Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ACTOR REPORT

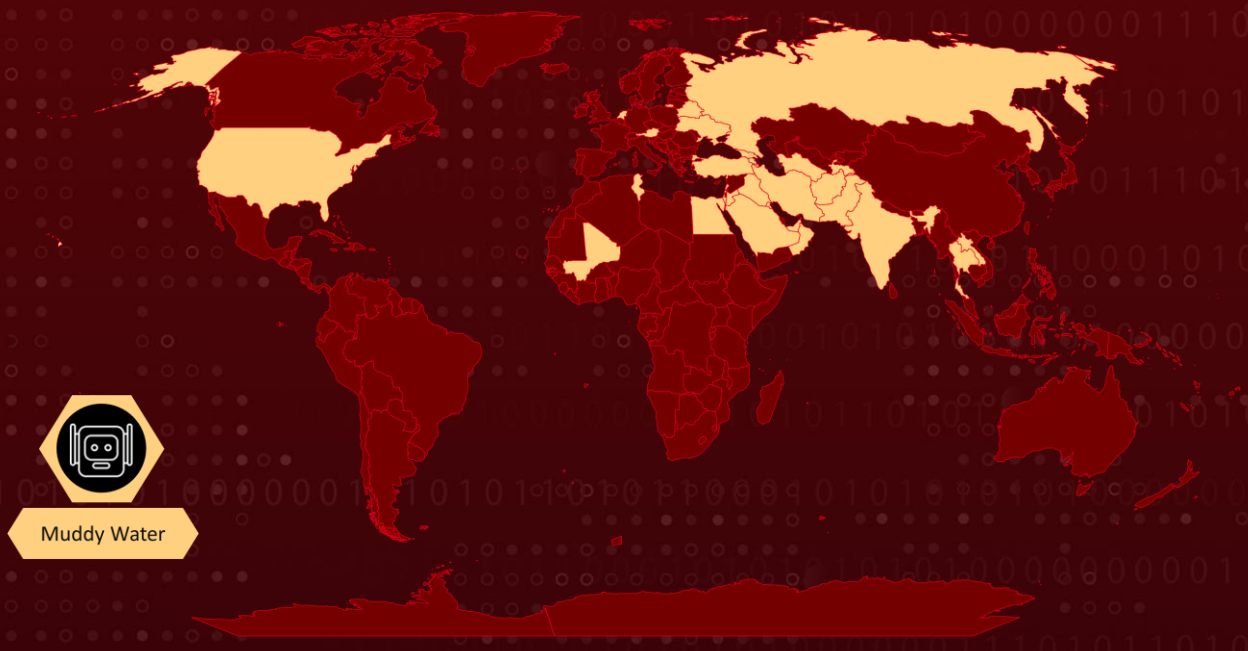
MuddyWater is back with new techniques

Date of Publication	Admiralty code	TA Number
December 13, 2022	A1	TA2022295

Summary

First Appearance: 2017
Threat Actor: MuddyWater
Target Regions: Middle East, Asia, Africa, Europe, and North America
Target Sectors: Defense, Education, Energy, Financial, Food and Agriculture, Gaming, Government, Healthcare, High-Tech, IT, Media, NGOs, Oil and gas, Telecommunications, Transportation, Aerospace

Actor Map



Actor Details

#1

MuddyWater used Dropbox links and document attachments with URLs redirected to ZIP archives as lures in its campaign, which also utilized compromised corporate email accounts. In addition to using Remote Utilities and ScreenConnect installers in their archive files, attackers have also switched to Atera Agent. Recent updates to the campaign have enabled the delivery of the Syncro remote administration tool, which could provide attackers with total machine control, enabling reconnaissance, additional backdoor delivery, and sale of access. With such capabilities, a threat actor has nearly unlimited options for accessing corporate machines

#2

Over time, the group added new attack techniques to its arsenal. The APT group has also targeted North American and European countries in the past. According to US Cyber Command (USCYBERCOM), MuddyWater APT group is affiliated with Iran's Ministry of Intelligence and Security (MOIS).

Actor Group

NAME	ORIGIN	TARGET COUNTRIES	TARGET INDUSTRIES
MuddyWater (Seedworm, TEMP.Zagros, Static Kitten, Mercury, TA450, Cobalt Ulster, ATK 51, T-APT-14, ITG17)	Iran **MOTIVE** Information theft and espionage	Afghanistan, Armenia, Austria, Azerbaijan, Bahrain, Belarus, Egypt, Georgia, India, Iran, Iraq, Israel, Jordan, Malta Kuwait, Laos, Lebanon, Mali, Netherlands, Oman, Pakistan, Russia, Saudi Arabia, Tajikistan, Thailand, Tunisia, Turkmenistan Turkey, UAE, Ukraine, USA	Defense, Education, Energy, Financial, Food and Agriculture, Gaming, Government, Healthcare, High-Tech, IT, Media, NGOs, Oil and gas, Telecommunications, Transportation, Aerospace

Recommendations

Security Leaders

Phishing simulations and routine education and awareness training and communications rarely account for MFA fatigue and web browser hygiene. Integrate and communicate all lessons learned.

Security Engineers

- **Uni5 Users:** This is an actionable threat advisory in HivePro Uni5. Prioritize and block all indicators attributed to the threat actor through your Command Center. Test your controls with Uni5's Breach & Attack Simulation.
- **All Engineers:** Refer to and action upon the 'Potential MITRE ATT&CK TTPs' & 'Indicators of Compromise (IoC)' on the following pages.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0011 Command and Control	T1566 Phishing
T1566.001 Spearphishing Attachment	T1566.002 Spearphishing Link	T1219 Remote Access Software	T1588 Obtain Capabilities
T1588.002 Tool	T1583 Acquire Infrastructure	T1583.006 Web Services	

Indicator of Compromise (IOC)

TYPE	VALUE
SHA256	f511bdd471096fc81dc8dad6806624a73837710f99b76b69c6501cb90e37c311 efd5271bdb57f52b4852bfda05122b9ff85991c0600befcbd045f81d7a78eac5 d65d80ab0ccdc7ff0a72e71104de2b4c289c02348816dce9996ba3e2a4c1dd62 1670a59f573037142f417fb8c448a9022c8d31a6b2bf93ad77a9db2924b502af dedc593acc72c352feef4cc2b051001bfe22a79a3a7852f0daf95e2d10e58b84 eae0acba9c9e6a93ce2d5b30a5f21515e8ccca0975fbd0e7d8862964fdfa1468 7e7292b5029882602fe31f15e25b5c59e01277abaab86b29843ded4aa0dcbdd1 c7a2a9e020b4bcbfa53b37dea7ebf6943af203b94c24a35c098b774f79d532ac 887c09e24923258e2e2c28f369fba3e44e52ce8a603fa3aee8c3fb0f1ca660e1 01dfa94e11b60f92449445a9660843f7bea0d6aad62f1c339e88252008e3b494 d550f0f9c4554e63b6e6d0a95a20a16abe44fa6f0de62b6615b5fdcdb82fe8e1 61dcf1eeb616104742dd892b89365751df9bb8c5b6a2b4080ac7cf34294d7675 653046fa62d3c9325dbff5cb7961965a8bf5f96fa4e815b494c8d3e165b9c94a 76ab046de18e20fd5cddbb90678389001361a430a0dc6297363ff10efbcb0fa8 c6cfd23282c9ff9d0d4c72ee13797a898b01cd5fd256d347e399e7528dad3bfd

TYPE	VALUE
SHA256	32339f7ac043042e6361225b594047dd4398da489a2af17a9f74a51593b14951 dab77aea8bf4f78628dcf45be6e2e79440c38a86e830846ec2bddc74ff0a36e4 b5c7acf08d3fd68ddc92169d23709e36e45cb65689880e30cb8f376b5c91be57 2a5f74e8268ad2d38c18f57a19d723b72b2dadd11b3ab993507dd2863d18008d e87fe81352ebda0cfc0ae785ebfc51a8965917235ee5d6dc6ca6b730eda494cf aa282daa9da3d6fc2dc6d54d453f4c23b746ada5b295472e7883ee6e6353b671 4e80bd62d02f312b06a0c96e1b5d1c6fd5a8af4e051f3f7f90e2976580842515 697580cf4266fa7d50fd5f690eee1f3033d3a706eb61fc1fca25471dbc36e684 dc7e102a2c68f7e3e15908eb6174548ce3d13a94caadf76e1a4ee834dc17a271 f24ce8e6679893049ce4e5a03bc2d8c7e44bf5b918bf8bf1c2e45c5de4d11e56 433b47f40f47bea0889423ab96deb1776f47e9faa946e7c5089494ed00c6cc29 011cb37733cdf01c689d12fedc4a3eda8b0f6c4dcdeef1719004c32ee331198e e217c48c435a04855cf0c439259a95392122064002d4881cf093cc59f813aba8 331b513cf17568329c7d5f1bac1d14f38c77f8d4adba40c48dab6baf98854f92 4d24b326d0335e122c7f6adaa22e8237895bdf4c6d85863cf8e84cfcc0503e69 a35a1c92c001b59605efd318655d912f2bcd4e745da2b4a1e385d289e12ee905 4550b4fa89ff70d8ea59d350ad8fc537ceaad13779877f2761d91d69a2c445b2 5578b7d126ebae78635613685d0cd07f4fb86f2e5b08e799bdc67d6d6053ede2
MD5	d1b4ca2933f49494b4400d5bf5ab502e aaa9db79b5d6ba319e24e6180a7935d6 2ed6ebaa28a9bfccc59c6e89a8990631

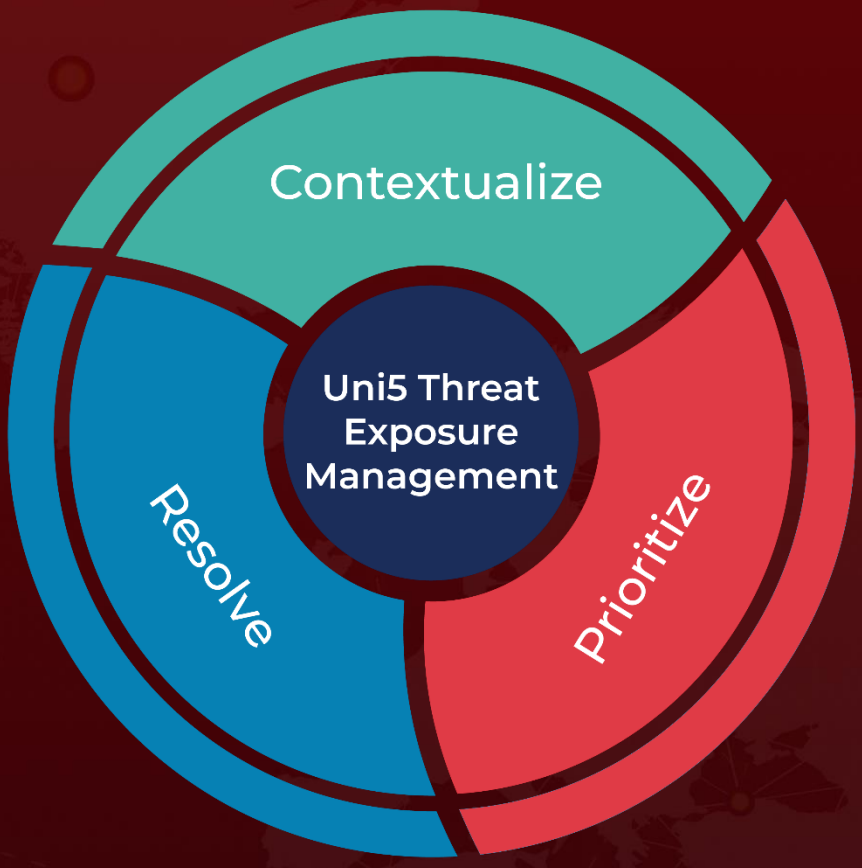
References

https://www.deepinstinct.com/blog/new-muddywater-threat-old-kitten-new-tricks

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

December 13, 2022 • 1:00 AM

More at www.hivepro.com