Falling on MuddyWater – Where security meets innovation

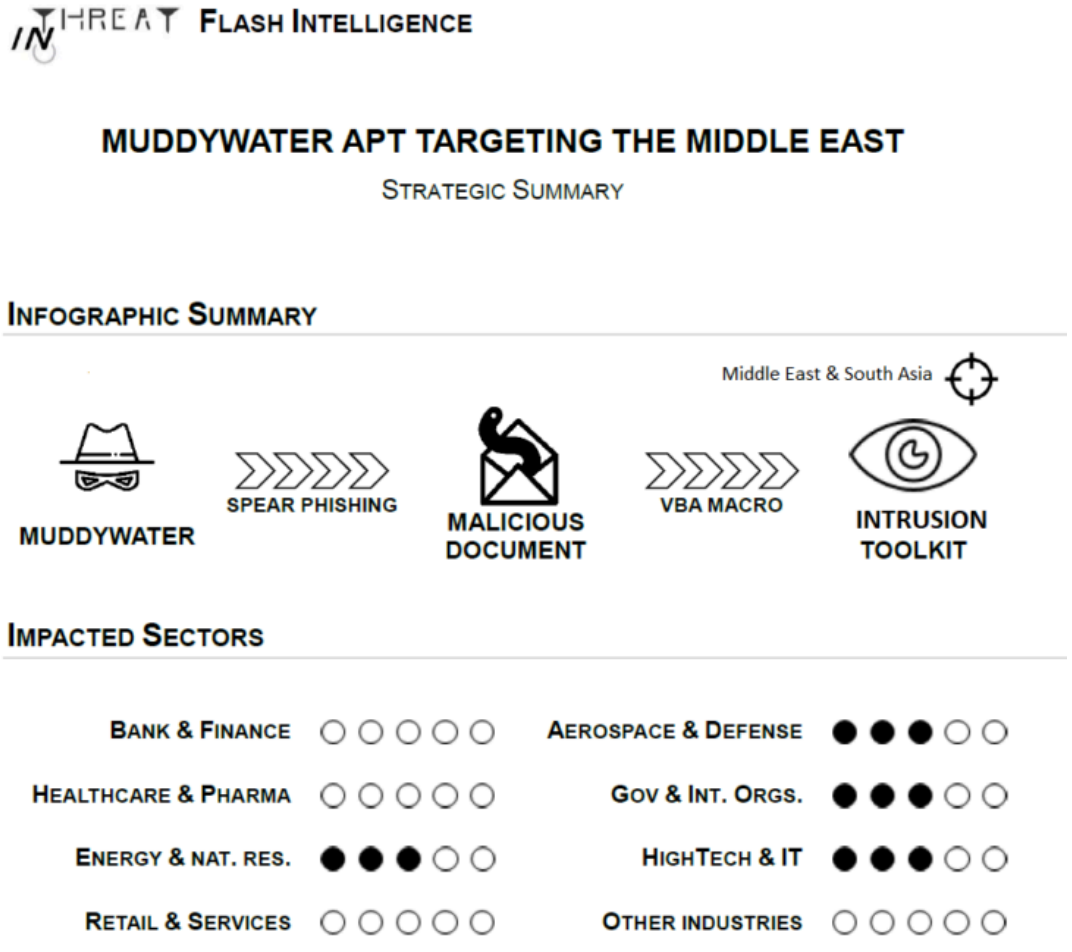
By inThreat Team

Archived: 2026-04-05 22:55:18 UTC

MuddyWater [1] is regularly mentioned in the headlines. We took time to summarize the past campaigns and try to establish liaisons between TTPs and targets.

Overview of MuddyWater

MuddyWater's TTPs were exposed in a MalwareBytes' blog in September 2017 [2]. We have been following their activity since this date to provide intelligence to our inThreat customers and below is an overview of this threat actor's modus operandi and targets:

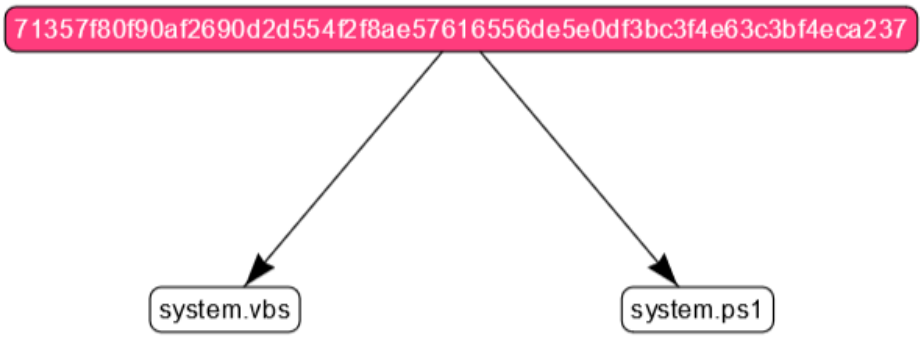


Extract from our Flash Intelligence Report

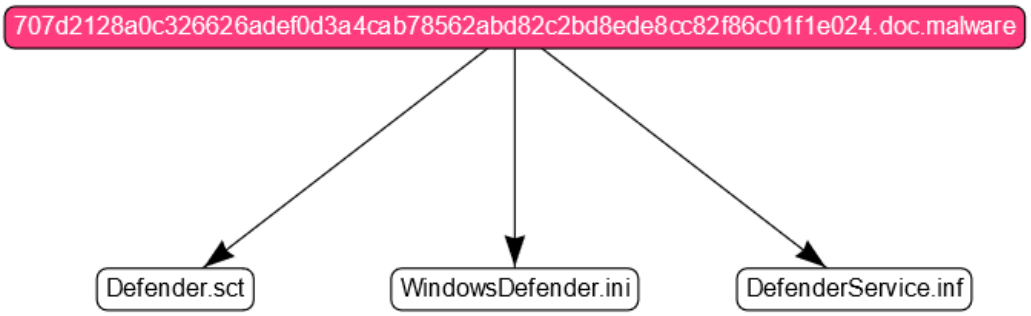
MuddyWater has stable TTPs… so far

From what we have learned so far, we associate the name MuddyWater with a threat group which has been consistently delivering a specific Powershell script, named POWERSTATS [3], to multiple targets in the Middle East and South Asia. POWERSTATS has been very well described by ReaQta, TrendMicro and FireEye [1] [4] [5]. Its main purpose is to collect data and execute other tools on the victim's machine. Researchers from Morphisec – who first spotted the backdoor back in March 2017- and from ReaQta were able to observe some post-compromise actions during which POWERSTATS was used to download several tools such as Meterpreter, a powershell DNS backdoor, a RAT named Koadic or a python password stealer [5] [6]. POWERSTATS remained stable in 2017 even though lateral movement functions appeared quite recently [1] [7].

MuddyWater's main delivery tactics for POWERSTATS is to lure a target into opening a malicious Word document which then drops POWERSTATS. These baits however require the execution of an embedded VBA macro code. The POWERSTATS script is also heavily obfuscated, with five to seven layers of powershell obfuscation. Testing the documents into a malware analysis engine will nonetheless easily unveal the VBA obfuscated code and the dropped files.



https://malware.sekoia.fr/results/71357f80f90af2690d2d554f2f8ae57616556de5e0df3bc3f4e63c3bf4eca237 (typical bait for 2017 campaigns)



https://malware.sekoia.fr/results/707d2128a0c326626adef0d3a4cab78562abd82c2bd8ede8cc82f86c01f1e024 (Bait from a 2018 campaign)

We believe these documents are sent via spear phishing emails. Consistent with this hypothesis, some of the most recent documents require that the victim enters a password which is most probably sent in an accompanying email.

Clearing the mud

There is no clear indication on what MuddyWater's ultimate motivation is yet. While some analysts think that their main goal is cyberespionnage, we are cautious with this idea. Indeed little information is currently known on MuddyWater's targets and their post-exploitation actions.

We do however have a good idea on what their areas of interest are. Indeed, the bait documents share a similar and typical look-and-feel which makes them quite characteristic. More interestingly, they are designed with a particular theme which is specific enough to provide a good hint on which countries or industries might be concerned. Based on our intel, we've summarized MuddyWater's intrusion campaigns in the following table:

	G/U*	GE	IQ	SA	AZ	PK	TK	TJ	IN	TOTAL
févr-17		2								2
mars-17	1									1
avr-17										0
mai-17	1	1								2
juin-17										0
juil-17	3									3
août-17	2		1							3
sept-17	1		1	4						6
oct-17	3			2	1	2	1			9
nov-17	2		2			2				6
déc-17						2	1	1		4
janv-18	2			1			5	3		11
févr-18						3	8		1	12
mars-18						1	4			5
TOTAL	15	3	4	7	1	10	19	4	1	64

Number of distinct malicious documents distributed by country according to their theme
G/U* Generic or Undefined theme

The first information which pops out of this data is that MuddyWater seem to have intensified their operations since the third quarter of 2017.

Secondly, their areas of interest have switched in 2018. Turkish organizations and/or individuals have become important targets. The themes used in malicious documents with a Turkish bait suggest that Turkish targets are linked to the government, Defense industry, or the economy. As an example, one spear phishing email was designed to spoof the Turkish Intelligence Services, and lure an employee of a Turkish company working for the Turkish armed forces.

Pakistani, Tajik and Indian organizations might also be current targets of MuddyWater intrusion campaigns, while Georgian, Iraqian, Saudi Arabian and Azerbaijani organizations do not seem to be targeted anymore, at least with

this delivery tactic.

Some questions remains

An analysis by ReaQta of MuddyWater's C&C traffic suggested that, although it had the highest number of infections, Pakistan was not one of the most interesting countries for MuddyWater, as opposed to Saudi Arabia, the United Arab Emirates or Iraq, which had much lower infection levels but higher C&C activities [5]. However, we currently count 10 different malicious documents with a clear Pakistan-related bait, which shows that MuddyWater put some efforts into targeting Pakistani individuals or organizations. On the other hand, while we noticed several documents targeting Iraq or Saudi Arabia, we found only one document with a loose focus on the UAE: the "veri peri branches information.doc" [8]. Veri Peri owns a franchise restaurant in the UAE – and in other countries in the Middle East [9]. Although there are even more documents with a generic theme for which we cannot infer the targeted intention, the current information on MuddyWater's malicious documents does not seem in accordance with ReaQta's findings.

Could it be possible that MuddyWater is targeting some groups among the Pakistani diaspora (Pakistani are the second largest group in the UAE, while Pakistani in Saudi Arabia and Pakistani in the UAE are respectively the second and third largest communities outside Pakistan [10]) ? Or that MuddyWater is using a different, yet uncharacterized or un-attributed, delivery tactic to target organizations in the UAE ?

The discovery of malicious .jar files installing POWERSTATS posted in an English-speaking cybersecurity community in January 2018 [11] suggests that the latter possibility is quite plausible. However, what could be the underlying rationale for a group which seems to have consistently targeted specific organizations to switch on random infections? We believe there is still a lot to discover about MuddyWater, and we think it's not time for early conclusions.

……..

[1] FireEye uses the name "Temp.Zagros". https://www.fireeye.com/blog/threat-research/2018/03/iranian-threat-group-updates-ttps-in-spear-phishing-campaign.html

[2] https://blog.malwarebytes.com/threat-analysis/2017/09/elaborate-scripting-fu-used-in-espionage-attack-against-saudi-arabia-government_entity/

[3] or TROJ_VALYRIA.PS

[4] see https://blog.trendmicro.com/trendlabs-security-intelligence/campaign-possibly-connected-muddywater-surfaces-middle-east-central-asia/

[5] https://reaqta.com/2017/11/muddywater-apt-targeting-middle-east/

[6] http://blog.morphisec.com/fileless-attack-framework-discovery

[7] https://sec0wn.blogspot.fr/2018/03/a-quick-dip-into-muddywaters-recent.html

[8] 97988dfdd7e49192186167e5bba901505b4b4a804f19b8747450964c8b84672c

[9] http://veri-peri.com/contact-us/

[10] https://en.wikipedia.org/wiki/Pakistanis_in_the_United_Arab_Emirates

[11] https://sec0wn.blogspot.fr/2018/02/burping-on-muddywater.html

---