MuddyWater campaign abusing Atera Agents

Identifier: TRR240402.

Summary

We have been closely monitoring the activities of the Iranian state-sponsored threat actor MuddyWater since the beginning of 2024. Our investigations reveal an active campaign that has been ramping up since October 2023, aligning with the Hamas attack that took place that month[1]. In this latest campaign, MuddyWater has been heavily relying on a legitimate remote monitoring and management (RMM) tool called Atera Agent.

Over the course of our investigation, several publications[234] have detailed various aspects of this attack campaign. Consequently, our report shares new insights and information regarding MuddyWater use of Atera Agents, not previously highlighted in these reports.

Background

MuddyWater, an Iranian state-sponsored threat actor, has been relying on legitimate remote monitoring and management (RMM) software as a first stage payload in its attacks, since at least 2021[5]. Since then, the actor has tested different RMM tools, from ScreenConnect, Syncro, SimpleHelp, RemoteUtilies and most recently, Atera Agent. Atera Agent does not require any infrastructure to be set up by the attackers, providing them with better operational security.

Since late October 2023, we have noticed a significant increase in the use of Atera Agent installation packages linked to MuddyWater, continuing through to April 2024:

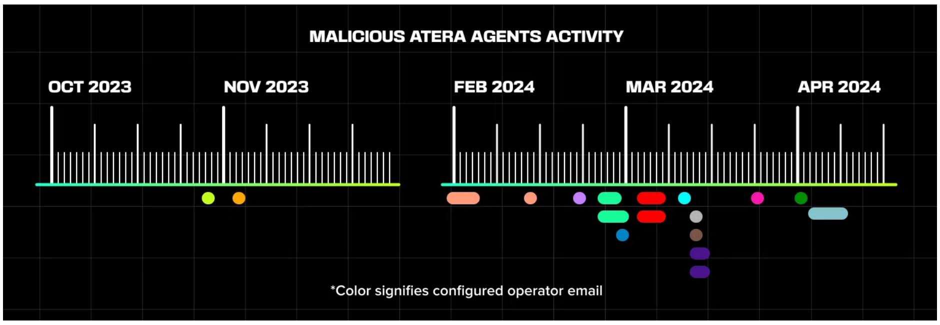


Figure 1 – Estimated timeline of Atera agent activity

Similarly to previously reported misuse cases[6], MuddyWater exploited Atera's free trial offers. The Atera Agent agents seen in this campaign has been registered using a mix of compromised business and private email accounts. We suspect that the threat actor accessed these accounts through a variety of methods, such as password spraying, exploiting reused passwords, utilizing credentials from data breaches, or even purchasing them. Additionally, there is a possibility that private email accounts were specifically registered for the purpose of creating Atera accounts.

Infection chain

The group continues to leverage free file hosting platforms for hosting their RMM installers, employing spearphishing emails to direct recipients to these files.

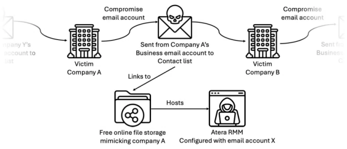

Compromise email account
Sent from Company A's Business email account to Contact list
Victim Company A
Compromise email account
Victim Company B
Links to
Hosts
Free online file storage mimicking company A
Atera RMM Configured with email account X

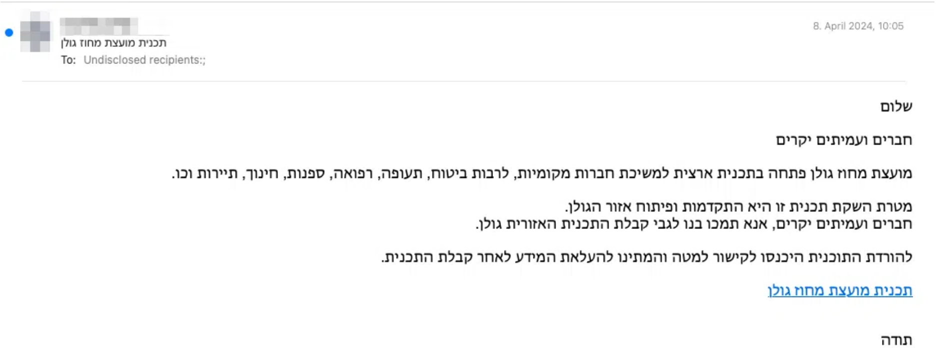
Figure 2 – Observed spreading methodology

These emails contained links leading to various file-sharing websites, which either hosted an archive with the Atera Agent installer or provided direct access to the installer itself.

It is important to note that, to our knowledge, the email accounts registered with Atera were distinct from those used to disseminate the spearphishing emails.

Spearphishing

The quality of MuddyWater's spearphishing emails has significantly improved since their earlier emails in October 2023. The threat actor has refined their social engineering tactics, crafting more convincing and tailored lures to deceive their targets. The emails observed in the recent campaign from April 2024 (see Fig. 3) demonstrate a higher level of sophistication compared to those from October 2023 (see Fig. 4), with more persuasive content and professional formatting:



[redacted]
תכנית מועצת מחוז גולן
To: Undisclosed recipients:;

8. April 2024, 10:05

שלום

חברים ועמיתים יקרים

מועצת מחוז גולן פתחה בתכנית ארצית למשיכת חברות מקומיות, לרבות ביטוח, תעופה, רפואה, ספנות, חינוך, תיירות וכו.

מטרת השקת תכנית זו היא התקדמות ופיתוח אזור הגולן.
חברים ועמיתים יקרים, אנא תמכו בנו לגבי קבלת התכנית האזורית גולן.

להורדת התוכנית היכנסו לקישור למטה והמתינו להעלאת המידע לאחר קבלת התכנית.

תכנית מועצת מחוז גולן

תודה

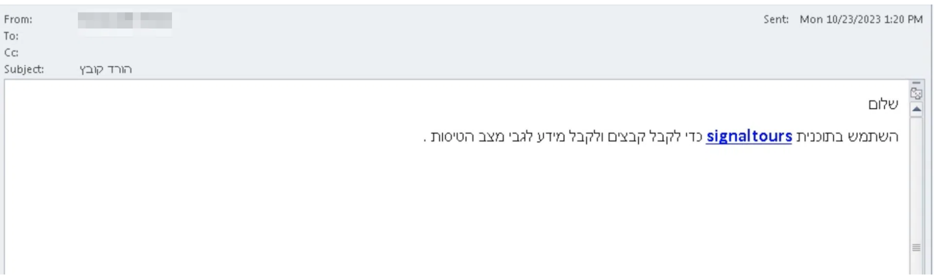
Figure 3 – Spearphishing email from April 2024. Atera Agent linked, hosted using "Egnyte" file sharing

Which translates to:

```
Hello,

Dear friends and colleagues

The Golan Regional Council has launched a national program to attract local
companies, including insurance, avation, medicine, shipping, education, tourism,
etc.

The goal of launching this program is to advance and develop the Golan region.
Dear friends and colleagues, please support us regarding the adoption of the Golan
regional program.

To download the program, click the link below and wait for the information to be
uploaded after receiving the program.

Golan Regional Council program [Link]

Thanks
```

Where as the email from October 2023 (Fig. 4) translates to:

```
Hello
Use the signaltours [Link] program to recieve files and get information about flight
status.
```



From: [redacted]
To:
Cc:
Subject: הורד קובץ

Sent: Mon 10/23/2023 1:20 PM

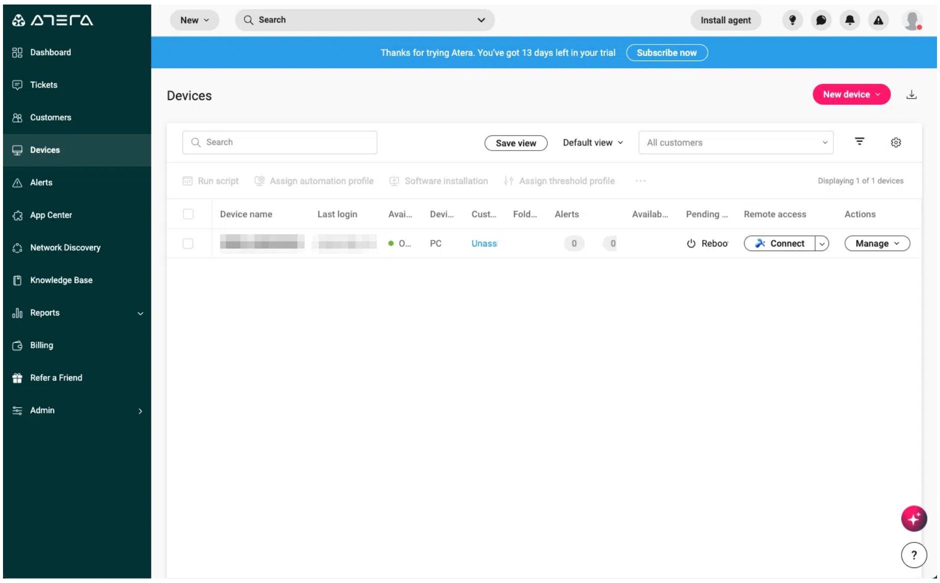
שלום

השתמש בתוכנית **signaltours** כדי לקבל קבצים ולקבל מידע לגבי מצב הטיסות .

Figure 4 – Spearphishing email from October 2023 linking to a SimpleHelp installer

Atera RMM

Atera offers users a free 30-day trial of their platform, which allows the generation of Atera ‘Agents’, using any email account. These agents are configured to call back to this account and could be controlled directly via the website:



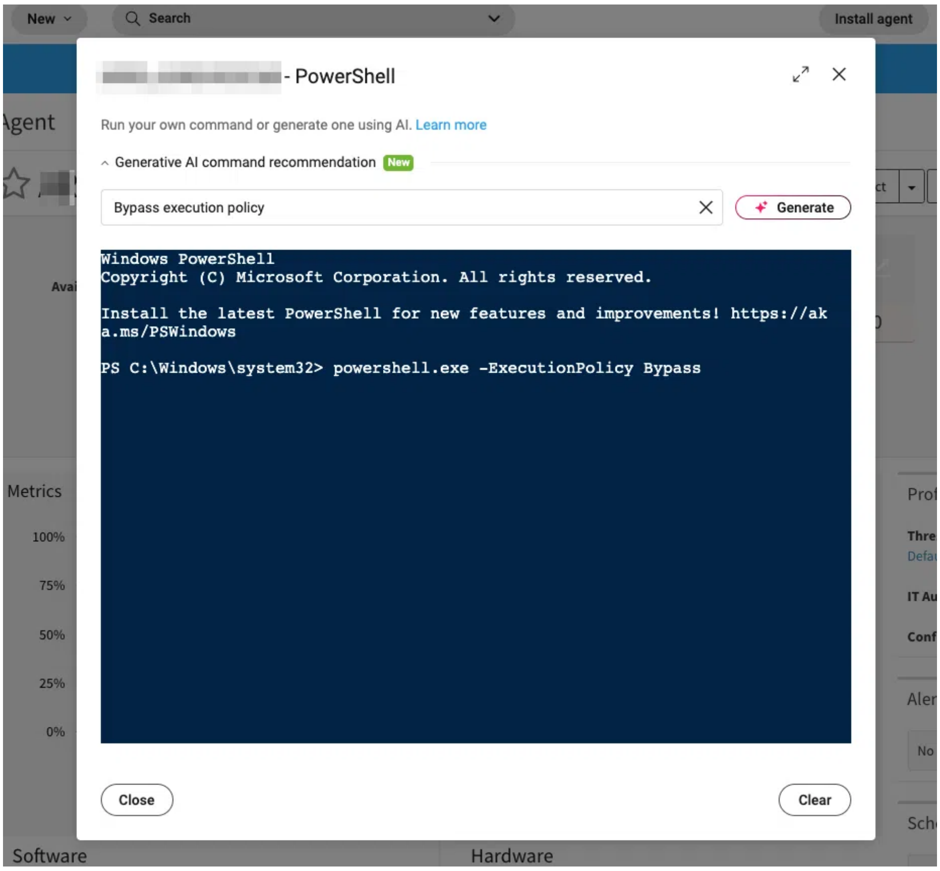
Thanks for trying Atera. You've got 13 days left in your trial

	Device name	Last login	Avai...	Devi...	Cust...	Fold...	Alerts	Availab...	Pending ...	Remote access	Actions
□	[redacted]	[redacted]	● O...	PC	Unass		0	0	Reboo	Connect	Manage

Figure 5 – Atera Web UI

This eliminates the need for the attacker to establish its own C2 infrastructure, making it a more appealing choice compared to previously used RMM solutions like SimpleHelp.

Atera provides comprehensive remote control capabilities directly from the Web UI, including the ability to upload/download files, run an interactive shell (see Fig. 6), and even use generative AI command assistance.



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://ak
a.ms/PSWindows

PS C:\Windows\system32> powershell.exe -ExecutionPolicy Bypass
```

Figure 6 – Atera Web PowerShell UI

While email verification is not required prior to generating agents, a ‘registration successful’ email is sent to the address used. Although the owner of the email address could naturally reset the password and access the Atera account, in the cases we studied, the attacker had access to the email account used to register with Atera.

We observed Atera Agent binaries configured using emails belonging to individuals whose other email account passwords had been leaked. We believe that MuddyWater exploited password reuse to gain access to additional email accounts, which were then used to register Atera Agents. In some cases, the email accounts used appeared to have been obtained through the sale of leaked OWA credentials. In other instances, the credentials of another email account belonging to the same person had been compromised, allowing the threat actor to access additional accounts through password reuse.

Malicious Atera Agents installation packages

The following Atera Agent installation packages are highly suspected to be registered and operated by MuddyWater, judging from their distribution method, the email account used to register them and in some cases, the targets that received said emails.

Leaked email credentials

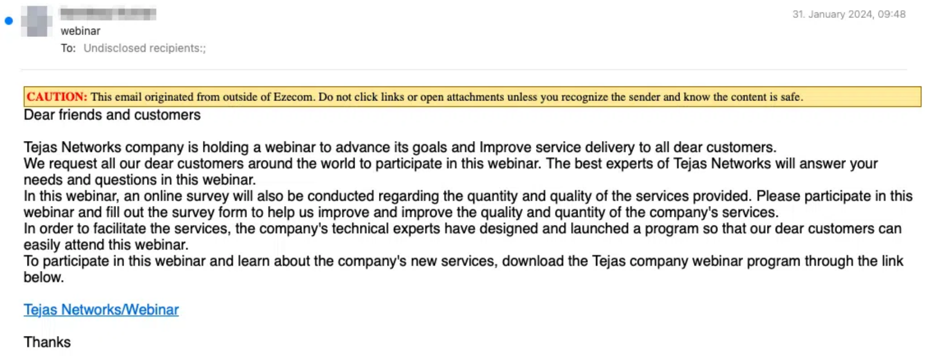
Filename	`N/A`
Hash (SHA256)	`5d7eb6c36d261adeef1a59bde9eb965f5d8d7f56a2e607da913e782167ba6cb6`
Est. time active	`2023-11-03`

This early Atera Agent sample caught our attention due to its configuration using what appears to be a student’s email address from an associate degree student at a university in Turkey. We found this exact email address in a partial sample of an OWA (Outlook Web Access) credentials leak that was published a month before the agent’s estimated active time. The leak sample suggests that the full set of compromised credentials may have been put up for sale.

Filename	`Tejasnetworks.com.webinar.msi`
Hash (SHA256)	`14c270cf53a50867e42120250abca863675d37abf39d60689e58288a9e870144`
Est. time active	`2024-01-31 - 2024-02-04`
Filename	`Polaristek.msi`
Hash (SHA256)	`638c7a4f833dc95dbab5f0a81ef03b7d83704e30b5cdc630702475cc9fff86a2`
Est. time active	`2024-02-11 - 2024-02-13`

These two Atera Agents were configured using an email address belonging to a 2019 graduate of the Royal College of Arts in London. The individual’s personal email address was exposed in a data breach that occurred in the same year they graduated, suggesting that the attacker likely exploited a case of credential stuffing.

However, the distribution of these Atera Agents was carried out using an email address belonging to the targeted organization. The attacker crafted a spearphishing email with a lure tailored specifically to the organization:



[redacted]
webinar
To: Undisclosed recipients:;

31. January 2024, 09:48

CAUTION: This email originated from outside of Ezecom. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Dear friends and customers

Tejas Networks company is holding a webinar to advance its goals and Improve service delivery to all dear customers.
We request all our dear customers around the world to participate in this webinar. The best experts of Tejas Networks will answer your needs and questions in this webinar.
In this webinar, an online survey will also be conducted regarding the quantity and quality of the services provided. Please participate in this webinar and fill out the survey form to help us improve and improve the quality and quantity of the company's services.
In order to facilitate the services, the company's technical experts have designed and launched a program so that our dear customers can easily attend this webinar.
To participate in this webinar and learn about the company's new services, download the Tejas company webinar program through the link below.

Tejas Networks/Webinar

Thanks

Figure 7 – Spearphishing email spreading Tejasnetworks.com.webinar.zip via Onehub

Distribution using Zendesk Chat

A more recent sample, uploaded on 1st of April 2024 demonstrates an interesting new distribution method, using Zendesk:

Filename	`N/A`
Hash (SHA256)	`ec553e14b84ccca9b84e96a9ed19188a1ba5f4bf1ca278ab88f928f0b00b9bd0`
Est. time active	`2024-03-31 - 2024-04-01`

Like other Atera Agent installers discribed in this report, this installer was packed in a ZIP archive. However, this parent archive was hosted on Zendesk Chat's (formerly Zopim Chat) file sharing infrastructure:
`https://v2uploads.zopim[.]io/2/u/K/2uKM8Mhn4WHvqm9pjHrjaogyOYub9ouO/892fedae59b274ca24916de33650d318168`

We suspect that the attacker uploaded the malicious archive during a chat session, likely posing as a visitor/customer, but possibly as an agent/support provider.

According to Zendesk's documentation, "*Attached files are uploaded as links in a chat session. Regardless of your authentication settings, those links can be accessed by anyone with the URL.*[7]". This allowed the attacker to obtain a direct, non-expiring link to the archive, which they could then distribute via email.

Further investigation revealed that the email address used to register the Atera Agent was part of multiple data breaches dating back to 2016, with the most recent breach potentially occurring just a month before the registration.

Hunting for additional Atera Agents distributed via Zendesk, we found another suspicious agent configured with a Gmail account. This particular agent dates back to October 2023:

Filename	`N/A`
Hash (SHA256)	`9b49d6640f5f0f1d68f649252a96052f1d2e0822feadd7ebe3ab6a3cadd75985`
Est. time active	`2023-10-26`

In this case, the Atera Agent installer was not packed in a ZIP archive but instead directly uploaded to Zendesk Chat.

Interestingly, the hosting URL contains the same identifier as the previously discovered agent, suggesting that both malware samples may have been uploaded within the same chat instance, albeit at different times.

It's important to note that while Zendesk typically scans files uploaded to tickets for malware, attachments to tickets originating from standalone Chat subscriptions are not scanned[8]. This limitation in Zendesk's malware scanning process appears to have been exploited by the threat actor to distribute the malicious Atera Agent installer.

Targeting Israel

Filename	`IronSword.msi`
Hash (SHA256)	`2722e289767ae391e3c3773b8640a8b9f6eb24c6a9d6e541f29c8765f7a8944b`
Est. time active	`2024-03-05 - 2024-03-08`
Filename	`IronSword.msi`
Hash (SHA256)	`ffbe988fd797cbb9a1eedb705cf00ebc8277cdbd9a21b6efb40a8bc22c7a43f0`
Est. time active	`2024-03-05 - 2024-03-08`

These Atera Agents are configured with an email address belonging to an individual working at the Ministry of Foreign Affairs of Paraguay. Notably, the same email was found in a leaked list of Outlook Web Access (OWA) credentials, also dating back at least a month earlier.

The agent, named after the Israeli Defense Forces (IDF) operation “Swords of Iron”, was distributed via `filetransfer[.]io`, likely linked in a spearphishing email sent by the threat actor.

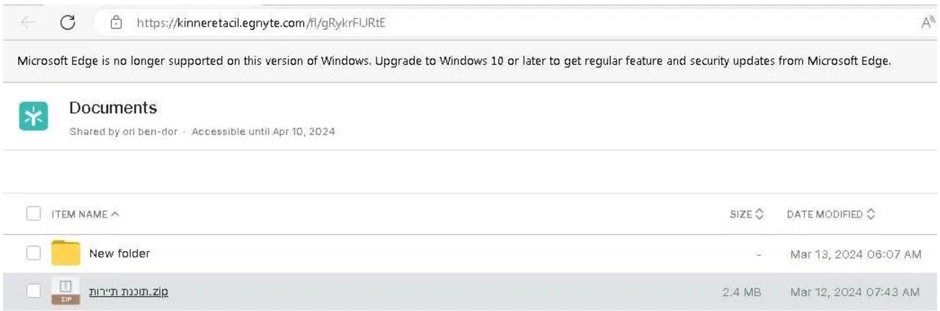
Filename	`setup_aleh_aleh.msi`
Hash (SHA256)	`165a80f6856487b3b4f41225ac60eed99c3d603f5a35febab8235757a273d1fd`
Est. time active	`2024-02-26 - 2024-02-28`

The email used to register this Atera Agent belongs to a graduate of “Kinneret Academic College”. MuddyWater have been targeting this academic institution following a compromise[9] to “Rashim Software”, an administration platform that Kinneret was using.

Filename	`תוכנת תיירות.msi`
Hash (SHA256)	`ff2ae62ba88e7068fa142bbe67d7b9398e8ae737a43cf36ace1fcf809776c909`
Est. time active	`2024-03-12 - 2024-03-14`
Filename	`Leonardo Hotels-tourism software.msi`
Hash (SHA256)	`c2f95299d8aa912e1b753f3f0780a00ea6e8b5dab0245d77fcf3b6499677c328`
Est. time active	`2024-03-12 - 2024-03-14`

These Atera Agents were configured with the same email address belonging to an individual working in an IT company. The filenames of the agents indicate that they were targeting an Israeli Tourism company (תוכנת תיירות.msi translates to ‘Tourism Program’ in Hebrew).

Both Atera Agents were hosted using “Egnyte” cloud file sharing platform. The attacker set up a custom Egnyte subdomain using the name of the aforementioned “Kinneret” University `kinneretacil.egnyte[.]com`, by a user named `ori ben-dor`.



https://kinneretacil.egnyte.com/fl/gRykrFURtE

Microsoft Edge is no longer supported on this version of Windows. Upgrade to Windows 10 or later to get regular feature and security updates from Microsoft Edge.

Documents

Shared by ori ben-dor · Accessible until Apr 10, 2024

□ ITEM NAME	SIZE	DATE MODIFIED
□ New folder	-	Mar 13, 2024 06:07 AM
□ תוכנת תיירות.zip	2.4 MB	Mar 12, 2024 07:43 AM

Figure 8 – Custom Egnyte folder

The same username was used to upload Atera Agent configured with a different email (belonging to an employment/immigration agency in Israel) to `onehub[.]com`:

Filename	`מילגה.msi`
Hash (SHA256)	`c6128f222f844e699760e32695d405bd5931635ec38ae50eddc17a0976ccefb4`
Est. time active	`2024-03-10`

Finally, the most recent Atera Agent was distributed using a very well made social engineering spearphising email (see Fig. 1):

Filename	`digitalform.msi`
Hash (SHA256)	`09e09503962a2a8022859e72b86ad8c69dcbf79839b71897c0bf8a4c4b9f4dd6`
Est. time active	`2024-04-03 - 2024-04-08`

This Atera Agent was configured with an email address belonging to an employee of an Airline in Algeria.

We found a tie to between this agent and another Atera Agent, spread to some of the same targets:

Filename	`תכנית מועצת מחוז גולן.msi`
Hash (SHA256)	`fb58c54a6d0ed24e85b213f0c487f8df05e421d7b07bd2bece3a925a855be93a`
Est. time active	`2024-04-08`

The malware was spread via a spearphishing email (Fig. 3) sent from an email account unrelated to the one used to register it with Atera. The spearphishing email contained a link to a custom Egnyte subdomain matching the lure’s contents. This Egnyte asset hosts a ZIP archive containing the Atera Agent installation package.

Our investigation suggests that the attacker compromised an email account at the victim organization, possibly by leveraging credentials from another leaked email account that we discovered within that org. Using the compromised account, the attacker then sent spearphishing emails to other organizations, targeting contacts in other organizations from the compromised email’s address book.

Targets

Basing on the accounts used to register the Atera Agents, as well as emails we analyzed, we believe that MuddyWater targeted the following sectors between October 2023 and April 2024:

Airlines, IT Companies, Telecommunication, Pharmaceutical, Automotive manufacturing, Logistics, Travel and Tourism, Employment/Immigration agency, as well as small businesses across Israel, India, Alegria, Turkey, Italy and Egypt (see Fig. 9).

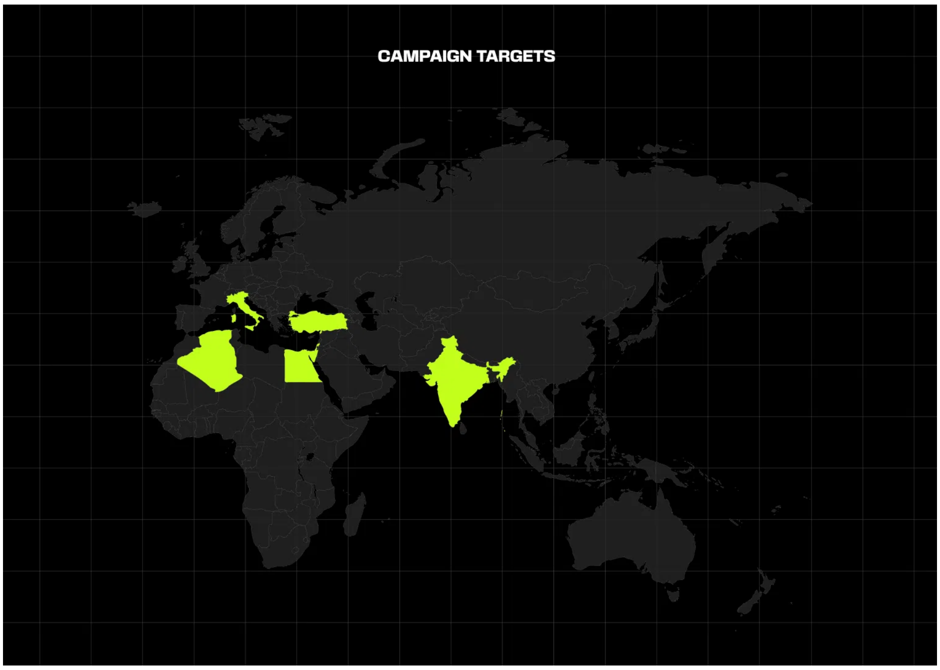


Fig. 9 – Map of suspected targets

Conclusions

MuddyWater places a high priority on gaining access to business email accounts as part of their ongoing attack campaigns. These compromised accounts serve as valuable resource, enabling the group to enhance the credibility and effectiveness of their spear-phishing efforts, establish persistence within targeted organizations, and evade detection by blending in with legitimate network traffic. Adding to that the use of RMM software (previously self-hosted, now in-cloud), as well as using various file hosting providers, makes this sort of activity challenging to detect and track.

Moreover, as highlighted in the Deep Instinct report on DarkBeatC2[3], there are indications of collaboration and hand-off of compromised targets between Iranian threat actors to conduct supply-chain attacks. This suggests that MuddyWater may not only actively compromise business email accounts themselves but also receive access to previously breached accounts from other affiliate groups. Similarly, the OP INNOVATE blog post on Lord Nemesis[9] demonstrates how the group exploited privileged credentials obtained from the Rashim Software breach to infiltrate the networks of Rashim's clients in the Israeli academic sector. This further underscores the value of compromised business email accounts as a stepping stone for launching additional attacks.

Unfortunately, we do not hold any information about the specific stages and actions the actor takes once it has successfully deployed the Atera Agent on a targeted system. We suspect that the group does not rely on the deployed RMM software for a long term, but rather uses it as a first stage in their attack, likely deploying a PowerShell implant as the next stage, as seen in previous attacks[10].

We encourage affected organizations and fellow researchers to collaborate with us in gaining a more comprehensive understanding of MuddyWater attack campaigns. Together we can offer the community better chances to detect, respond to and hunt for new malicious activity.

Appendix

Indicators of compromise (IOCs)

Associated IOCs are also available on our GitHub repository.

Hashes (SHA-256)

```
9b49d6640f5f0f1d68f649252a96052f1d2e0822feadd7ebe3ab6a3cadd75985|Atera Agent
5d7eb6c36d261adeef1a59bde9eb965f5d8d7f56a2e607da913e782167ba6cb6|Atera Agent
14c270cf53a50867e42120250abca863675d37abf39d60689e58288a9e870144|Atera Agent,
Tejasnetworks.com.webinar.msi
638c7a4f833dc95dbab5f0a81ef03b7d83704e30b5cdc630702475cc9fff86a2|Atera Agent,
Polaristek.msi
dd2675e2f6835f8a8a0e65e9dbc763ca9229b55af7d212da38b949051ae296a5|Atera Agent,
karel.com.tr.telekomünikasyonWebsemineri.msi / comviva.com.webinar.msi
165a80f6856487b3b4f41225ac60eed99c3d603f5a35febab8235757a273d1fd|Atera Agent,
setup_aleh_aleh.msi
d22fd0cdd6ace24e117d7330e9996a2809c2c2cb280b12f9ea43c484d2bfcfd4|Atera Agent,
setup_aleh_aleh (1).msi
f9c1a117de8519060a3bf189e72277e895345b8fece73fc0d750946c7f288367|Atera Agent,
BLUMENTAL.WEBINAR.msi
2722e289767ae391e3c3773b8640a8b9f6eb24c6a9d6e541f29c8765f7a8944b|Atera Agent,
IronSword.msi
ffbe988fd797cbb9a1eedb705cf00ebc8277cdbd9a21b6efb40a8bc22c7a43f0|Atera Agent
2ae6c5c2b71361f71ded4ad90bbf6ef0b0f4778caf54078c928e2017302fbe69|Atera Agent
c6128f222f844e699760e32695d405bd5931635ec38ae50eddc17a0976ccefb4|Atera Agent,
מילגה.msi
ff2ae62ba88e7068fa142bbe67d7b9398e8ae737a43cf36ace1fcf809776c909|Atera Agent, תוכנת
תיירות.msi
c2f95299d8aa912e1b753f3f0780a00ea6e8b5dab0245d77fcf3b6499677c328|Atera Agent,
Leonardo Hotels-tourism software.msi
e89f48a7351c01cbf2f8e31c65a67f76a5ead689bb11e9d4918090a165d4425f|Atera Agent,
Salary.msi
326dd85d76d33f3f04cbe7eef6d10ea73f800c84bfc3ed6f3963403c981bbb6e|Atera Agent,
virtual-library.msi
ec553e14b84ccca9b84e96a9ed19188a1ba5f4bf1ca278ab88f928f0b00b9bd0|Atera Agent
09e09503962a2a8022859e72b86ad8c69dcbf79839b71897c0bf8a4c4b9f4dd6|Atera Agent,
digitalform.msi
fb58c54a6d0ed24e85b213f0c487f8df05e421d7b07bd2bece3a925a855be93a|Atera Agent, תכנית
מועצת מחוז גולן.msi
4b41b605ffc0e31bd9d460d5a296ac6e8cfd56a215dc131e90ec2654f0ffe31b|Malicious Zip
archive, karel.com.tr.telekomünikasyonWebsemineri.zip
85103955e35a1355ce68a92eaedd8f9376de1927d95bf12657b348dea6a8077b|Malicious Zip
archive, Tejasnetworks.com.webinar.zip
bab601635aafeae5fbfe1c1f7204de17b189b345efd91c46001f6d83efbb3c5a|Malicious Zip
archive, comviva.com.webinar.zip
900d08037d303d9b3d4a855e1a97d1f9283c28fe279e67eefe9997f856eeb439|Malicious Zip
archive
cc8be1d525853403f6cfabcf0fc3bd0ca398ece559388102a7fc55e9f3aa9b33|Malicious Zip
archive
7daab239271e088f04cae95627cc0066f48a1b178a1ff60b1140aa729126e928|Malicious Zip
archive, Leonardo Hotels-tourism software.zip
cc4cc20b558096855c5d492f7a79b160a809355798be2b824525c98964450492|Malicious Zip
archive, Salary.zip
31591fcf677a2da2834d2cc99a00ab500918b53900318f6b19ea708eba2b38ab|Malicious Zip
archive, תכנית מועצת מחוז גולן.zip
f17f6866f4748e6e762752062acdf983d3b083371db83503686b91512b9bcae3|Malicious Zip
archive, digitalform.zip
7e6a5e32596b99f45ea9099a14507a82c10a460c56585499d7cd640f2625567f|Malicious Zip
archive, Polaristek.zip
fb02e97d52a00fca1580ca71ed152dd28dd5ae28ab0a9c8e7b32cebd7f1998a1|Malicious Zip
archive, מילגה.zip
```

URLs

```
https://v2uploads.zopim[.]io/2/u/K/2uKM8Mhn4WHvqm9pjHrjaogyOYub9ouO/892fedae59b274ca24916de33650d31816
 Agent Distribution
https://v2uploads.zopim[.]io/2/u/K/2uKM8Mhn4WHvqm9pjHrjaogyOYub9ouO/064eab6bff1b47eb92cbf1ed35f57098e5
 Agent Distribution
https://ln5.sync[.]com/dl/cc84c9a40/grefpuhc-p9kmxpkx-kw6waakz-e8xp8atm|Atera Agent
Distribution
https://filetransfer[.]io/data-package/tuMe19fV/download|Atera Agent Distribution
https://freeupload[.]store/rALE7/wIHItUcE08.msi/download|Atera Agent Distribution
```

```
https://ws.onehub[.]com/files/x68hqy91|Atera Agent Distribution
https://megolan.egnyte[.]com/|Atera Agent Distribution
https://kinneretacil.egnyte[.]com/|Atera Agent Distribution
https://rimonnet.egnyte[.]com/|Atera Agent Distribution
https://ws.onehub[.]com/files/x68hqy91|Atera Agent Distribution
```

Yara rules

```
rule MuddyWater_AteraAgent_Operators
{
meta:
    description = "Detect Atera Agent abused by MuddyWater"
    references = "TRR240402"
    hash = "9b49d6640f5f0f1d68f649252a96052f1d2e0822feadd7ebe3ab6a3cadd75985"
    date = "2024-04-17"
    author = "HarfangLab"
    context = "file"
strings:
    $s1 = "COMPANYID001Q3000009snPyIAIACCOUNTID"
    $s2 = "COMPANYID001Q3000006FpmoIACACCOUNTID"
    $s3 = "COMPANYID001Q3000008IyacIACACCOUNTID"
    $s4 = "COMPANYID001Q3000009QoSEIA0ACCOUNTID"
    $s5 = "COMPANYID001Q30000023c7iIAAACCOUNTID"
    $s6 = "COMPANYID001Q3000008qXbDIAUACCOUNTID"
    $s7 = "COMPANYID001Q3000008cfLjIAIACCOUNTID"
    $s8 = "COMPANYID001Q3000007hJubIAEACCOUNTID"
    $s9 = "COMPANYID001Q3000008ryO3IAIACCOUNTID"
    $s10 = "COMPANYID001Q300000A5nnAIARACCOUNTID"
    $s11 = "COMPANYID001Q3000008JfioIACACCOUNTID"
    $s12 = "COMPANYID001Q300000BeUp3IAFACCOUNTID"
    $s13 = "COMPANYID001Q3000005gMamIAEACCOUNTID"
    $s15 = "mrrobertcornish@gmail.comINTEGRATORLOGINCOMPANYID"

    $sc1 = { 0A 28 49 99 78 E5 89 8D F4 0A 23 8E B8 A5 52 E8 } // Atera Network
certificate 2024-02-15 - 2025-03-18
    $sc2 = { 06 7F 60 47 95 66 24 A7 15 99 61 74 3D 81 94 93 } // Atera Network
certificate 2022-02-17 - 2024-03-16

condition:
    filesize > 1MB and filesize < 4MB
    and (uint16be(0) == 0xD0CF)
    and any of ($s*)
    and any of ($sc*)
}
```

Atera Agent hunting template

```
rule Custom_AteraAgent_Operator
{
meta:
    description = "Detect Atera Agent configured to certain email addresses, or
email domains"
    references = "TRR240402"
    date = "2024-04-17"
    author = "HarfangLab"
    context = "file"
strings:
    $email = "email@domain.tld" // Change email address
    $s1 = "PREVIOUSFOUNDWIX_UPGRADE_DETECTED"
    $s2 = "INTEGRATORLOGIN"
    $sc1 = { 0A 28 49 99 78 E5 89 8D F4 0A 23 8E B8 A5 52 E8 } // Atera Network
certificate 2024-02-15 - 2025-03-18
    $sc2 = { 06 7F 60 47 95 66 24 A7 15 99 61 74 3D 81 94 93 } // Atera Network
certificate 2022-02-17 - 2024-03-16
condition:
    filesize > 1MB and filesize < 4MB
    and (uint16be(0) == 0xD0CF)
    and @s1 < @email
    and @email < @s2[3]
    and any of ($sc*)
}
```

Icons created by juicy_fish – Flaticon

1. https://en.wikipedia.org/wiki/2023_Hamas-led_attack_on_Israel ↩ ↩
2. https://www.proofpoint.com/us/blog/threat-insight/security-brief-ta450-uses-embedded-links-pdf-attachments-latest-campaign ↩ ↩
3. https://www.deepinstinct.com/blog/darkbeatc2-the-latest-muddywater-attack-framework ↩ ↩ ↩ ↩
4. https://www.gov.il/he/departments/publications/reports/alert_1728 ↩ ↩
5. https://www.anomali.com/blog/probable-iranian-cyber-actors-static-kitten-conducting-cyberespionage-campaign-targeting-uae-and-kuwait-government-agencies ↩ ↩
6. https://syncromsp.com/blog/syncro-official-response-muddywaters/ ↩ ↩
7. https://support.zendesk.com/hc/en-us/articles/4408828723738-Sending-files-in-a-chat ↩ ↩
8. https://support.zendesk.com/hc/en-us/articles/4483794022170-Managing-malicious-attachments) ↩ ↩
9. https://op-c.net/blog/lord-nemesis-strikes-supply-chain-attack-on-the-israeli-academic-sector/ ↩ ↩ ↩ ↩
10. https://therecord.media/muddywater-cyber-espionage-africa-telecoms-iran ↩ ↩

Published on 22 April, 2024 Last update on 2 May, 2024