Lookout Discovers MuddyWater Leveraging DCHSpy For Israel-Iran Conflict

By Lookout

Published: 2025-07-21 · Archived: 2026-04-05 12:52:11 UTC

DCHSpy is an Android surveillanceware family that Lookout customers have been protected from since 2024. It is likely developed and maintained by MuddyWater, which is a cyber espionage group believed to be affiliated with Iran's Ministry of Intelligence and Security (MOIS). This group targets diverse government and private entities in various sectors, such as telecommunications, local government, defense, and oil and natural gas, across the Middle East, Asia, Africa, Europe, and North America.

In light of the recent conflict in Iran, it appears that new versions of DCHSpy are being deployed against adversaries. It uses political lures and disguises as legitimate apps like VPNs or banking applications. This modular malware collects the following data:

- Accounts logged into on the device
- Contacts
- SMS messages
- Files stored on the device
- Location data
- Call logs
- Audio by taking control of the microphone
- Photos by taking control of the camera
- WhatsApp data

DCHSpy shares infrastructure with another Android malware known as SandStrike, an Android surveillanceware targeting Bahá’í practitioners originally reported publicly by Kaspersky in 2022. Lookout researchers discovered that the hardcoded command and control (C2) IP address in the SandStrike sample was also used multiple times to deploy a PowerShell RAT attributed to MuddyWater. Notably, the SandStrike sample also contained a malicious VPN configuration file tied to threat actor controlled infrastructure.

DCHSpy uses similar tactics and infrastructure as SandStrike. It is distributed to targeted groups and individuals by leveraging malicious URLs shared directly over messaging apps such as Telegram.

New Capabilities, Targeting, and StarLink Lures

About a week after Israel launched its initial strikes on Iranian nuclear infrastructure, Lookout acquired four new samples of DCHSpy. These new samples show that MuddyWater has continued to develop the surveillanceware with new capabilities - this time exhibiting the ability to identify and exfiltrate data from files of interest on the device as well as WhatsApp data.

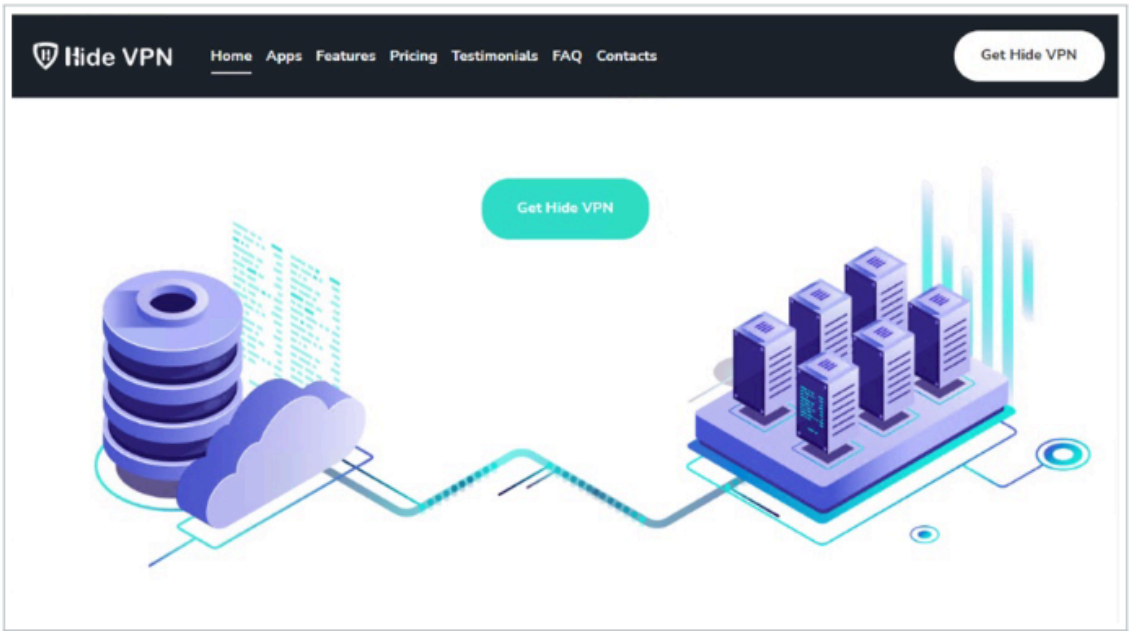
Title	Package Name	SHA1	Acquired Date
Earth VPN	com.earth.earth_vpn	556d7ac665fa3cc6e56070641d4f0f5c36670d38	02.07.2025
Comodo VPN	com.comodoapp.comodovpn	7010e2b424eadfa261483ebb8d2cca4aac34670c	25.06.2025
Earth VPN	com.earth.earth_vpn	8f37a3e2017d543f4a788de3b05889e5e0bc4b06	23.06.2025
Earth VPN	com.earth.earth_vpn	9dec46d71289710cd09582d84017718e0547f438	20.06.2025
حضرت عشق (Hazrat Eshg)	hazrateeshgh.apk	6c291b3e90325bea8e64a82742747d6cdce22e5b	2024-04-12
Hide VPN	com.hv.hide_vpn	7267f796581e4786dbc715c6d62747d27df09c61	2023-07-16

One of the Earth VPN samples, SHA1:9dec46d71289710cd09582d84017718e0547f438, was uploaded with an APK filename of starlink_vpn(1.3.0)-3012 (1).apk. This may indicate that DCHSpy VPN samples are also being spread with Starlink lures, especially given recent reports of Starlink offering internet services to the Iranian population during the internet outage imposed by the Iranian government following hostilities between Israel and Iran.

Once data is collected off of an infected device, it is compressed and encrypted with a password it receives from the command and control (C2) server. Following additional commands from the C2 server, the data is uploaded to the destination Secure File Transfer Protocol (SFTP) server.

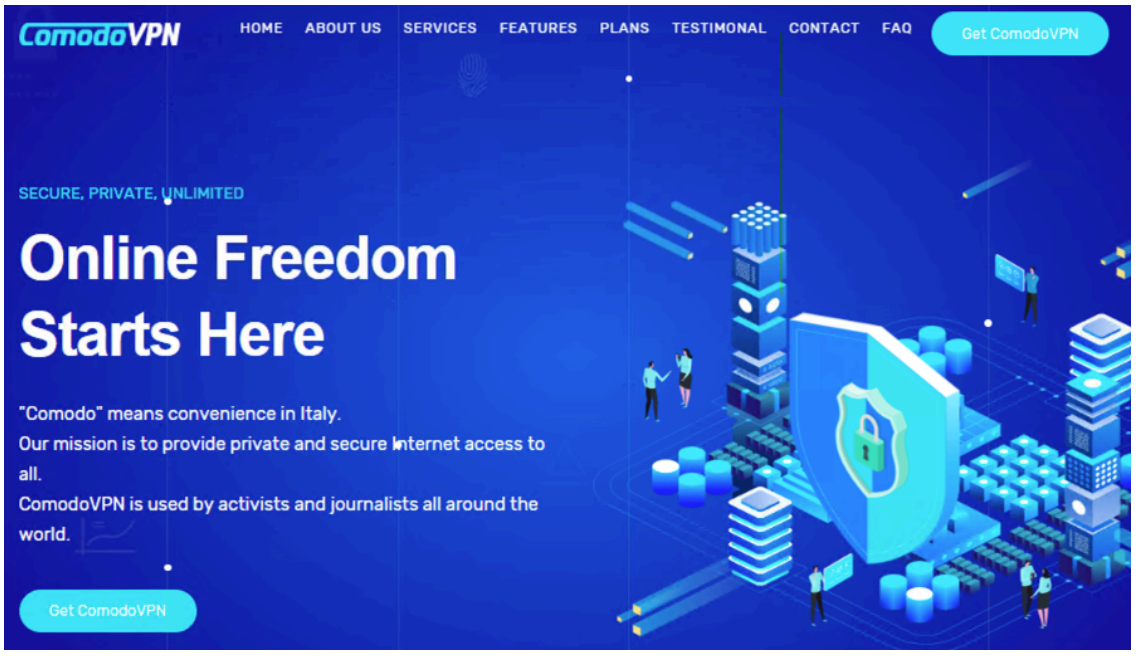
Parallel Tactics

When Lookout first disclosed research on DCHSpy to its Threat Advisory Service customers, we highlighted that MuddyWater leveraged a malicious VPN app that was distributed via Telegram as these new samples are. The Telegram channels advertise the malicious VPN applications to English and Farsi speakers, and feature themes and language consistent with views contrary to the Iranian regime. In previous reporting, the threat actor advertised *HideVPN* and led victims to the following webpage:



The malicious VPN distribution page from July 2024

In the discovery of this most recent version of DCHSpy, the actor is now advertising two malicious VPN services called *EarthVPN* and *ComodoVPN*. Below is an example of the ComodoVPN distribution page, which is a similarly simple webpage as we saw with the *Hide VPN* page above. Comodo VPN claims to be located in Canada and Earth VPN claims to be located in Romania. They list addresses and contact numbers from these countries which actually belong to random businesses in those respective countries.



The malicious VPN distribution page from June 2025, which is notably targeted at activists and journalists globally.

Continued Observation and Research

Threat actors tied to the Iranian government are no strangers in the mobile surveillanceware landscape. Lookout's research team tracks 17 unique mobile malware families tied to at least 10 Iranian APTs with activity spanning over a decade, along with multiple campaigns conducted with commodity spyware such as Metasploit, AndroRat and AhMyth. In addition to this continued activity around DCHSpy, Lookout researchers also disclosed BouldSpy in 2023. At the time, BouldSpy was a novel Android surveillanceware tool used by the Law Enforcement Command of the Islamic Republic of Iran (FARAJA).

These most recent samples of DCHSpy indicate continued development and usage of the surveillanceware as the situation in the Middle East evolves, especially as Iran cracks down on its citizens following the ceasefire with Israel. Lookout researchers have observed countless instances of nation-states monitoring threats to their authority and spying on enemy soldiers during times of conflict by quietly delivering malicious apps to their mobile devices through social engineering. Recent examples include the GuardZoo surveillanceware tied to the Houthis, an Iranian proxy, and campaigns targeting Assad's forces in Syria using the commodity malware SpyMax.

Lookout will continue to track MuddyWater's activity and inform our threat intelligence customers of any relevant updates.

Indicators of Compromise (IoCs)

SHA1s

556d7ac665fa3cc6e56070641d4f0f5c36670d38

7010e2b424eadfa261483ebb8d2cca4aac34670c

8f37a3e2017d543f4a788de3b05889e5e0bc4b06

9dec46d71289710cd09582d84017718e0547f438

6c291b3e90325bea8e64a82742747d6cdce22e5b

7267f796581e4786dbc715c6d62747d27df09c61

67ab474e08890c266d242edaca7fab1b958d21d4

f194259e435ff6f099557bb9675771470ab2a7e3

cb2ffe5accc89608828f5c1cd960d660aac2971d

Command and Control:

https://it1[.]comodo-vpn[.]com:1953

https://it1[.]comodo-vpn[.]com:1950

https://r1[.]earthvpn[.]org:3413

https://r2[.]earthvpn[.]org:3413

http://192.121.113[.]60/dev/run.php

http://79.132.128[.]81/dev/run.php

n14mit69company[.]top

https://hs1.iphide[.]net:751

https://hs2.iphide[.]net:751

https://hs3.iphide[.]net:751

https://hs4.iphide[.]net:751

http://194.26.213[.]176/class/mcrypt.php

http://45.86.163[.]10/class/mcrypt.php

http://46.30.188[.]243/class/mcrypt.php

http://77.75.230[.]135/class/mcrypt.php

http://185.203.119[.]134/DP/dl.php
