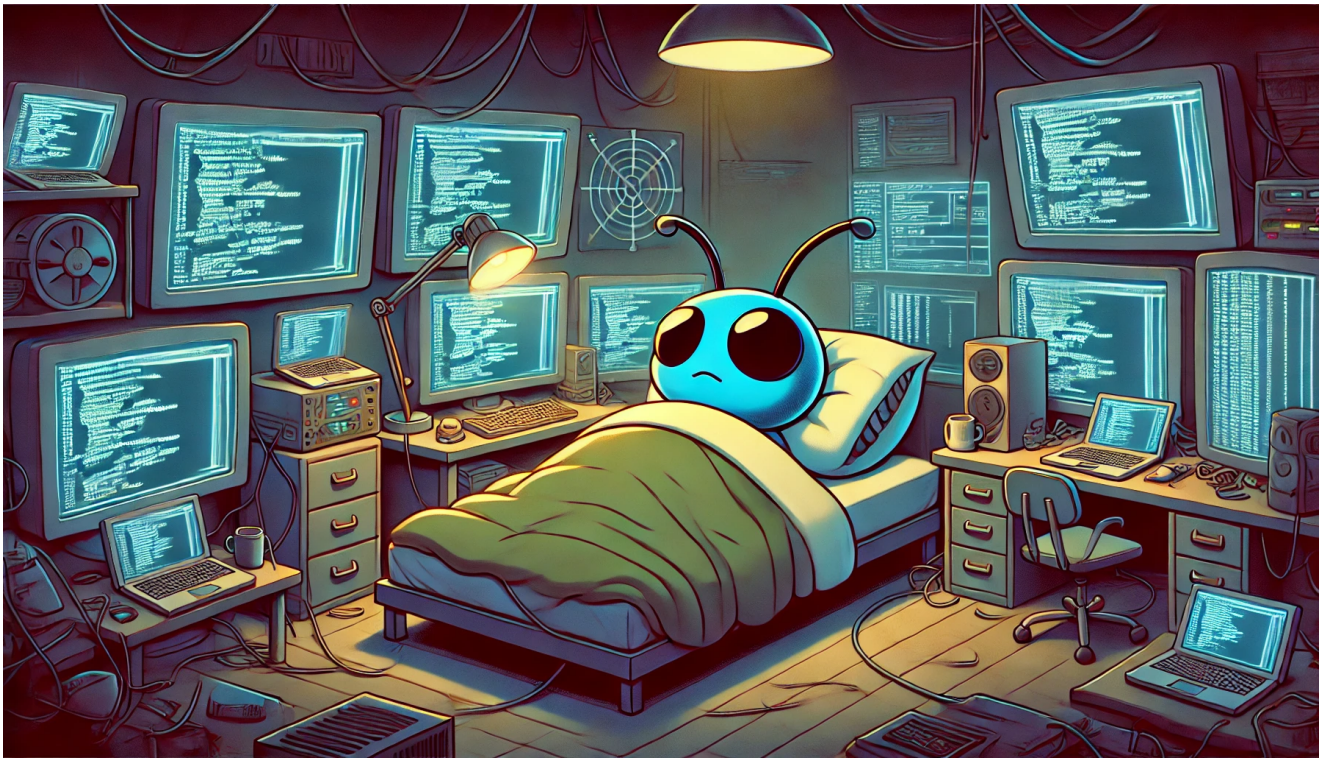
New BugSleep Backdoor Deployed in Recent MuddyWater Campaigns

research.checkpoint.com/2024/new-bugsleep-backdoor-deployed-in-recent-muddywater-campaigns/

July 15, 2024



Key Findings

- MuddyWater, an Iranian threat group affiliated with the Ministry of Intelligence and Security (MOIS), has significantly increased its activities in Israel since the beginning of the Israel-Hamas war in October 2023. This parallels with activities against targets in Saudi Arabia, Turkey, Azerbaijan, India and Portugal.
- The threat actors consistently use phishing campaigns sent from compromised organizational email accounts. The phishing campaigns typically lead to the deployment of legitimate Remote Management Tools (RMM) such as Atera Agent and Screen Connect.
- Recently, Muddy Water campaigns also led to the deployment of a new, previously undocumented tailor-made backdoor we dubbed BugSleep, that is used to target organizations in Israel.
- BugSleep is a backdoor designed to execute the threat actors' commands and transfer files between the compromised machine and the C&C server. The backdoor is currently in development, with the threat actors continuously improving its functionality and addressing bugs.

Introduction

MuddyWater, an Iranian threat group affiliated with the Ministry of Intelligence and Security (MOIS), is known to be active since at least 2017. During the last year, MuddyWater engaged in widespread phishing campaigns targeting the Middle East, with a particular focus on Israel. Since October 2023, the actors' activities have increased significantly. Their methods remain consistent, utilizing phishing campaigns sent from compromised email accounts targeting a wide array of organizations in countries of interest. These campaigns typically lead to the deployment of legitimate Remote Management Tools (RMM) such as Atera Agent or Screen Connect. Recently, however, they have deployed a custom backdoor we track as BugSleep.

In this report, we discuss the details of the most recent phishing campaigns and how they reflect the group's interests. In addition, we provide an analysis of MuddyWater's most recent techniques, tactics, and procedures (TTPs) including the BugSleep custom backdoor and the abuse of Egnyte, a legitimate file-sharing service.

Emails and Lures

MuddyWater campaigns usually consist of sending large numbers of emails to a wide range of targets from a compromised email account. Although their lures are aimed at a large and varied set of organizations or individuals, they often focus on specific industries or sectors, highlighting the group's points of interest. Among those are notable phishing campaigns aimed at Israeli municipalities as well as a broader group of airlines, travel agencies, and journalists. Overall, since February 2024 we identified over 50 spear phishing emails targeting more than 10 sectors that were sent to hundreds of recipients.

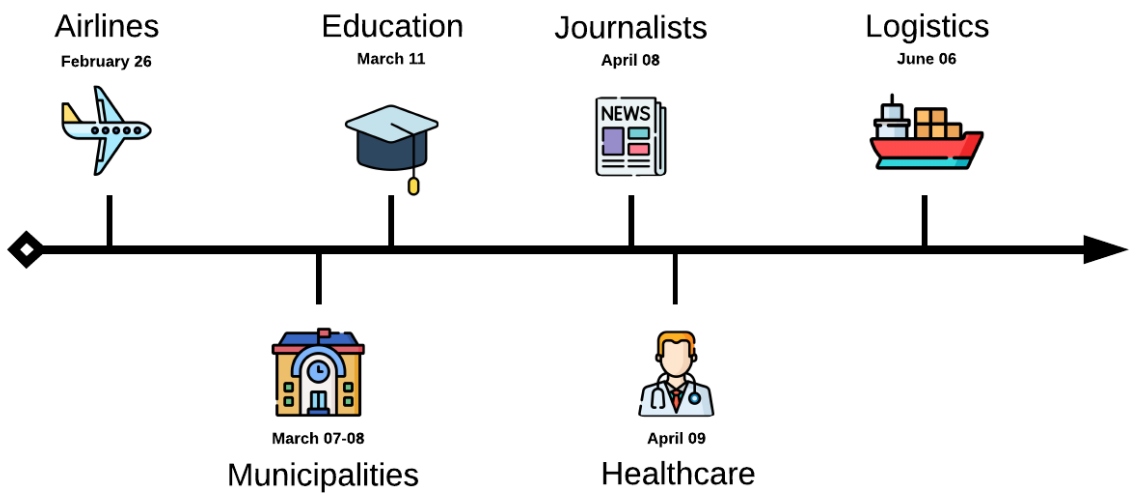


Figure 1 – Notable phishing campaigns.

In each of these campaigns, the actors used a tailored lure that was sent to dozens of targets in the same sector. For example, lures aimed at municipalities contained a suggestion to download a new app created just for municipalities:

Figure 2 – Lure email sent to municipalities in Israel.

> **Translated email:**
>
> > Subject: Special Offer: New App for Municipalities – Limited Time Only!
> >
> > Dear Customer, in celebration of International Mother's Day, we are excited to announce the launch of our latest municipal app. This innovative tool is meticulously designed to automate tasks, enhance efficiency, and ensure maximum safety in operations.
> >
> > For today only, we are offering this app as a free download. Empower your municipality to streamline workflows and securely prepare for future tasks. Download Now
> >
> > Take advantage of this opportunity to revolutionize your municipality's operations with our innovative solution. Don't miss out!
> >
> > Best regards, [Redacted]

In more recent campaigns, the group shifted to more generic-themed, yet well-crafted phishing lures, such as invitations to webinars and online courses. This approach allows them to reuse the same lure across different targets and regions. Additionally, while they primarily used the locally spoken languages of their targets, they now use the English language more frequently.

This shift is exemplified in two different emails that use the same exact lure: one sent to targets in Saudi Arabia and the other to Israel. The main differences were the email addresses used to send them, and the final payload. In Saudi Arabia it was an RMM, and in Israel, the custom backdoor BugSleep.

Comparison of two emails about online courses using the same lure:

Characteristics of email	Version 1	Version 2
From	A compromised email account of a Saudi Arabian company.	A compromised email account of an Israeli company.
To	Companies in Saudi Arabia.	Companies in Israel.
Link	Email includes a direct link to an Egnyte subdomain.	Email contains a PDF attachment with an embedded link.
Payload	Atera RMM tool.	BugSleep backdoor.

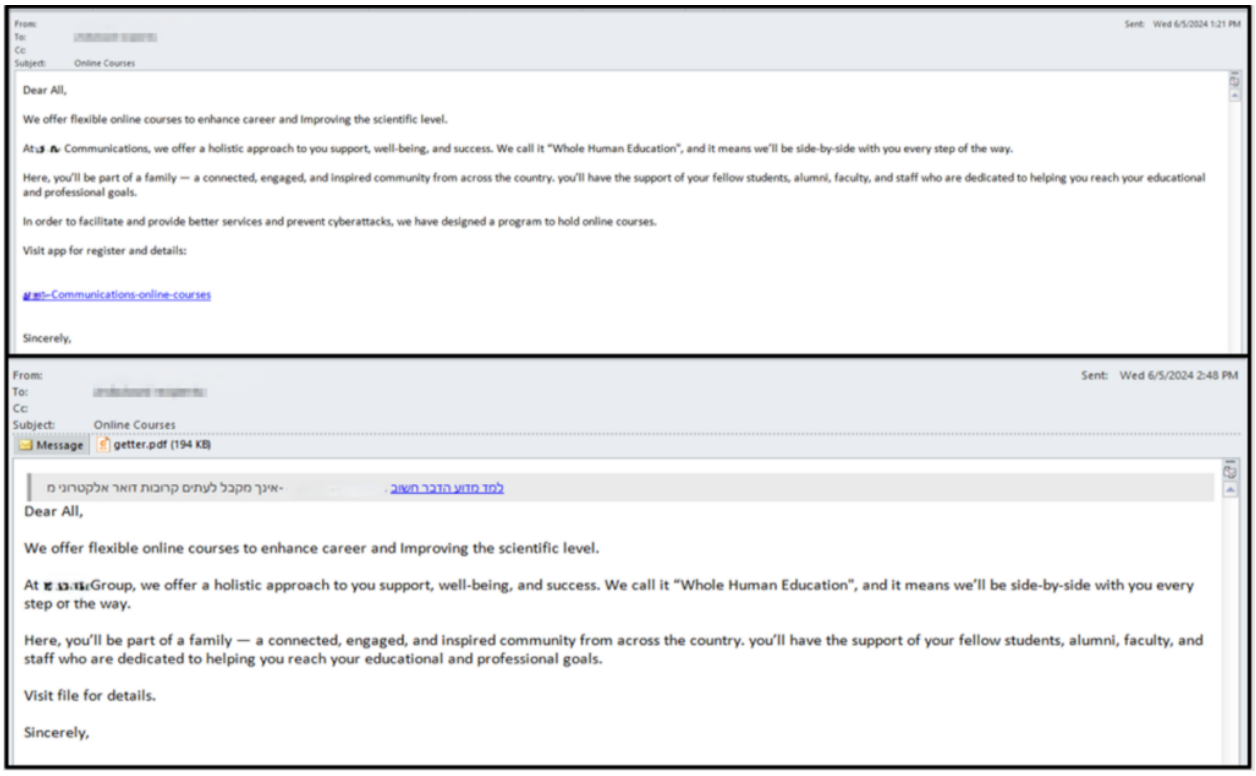


Figure 3 – Email comparison (version 1 on the top).

The only differences in the content between the two emails are the company name and the last two lines with the link that can be found in the PDF attachment.

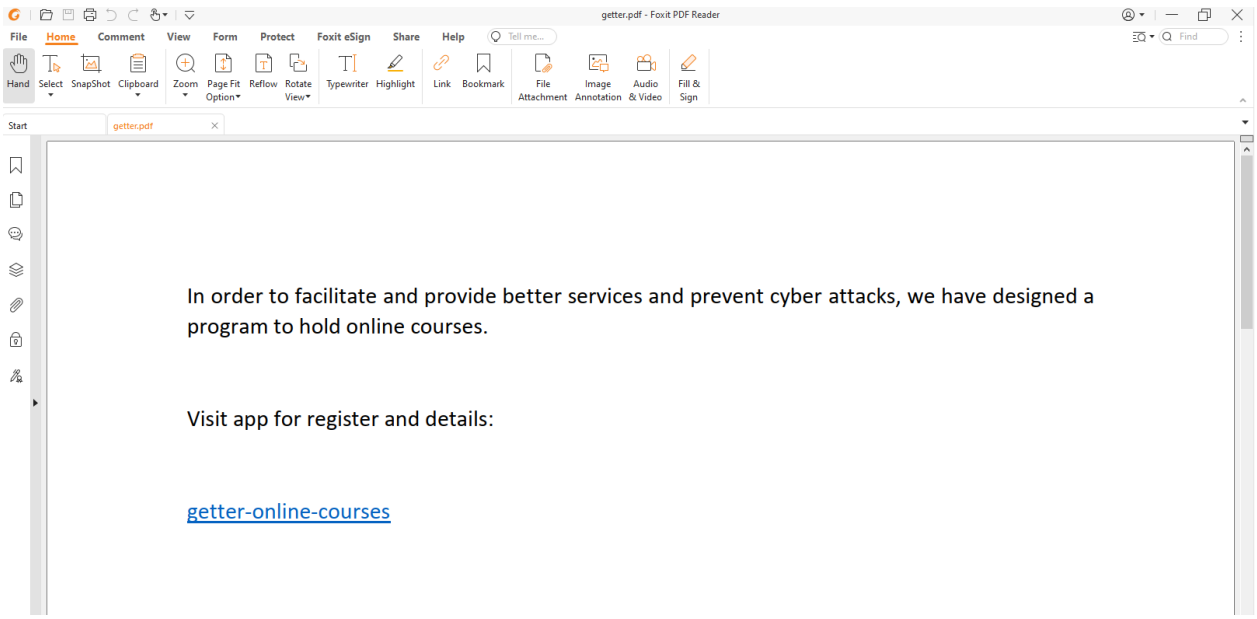


Figure 4 – PDF attachment of email version 2.

Attribution of these campaigns to MuddyWater is supported by the distinct patterns of behavior and RMM tools they employ, which have been consistently observed in their operations over the past few years.

BugSleep Infection Chain

The typical infection chain that delivers the BugSleep backdoor is as follows:

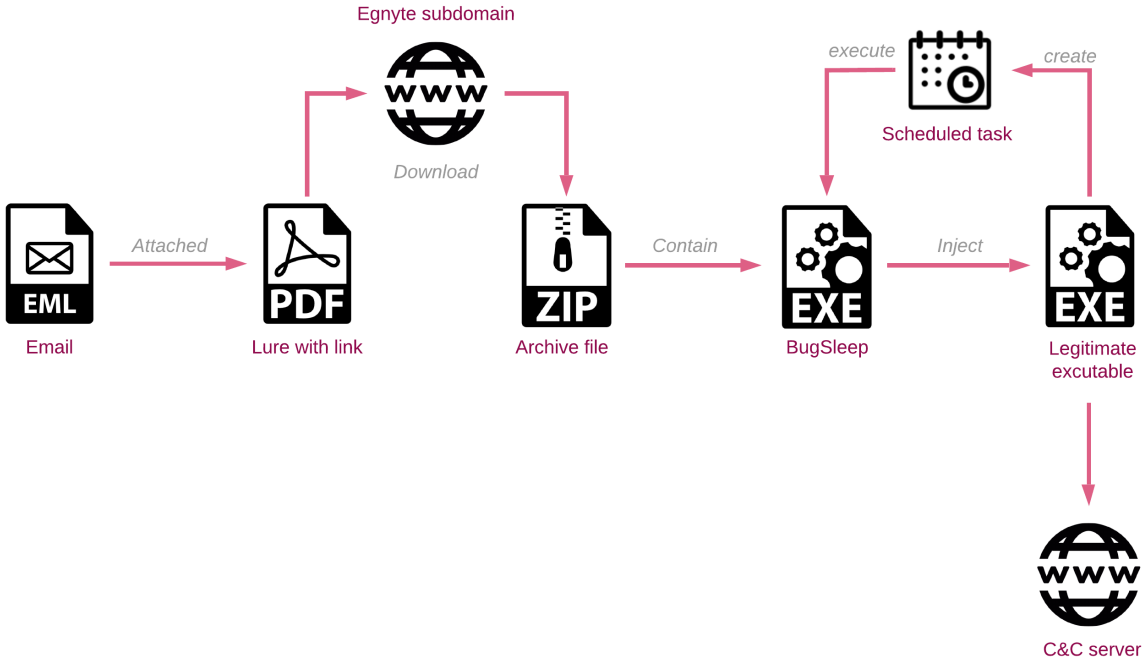


Figure 5 – MuddyWater new infection chain.

Egnyte Abuse

Egnyte is a secure file-sharing platform that allows employees and companies to easily share files via a web browser. Recently, MuddyWater has frequently used Egnyte subdomains, aligning them with the company names used in their phishing emails. Upon opening the shared link, recipients can see the name of the purported sender, which often appears legitimate, and matches the naming conventions of the targeted country.

In a link sent to a transportation company in Saudi Arabia, the displayed name of the owner was Khaled Mashal, the former head of Hamas and one of its prominent leaders.

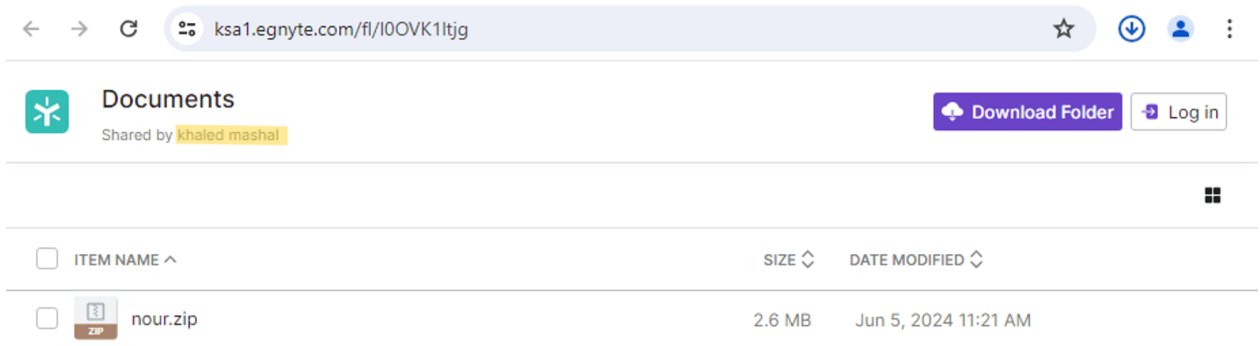


Figure 6 – Archive file shared by ‘Khaled Mashal’.

BugSleep Technical Analysis

BugSleep is a new tailor-made malware used in MuddyWater phishing lures since May 2024, partially replacing their use of legitimate RMM tools. We discovered several versions of the malware being distributed, with differences between each version showing improvements and bug fixes (and sometimes creating new bugs). These updates, occurring within short intervals between samples, suggest a trial-and-error approach.

BugSleep main logic is similar in all versions, starting with many calls to the `Sleep` API to evade sandboxes and then it loads the APIs it needs to run properly. It then creates a mutex (we observed `“PackageManager”` and `“DocumentUpdater”` in our samples) and decrypts its configuration which includes the C&C IP address and port. All the configurations and strings are encrypted in the same way, where every byte is subtracted with the same hardcoded value.

In most BugSleep samples, the malware then creates a scheduled task with the same name as the mutex and adds the comment `"sample comment”` to it. The scheduled task, which ensures persistence for BugSleep, runs the malware and is triggered every 30 minutes on a daily basis.

```
(Itask->lpVtbl->SetComment)(Itask, L"sample comment");
w_TaskName = to_multi_byte(TaskName);
ItaskVtbl = Itask->lpVtbl;
(ItaskVtbl->SetApplicationName)(Itask, w_TaskName);
(Itask->lpVtbl->SetWorkingDirectory)(Itask, L"C:\\Windows\\System32");
(Itask->lpVtbl->SetParameters)(Itask, &dword_140016478);
(Itask->lpVtbl->SetFlags)(Itask, 0x2000i64);
if ( (Itask->lpVtbl->SetAccountInformation)(Itask, AccountName, 0i64) < 0
  || (Itask->lpVtbl->CreateTrigger)(Itask, Trigger, &ppTrigger) < 0 )
{
  (Itask->lpVtbl->Release)(Itask);
  CoUninitialize();
  return 0i64;
}
else
{
  memzero_wrapper(&pTrigger, 48);
  v40.wYear = 16;
  memset(&v40.wMonth, 0, 0xEui64);
  lpSystemTime = &v40;
  GetLocalTime(&v40);
  pTrigger.wBeginDay = lpSystemTime->wDay;
  pTrigger.wBeginMonth = lpSystemTime->wMonth;
  pTrigger.wBeginYear = lpSystemTime->wYear;
  pTrigger.cbTriggerSize = 48;
  pTrigger.wStartHour = lpSystemTime->wHour;
  pTrigger.wStartMinute = lpSystemTime->wMinute + 1;
  pTrigger.MinutesDuration = 0x5A0;
  pTrigger.MinutesInterval = 30;
  pTrigger.TriggerType = TASK_TIME_TRIGGER_DAILY;
  pTrigger.Type.Daily.DaysInterval = 1;
  if ( (ppTrigger->lpVtbl->SetTrigger)(ppTrigger, &pTrigger) >= 0 )
```

Figure 7 – Scheduled task method of setting up persistence used by BugSleep.

The malware communication is also encrypted the same way as its strings, adding 3 to every byte modulo 256. Every message exchanged between BugSleep and its C&C domain follows this format: `[size_of_data][data]`.

BugSleep starts by sending the ID of the victim, consisting of the computer name followed by the username, formatted as `[computer_name][username]`.

The malware has several commands it can perform based on the data sent from the C&C:

# Of Command	Arguments	Description
1	File name	Send a file content to C&C.
2	File name	Write content into a file.
3	Command	Run commands through cmd pipe until the command ‘terminate’.
4	Timeout value	Update ‘receive timeout’ by adding the new timeout value.
6	–	Stop communication.
9	–	Delete the persistence task.
10	–	Get the status of the persistence task.
11	–	Create the persistence task.
97	Sleep time	Update sleep time (not found in the first version).
98	Timeout value	Update the receive timeout (not found in the first version).
99	–	Sends the same value back (type of ping).

Evasions

In one of the malware versions, the developers implemented a couple of evasion methods from EDR solutions. First, the malware enables the `MicrosoftSignedOnly` flag of the `ProcessSignaturePolicy` structure to prevent the process from loading images that are not signed by Microsoft. This prevents other processes from injecting DLLs into the process.

Next, it enables the `ProhibitDynamicCode` flag of the `ProcessDynamicCodePolicy` structure to prevent the process from generating dynamic code or modifying existing executable code. Enabling `ProcessDynamicCodePolicy` may be useful for protecting it from EDR solutions that hook userland API functions to inspect programs’ intents.

```
memset(&SignaturePolicy, 0, sizeof(SignaturePolicy));
GetProcessMitigationPolicy(hProcess, ProcessSignaturePolicy, &SignaturePolicy, 4i64);
SignaturePolicy.Flags |= 1;
SetProcessMitigationPolicy(ProcessSignaturePolicy, &SignaturePolicy, 4i64);
memset(&DynamicCodePolicy, 0, sizeof(DynamicCodePolicy));
GetProcessMitigationPolicy(hProcess, ProcessDynamicCodePolicy, &DynamicCodePolicy, 4i64);
DynamicCodePolicy.Flags |= 1;
return SetProcessMitigationPolicy(ProcessDynamicCodePolicy, &DynamicCodePolicy, 4i64);
```

Figure 8 – Evasions method.

BugSleep Loader

One of the samples we analyzed came with a custom loader. The loader injects a shellcode that loads BugSleep in-memory into one of the following processes, based on whether they are already running:

- msedge.exe
- opera.exe
- chrome.exe
- anydesk.exe
- Ondedrive.exe
- powershell.exe

The shellcode in this case is also encrypted with the same algorithm as the strings in BugSleep but with a different shift: every byte is subtracted with a hardcoded value of 6. After the decryption, the loader writes the shellcode inside the process with the `WriteProcessMemory` API and invokes the shellcode with the `CreateRemoteThread` API.

Bugs and Unused Code

Some of the samples contained several bugs, and parts of the code appear poorly written, with questionable omissions or additions that seem to be mistakes.

- One of the samples checks if the file `"C:\users\public\a.txt"` exists and if it doesn't, it creates the file which it later deletes. The purpose of this code is not entirely clear and may be unfinished code inserted by the authors or borrowed from other places without fully understanding what the code does.
- In one sample, some of the API names were not encrypted like the others, probably due to lack of attention.
- In some samples, instead of properly encrypting (adding 3 to each byte), the malware runs the decryption algorithm (subtracting each byte by 3), which is probably by mistake. In a newer sample, the malware authors fixed that bug but did not do the same for all of the commands. Another questionable action is that the malware decrypts the data after it's sent. We assume that their intent was to encrypt the strings again so they would not be seen in memory, but in this case, it does the opposite.

```
cur_size = 0;
if ( !data )
  return 0xFFFFFFFFi64;
for ( i = 0; i < overall_size; ++i )
  data[i] -= enc_key;
while ( overall_size > cur_size )
{
  send_size = send(sock, &data[cur_size], overall_size - cur_size, 0);
  if ( send_size == -1 )
    return 0xFFFFFFFFi64;
  cur_size += send_size;
  if ( ++tries == 10 )
  {
    tries = 0;
    return 0xFFFFFFFFi64;
  }
}
for ( j = 0; j < overall_size; ++j )
  data[j] += enc_key;
tries = 0;
return 1i64;
```

Figure 9 – Encryption/Decryption confusion in the send method.

Targets

According to our telemetry, these MuddyWater campaigns target a diverse array of sectors, ranging from government entities and municipalities to media outlets and travel agencies. While the majority of the emails was directed at companies in Israel, others were aimed at entities in Turkey, Saudi Arabia, India and Portugal.

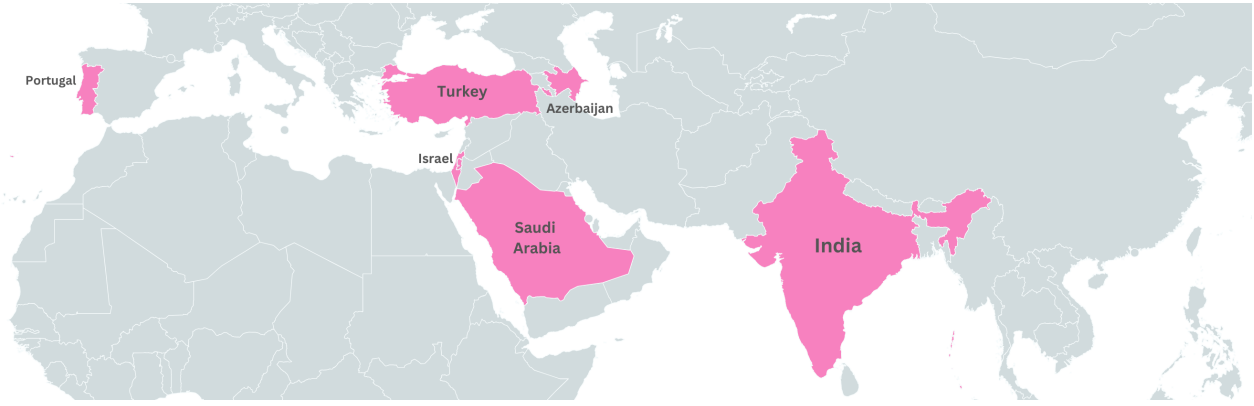


Figure 10 – Map of targeted countries.

In addition, files associated with the latest campaign were uploaded to VirusTotal from various IP locations, including Azerbaijan and Jordan. Notably, in the case of Azerbaijan, we can establish correlation with the target due to the Azerbaijani language used in the PDF lure.


Əziz dostlar və həmkarlar

CASPEL beynəlxalq şirkəti informasiya texnologiyaları və şəbəkə həlləri üzrə onlayn vebinar təşkil edir.

Bu beynəlxalq vebinarın keçirilməsində məqsəd hər hansı kiber vandalizmin qarşısını almaq və Afrika və Yaxın Şərqdəki informasiya texnologiyaları şirkətləri ilə dərin əlaqələr qurmaqdır.

Bu seminarda regionun bir çox nüfuzlu şirkətləri iştirak edəcək və bu sahədə bir çox ekspertlər müzakirə və fikir mübadiləsi aparacaqlar.

Bu sahədə olan bütün dostlar və şirkətlər bu vebinarda iştirak etməyə dəvət olunur.

Bu vebinarda iştirak etmək üçün aşağıdakı linkə daxil olun və vebinar proqramını yükləyin.

CASPEL-vebinar

təşəkkürlər

Figure 11 – PDF lure written in Azerbaijani.

Translated PDF document:

> Dear friends and colleagues
> International company CASPEL organizes an online webinar on information technologies and network solutions.
> The purpose of this international webinar is to prevent any cyber vandalism and build deep relationship with information technology companies in Africa and the Middle East.
> Many reputable companies of the region will participate in this seminar, and any experts in this field will discuss and exchange ideas.
> To participate in the webinar, visit the link below and download the webinar software.
>
> [Link]
>
> Thank you.

Conclusion

The increased activity of MuddyWater in the Middle East, particularly in Israel, highlights the persistent nature of these threat actors, who continue to operate against a wide variety of targets in the region. Their consistent use of phishing campaigns, now incorporating a

custom backdoor, BugSleep, marks a notable development in their techniques, tactics and procedures (TTPs).

The campaigns reflect the group's interests, focusing on specific sectors such as municipalities, airlines, travel agencies, and media outlets. Although they are aimed at specific sectors, the nature of the lures themselves have become much simpler over time. The shift from highly customized lures to more generic themes such as webinars and online courses, combined with the increased use of the English language, allows the group to focus on higher volume rather than specific targets.

Check Point Customers Remain Protected Against the Threats Described in this Report.

Harmony Email and Collaboration provides comprehensive inline protection at the highest security level.

Threat Emulation signatures:

APT.Wins.MuddyWater.ta.X

APT.Wins.MuddyWater.ta.Y

APT.Win.MuddyWater.X

Harmony Endpoint signatures:

APT.Win.MuddyWater.U

APT.Win.MuddyWater.V

APT.Win.MuddyWater.W

IOCs

Domains:

kinneretacil.egnyte[.]com
salary.egnyte[.]com
gcare.egnyte[.]com
rimonnet.egnyte[.]com
alltrans.egnyte[.]com
megolan.egnyte[.]com
bgu.egnyte[.]com
fbcsoft.egnyte[.]com
cnsmportal.egnyte[.]com
alkan.egnyte[.]com
getter.egnyte[.]com
ksa1.egnyte[.]com
filecloud.egnyte[.]com
nour.egnyte[.]com
airpazfly.egnyte[.]com
cairoairport.egnyte[.]com
silbermintz1.egnyte[.]com
smartcloudcompany[.]com
onlinemailerservices[.]com
smtpcloudapp[.]com
softwarehosts[.]com
airpaz.egnyte[.]com
airpazflys.egnyte[.]com
fileuploadcloud.egnyte[.]com
downloadfile.egnyte[.]com

URLs:

https://shorturl[.]at/NCxJk
https://shorturl[.]at/bYqUx
https://ws.onehub[.]com/files/bbmiio1c
https://ws.onehub[.]com/files/zgov9aqy

IP addresses:

C&C:

146.19.143[.]14
91.235.234[.]202
85.239.61[.]97

Other:

95.164.32[.]69
5.252.23[.]52
194.4.50[.]133
193.109.120[.]59

IP address used for sending emails:

89.221.225[.]81
45.150.108[.]198
200.200.200[.]248
169.150.227[.]230
169.150.227[.]205
185.248.85[.]20
141.98.252[.]143
31.171.154[.]54
146.70.172[.]227
198.54.131[.]36

Hashes:

BugSleep:

73c677dd3b264e7eb80e26e78ac9df1dba30915b5ce3b1bc1c83db52b9c6b30e
960d4c9e79e751be6cad470e4f8e1d3a2b11f76f47597df8619ae41c96ba5809
b8703744744555ad841f922995cef5dbca11da22565195d05529f5f9095fbfca
94278fa01900fdbfb58d2e373895c045c69c01915edc5349cd6f3e5b7130c472
5df724c220aed7b4878a2a557502a5cefee736406e25ca48ca11a70608f3a1c0

RMM MSI:

39da7cc7c627ea4c46f75bcec79e5669236e6b43657dcad099e1b9214527670e
c23f17b92b13464a570f737a86c0960d5106868aaa5eac2f2bac573c3314eb0f
fb58c54a6d0ed24e85b213f0c487f8df05e421d7b07bd2bece3a925a855be93a
7e6b04e17ae273700cef4dc08349af949dbd4d3418159d607529ae31285e18f7
ff2ae62ba88e7068fa142bbe67d7b9398e8ae737a43cf36ace1fcf809776c909
e2810cca5d4b74e0fe04591743e67da483a053a8b06f3ef4a41bdabee9c48cf7
90f94d98386c179a1b98a1f082b0c7487b22403d8d5eb3db6828725d14392ded
20aaeac4dbea89b50d011e9becdf51afc1a1a1f254a5f494b80c108fd3c7f61a
55af6a90ac8863f27b3fcaa416a0f1e4ff02fb42aa46a7274c6b76aa000aacc2
f925d929602c9bae0a879bb54b08f5f387d908d4766506c880c5d29986320cf9

Archives:

424a9c85f97aa1aece9480bd658266c366a60ff1d62c31b87ddc15a1913c10e4
c80c8dd7be3ccf18e327355b880afb5a24d5a0596939458fb13319e05c4d43e9
c88453178f5f6aaab0cab2e126b0db27b25a5cfe6905914cc430f6f100b7675c
31591fcf677a2da2834d2cc99a00ab500918b53900318f6b19ea708eba2b38ab
a0968e820bbc5e099efd55143028b1997fd728d923c19af03a1ccec34ce73d9b
88788208316a6cf4025dbabbef703f51d77d475dc735bf826b8d4a13bbd6a3ee
4064e4bb9a42549480478583012b75e276a878321b0cc02710e1738b42548ca
e7896ccb82ae35e1ee5949b187839faab0b51221d510b25882bbe711e57c16d2
1c0947258ddb608c879333c941f0738a7f279bc14630f2c8877b82b8046acf91
8fbd374d4659efdc5b5a57ff4168236aeaab6dae4af6b92d99ac28e05f04e5c1
7e14ca8cb7980e85aff4038f489442eace33530fd02e2b9c382a4b6907601bee
02060a9ea0d0709e478e2fba6e9b71c1b7315356acc4f64e40802185c4f42f1c
53b4a4359757e7f4e83929fba459677e76340cbec7e2e1588bbf70a4df7b0e97
0ab2b0a2c46d14593fe900e7c9ce5370c9cfbf6927c8adb5812c797a25b7f955

GO UP
BACK TO ALL POSTS