft observed in this chain: RWX memory allocation via VirtualAlloc followed by CreateThread, .NET BinaryFormatter deserialization, AmsiScanBuffer patching, COMPLUS_Version environment-variable manipulation, and reflective Assembly.Load of in-memory payloads.

Constrain LOLBIN and Script-Host Abuse: Deploy WDAC or AppLocker rules to restrict or block execution of mshta.exe and HTA files where they are not operationally required, and disable or tightly limit Windows Script Host, ActiveX, and legacy Internet Explorer script-host functionality that the JScript loader depends on.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1566: Phishing	T1566.001: Spearphishing Attachment
Execution	T1218: System Binary Proxy Execution	T1218.005: Mshta
	T1059: Command and Scripting Interpreter	T1059.003: Windows Command Shell
		T1059.007: JavaScript
	T1129: Shared Modules	
	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
Defense Evasion	T1140: Deobfuscate/Decode Files or Information	
	T1027: Obfuscated Files or Information	T1027.011: Fileless Storage
	T1620: Reflective Code Loading	
	T1564: Hide Artifacts	T1564.001: Hidden Files and Directories
	T1055: Process Injection	
	T1562: Impair Defenses	T1562.001: Disable or Modify Tools

Tactic	Technique	Sub-technique
Defense Evasion	T1070: Indicator Removal	T1070.004: File Deletion
Discovery	T1012: Query Registry	
	T1082: System Information Discovery	
	T1518: Software Discovery	T1518.001: Security Software Discovery
Collection	T1056: Input Capture	T1056.001: Keylogging
	T1113: Screen Capture	
	T1115: Clipboard Data	
	T1123: Audio Capture	
	T1125: Video Capture	
Command and Control	T1071: Application Layer Protocol	T1071.001: Web Protocols
	T1095: Non-Application Layer Protocol	
	T1573: Encrypted Channel	T1573.001: Symmetric Cryptography
	T1090: Proxy	T1090.002: External Proxy
	T1568: Dynamic Resolution	
Resource Development	T1583: Acquire Infrastructure	T1583.001: Domains
	T1584: Compromise Infrastructure	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	194B912C242604D6F9A79369F22338C58A13CE0CC2ED280CE505075808BC2F14, 3B4194BDFE40D94031A94B30397FFD8A4B09D0A4057668E897B8BDCD1703DD01, DF9173A28C0B0B878C10A53D35CD7CE6F6ED66D207B6B7C4FF723721F1C027AB, A63E90EE57A1F213A8FE76EF1A6CFF5AE9ED7EBCEDA258431533825E648C0C67, 5833917BD137804F5A021D2CB37ADFE5C4B7B67DBB06D59C3B9C5CF393835E45, 99127C8C67D90E2776BEEB85281F9C68399BF4567B07A6B638D68B760212E88D, 8F2D979EF33B2900351C94C7335275A9342C75189E1A901998E90A539E944A1A, 0019212F25EB04BBB33BB194879C095265DB7855D6003BDD777CF0CBB90EB772, 9AE3D785486022AF82EA92E51B26E3F55C1BBA88A7BE2AD9790F4240E8499D14
Domain	abimj[.]edu[.]af
IPv4	185[.]235[.]137[.]106, 103[.]132[.]98[.]224, 103[.]132[.]98[.]226
CIDR	103[.]132[.]98[.]0/23
URLs	hxxp[:]//abimj[.]edu[.]af/index[.]php, hxxp[:]//abimj[.]edu[.]af/institute/cloudiyaf/document[.]pdf, hxxp[:]//abimj[.]edu[.]af/institute/cloudiya/, hxxps[:]//abimj[.]edu[.]af/institute/10/, hxxps[:]//abimj[.]edu[.]af/institute/7/
Filenames	ugayt.hta, noway.bat, zuidrt.hta, WayBroad.dll, Aotestpass.dll, ayui.vmxx, ayhui.vmxx

TYPE	VALUE
File Path	C:\Users\Public\USOShared-1de48789-1285\zuidrt.hta, C:\Users\Public\firefx-1de87eec8-1241
Mutex	clouda
Registry Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Run (value: Edgre)
Scheduled Task	XenoUpdateManager

References

https://www.seqrite.com/blog/operation-xenofiscal-sidecopy-deploying-persistent-xenorat-targeting-the-mof-afghanistan/

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 02, 2026 • 09:00 AM

More at www.hivepro.com