New MuddyWater Campaigns After Operation Swords of Iron

Threat.Zone

Introduction

MuddyWater APT has targeted government and private companies since **2017**, including critical sectors such as energy, telecommunications, government, and defense. In **February 2024**, MuddyWater resumed spear-phishing attacks using new techniques. The National Cyber Directorate of Israel attributed the team's attack toolkit and attack pattern findings to the MuddyWater group in **March 2024**, following an increase in new attacks. [1]

The **Malwation Threat Research Team** has been closely monitoring the activities of the MuddyWater group in Turkiye. The group has recently launched new attacks in **Israel**, **Africa**, and **Turkiye**. MuddyWater has been active in the **EMEA** region for many years, and its attack style aligns with Iran's foreign policies. The group has been launching new attacks since February using products developed in-house. As of March, they are also taking over third-party tools. Our team detected active attacks where agents of **Atera** and **ConnectWise ScreenConnect** remote administration management (**RMM**) software were created using compromised accounts. The agent build files of this software were then sent to victims via spear-phishing attacks. Phishing attacks often use PDF attachments that contain agents downloaded from third-party file upload services. Once these agents are run on the victim's device, MuddyWater actors gain privileges to upload, extract, monitor, and execute files.

For many years, the team has been known for its expertise in social engineering attacks and stealth. However, it is now expanding its tactics to reduce its digital footprint. Our analysis of malicious samples suggests that the team will likely increase its use of spear-phishing attacks distributed through compromised accounts (**Business Email Compromise—BEC**) soon.

Technical Analysis

In October 2023, the MuddyWater APT group re-emerged and began targeting North and East Africa using its **MuddyC2Go** toolkit, a Golang-based replacement for **PhonyC2**. In February, it shifted its attack toolkits to Atera, ConnectWise ScreenConnect, Advanced Monitoring Tool, and MeshCentral Remote Monitoring & Management (RMM) software. The **Israeli CERT** first announced this attack chain, which security researchers have now detected on Twitter (**@k3yp0d** [2]).

Since March, new attacks have been observed targeting specific organizations or individuals. During the Weaponisation phase, the attackers are producing attack campaigns. They have added meta information of each file downloaded from the links given in the **PDF** in spear-phishing e-mails. Additionally, **IntegratorLogin** information has been added in the case of Atera Agent and domain information in the case of ScreenConnect. Although some of the third-party file upload services used by the team are still from older services, new ones have been added.

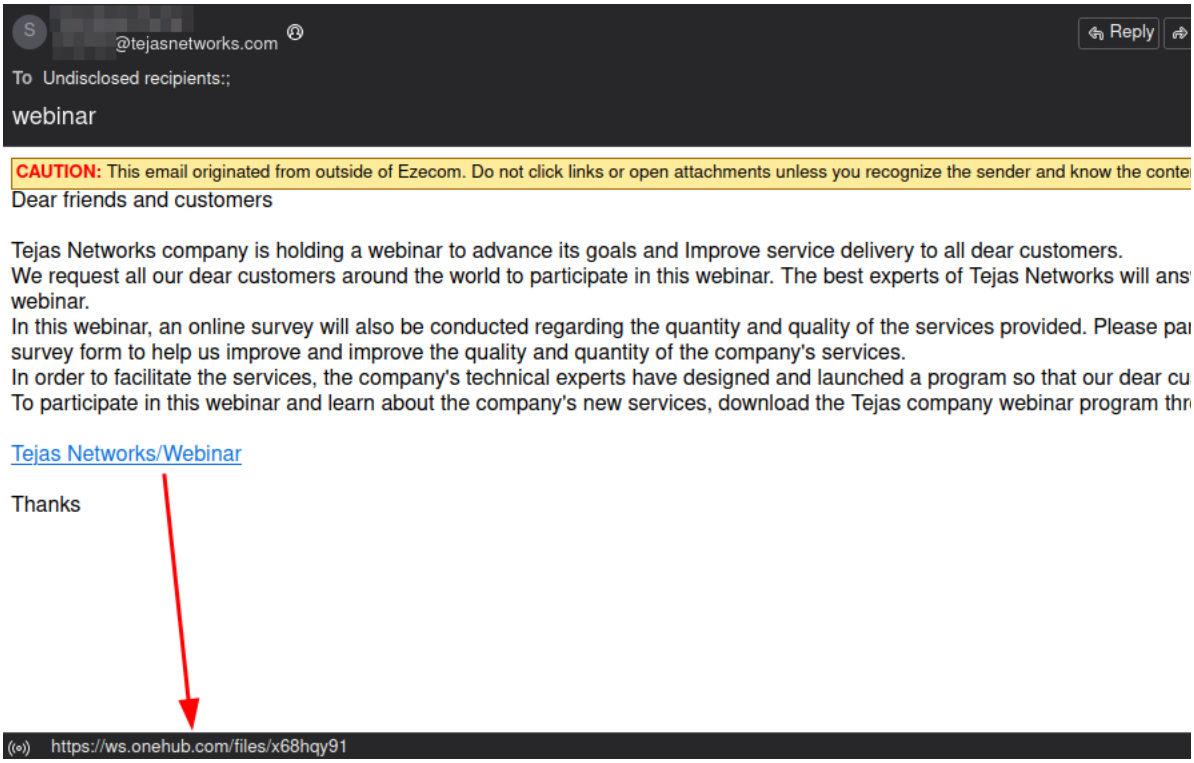

Figure 1. A phishing email was sent to victims via email by hacking into the employee's account. The email contains a download link.

Attackers prepare spear-phishing attacks by creating specific mail templates and malicious files named with the target's name. The attackers use common names in the company or industry, or directly the target's name, to obtain an RMM agent build and add it to a **ZIP** file. These ZIP files are uploaded to various file upload platforms. They then attach the malicious file download links directly in emails or PDF files. In the new attack chain after March 2024, Muddywater APT continues using services it has actively used since 2019. The group has used **onehub.com** for many years and other file upload services like **freeupload.store**, **filetransfer.io, egnyte.com, sync.com**, and **terabox.com**. When the victim clicks on the link in the email, they download a ZIP file from these services.

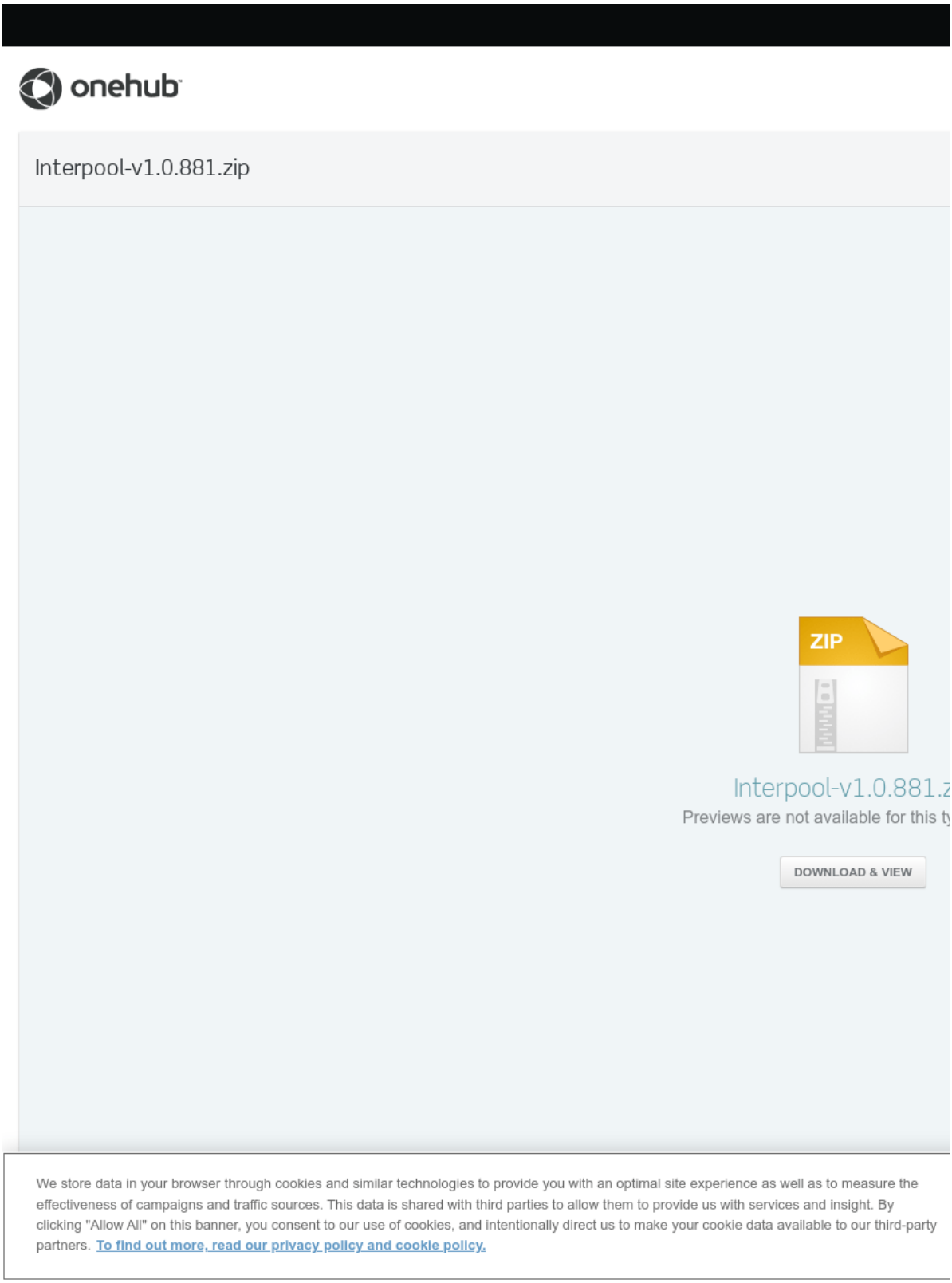

Figure 2. Download links for the tool ZIP file containing the RMM agent from Onehub.

After running the Atera Agent or ConnectWise ScreenConnect installation **MSI** file from the ZIP, the victim user will have the free legitimate RMM tool installed on their device, providing them with various controls.

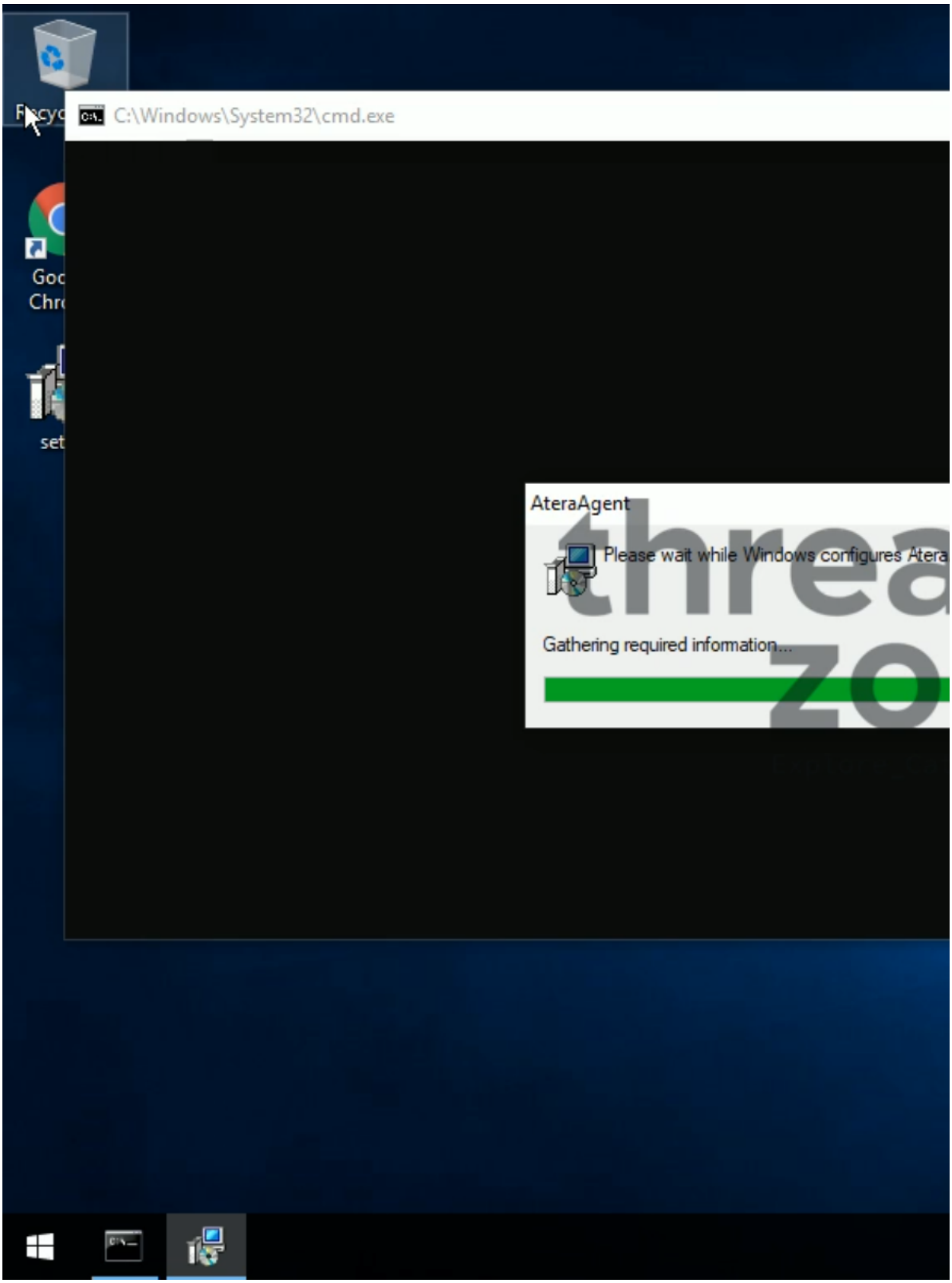

Figure 3. Looking at an example Atera Agent installation on our Threat.Zone [3] platform.

RMM Tools: Atera and ScreenConnect are applications that offer device management (RMM) through remote connection for IT managers. Although they provide IT automation and system management, due to their legitimate software, they are often the preferred access method for various ransomware and APT groups.

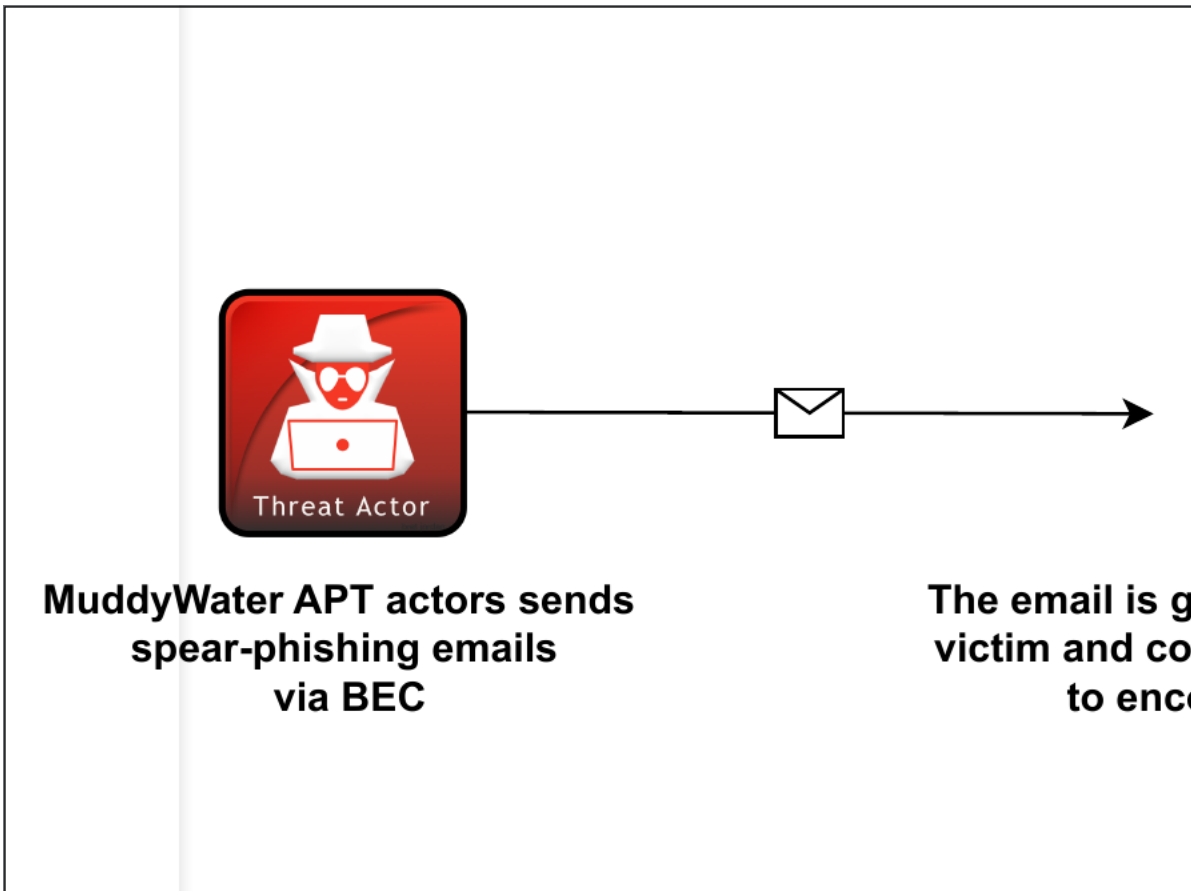

Figure 4. MuddyWater APT's latest attack pattern graph.

During the building process of Atera and ScreenConnect software, user information is required to customize it for the account. Our team has observed that many business email accounts (**BEC**) are captured and used in attacks. By building these builders on these accounts, the software becomes less attractive and increases the victim's persuasion power to download and run it. Attackers can use RMM tools to build agents on legitimate sites using compromised accounts.

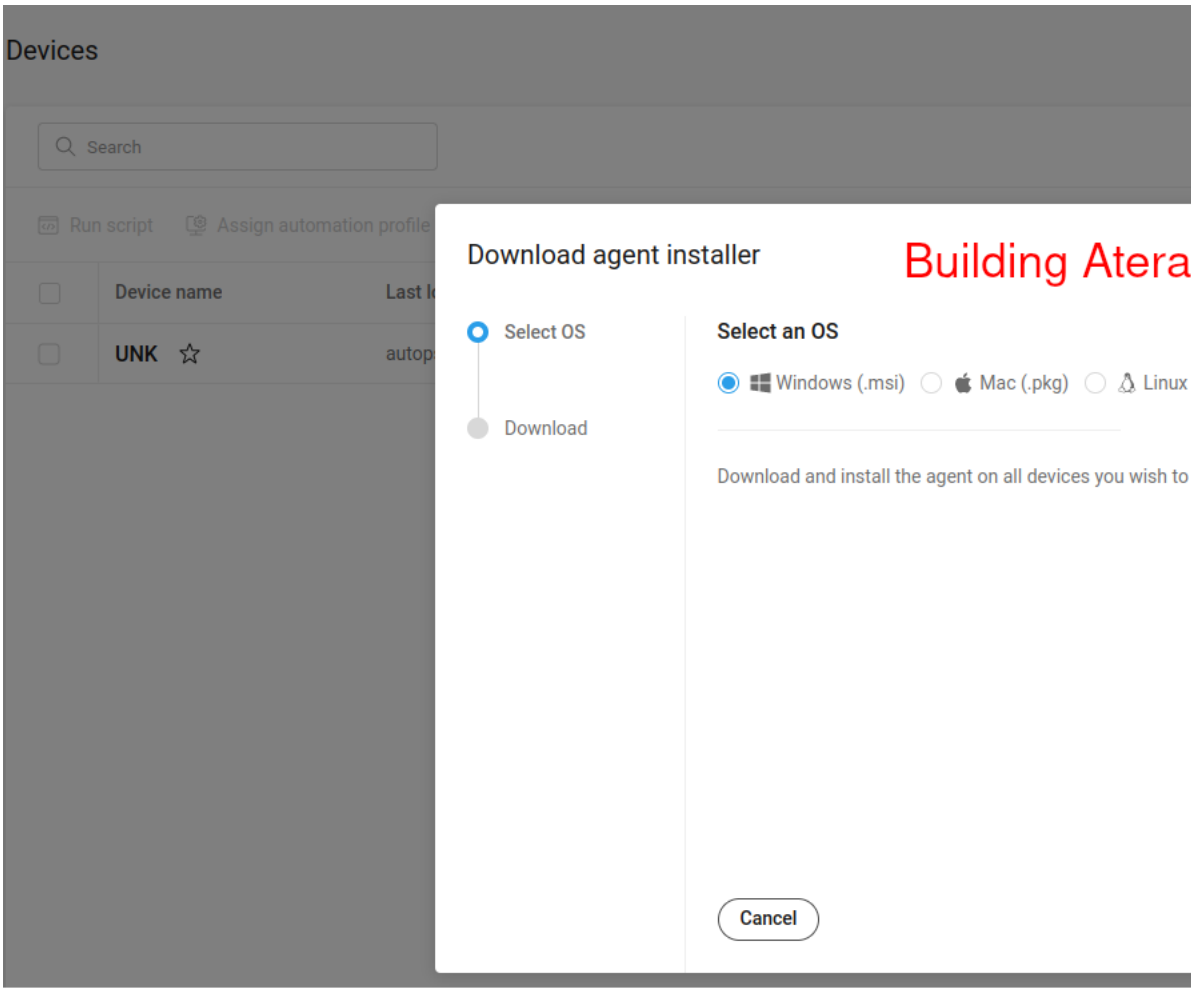

Figure 5. Looking at a sample Atera build and management functions after installation.

Figure 5 shows that running third-party RMM tools on the system ensures persistence and provides various capabilities such as command execution, file download, upload, and monitoring. Once the files are customized for the target, metadata is stored. The hashes and file names of the files generated in this manner have been tracked since their initial release. They are as follows:

SHA256	File Name
e89f48a7351c01cbf2f8e31c65a67f76a5ead689bb11e9d4918090a165d4425f	Salary.msi
ff2ae62ba88e7068fa142bbe67d7b9398e8ae737a43cf36ace1fcf809776c909	תוכנת תיירות.msi ('tourism program')
c2f95299d8aa912e1b753f3f0780a00ea6e8b5dab0245d77fcf3b6499677c328	Leonardo Hotels-tourism software.msi
77cb08c7889c7b0d443aeacfdcbc1cc6745d3e3441f4b42ddbf7fde6113491ae	Interpool-v1.0.881.msi
638c7a4f833dc95dbab5f0a81ef03b7d83704e30b5cdc630702475cc9fff86a2	Polaristek.msi
14c270cf53a50867e42120250abca863675d37abf39d60689e58288a9e870144	Tejasnetworks.com.webinar.msi
ffbe988fd797cbb9a1eedb705cf00ebc8277cdbd9a21b6efb40a8bc22c7a43f0	IronSwords.msi
c6128f222f844e699760e32695d405bd5931635ec38ae50eddc17a0976ccefb4	מילגה.msi ('scholarship')
dd2675e2f6835f8a8a0e65e9dbc763ca9229b55af7d212da38b949051ae296a5	karel.com.tr.telekomünikasyonWebsemineri.msi ('telecomunication webinar')

Table 1. File name examples of MuddyWater campaigns.

Upon examining the file names in the IOC table, it is evident that the files are tailored to the target company and named according to the language of each country, whether it be **English** (Polaristek), **Hebrew** (תוכנת תיירות), or **Turkish** (telekomünikasyonWebsemineri). However, the file names, such as **IronSwords.msi**, explicitly pointing to **7 October 2023**, the start date of the Operation Swords of Iron attacks on Hamas, and the compromised accounts distributing the file indicate that the group is acting following political interests.

The targeted attack on **Karel**, a Turkish telecommunications company, is evident in the file karel.com.tr.telekomünikasyonWebsemineri.msi (SHA256 hash:

dd267575e2f6835f8a8a0e65e9dbc763ca9229b55af7d212da38b949051ae296a5). The legitimate structure of the Atera file remains intact, with only the target-specific build being affected. After executing the Atera Agent on the system using the command C:\Windows\System32\msiexec.exe /i "C:\Users\User\Desktop\sample_file.msi", the file retrieves the account (**IntegratorLogin**) and its corresponding ID (**AccountID**) from the MSI tables. The accounts that distribute the file are also explicitly selected for the targeted attacks.

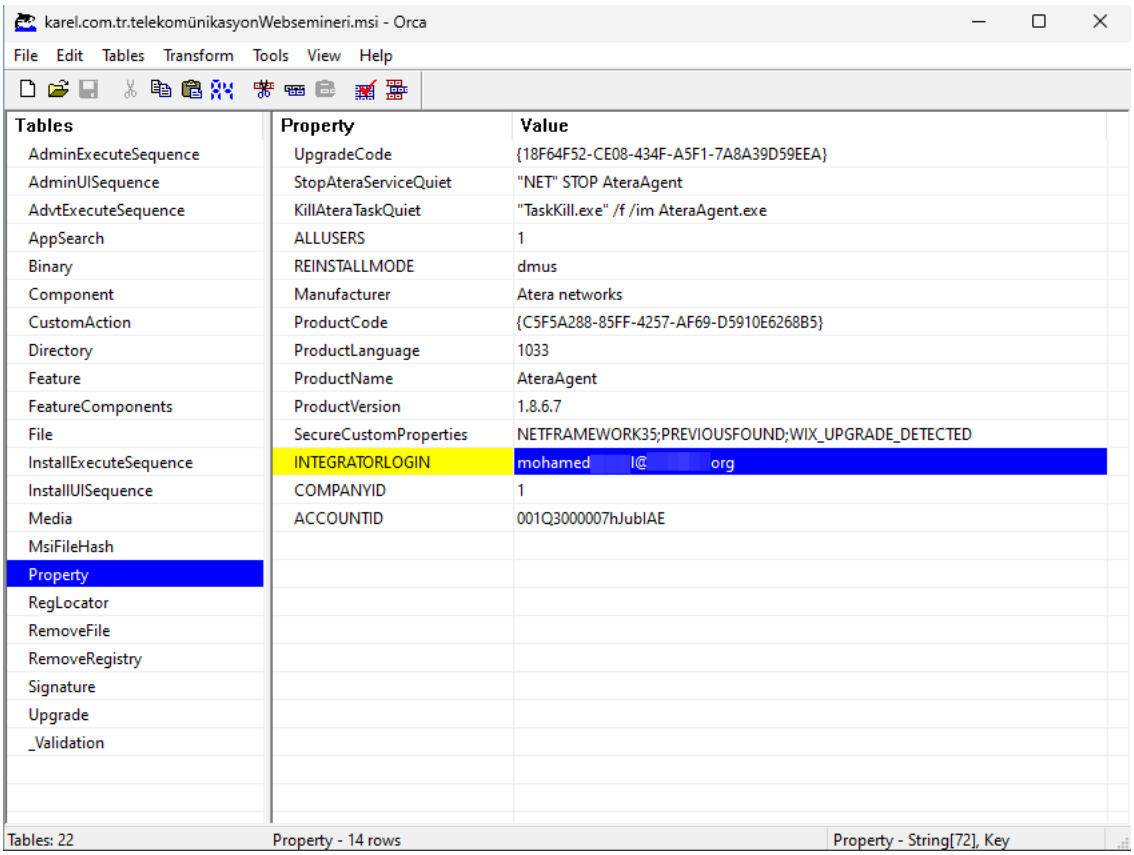

Figure 6. Atera agent IntegratorLogin and AccountID meta fields.

Analysis of the Atera installer revealed which compromised attacker account was used in this attack, as in Figure 6. The running process command can also be used to monitor this information. The attacker account then proceeds to carry out its actions on the victim machine's objectives. In all malware examples, it is easy to identify the compromised accounts through which these files are transmitted. When viewed through **Threat.Zone**, malware can collect IntegratorLogin information. Only chrchill[.]com information is noticeable in the meta information of ScreenConnect software [4].

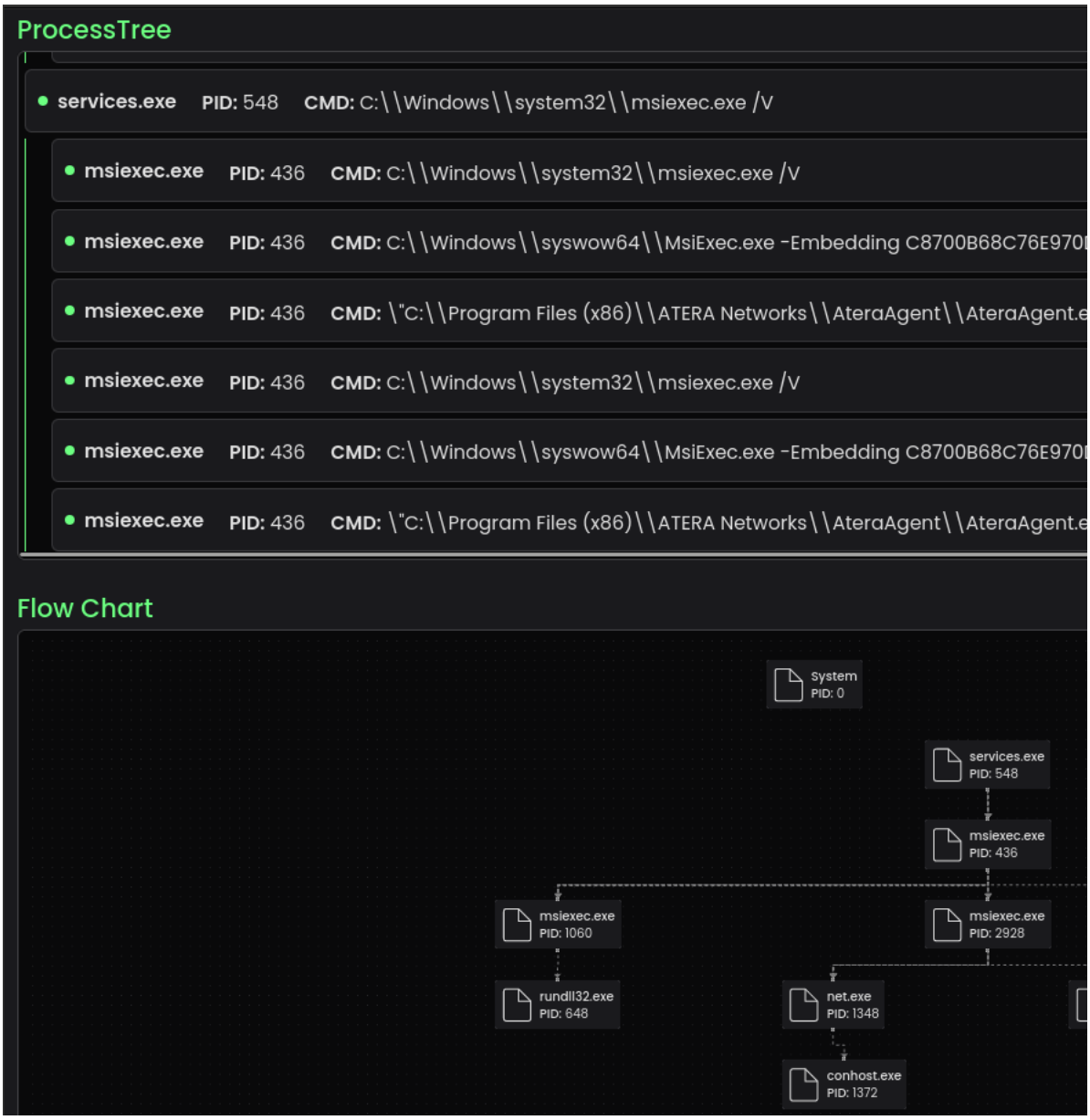

Figure 7. Meta information in the processes run by Atera in Threat.Zone. [5]

Conclusion

Since 2017, the MuddyWater APT group has been targeting entities aligned with Iran's political interests and agenda. They add new attack techniques every year and learn from past **OPSEC** mistakes. They seek ways to remain anonymous by abusing legitimate tools. Remote Monitoring and Management (RMM) tools have become more common for Advanced Persistent Threat (APT) activities and ransomware attacks. However, fewer threat actors are expanding their attack vectors by developing their software. Those who use a combination of public and legitimate tools instead of their own are making less conspicuous moves. The MuddyWater APT group, for example, accelerated its attacks after Operation Swords of Iron. Due to the expected increase in attacks, it is crucial to be cautious, particularly against file upload services and BEC attacks used by the group.

As we prepare this article, some questions remain unanswered,

* What happens after the post-infection phase?

* How do MuddyWater actors compromise business e-mails in initial access?

The new type of MuddyWater APT malware we identified as Malwation Threat Research Team is confirmed by ProofPoint's latest report [6] with the Salary.msi file [7].

Recommendations

1- RMM network indicators and file upload services:

Since MuddyWater activities are actively coming from certain file upload services, it is recommended to follow the services written in the blog post on the internal network and examine the traffic from these services in the last period. In addition, after the installation of the RMM tool provided by Atera and ScreenConnect, related Atera domains [8] and ScreenConnect ports (Outbound 8040-8041) should be checked as outbound traffic will be communicated with certain addresses. Attention should also be paid to inbound traffic coming from the domains of the online file-upload services mentioned in the blog (onehub.com, freeupload.store, filetransfer.io, egnyte.com, snyc.com, and terabox.com).

2- Use sandbox and CDR:

To provide more effective protection and prevention, you can run attachments in your corporate e-mails through CDR, or check your malware scores by testing files in a sandbox. Threat.Zone sandbox and CDR acts as an intermediate layer to help you at this point and checks the malicious detection of the relevant files especially against BEC attack methods often favoured by threat actors in isolated environments before threats occur.

Indicators of compromise (IOCs)

cc4cc20b558096855c5d492f7a79b160a809355798be2b824525c98964450492
c6128f222f844e699760e32695d405bd5931635ec38ae50eddc17a0976ccefb4
dd2675e2f6835f8a8a0e65e9dbc763ca9229b55af7d212da38b949051ae296a5
cc8be1d525853403f6cfabcf0fc3bd0ca398ece559388102a7fc55e9f3aa9b33
fb02e97d52a00fca1580ca71ed152dd28dd5ae28ab0a9c8e7b32cebd7f1998a1
ffbe988fd797cbb9a1eedb705cf00ebc8277cdbd9a21b6efb40a8bc22c7a43f0
2ae6c5c2b71361f71ded4ad90bbf6ef0b0f4778caf54078c928e2017302fbe69
14c270cf53a50867e42120250abca863675d37abf39d60689e58288a9e870144
638c7a4f833dc95dbab5f0a81ef03b7d83704e30b5cdc630702475cc9fff86a2
77cb08c7889c7b0d443aeacfdcbc1cc6745d3e3441f4b42ddbf7fde6113491ae
c2f95299d8aa912e1b753f3f0780a00ea6e8b5dab0245d77fcf3b6499677c328
7daab239271e088f04cae95627cc0066f48a1b178a1ff60b1140aa729126e928
ff2ae62ba88e7068fa142bbe67d7b9398e8ae737a43cf36ace1fcf809776c909
e89f48a7351c01cbf2f8e31c65a67f76a5ead689bb11e9d4918090a165d4425f

https://ws.onehub[.]com/files/4mbha9wd
https://ws.onehub[.]com/files/kwdphknm
https://kinneretacil.egnyte[.]com/fl/wERX5mfnFx
https://kinneretacil.egnyte[.]com/fl/gRykrFURtE
https://freeupload[.]store/rALE7/wIHItUcE08.msi/download
https://filetransfer[.]io/data-package/tuMe19fV/download

References

1- https://www.gov.il/BlobFolder/reports/alert_1718/he/ALERT-CERT-IL-W-1718.pdf

2- https://twitter.com/k3yp0d/status/1761736544061198704

3- https://app.threat.zone/submission/66b6a3b3-7a75-4bef-a8a2-355ed20eb503/dynamic-scan-report/overview

4- https://app.threat.zone/submission/c5fe6cc4-41a7-49f0-b3c7-c22298f5feaf/dynamic-scan-report/overview

5- https://app.threat.zone/submission/865323e6-e9da-4629-a7ee-827ef432e32b/dynamic-scan-report/overview

6- https://www.proofpoint.com/us/blog/threat-insight/security-brief-ta450-uses-embedded-links-pdf-attachments-latest-campaign

7- https://www.virustotal.com/gui/file/cc4cc20b558096855c5d492f7a79b160a809355798be2b824525c98964450492/detection

8- https://support.atera.com/hc/en-us/articles/360015461139-Firewall-Settings-for-Atera-s-Integrations