MuddyWater Operations in Lebanon and Oman – ClearSky Cyber Security

Published: 2018-11-28 · Archived: 2026-04-05 16:35:59 UTC

Abstract

MuddyWater is an Iranian high-profile threat actor that's been seen active since 2017. The group is known for espionage campaigns in the Middle East. Over the past year, we've seen the group extensively targeting a wide gamut of entities in various sectors, including Governments, Academy, Crypto-Currency, Telecommunications and the Oil sectors.

MuddyWater has recently been targeting victims likely from Lebanon and Oman, while leveraging **compromised domains, one of which is owned by an Israeli web developer.** The investigation aimed to uncover additional details regarding the compromise vector. Further, we wished to determine the infection vector, which is currently unknown. With that in mind, past experience implies that this might be a two-stage spear-phishing campaign.

In the first stage of the operation the attackers deliver a macro-embedded document. Depending on each sample, the content of document is either a fake resume application, or a letter from the Ministry of Justice in Lebanon or Saudi Arabia. Note that these documents' content is falsely blurred in order to increase the chances of infection. As stated, the obfuscated code used in the campaign was hosted on three compromised domains, including an Israeli domain (pazazta[.]com).

An interesting aspect of this campaign is that the attackers, uncharacteristically to the group, implemented a manual override to the attack process; which in turn provided them with more control over the payload. Moreover, previously the group only executed single-stage attacks; however, this time around they split the course of attack into two stages. Thus, spreading MuddyWater's main PowerShell Backdoor dubbed POWERSTATS in a stealthier method.

Special thanks for the researchers Jacob Soo and Mo Bustami that assisted us.

Read the full report: MuddyWater Operations in Lebanon and Oman

Figure 1: Blurred resume document showing a deceptive error message.

Figure 2: Blurred document disguised as a letter from the Ministry of Justice in Lebanon

Figure 3: Blurred document disguised as a letter from the Ministry of Justice in Saudi Arabia (target from Oman)

Attribution

As MuddyWater has consistently been using POWERSTATS as its main tool, they are relatively easy to distinguish from other actors. Nevertheless, this time we observed a slightly similar but different pattern, depicting conservation of TTPs alongside developing new capabilities.

Our findings corroborate several TTPs changes that were foreseen by other researchers. These assessments were based on leaked test documents attributed to the group, that were observed during the past year. It appears MuddyWater recent efforts to evolve are beginning to bear fruit, as they also added evasion capabilities to their arsenal.

TTPs

One of the most noteworthy aspects of MuddyWater's recent transformation is the progression from a single-stage to a **two-stage attack** process.

- Malicious macro-embedded document used to launch an Excel process and a PowerShell command as first stage. The group leverages **commands execution via 3rd party processes** (e.g. Excel) used not only for

POWERSTATS functionality as seen before, but also for first-stage needs – pertaining to downloading the second stage from a certain open-directory.
- Obfuscated source code hosted on compromised domains is retrieved and executed as second stage for POWERSTATS Backdoor propagation. Main source code consists of PowerShell commands and variables. These variables are then divided into multiple layers of obfuscated intertwined encoded VBScript (VBE), JavaScript and PowerShell code.

This point is of particular importance, as it is the basis for a new **three-steps backdoor execution mechanism** (this will be further detailed later in the blog).

Moreover, it appears **MuddyWater operators do not cover their tracks** and do not remove their code from these open-directories that are currently accessible and available to everyone.

Conclusions

The Iranian MuddyWater group keeps evolving, improving its capabilities with every new campaign. We encourage the security community to harness these IOCs and knowledge to detect and defend from the threat.

Pivot

The Maltego graph below depicts the relationship among the indicators (click to enlarge):

Indicators of Compromise

Macro-embedded Documents:

SHA256 Hash	File Name	Impersonation

65bd49d9f6d9b92478e3653362c0031919607302db6cfb3a7c1994d20be18bcc	MyCV.doc	Fake resume
294a907c27d622380727496cd7c53bf908af7a88657302ebd0a9ecdd30d2ec9d	Cv.doc	Fake resume
ac360ec9dbf84ab7e26effcb1d28ca4d0ac4381c9376ac1eddee7a8f7f26ccb0	shakva-lb (1).zip	Ministry of Justice in Lebanon
b6c483536379840e89444523d27ac7828b3eb50342b992d2c8f608450cd7bb53	shakva-lb.doc	
a6ba3480f3c7055dce2a7a43c3f70d3d6b266290f917be150a0e17b6ac4a3724	shakva-om.zip	Ministry of Justice in Saudi Arabia
e5c56c5b9620fb542eab82bdf75237d179bc996584b5c5f7a1c34ef5ae521c7d	shakva-om.doc	

Network Indicators:

Second-stage delivery URLs:

- hxxp://3cbc[.]net/dropbox/icon[.]icon
- hxxp://pazazta[.]com/app/icon[.]png
- hxxp://ohe[.]ie/cli/icon[.]png
- hxxp://ohe[.]ie/cp/icon[.]png

Proxy-List of POWERSTATS backdoor:

- hxxp://andreabelfi[.]com/main.php
- hxxp://andreasiegl[.]com/main.php
- hxxp://andresocana[.]com/main.php
- hxxp://amorenvena[.]com/main.php
- hxxp://amphira[.]com/main.php
- hxxp://amphibiblechurch[.]com/main.php

Source: https://www.clearskysec.com/muddywater-operations-in-lebanon-and-oman/