Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

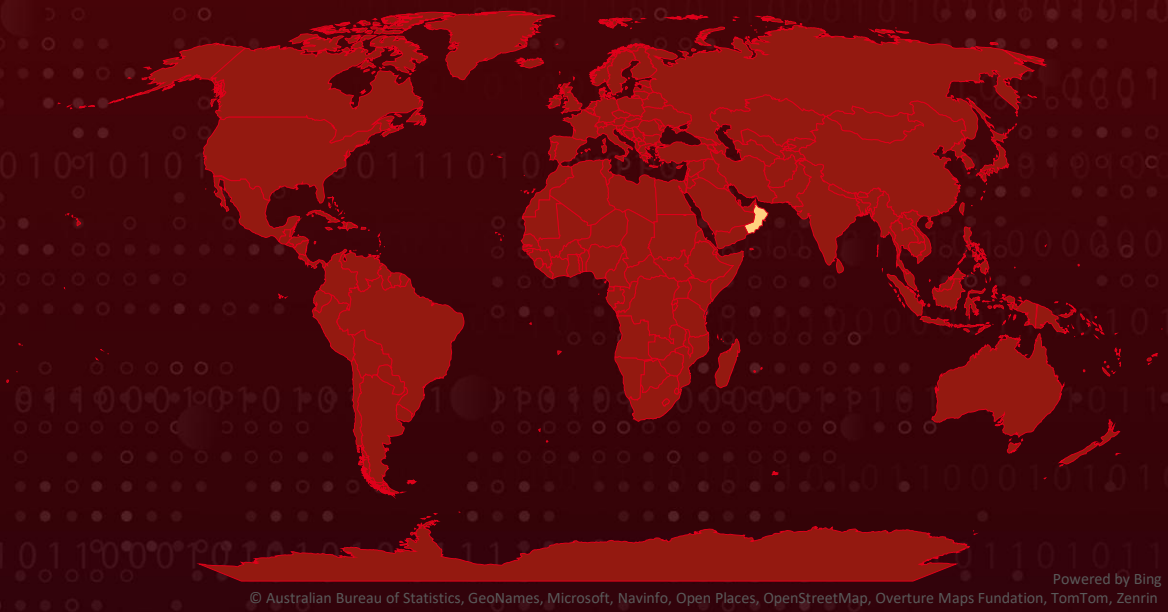
Iranian-Nexus Intrusion Targeting Oman's Government

Date of Publication	Admiralty Code	TA Number
June 2, 2026	A2	TA2026151

Summary

First Seen: April 8, 2026
Targeted Region: Oman
Targeted Platforms: Windows, Linux
Targeted Products: Microsoft Exchange Server, DotNetNuke (DNN)
Targeted Industries: Government, Defense
Threat Actor: Unattributed Iranian-nexus operator
Malware: GodPotato, Chisel
Attack: An Iranian-aligned espionage campaign hit 12 Omani government ministries, with the Ministry of Justice (MJLA) as the primary victim, exposed after the attacker left their staging VPS open with the full toolkit, C2 code, and stolen data in plaintext. Initial access came via CVE-2025-32372 (DotNetNuke SSRF), with ProxyShell (CVE-2021-34473/34523/31207) used against Exchange servers at other ministries. The operator deployed a custom ASPX webshell, Python C2 with PowerShell beacon, Chisel, and GodPotato, exfiltrating 26,000+ MJLA user records, judicial case data, citizen IDs, and SAM/SYSTEM registry hives. No group-level attribution, but TTPs strongly overlap with MOIS-linked APT34 (OilRig) and MuddyWater.

Attack Regions



Targeted Non-Targeted

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2021-34473	PROXYSHELL (Microsoft Exchange Server Remote Code Execution Vulnerability)	Microsoft Exchange Server	✗	✓	✓
CVE-2021-34523	PROXYSHELL (Microsoft Exchange Server Privilege Escalation Vulnerability)	Microsoft Exchange Server	✗	✓	✓
CVE-2021-31207	PROXYSHELL (Microsoft Exchange Server Security Feature Bypass Vulnerability)	Microsoft Exchange Server	✗	✓	✓
CVE-2025-32372	DotNetNuke Server-Side Request Forgery Vulnerability	DotNetNuke (DNN) Platform	✗	✗	✓

Attack Details

#1

An active Iranian-aligned cyber espionage operation has been identified targeting twelve Omani government ministries, with the Ministry of Justice and Legal Affairs (MJLA) as the primary victim. The campaign was uncovered after the threat actor left an attacker-controlled staging VPS (172.86.76[.]127, resolving to dubai-10.vaermb[.]com, UAE-hosted) publicly exposed, revealing the complete operator toolkit, command-and-control source code, session logs, and exfiltrated victim data in plaintext. Operator sessions were observed between April 8–10, 2026. The targeting builds on a 2025 incident attributed to the Homeland Justice persona, tracked as Void Manticore, in which Oman's Ministry of Foreign Affairs mailbox in Paris was hijacked to spear-phish embassies worldwide.

#2

Targeting extended across twelve government bodies, including MJLA, the Royal Oman Police, Royal Fleet of Oman, Tax Authority of Oman, State Audit Institution, Royal Court Affairs, Authority for Public Services Regulation, Civil Aviation Authority, Information Technology Authority, Ministry of Finance, MTCIT, and the Office of Public Prosecution. Initial access against MJLA most likely came through CVE-2025-32372, an SSRF flaw in DotNetNuke versions prior to 9.13.8. Secondary vectors included ProxyShell exploitation (CVE-2021-34473/34523/31207) against Exchange servers, a chain previously leveraged by MuddyWater in regional intrusions, and credential brute-force attempts against the eVisa portal and the State Audit Institution training platform.

#3

The webshell provided persistent remote command execution, while a host-level persistence attempt using a scheduled task named MicrosoftEdgeUpdate was blocked by Microsoft Defender. The operator deployed a Python HTTP C2 paired with a PowerShell beacon polling every 30 seconds and returning base64-encoded results in 1,500-character chunks. Chisel was staged for encrypted tunneling, and GodPotato (later replaced by a reflective in-memory variant) abused SeImpersonatePrivilege for escalation, tradecraft consistent with APT34's documented Gulf-targeted kernel-level operations.

#4

On April 10, 2026 at 03:00 UTC, the operator exfiltrated over 26,000 MJLA user records, staff emails and credentials, alongside judicial judgments, case session attachments, committee decisions, and queries against the eGov_Person table targeting national IDs, names, birthdates, and nationality. SAM and SYSTEM registry hives were staged in C:\Windows\Temp.

#5

No definitive group-level attribution has been made, though TTPs strongly overlap with MOIS-linked clusters APT34 (OilRig) and MuddyWater (Mango Sandstorm). The activity continues a broader pattern of Iranian state-nexus targeting against GCC critical infrastructure, alongside the Handala destructive wiper campaign and MOIS-aligned dissident espionage operations.

Recommendations

Patch Microsoft Exchange Against the ProxyShell Chain: Apply the Microsoft Exchange Server security updates that address CVE-2021-34473, CVE-2021-34523, and CVE-2021-31207. Any internet-facing Exchange that has not received the May 2021 cumulative update or later remains vulnerable to the full ProxyShell exploit chain demonstrated in this campaign.

Upgrade DotNetNuke to 9.13.8 or Later: Update all DotNetNuke (DNN) Platform instances to version 9.13.8 or newer to remediate CVE-2025-32372. Particular attention should be paid to ministry and government portals that expose DNN as a public-facing CMS, including those sharing identity-provider infrastructure such as SimpleSAMLphp federation.

Audit and Restrict the /Portals/0/ Path on DotNetNuke: Inspect the DotNetNuke /Portals/0/ directory for unauthorized ASPX files matching webshell patterns such as health_check_t.aspx or hc2.aspx, restrict write permissions to the path, and configure the IIS handler mapping so that arbitrary ASPX files placed in content directories cannot be served as executable script.

Reset MJLA and DotNetNuke Application Credentials: For the Ministry of Justice and Legal Affairs and any organization sharing federation with MJLA's SimpleSAMLphp identity provider, force-reset all DotNetNuke application accounts (with priority to superuser and aspnet_Membership-backed accounts), invalidate active sessions, and rotate any service-account passwords accessible from compromised hosts.

Rotate Domain Credentials and Re-secure SAM/SYSTEM Material: Because both SAM and SYSTEM registry hives were extracted from the MJLA environment, treat all local-machine secrets, cached domain credentials, and machine-account secrets within that environment as compromised; reset them, force a krbtgt double-rotation if Active Directory was reachable, and audit Kerberos ticket lifetimes for anomalies.

Adopt Network Segmentation Between Ministry Portals: Because the ITA and MTCIT portals share the /ITAPortal_AR/ URL structure and likely a common codebase, and because MJLA's SimpleSAMLphp identity provider could federate authentication across ministries, segment ministry portals from one another, isolate the identity provider in a dedicated security zone, and apply per-ministry boundary controls so that a single portal compromise cannot pivot horizontally.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Reconnaissance	T1595: Active Scanning	T1595.002: Vulnerability Scanning
Resource Development	T1583: Acquire Infrastructure	T1583.003: Virtual Private Server
	T1588: Obtain Capabilities	T1588.002: Tool
Initial Access	T1190: Exploit Public-Facing Application	
	T1110: Brute Force	T1110.001: Password Guessing
Execution	T1059: Command and Scripting Interpreter	T1059.001: PowerShell
		T1059.003: Windows Command Shell
		T1059.006: Python
Persistence	T1505: Server Software Component	T1505.003: Web Shell
	T1053: Scheduled Task/Job	T1053.005: Scheduled Task
Privilege Escalation	T1134: Access Token Manipulation	T1134.001: Token Impersonation/Theft
Defense Evasion	T1562: Impair Defenses	T1562.001: Disable or Modify Tools
	T1620: Reflective Code Loading	
	T1027: Obfuscated Files or Information	
	T1036: Masquerading	T1036.004: Masquerade Task or Service
		T1036.005: Match Legitimate Name or Location
Credential Access	T1003: OS Credential Dumping	T1003.002: Security Account Manager
	T1110: Brute Force	T1110.002: Password Cracking

Tactic	Technique	Sub-technique
Credential Access	T1555: Credentials from Password Stores	
	T1539: Steal Web Session Cookie	
Discovery	T1082: System Information Discovery	
	T1016: System Network Configuration Discovery	
	T1033: System Owner/User Discovery	
	T1083: File and Directory Discovery	
	T1046: Network Service Discovery	
Collection	T1005: Data from Local System	
	T1213: Data from Information Repositories	
	T1560: Archive Collected Data	
Command and Control	T1071: Application Layer Protocol	T1071.001: Web Protocols
	T1090: Proxy	
	T1572: Protocol Tunneling	
	T1132: Data Encoding	T1132.001: Standard Encoding
Exfiltration	T1041: Exfiltration Over C2 Channel	

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	172[.]86[.]76[.]127, 172[.]86[.]76[.]101, 172[.]86[.]76[.]94, 172[.]86[.]76[.]108, 172[.]86[.]76[.]112, 172[.]86[.]76[.]120, 172[.]86[.]76[.]121, 172[.]86[.]76[.]124, 172[.]86[.]76[.]129, 172[.]86[.]76[.]130, 45[.]59[.]114[.]60, 104[.]21[.]27[.]95, 172[.]67[.]142[.]35
Domain	dubai-10.vaermb[.]com, dubai-1.vaermb[.]com, dubai-2.vaermb[.]com, dubai-3.vaermb[.]com, dubai-4.vaermb[.]com, dubai-5.vaermb[.]com, dubai-6.vaermb[.]com, dubai-7.vaermb[.]com, dubai-8.vaermb[.]com, dubai-9.vaermb[.]com, regorixa[.]com, myjitsi.exceptionnotfound[.]ir, shop.exceptionnotfound[.]ir, price.exceptionnotfound[.]ir, tools.exceptionnotfound[.]ir, myjitsi.mrnajafipour[.]ir, s5.sideliner[.]ir, suanefllix[.]com, brnettlix[.]com, brttfrixx[.]com, realprimefix[.]com, identificara[.]com
Filename	hc2.aspx

TYPE	VALUE
Filename	health_check_t.aspx, proxyshell_01.sh, evisa_cookies.txt, c2_fixed.py, c2_fixed_v2.py, c2_json_v2.py, new_beacon.ps1, gp_v6_exec.py
File Path	/Portals/0/health_check_t.aspx, /opt/c2/loot/, /opt/c2/payloads/, C:\Windows\Temp (registry hive staging)
SHA256	ECC3611F7DCBAA53ACF44E67DE2F10D78A26E03B3C77BA28BBD3EE16B2E66437
Port	8001 (C2 beacon listener), 7777 (Chisel host), 9002 (Registry hive exfiltration), 9003 (Reverse SOCKS5 listener)

Patch Links

https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-34473

https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-34523

https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-31207

https://github.com/dnnsoftware/Dnn.Platform/releases/

References

https://hunt.io/blog/iranian-nexus-oman-government-intrusion

https://hivepro.com/threat-advisory/void-manticore-irans-evolving-cyber-warfare-model/

https://hivepro.com/threat-advisory/muddywater-is-taking-advantage-of-old-vulnerabilities/

https://hivepro.com/threat-advisory/apt34-tightens-cyber-espionage-grip-on-gulf-with-kernel-exploitation/

https://hivepro.com/threat-advisory/prolonged-pursuit-of-oilrig-apt-targeting-middle-east-government/

https://hivepro.com/threat-advisory/muddywater-irans-adaptive-cyber-espionage-machine/

https://hivepro.com/threat-advisory/handala-claims-destructive-wiper-attack-on-gcc-nations-critical-infrastructure/

https://hivepro.com/threat-advisory/iranian-mois-leverages-telegram-based-c2-in-espionage-campaign-targeting-dissidents/

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 • 11:40 AM

More at www.hivepro.com