Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

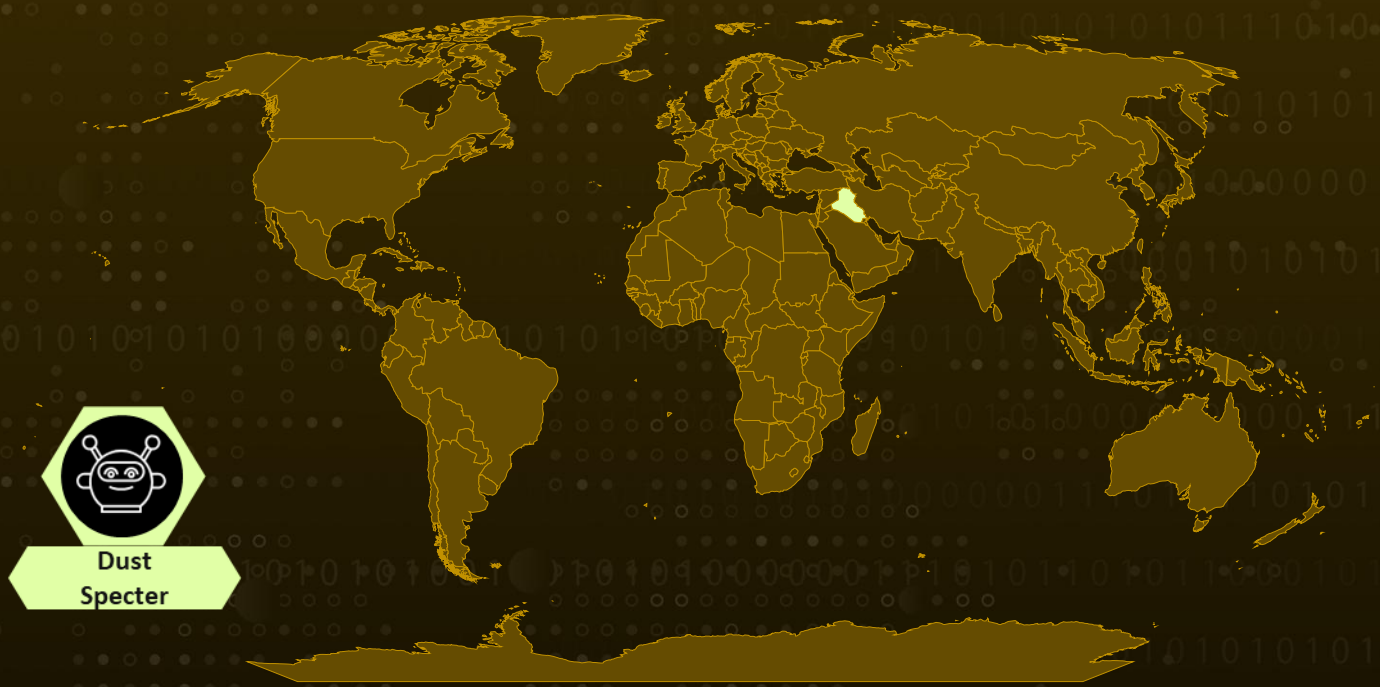
Iran-Linked Dust Specter Launches Cyberattack on Iraqi Officials

Date of Publication	Admiralty Code	TA Number
March 05, 2026	A1	TA2026060

Summary

First Seen: January 2026
Targeted Region: Iraq
Targeted Platform: Windows
Targeted Industry: Government
Threat Actor: Dust Specter
Malware: SPLITDROP, TWINTASK, TWINTALK, GHOSTFORM
Attack: In January 2026, a suspected Iran-nexus threat actor tracked as Dust Specter targeted government officials in Iraq by impersonating Iraq's Ministry of Foreign Affairs. The actor deployed two distinct attack chains using previously undocumented custom .NET-based malware - SPLITDROP, TWINTASK, TWINTALK, and GHOSTFORM, distributed via password-protected RAR archives and ClickFix-style social engineering lures. Compromised Iraqi government infrastructure was leveraged to host malicious payloads, and evidence of generative AI use in malware development was identified.

Attack Regions



Attack Details

#1

Dust Specter APT, a suspected Iran-linked threat group, launched a campaign targeting Iraqi government officials using two related attack chains designed to gain initial access and remote control of specific individuals. In the first attack chain, the group distributed a password-protected RAR archive named "mofa-Network-code.ra", crafted to appear as internal material from Iraq's Ministry of Foreign Affairs.

#2

The archive targeted individuals connected to the ministry and contained a 32-bit .NET file disguised as a WinRAR application. This file functioned as the SPLITDROP dropper. When opened, it displayed a password prompt and later a message claiming the download had failed, masking the malware's real activity.

#3

Once active, SPLITDROP extracted additional files and launched a legitimate copy of VLC media player. This allowed the attackers to sideload a malicious DLL called TWINTASK, which then loaded TWINTALK, the command-and-control component responsible for managing the infected system. The group also used social engineering. In July 2025, they hosted a fake Cisco Webex for Government meeting page that instructed targets to run a PowerShell command. This command downloaded a malicious file and scheduled it to run repeatedly on the system.

#4

The second attack chain relied on GHOSTFORM, a single .NET remote access trojan that combined the functions of both TWINTASK and TWINTALK. It executed PowerShell commands in memory to reduce visible files on the system. The malware ran inside an invisible Windows form and used timed delays before contacting its command server, helping it avoid common detection methods. Persistence was maintained through Windows Run registry entries.

#5

Both TWINTALK and GHOSTFORM communicated with command-and-control servers over HTTPS while using a User-Agent string that imitated the Chrome browser. The attackers also hosted malicious files on compromised Iraqi infrastructure, including the legitimate domain ca[.]iq, which delivered the ZIP archive containing the GHOSTFORM malware.

Recommendations

Deploy Detection Rules for DLL Sideloading: Create endpoint detection rules to flag unexpected DLL loads from `C:\ProgramData\` directories, particularly when initiated by legitimate binaries such as VLC.exe or WingetUI.exe, which are not expected to load DLLs from non-standard paths.

Monitor and Alert on Suspicious Registry Persistence: Implement monitoring for new entries created under `HKCU:\Software\Microsoft\Windows\CurrentVersion\Run` by processes running from `C:\ProgramData\`, which is a non-standard persistence path indicative of this campaign and similar techniques.

Restrict Execution of Password-Protected Archives from Untrusted Sources: Enforce policies that quarantine or flag password-protected RAR and ZIP archives received via email or downloaded from external sources, as this delivery mechanism is central to Dust Specter's Attack Chain 1.

Deploy JWT and Anomalous HTTP Header Inspection: Configure network inspection tools to detect JWT tokens in HTTP Authorization headers that contain non-standard fields, particularly numeric `iat` values inconsistent with Unix timestamps, as employed by TWINTALK and GHOSTFORM for bot identification.

Establish Geofencing and User-Agent Egress Filtering: Implement egress filtering policies that flag or block outbound HTTPS requests where the User-Agent is an exact static match to known malicious strings used by this campaign, and apply geofencing controls to restrict unexpected outbound connections to infrastructure in unusual geolocations.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Resource Development	T1583: Acquire Infrastructure	T1583.001: Domains
	T1587: Develop Capabilities	T1587.001: Malware
Initial Access	T1566: Phishing	T1566.002: Spearphishing Link
Execution	T1204: User Execution	T1204.004: Malicious Copy and Paste
	T1059: Command and Scripting Interpreter	T1059.001: PowerShell
	T1574: Hijack Execution Flow	T1574.001: DLL Side-Loading
Persistence	T1112: Modify Registry	
	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	
	T1205: Traffic Signaling	
	T1036: Masquerading	T1036.001: Invalid Code Signature
Discovery	T1082: System Information Discovery	
Command and Control	T1071: Application Layer Protocol	T1071.001: Web Protocols
	T1001: Data Obfuscation	T1001.003: Protocol or Service Impersonation
	T1132: Data Encoding	T1132.001: Standard Encoding
Exfiltration	T1041: Exfiltration Over C2 Channel	

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	b8254efd859f5420f1ce4060e4796c08, 78275f3fc7e209b85bff6a6f99acc68a, d5ddf40ba2506c57d3087d032d733e08, 8f44262afaa171b78fc9be20a0fb0071, 19ab3fd2800f62a47bf13a4cc4e4c124, 63702bd6422ec2d5678d4487146ea434, aa887d32eb9467abba263920e55d6abe, b19add5ccaa17a1308993e6f3f786b06, 7f17fa22feaced1a16d4d39c545cdb16, 70a9b537b9b7e1b410576d798e6c5043, a7561eb023bb2c4025defcfe758d8ac2, 809139c237c4062baecab43570060d67
SHA1	8621be9e1aa730d1ac8eb06fa8f66d9da70ff293, fc08f8403849c6233978a363f4cdc58cd7041823, 682c043443cb81b6c2fde8c5df43333f5d1fec53, 1debc4c512ded889464e386739d5d2f61b87ff13, c79c261457def606c3393dde77c82832a5c0ded3, c7dff3a0675f330feb9a7c469f8340369451d122, ad97e1bba1d040a237727afdb2787d6867d72b74, 51a746c85bd486f223130173b7e674379a51b694, 369b56a89b2fce2cbdc36f5a23bdec6067242911, cb1760c90fb6c399e0125c7aa793efe37c4ce533, df04e36c106691f9fe88e5798e4ae86438bd4f1d, 8735ee29c409b8d101eb3170f011455be41b7a91
SHA256	903f7869a94d88d43b9140bb656f7bb86ef725efc78ef2ff9d12fd7c7c2aca74, 6bb0d45799076b3f2d7f602b978a0779868fc72a1188374f6919fbbfba23efce, 797325b3c8a9356dcace75d93cb5cfb7847d2049c66772d4cc2cee821618cb96, 293ee1fe8d36aa79cf1f64f5ddef402bc6939d229c6fca955c7b796119564779, ad26cd72a83b884a8bc5aaa87309683953e151ebb3fde42eda7bf9a4406e530d, f3f2dc31f70a105db161a5e7b463b2215d3cbd64ac0146fd68e39da1c279f7ef, 6af71297ce7681e64d9a4c5449a7326f17f3f107cb7940ec5e0840390c457a47, 69294ad90aeb7f05e501e7191c95beb14e23da5587dd75557c867e2944a57fdc,

TYPE	VALUE
SHA256	fa51aff99d86a9f1f65aa0ebbf6ca40411d343cea59370851ab328b97e2164bb, a27d53608ab05b5c7cb86bcf4a273435238beeb7e7efd7845375b2aa765f51e2, eb5b7275c41de8e98d72696eeac9cba3719f334f8e7974e6b8760ece820b1d0c, 3a66ae5942f6feb79cf81ee70451f761253e0e0bde95f0840abdd42a804fad39
Filename	mofa-Network-code.rar, CheckFopil.exe, lecGen.exe, mofa-secret-code-92,110-135_118-128.rar, libvlc.dll, hostfxr.dll, in.txt, RiroDiog.exe, 893506.zip, webInfo.exe, mofaSurvey_20_30_oct.zip, file_oct_surv.exe
Domain	lecturegenieltd[.]pro, meetingapp[.]site, afterworld[.]store, girlsbags[.]shop, onlinepettools[.]shop, web14[.]info, web27[.]info
URL	hxxps[:]//ca[.]iq/packages/mofaSurvey_20_30_oct[.]zip

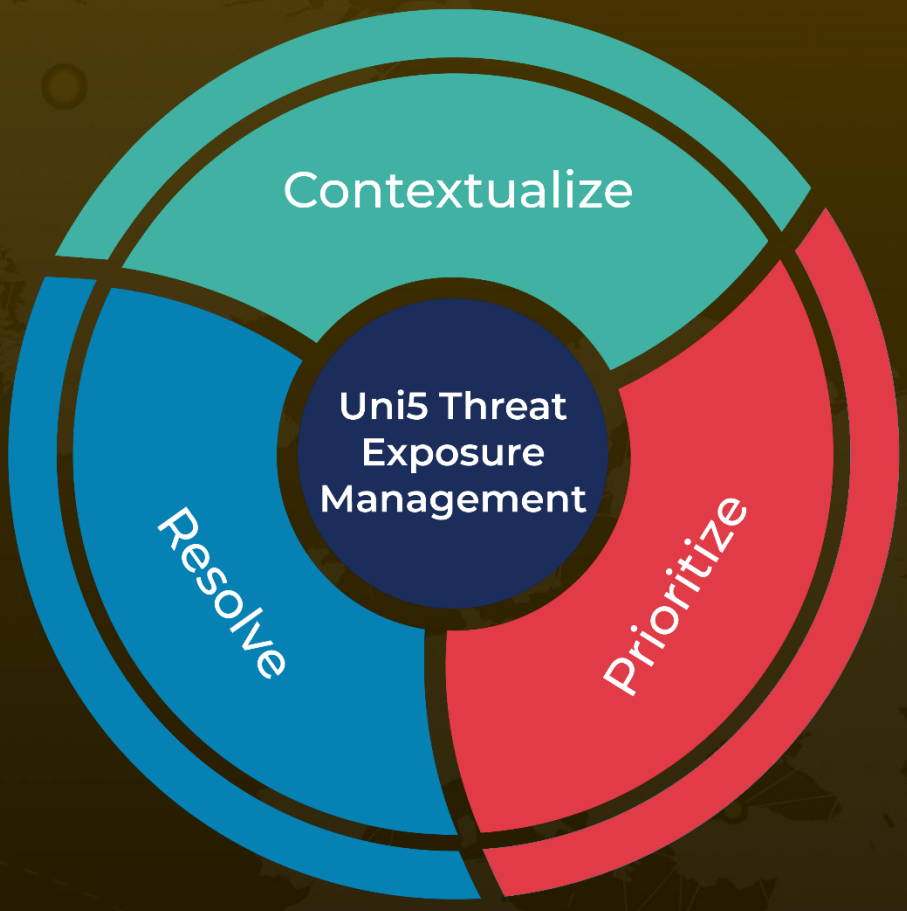
References

https://www.zscaler.com/blogs/security-research/dust-specter-apt-targets-government-officials-iraq

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

March 05, 2026 • 04:00 AM

More at www.hivepro.com