THREAT CURE

RE-ARCHITECT YOUR THREAT LANDSCAPE

Cyber Threat Advisory

MuddyWater

Threat Actor Malware

CATEGORY

Malware

SEVERITY

High

Platforms

Windows

IMPACT

- Low Detection Profile
- Geopolitical Focus
- Economic Impact
- Governmental Risks
- Persistent Threat

Description

MuddyWater

MuddyWater is an APT group that has been active since 2017, primarily targeting victims in the Middle East using in-memory vectors with PowerShell. These attacks are part of the "Living off the Land" strategy, which avoids creating new binaries on the victim's machine, thus maintaining a low detection profile and minimal forensic footprint. The operators behind MuddyWater appear to be espionage-motivated, as indicated by data analysis and backdoor behaviors. Although there is a significant number of victims from Pakistan, the most active targets are in Saudi Arabia, the UAE, and Iraq. The victims include a variety of entities, with a stronger focus on governments, telecommunications companies, and oil companies. By tracking their operations, it has been deduced that the attacks likely originate from Iran, although it remains unclear whether MuddyWater is state-sponsored or a criminal organization with espionage tendencies.

While MuddyWater primarily targets Middle Eastern nations, attacks have also been observed in surrounding regions and beyond, including India and the USA. The group’s attacks are characterized by the use of a slowly evolving PowerShell-based first-stage backdoor known as “POWERSTATS.” Despite extensive scrutiny and reports on MuddyWater’s activities, the group continues its operations with only incremental changes to their tools and techniques.

Indicator of compromise

SHA-256

d2a0eec18d755d456a34865ff2ffc14e3969ea77f7235ef5dfc3928972d7960f
1421a5cd0566f4a69e7ca9cdefa380507144d7ed59cd22e53bfd25263c201a6f
4e3c7defd6f3061b0303e687a4b5b3cc2a4ae84cdc48706c65a7b1e53402efc0
8b96804d861ea690fcb61224ec27b84476cf3117222cca05e6eba955d9395deb
16985600c959f6267476da614243a585b1b222213ec938351ef6a26560c992db
cf87a2ac51503d645e827913dd69f3d80b66a58195e5a0044af23ea6ba46b823
3030d80cfe1ee6986657a2d9b76b626ea05e2c289dee05bd7b9553b10d14e4a1
99077dcb37395603db0f99823a190f50313dc4e9819462c7da29c4bc983f42fd
1b60b7f9b0faf25288f1057b154413921a6cb373dcee43e831b9263c5b3077ce
2c8d18f03b6624fa38cae0141b91932ba9dc1221ec5cf7f841a2f7e31685e6a1
367021beedb3ad415c69c9a0e657dc3ed82b1b24a41a71537d889f5e2b7ca433
58282917a024ac252966650361ac4cbbbed48a0df7cab7b9a6329d4a04551c0d
58898648a68f0639c06bedc8242ca48bc6ec56f11ed40d00aa5fdda4e5553482
917a6c816684f22934e2998f43633179e14dcc2e609c6931dd2fc36098c48028
db7bdd6c3ff7a27bd4aa9acc17dc35c38b527fb736a17d0927a0b3d7e94acb42
de6ce9b75f4523a5b235f90fa00027be5920c97a972ad6cb2311953446c81e1d
a6673c6d52dd5361afd96f8143b88810812daa97004f69661da625aaaba9363b
40a6b4c6746e37d0c5ecb801e7656c9941f4839f94d8f4cd61eaf2b812feaabe
81523e0199ae1dc9e87d2b952642785bfbda6326f22e4c0794a19afdf001a9a3
90b66b3fef77962fbfda364a4f8799bfcc9ab73772026d7a8922a7cf5556a024
96101de2386e35bc5e38d32524a02c6c5ca7cc6624e656a629b2e0f1693a76fd
964aaf5d9b1c749df0a2df1f1b4193e5a643893f251e2d74b47663f895da9b13
97f9a83bc6bb1b3f5cb7ac9401f95265597bff796bb4901631d6fa2c79a48bdc
a3c1fd46177a078c4b95c744a24103df7d0a58cee1a3be92bc4cdd7dec1b1aa5

0ab2b0a2c46d14593fe900e7c9ce5370c9cfbf6927c8adb5812c797a25b7f955
55af6a90ac8863f27b3fcaa416a0f1e4ff02fb42aa46a7274c6b76aa000aacc2
3a5f7d40e51ddecfa6f081d11f8768383b32f6e65d1860d7afe4336f009614d5
73c677dd3b264e7eb80e26e78ac9df1dba30915b5ce3b1bc1c83db52b9c6b30e
94278fa01900fdbfb58d2e373895c045c69c01915edc5349cd6f3e5b7130c472
7b1b332c653d62effffffd27a8da5bf78c0a5e5c1fb04191e0943333671c46c3
d2809e3e60e5d9671be8644750ad1b385aaa6b4ff01fef8fc594d81c69275a33
f9c1a117de8519060a3bf189e72277e895345b8fece73fc0d750946c7f288367
f17f6866f4748e6e762752062acdf983d3b083371db83503686b91512b9bcae3
fb58c54a6d0ed24e85b213f0c487f8df05e421d7b07bd2bece3a925a855be93a
cc8be1d525853403f6cfabcf0fc3bd0ca398ece559388102a7fc55e9f3aa9b33
bab601635aafeae5fbfe1c1f7204de17b189b345efd91c46001f6d83efbb3c5a
d22fd0cdd6ace24e117d7330e9996a2809c2c2cb280b12f9ea43c484d2bfcfd4
900d08037d303d9b3d4a855e1a97d1f9283c28fe279e67eefe9997f856eeb439
85103955e35a1355ce68a92eaedd8f9376de1927d95bf12657b348dea6a8077b
9b49d6640f5f0f1d68f649252a96052f1d2e0822feadd7ebe3ab6a3cadd75985
ec553e14b84ccca9b84e96a9ed19188a1ba5f4bf1ca278ab88f928f0b00b9bd0
31591fcf677a2da2834d2cc99a00ab500918b53900318f6b19ea708eba2b38ab
4b41b605ffc0e31bd9d460d5a296ac6e8cfd56a215dc131e90ec2654f0ffe31b
165a80f6856487b3b4f41225ac60eed99c3d603f5a35febab8235757a273d1fd
09e09503962a2a8022859e72b86ad8c69dcbf79839b71897c0bf8a4c4b9f4dd6
2722e289767ae391e3c3773b8640a8b9f6eb24c6a9d6e541f29c8765f7a8944b
5d7eb6c36d261adeef1a59bde9eb965f5d8d7f56a2e607da913e782167ba6cb6
d22fd0cdd6ace24e117d7330e9996a2809c2c2cb280b12f9ea43c484d2bfcfd4

SHA-256

fcfbdffbcad731e0a5aad349215c87ed919865d66c287a6723fd8e2f896c5834
2bb1637c80f0a7df7260a8583beb033f4afbdd5c321ff5642bc8e1868194e009
58aec38e98aba66f9f01ca53442d160a2da7b137efbc940672982a4d8415a186
605fefc7829cfa41710e0b844084eab1f180fe513adc1d8f0f82501a154db0f4
e8a832b04dbdc413b71076754c3a0bf07cb7b9b61927248c482ddca32e1dab89
5d049bd7f478ea5d978b3c78f7f0afdf294a94f526fc20ffd6e33022d40d15ae
12a7898fe5c75e0b57519f1e7019b5d09f5c5cbe49c48ab91daf6fcc09ee8a30
2602e817a67949860733b3548b37792616d52ffd305405ccab0409bcfedc5d63
42a4d9527063f73004b049a093a34a4fc3b6ea9505cb9b50b895486cb2dca94b
5ed5fc6c6918ff6fa4eab7742c03d59155ca87e0fe12bac339f18928e2924a96
a2ad6bfc47c4f69a2170cc1a9fd620a68b1ebb474b7bdf601066e780e592222f
c23ece07fc5432ca200f3de3e4c4b68430c6a22199d7fab11916a8c404fb63dc
cb96cd26f36a3b1aacabfc79bbb5c1e0c9850b1c75c30aa498ad2d4131b02b98
ed2f9c9d5554d5248a7ad9ad1017af5f1bbadbd2275689a8b019a04c516eeec2
fe16543109f640ddbf3725e4d9f593de9f13ee9ae96c5e41e9cdccb7ab35b661
886e3a2f74bf8f46b23c78a6bad80c74fe33579f6fe866bc5075b034c4d5d432
8ec108b8f66567a8d84975728b2d5e6a2786c2ca368310cca55acad02bb00fa6
96d80ae577e9b899772a940b4941da39cf7399b5c852048f0d06926eb6c9868a
bb1a5fb87d34c63ade0ed8a8b95412ba3795fd648a97836cb5117aff8ea08423
d65e2086aeab56a36896a56589e47773e9252747338c6b59c458155287363f28
588cd0fe3ae6fbd2fa4cf8de8db8ae2069ea62c9eaa6854caedf45045780661f
917a6c816684f22934e2998f43633179e14dcc2e609c6931dd2fc36098c48028
db7bdd6c3ff7a27bd4aa9acc17dc35c38b527fb736a17d0927a0b3d7e94acb42
de6ce9b75f4523a5b235f90fa00027be5920c97a972ad6cb2311953446c81e1d
a6673c6d52dd5361afd96f8143b88810812daa97004f69661da625aaaba9363b
40a6b4c6746e37d0c5ecb801e7656c9941f4839f94d8f4cd61eaf2b812feaabe
c88453178f5f6aaab0cab2e126b0db27b25a5cfe6905914cc430f6f100b7675c

ec553e14b84ccca9b84e96a9ed19188a1ba5f4bf1ca278ab88f928f0b00b9bd0
c7e525b8125265b507e3fb9b8f0b7d9b93de574ad31b272ccf1e82e9b73ec721
aef4d98dcdeda987e6f49c5e8be47385f750d24176619851ad38534f26ad5267
d7588487206137cbdc95d990bc5266af6a0538653862665534c14bb8f56b76c6
536b0427ac9c74704594f0c406ccc303f6e04f0e68f24522b31cfe6543e44449
0f06f11ae1a611ff4a415aec1540aebe2d9ce3a27ef5acff426d97bea1c8202a
e7896ccb82ae35e1ee5949b187839faab0b51221d510b25882bbe711e57c16d2
e2810cca5d4b74e0fe04591743e67da483a053a8b06f3ef4a41bdabee9c48cf7
f925d929602c9bae0a879bb54b08f5f387d908d4766506c880c5d29986320cf9
c80c8dd7be3ccf18e327355b880afb5a24d5a0596939458fb13319e05c4d43e9
c23f17b92b13464a570f737a86c0960d5106868aaa5eac2f2bac573c3314eb0f
c88453178f5f6aaab0cab2e126b0db27b25a5cfe6905914cc430f6f100b7675c
b8703744744555ad841f922995cef5dbca11da22565195d05529f5f9095fbfca
a0968e820bbc5e099efd55143028b1997fd728d923c19af03a1ccec34ce73d9b
90f94d98386c179a1b98a1f082b0c7487b22403d8d5eb3db6828725d14392ded
7e14ca8cb7980e85aff4038f489442eace33530fd02e2b9c382a4b6907601bee
7e6b04e17ae273700cef4dc08349af949dbd4d3418159d607529ae31285e18f7
960d4c9e79e751be6cad470e4f8e1d3a2b11f76f47597df8619ae41c96ba5809
88788208316a6cf4025dbabbef703f51d77d475dc735bf826b8d4a13bbd6a3ee
8fbd374d4659efdc5b5a57ff4168236aeaab6dae4af6b92d99ac28e05f04e5c1
424a9c85f97aa1aece9480bd658266c366a60ff1d62c31b87ddc15a1913c10e4
4064e4bb9a4254948047858301f2b75e276a878321b0cc02710e1738b42548ca
53b4a4359757e7f4e83929fba459677e76340cbec7e2e1588bbf70a4df7b0e97
20aaeac4dbea89b50d011e9becdf51afc1a1a1f254a5f494b80c108fd3c7f61a
b8703744744555ad841f922995cef5dbca11da22565195d05529f5f9095fbfca
960d4c9e79e751be6cad470e4f8e1d3a2b11f76f47597df8619ae41c96ba5809
a0968e820bbc5e099efd55143028b1997fd728d923c19af03a1ccec34ce73d9b

SHA-1

481f30675ef71b0cecea32b227f0f930573459a7
57a35ad499a93bff43d7b312f98f8f363f666c22
72775239683ea6a651b5c73d2e3ed006af5e1cad
7badbd6ee555a882a02ed345472a20ce211b1d5f
17239764355e7f21237ff5ca05c36cc9dd1c934f
27810d36a8c07ae78bd15ee79bacc20f9954943d
5d340a54081fe37832690a5a73060fa34b5a3527
7160edebb59ba860f84f7b0658e5598c2af6a030
00a2639215e4c2c790bb84cd952539e3d7eacdf5
1121bcd922a493585ff7d8d43a7f54ac71c26308
8761d79aaef37b92593f772f6a26359696e31187
57a35ad499a93bff43d7b312f98f8f363f666c22
7badbd6ee555a882a02ed345472a20ce211b1d5f
dc6005970d96982d5a992f36f353b5ac30cdcd59
e2561fe1a6f120558455969be358050561006871
04224ab9da82d078d5b9e48589c56e9bde707fcf
fa9f02565e90ce59d64ed1449e3f24a5481594ee
b99d3ac574d6611c7304ef87e9c51c187bb5dd42
d76e5ac85cd57425dc3c5dc27c438b0725d6eaa4
df367846d0118f8748c886fee5e633efee1411b4
b68030b766462621a5c3ab27448e62327eb0fcfe
a65d4b46ba7fcb3b023f61303e65f0c494b63386
bb8647eeaf1acadbb2aa7d67222d4ab8054ac645
68717f7d00d51a31b5f9e0ed46ba4ddda4869181
98462944e128fb7660359bfa3e2cece4eaf5b88b

3e6f2c6ef018528dc65b97331f3ce745b3c386a0
6ec4ed78d8930f290555ec65181d88dfef325a1d
3b53fa6eca3e2088da07f6f2dc51f952565d958b
272199dba36d45e0b724db571c75b271a52dc8cd
71093d587278185fd831783acb2a97444ad661d8
df367846d0118f8748c886fee5e633efee1411b4
71093d587278185fd831783acb2a97444ad661d8
272199dba36d45e0b724db571c75b271a52dc8cd
892fedae59b274ca24916de33650d318168ce335
8103cbffd4f7651c32a1cc602f0398027fb3207f
99ead1a4c767d8f201d538097762740b0765d1c7
6fb8b0e4e31f678f53b22e7b8a1b70f0deef1545
5319b3015318816396125002 7e1eae780e44ff30
7918e2c9c6f2847078bb736968f8f21b7e70a0af
cc7afffdb88729a5e977fa8f75a898d09624f54a
064eab6bff1b47eb92cbf1ed35f57098e5e686b2
0fc0e1ab30f55d1709532496ac6adac107a4729e
18a6ee322f30fe17f896686fbc162e4c8d628e5a
d005ebee72feb5ac50ee81e872665cae32d6c1c9
a173803357133cc5d61b8b31825b2938808e7850
9662c1912d21a29eb02c92936e57681ce0d5fc0f
a63c56b6e7ca1d11e52a786a6ada658bad4f0cf2
b9a01912e0f91d6040c934c68f4c708d4611fa0d
a6e728c3331f46763f643f7192959716034767e5
b7522d2f1fb7b9b92348b4d88c62480683d3485c

MD-5

585732e25a73b4b7d3dff51edae1b30

0ddb00c7632b2d443b6293d9cc810a9b

b868885719d2244fc2eee84200f456c7

f9ffe8ec3d808da08bc335583a0631ce

e7df84a5a22aeafcf1c3abf4fd986c91

1986e572654593df8e08ff69bb284dc6

242098c3e87822bffa7c337987065fbe

fc3f730f2253db14076fa2e3c37aeb1b

0993e8ffdc69c202e56b8070a0ceb8cd

9c63b57d1250cd89fbd82ae2b4062aa3

b77259eb3279ef1f5eb7cfae7d818ff1

c8f6081c824d17c5efba58def4d7e33a

d1e400e1e8100872d1f0f6a4f99eb51d

b77259eb3279ef1f5eb7cfae7d818ff1

fc3f730f2253db14076fa2e3c37aeb1b

c8f6081c824d17c5efba58def4d7e33a

af6d4ffcaf5d3dab814d16429cb76754

d783001d1f98fe3b33e7b97b0b7d96dc

c17f4bb8e415e21e6010b98e13c6dff3

473dfccda44f85d119aadefb92cd085e

93be13bbcad30440a0d0ef3868d67003

4ff6ada093a155494cf6a7866140843f

a2571577f281eda9548d9047b37cbbb8

fa55d4fe55eb4b9b34804d94bcd2f88f

6bc591f4e8eb1ea54b4d6defd019bee8

f1c935ce028022ab2a495eae83adacc6

dab63e3d8fdc6800c983430e25bce791

5d61614099d6d567441d15c58d6517b0

473dfccda44f85d119aadefb92cd085e

4ff6ada093a155494cf6a7866140843f

72f1345a5ba43c0e0c906d6f0123050d

7675b919678e71e01c145f79c6452607

93be13bbcad30440a0d0ef3868d67003

a2571577f281eda9548d9047b37cbbb8

cdeb7abfc7775c63745135431272dda3

ef6ec560efd05d21976a6fd3f489e206

b181ecbb7394e3b1394a8c97af65b7e2

aba760ec55fdeccb35adb068443feb89

MD-5

a713e686fd984588a4db74f34bf32275

95c0055aa09646a27ac9864477ac9269

8d0bff13167e46249105942b77c36bfd

a24d25af9985c28cb0d93443cc899aa2

5b9b3397ab00095d1b50a8e6bd569a32

4d5ca8c51171d9d9b944d9c4b2cd6e61

7b88765f265124a80a443a353493b88e

a46206daae98334e47e178bc718d9baf

b93b8a0a1d3779e68eda04622691609d

5b9b3397ab00095d1b50a8e6bd569a32

7b88765f265124a80a443a353493b88e

72f1345a5ba43c0e0c906d6f0123050d

bede9522ff7d2bf7daff04392659b8a8

353b4643ec51ecff7206175d930b0713

32bfe46efceae5813b75b40852fde3c2

c381c2cb8fdd6acf1636280b9424f573

23d99f912f2491749b89e4fd337273bc

24c72ffef74be81c5a7d4cb024110328

aba760ec55fdeccb35adb068443feb89

43b851109fc2d534e2ac5d157f90fe65

23d99f912f2491749b89e4fd337273bc

24c72ffef74be81c5a7d4cb024110328

5d61614099d6d567441d15c58d6517b0

5d013b96a25f0610cd1ac45d61d44d7e

5f8a2be246a6e0535586340fe7620176

809334c0b55009c5a50f37e4eec63c43

6bc591f4e8eb1ea54b4d6defd019bee8

7675b919678e71e01c145f79c6452607

3dd1f91f89dc70e90f7bc001ed50c9e7

b7d15723d7ef47497c6efb270065ed84

Remediation

- **PowerShell Constrained Language Mode:** Use PowerShell's Constrained Language Mode to restrict the execution of risky scripts and commands.
- **Regular Patch Management:** Ensure all systems, especially those using PowerShell, are regularly updated with the latest security patches to mitigate vulnerabilities.
- **Network Segmentation:** Segment the network to limit lateral movement and isolate critical assets from less secure areas.
- **User Awareness Training:** Educate employees on phishing and social engineering tactics, as these are common initial vectors for APT attacks.
- **Monitor and Analyze Network Traffic:** Use network monitoring tools to detect unusual patterns and behaviors indicative of APT activities.
- **Behavioral Analysis:** Implement behavioral analysis tools to identify anomalies in user and system behaviors that could indicate an APT attack.
- **Implement Multi-Factor Authentication (MFA):** Use MFA to secure access to critical systems and reduce the risk of credential compromise.
- Block all IOCs on your XDR, EDR and other security tools.

+1 (832) 271 2738
info@threatcure.net
https://threatcure.net/