New MuddyWater Threat: Old Kitten; New Tricks

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

December 8, 2022

Learn more

MuddyWater, also known as Static Kitten and Mercury, is a cyber espionage group that's most likely a subordinate element within Iran's Ministry of Intelligence and Security (MOIS).

Since at least 2017 MuddyWater has targeted a range of government and private organizations across sectors, including telecommunications, local government, defense, and oil and natural gas organizations, in the Middle East, Asia, Africa, Europe, and North America.

MuddyWater has various campaigns that are entirely different from each other. In this post we will focus on the most recent changes and observations of their campaign which utilizes spearphishing with legitimate remote administration tools.

Executive summary:

- Deep Instinct's Threat Research team has identified a new campaign of the MuddyWater group.
- The campaign has been observed targeting Armenia, Azerbaijan, Egypt, Iraq, Israel, Jordan, Oman, Qatar, Tajikistan, and United Arab Emirates.
- The campaign exhibits updated TTPs to previously reported MuddyWater activity.

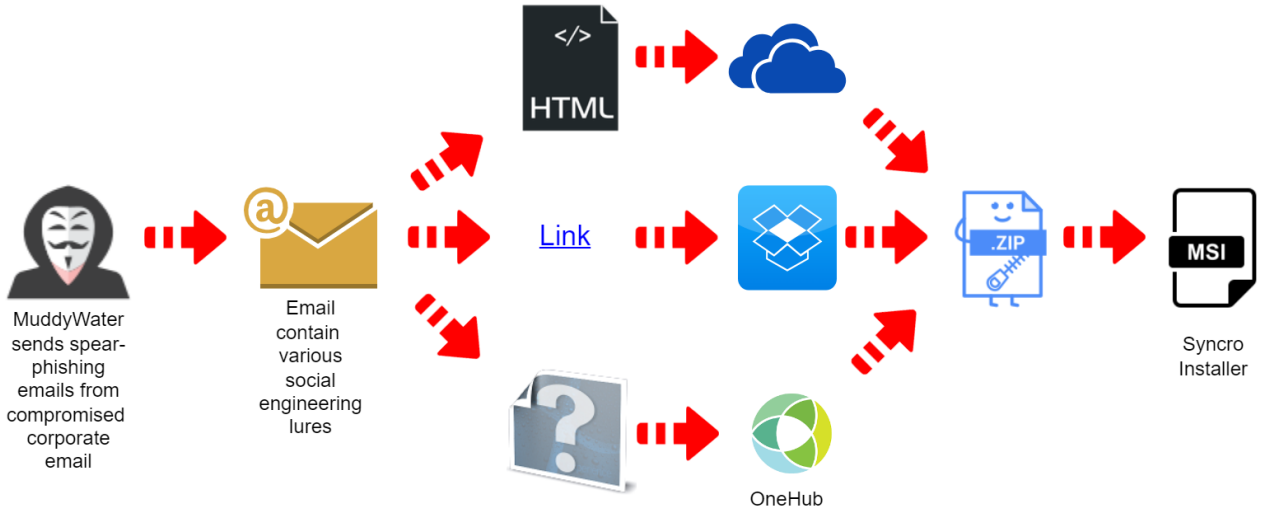

Figure 1: Campaign overview

MuddyWater Exploiting Legitimate Tools

Previous research has shown that in 2020 MuddyWater sent spearphishing emails with direct links as well as PDF and RTF attachments containing links to archives hosted at "ws.onehub.com."

Those archives contained the installer for "RemoteUtilities," a legitimate remote administration tool.

Since the beginning of 2021, MuddyWater has been observed sending spearphishing emails containing either direct links or Word documents with links to archives hosted at "ws.onehub.com."

The archives from 2021 contained installers for ScreenConnect, another legitimate remote administration tool.

This activity was observed intermittently through the end of 2021 and until July 2022.

In July 2022 a potential file related to this campaign was observed, but it contained Atera Agent instead of the usual ScreenConnect, potentially signaling the threat actor switched to another remote administration tool to avoid detection of their long running campaign.

A new discovery: The current MuddyWater campaign

The most recent MuddyWater campaign was observed by Deep Instinct in the beginning of October and possibly started in the September timeframe.

What makes this campaign different from previous waves is the use of a new remote administration tool named "Syncro."

A new lure in the form of an HTML attachment was observed, along with the addition of other providers for hosting the archives containing the installers of the remote administration tool.

The previous July sample with ScreenConnect mentioned earlier, was named "promotion.msi."

In the current campaign there was a sample that had few names; one of them was also "promotion.msi."

The above ScreenConnect sample was communicating with "instance-q927ui-relay.screenconnect.com." This instance was communicating with another MuddyWater MSI installer named "Ertiqa.msi" which is a name of a Saudi organization.

In the current wave, MuddyWater used the same name "Ertiqa.msi," but with Syncro installer.

The target geolocations and sectors also align with previous targets of MuddyWater. Combined, these indicators provide us with enough proof to confirm that this is the MuddyWater threat group.

EXAMPLE #1: Egyptian Hosting Company

Direct links to Dropbox:

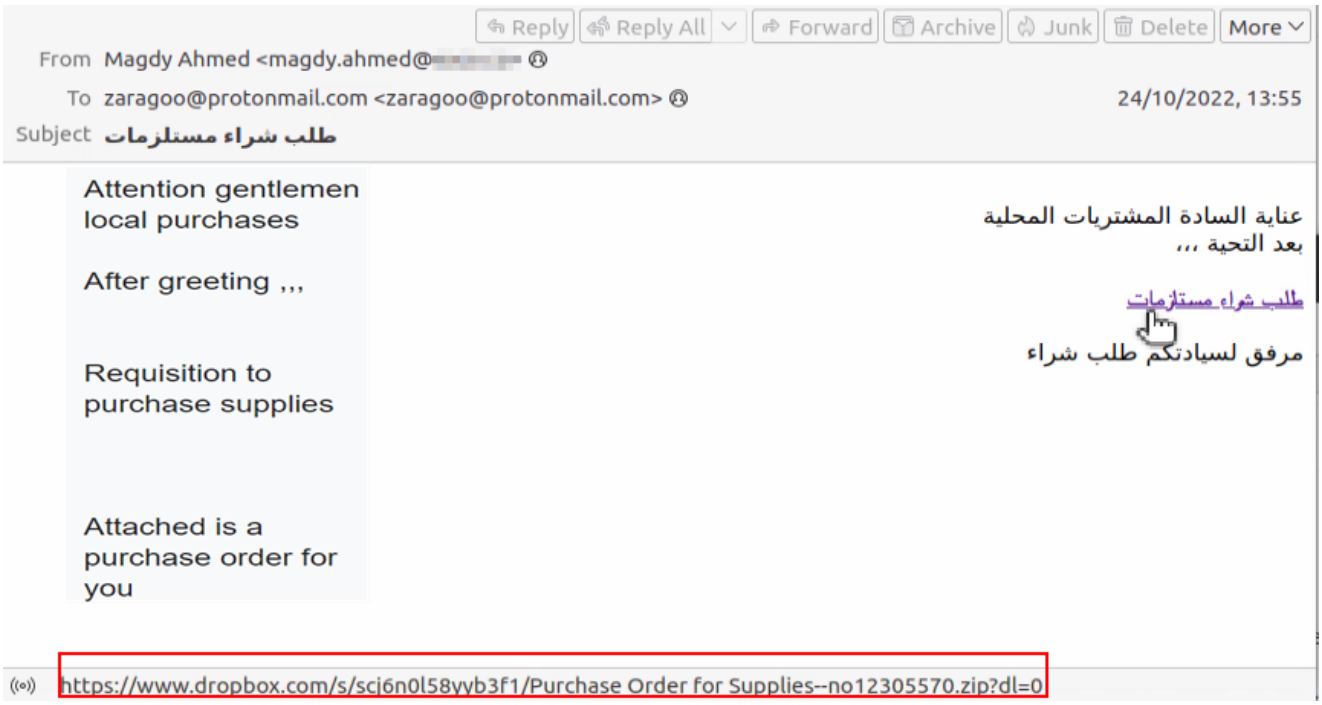

Figure 2: Email containing direct link to Dropbox

This mail was sent from an Egyptian data hosting company, unlike previous campaigns using OneHub. This time MuddyWater used Dropbox to host the archive with the Syncro installer:

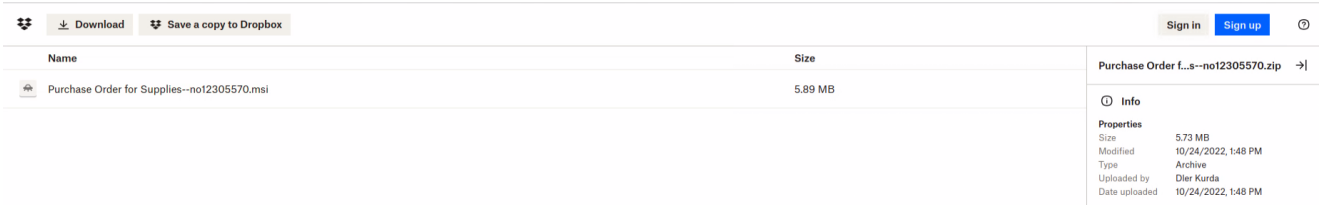

Figure 3: Zip archive hosted on Dropbox containing MSI installer for Syncro

HTML attachment leading to OneDrive:

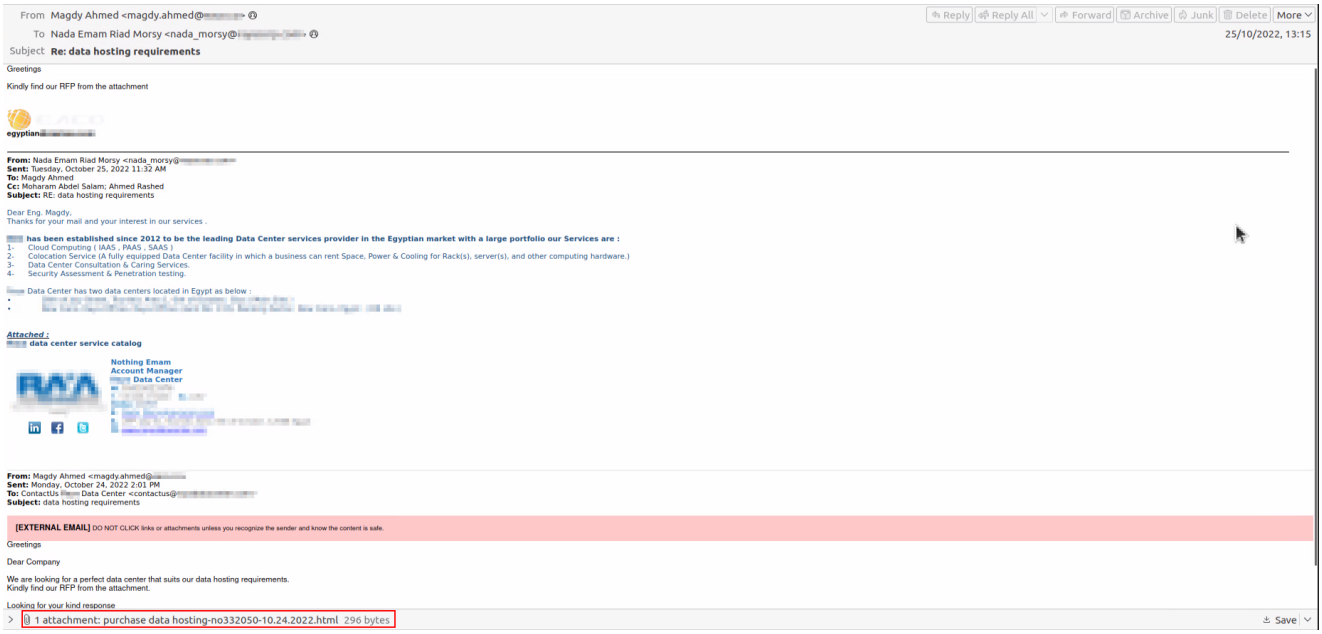

Figure 4: Email containing HTML attachment

On the same date the email with the Dropbox link was sent, MuddyWater sent another email from the same address of an Egyptian hosting company to another Egyptian hosting company.

Instead of embedding a direct link in the email message, an HTML attachment was sent. This is a well-known technique to build trust. The receiving end knows the company who sent the mail. The attachment is not an archive or an executable which doesn't raise end-user suspicion because HTML is mostly overlooked in phishing awareness trainings and simulations.

HTML is considered "safer," at least from an anti-virus (AV) and email security solutions point of view. Although those solutions have the ability to scan HTML, they are often still delivered to the recipients and not blocked.

The HTML itself is very small; its main function is most likely to bypass email solutions that replace any link with "safe" link.

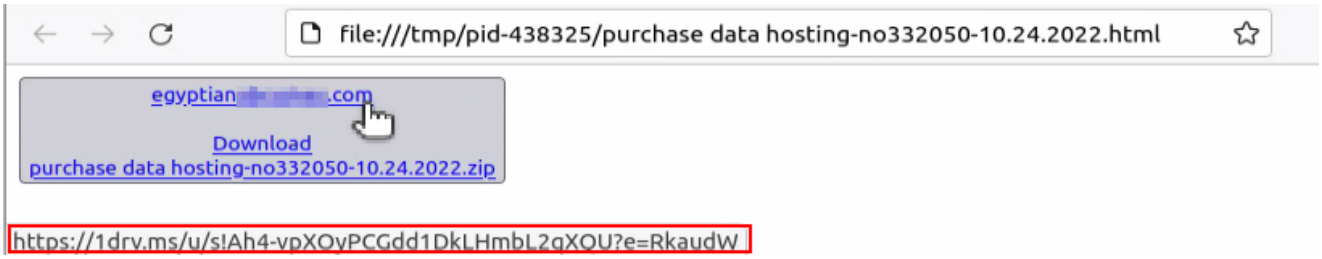

Figure 5: HTML attachment containing link to OneDrive
The link inside the HTML file leads to OneDrive this time, hosting an archive containing Syncro MSI installer.

EXAMPLE #2: Israeli Hospitality Industry

In another example from early November, MuddyWater sent an email from a company in the Israeli hospitality industry to a wide number of contacts across different Israeli insurance companies:

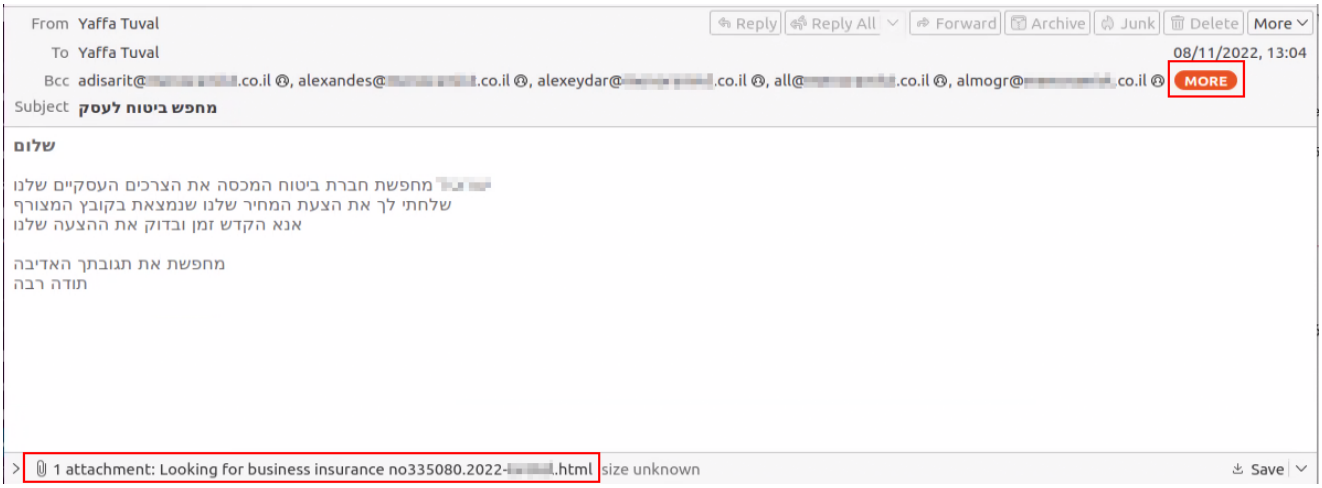

Figure 6: Email containing HTML attachment
In this mail the company from the hospitality industry is looking for insurance.

The text is written in Hebrew, but a native speaker will find it suspicious due to a poor choice of words.

Once again, the link leads to an archive hosted on OneDrive which contain Syncro MSI installer:

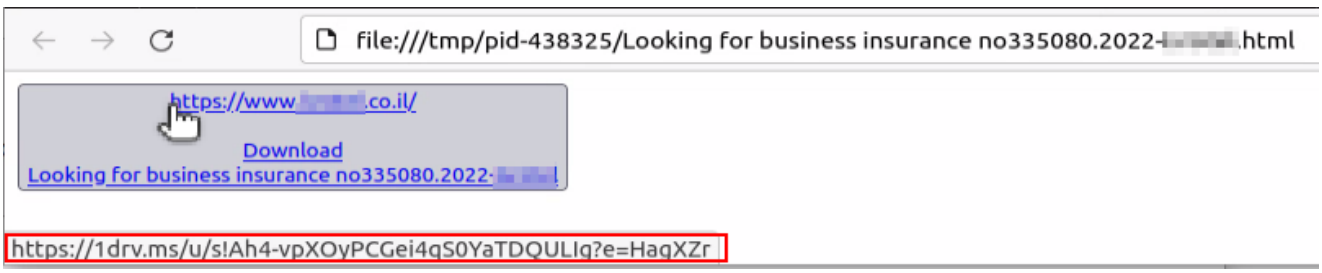

Figure 7: HTML attachment containing link to OneDrive
Despite those new TTPs, most of the Syncro installers are still hosted in OneHub:

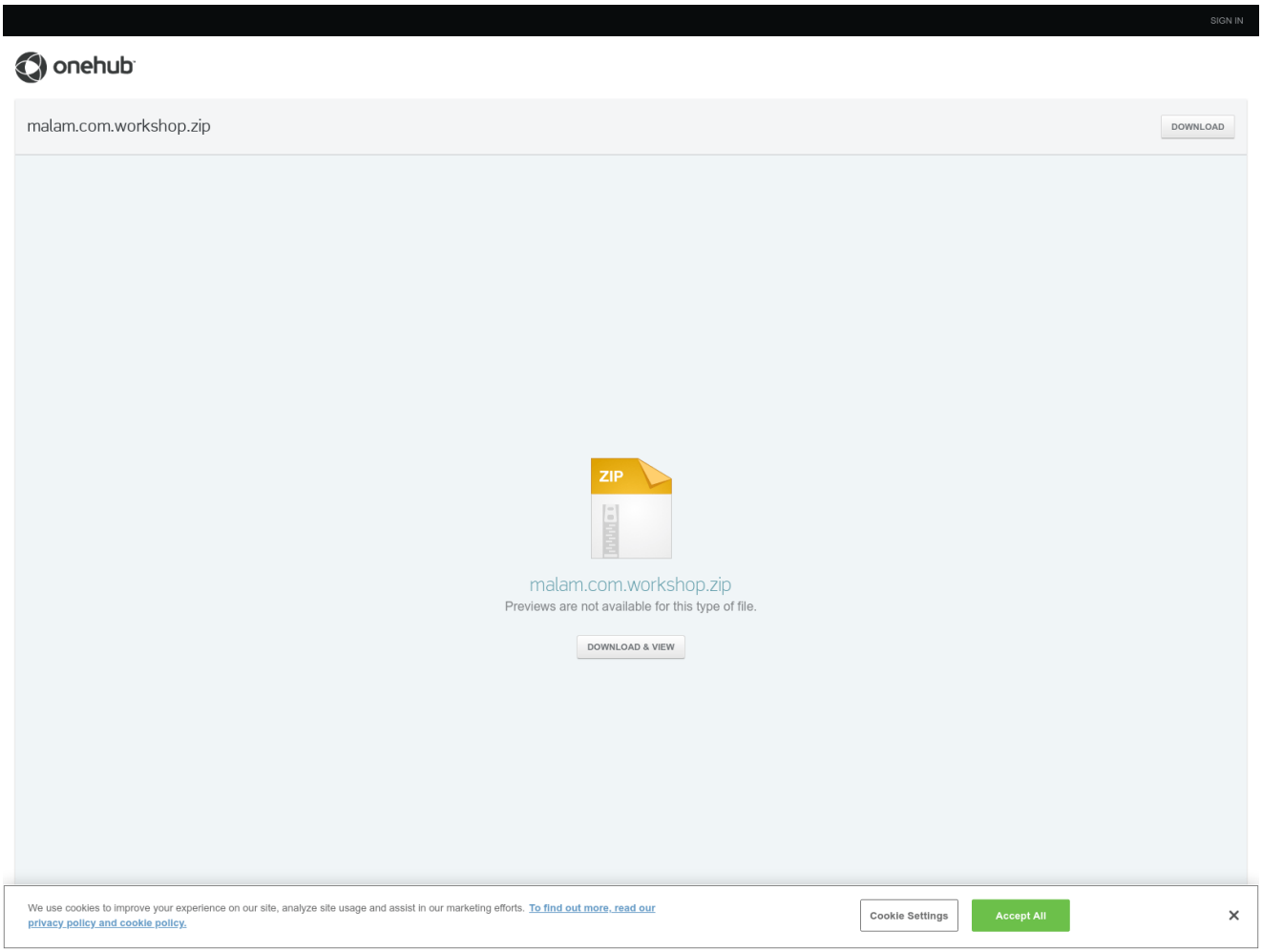

Figure 8: Archive hosted on OneHub containing Syncro MSI installer

What is unclear is whether or not MuddyWater gained full access to the email server or only the credentials to one email box. The emails are sent from legitimate corporate accounts. We see that in spite of the low level of sophistication that this tactic can be effective.

Syncro: A tool used by multiple threat actors

MuddyWater is not the only actor abusing Syncro. It has also been observed recently in BatLoader and Luna Moth campaigns.

Syncro is a fully-featured platform for Managed Service Provider's (MSPs) to run their business.

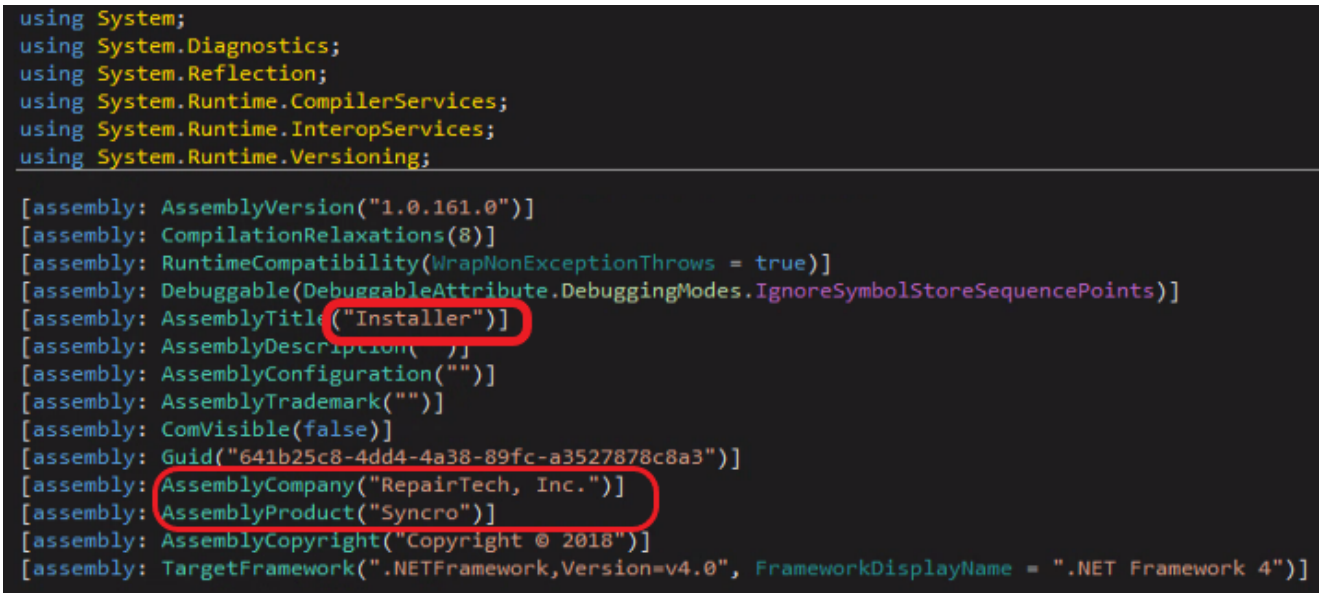

Figure 9: Sycnro Installer inside the MSI

Syncro provides an agent for MSPs to manage any device that has Syncro installed with the custom-made provided MSI file that includes the customerID.

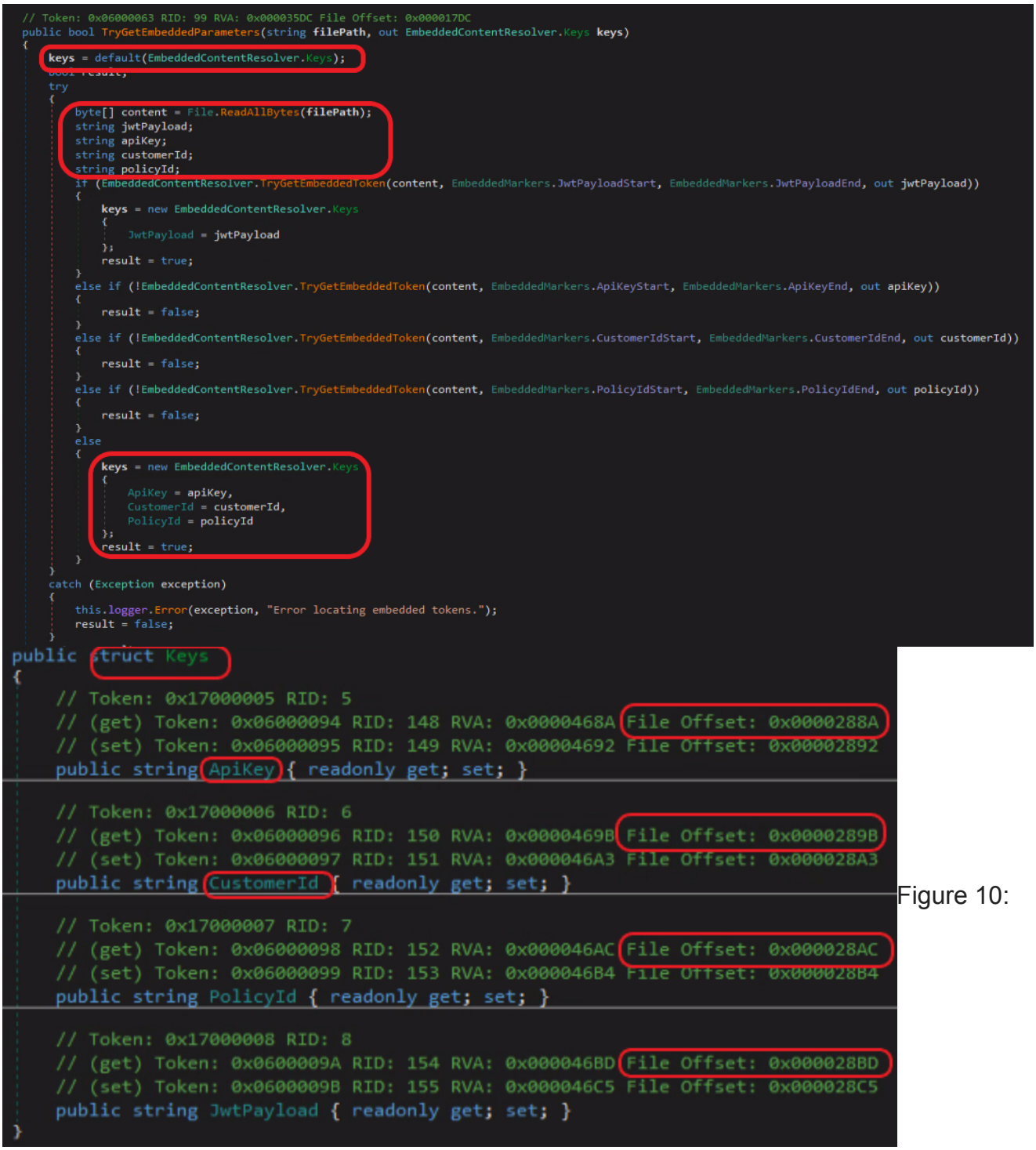

Figure 10: Syncro installation process with the customerID and ApiKey

Syncro has a 21-day trial offer. You choose the subdomain to be used by your MSP:

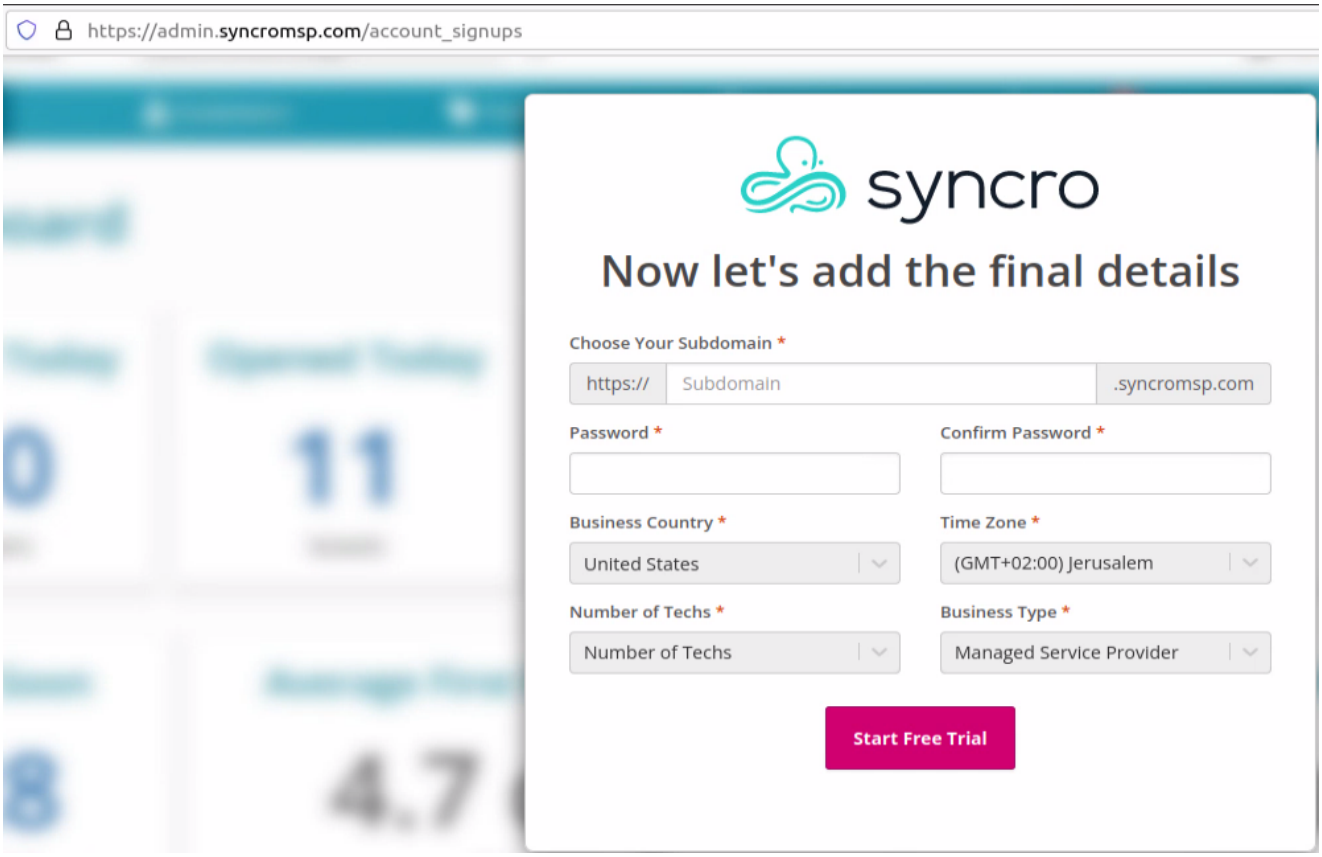

Figure 11: Syncro trial sign-up screen with choice of syncromsp.com subdomain

While investigating some of the installers that MuddyWater used, we see that for each unique mail a new MSI was used. In most cases MuddyWater used a single subdomain with a single MSI installer.

It seems that most of the subdomains don't have any useful meaning, although a few are clear:

- mohammadosman6060 and osmandembele4040 are football players
- netanyahu8585 and benet5050 are the current and former prime ministers of Israel
- Cham Wings is the name of a Syrian airline

The trial version contains the fully featured web GUI which allows complete control over a computer with the Syncro agent installed:

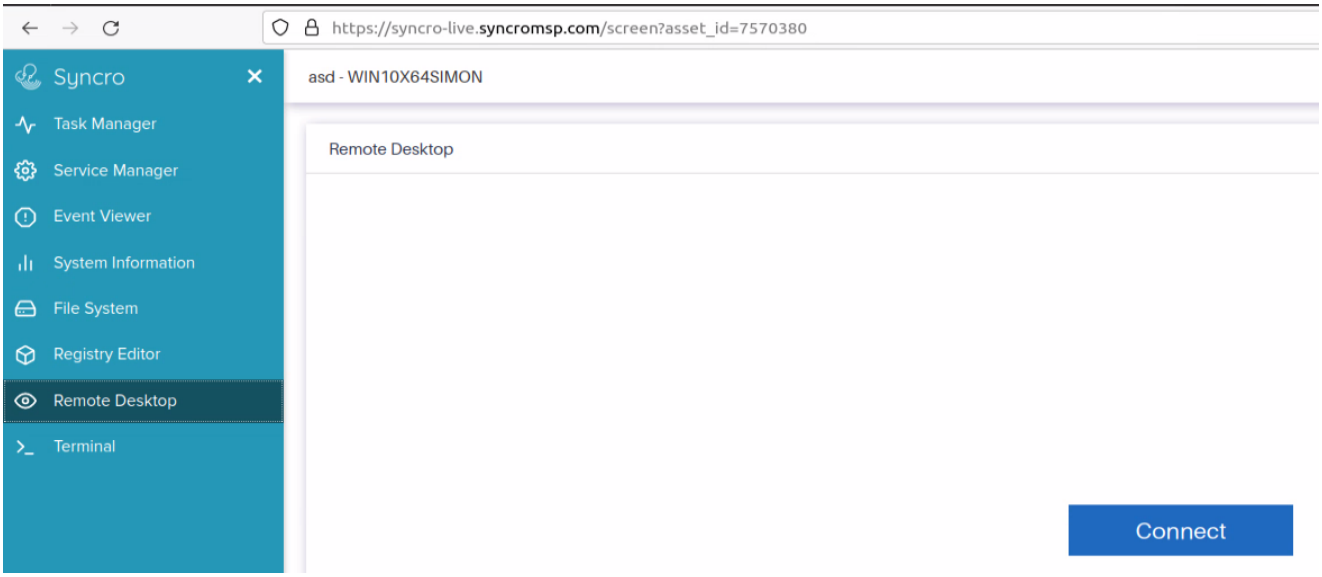

Figure 12: Web GUI of Syncro with available remote administration features

Those features are standard for remote administration tools, such as terminal with SYSTEM privileges, remote desktop access, full file system access, tasks, and services manager.

All those features combined with a signed MSI installer creates the perfect weapon for a threat actor to gain initial access and start performing recon on the target. Later, they enable the threat actors to deploy additional backdoors, exfiltrate files, or hand-off access to other threat actors. A threat actor that has access to a corporate machine via such capabilities has nearly limitless options.

Recommendations:

We have recently described other dual-use tools that are being abused for malicious purposes. We recommend that security teams monitor for remote desktop solutions that are not common in the organization as they have a higher chance of being abused.

MITRE ATT&CK:

Tactic	Technique	Description	Observable

Tactic	Technique	Description	Observable
Initial Access	T1566.001 Phishing: Spearphishing Attachment	MuddyWater has compromised third parties and used compromised accounts to send spearphishing emails with targeted attachments to recipients.	aaa9db79b5d6ba319e24e6180a7935d
Initial Access	T1566.002 Phishing: Spearphishing Link	MuddyWater has compromised third parties and used compromised accounts to send spearphishing emails containing links to legitimate domains hosting archives with remote management software.	d1b4ca2933f49494b4400d5bf5ab502e
Command and Control	T1219 Remote Access Software	MuddyWater has used a legitimate application, Syncro, to manage systems remotely and move laterally.	2ed6ebaa28a9bfccc59c6e89a8990631

Tactic	Technique	Description	Observable
Resource Development	T1588.002 Obtain Capabilities: Tool	MuddyWater has used a legitimate application, Syncro, to manage systems remotely and move laterally.	2ed6ebaa28a9bfccc59c6e89a8990631
Resource Development	T1583.006Acquire Infrastructure: Web Services	MuddyWater has used file sharing services including OneHub, Dropbox, and OneDrive to distribute tools.	https://urlscan.io/result/c6f46810-ee19-47b4-8717-40dc09b4ea09/ - archived scan of a Dropbox URL containing an archive with Syncro installer.

IOC:

f511bdd471096fc81dc8dad6806624a73837710f99b76b69c6501cb90e37c311
efd5271bdb57f52b4852bfda05122b9ff85991c0600befcbd045f81d7a78eac5
d65d80ab0ccdc7ff0a72e71104de2b4c289c02348816dce9996ba3e2a4c1dd62
1670a59f573037142f417fb8c448a9022c8d31a6b2bf93ad77a9db2924b502af
dedc593acc72c352feef4cc2b051001bfe22a79a3a7852f0daf95e2d10e58b84
eae0acba9c9e6a93ce2d5b30a5f21515e8ccca0975fbd0e7d8862964fdfa1468
7e7292b5029882602fe31f15e25b5c59e01277abaab86b29843ded4aa0dcbdd1
c7a2a9e020b4bcbfa53b37dea7ebf6943af203b94c24a35c098b774f79d532ac
887c09e24923258e2e2c28f369fba3e44e52ce8a603fa3aee8c3fb0f1ca660e1
01dfa94e11b60f92449445a9660843f7bea0d6aad62f1c339e88252008e3b494
d550f0f9c4554e63b6e6d0a95a20a16abe44fa6f0de62b6615b5fdcdb82fe8e1
61dcf1eeb616104742dd892b89365751df9bb8c5b6a2b4080ac7cf34294d7675
c6cfd23282c9ff9d0d4c72ee13797a898b01cd5fd256d347e399e7528dad3bfd
5578b7d126ebae78635613685d0cd07f4fb86f2e5b08e799bdc67d6d6053ede2
32339f7ac043042e6361225b594047dd4398da489a2af17a9f74a51593b14951
dab77aea8bf4f78628dcf45be6e2e79440c38a86e830846ec2bddc74ff0a36e4
b5c7acf08d3fd68ddc92169d23709e36e45cb65689880e30cb8f376b5c91be57
2a5f74e8268ad2d38c18f57a19d723b72b2dadd11b3ab993507dd2863d18008d
e87fe81352ebda0cfc0ae785ebfc51a8965917235ee5d6dc6ca6b730eda494cf

aa282daa9da3d6fc2dc6d54d453f4c23b746ada5b295472e7883ee6e6353b671
4e80bd62d02f312b06a0c96e1b5d1c6fd5a8af4e051f3f7f90e2976580842515
697580cf4266fa7d50fd5f690eee1f3033d3a706eb61fc1fca25471dbc36e684
dc7e102a2c68f7e3e15908eb6174548ce3d13a94caadf76e1a4ee834dc17a271
f24ce8e6679893049ce4e5a03bc2d8c7e44bf5b918bf8bf1c2e45c5de4d11e56
433b47f40f47bea0889423ab96deb1776f47e9faa946e7c5089494ed00c6cc29
011cb37733cdf01c689d12fedc4a3eda8b0f6c4dcdeef1719004c32ee331198e
e217c48c435a04855cf0c439259a95392122064002d4881cf093cc59f813aba8
331b513cf17568329c7d5f1bac1d14f38c77f8d4adba40c48dab6baf98854f92
4d24b326d0335e122c7f6adaa22e8237895bdf4c6d85863cf8e84cfcc0503e69
a35a1c92c001b59605efd318655d912f2bcd4e745da2b4a1e385d289e12ee905
4550b4fa89ff70d8ea59d350ad8fc537ceaad13779877f2761d91d69a2c445b2
653046fa62d3c9325dbff5cb7961965a8bf5f96fa4e815b494c8d3e165b9c94a
76ab046de18e20fd5cddbb90678389001361a430a0dc6297363ff10efbcb0fa8

Back To Blog