

MuddyWater eN-Able spear-phishing with new TTPs

[Learn more](#)

Executive summary:

- Deep Instinct’s Threat Research team has identified a new campaign from the “MuddyWater” group
- The campaign has been observed attacking two Israeli targets
- The campaign exhibits updated TTPs to previously reported MuddyWater activity

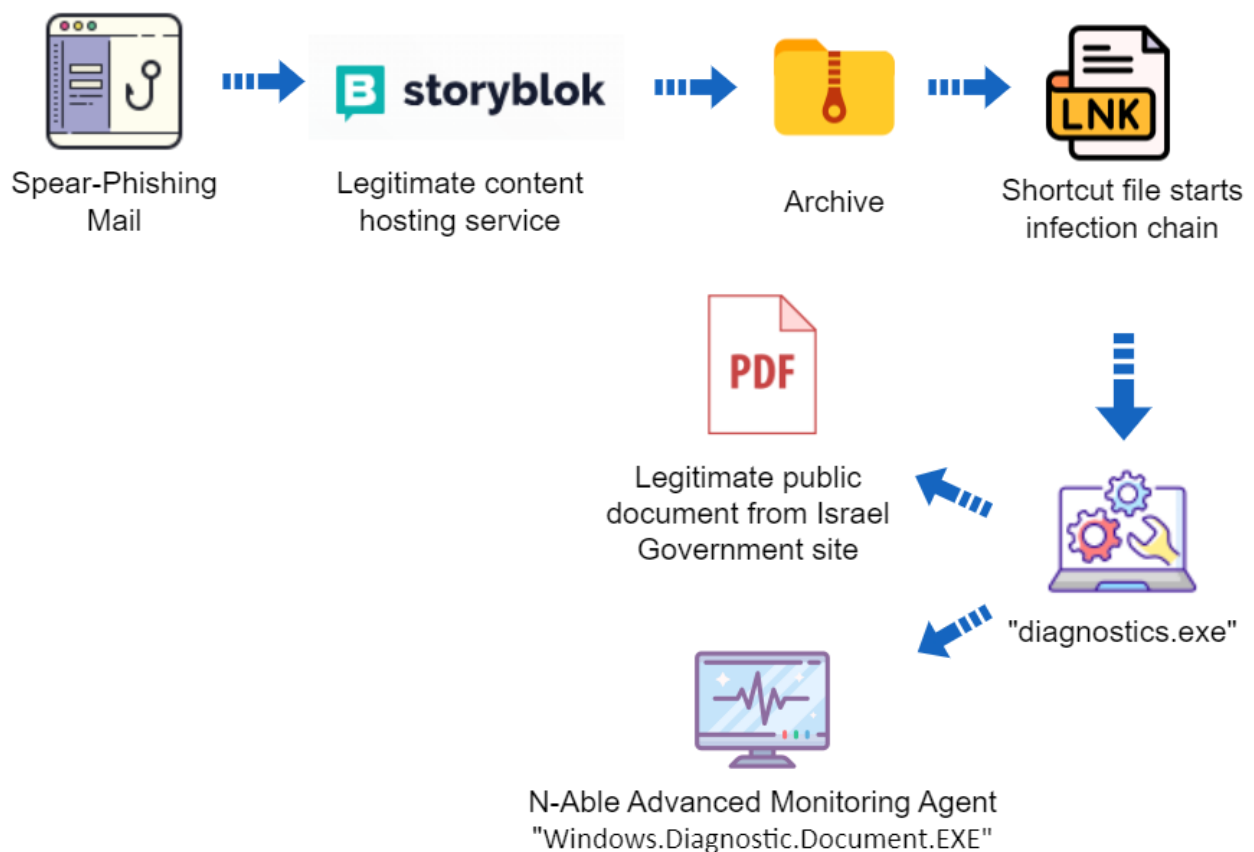


Figure 1: Campaign overview

Introduction

Previous research showed that MuddyWater has sent spear-phishing emails, starting back in 2020, with direct links, as well as PDF, RTF, and HTML attachments containing links to archives hosted on various file-sharing platforms.

Those archives contained installers for various legitimate remote administration tools.

Before launching the new campaign during the Israel-Hamas war, MuddyWater reused previously known remote administration tools, utilizing a new file-sharing service called “Storyblok.”

On October 30th Deep Instinct identified two archives hosted on “Storyblok” containing a new multi-stage infection vector. It contains hidden files, an LNK file that initiates the infection, and an executable file designed to unhide a decoy document while executing Advanced Monitoring Agent, a remote administration tool.

This is the first public report about MuddyWater utilizing this remote administration tool.

The Multi-stage Social Engineering Campaign

While Deep Instinct could not verify the spreading mechanism of the new campaign, it most likely starts with a spear-phishing email, similar to previous campaigns.

The content of the email lures the victim into downloading an archive hosted at “a.storyblok[.]com”

In this analysis, we examine the “defense-video.zip” file.

When the archive is extracted, several folders must be navigated until a LNK shortcut, which looks like another folder named “Attachments,” is found:

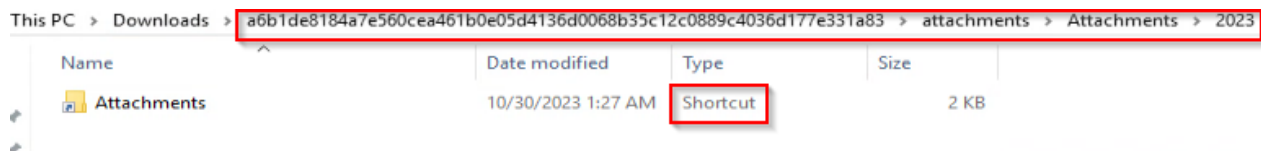


Figure 2: LNK Shortcut

However, there are additional hidden folders and files extracted from the archive:



Figure 3: Hidden folders

When the victim opens the LNK file, the infection chain starts.

By examining the LNK file, we can see that it executes an executable from one of the hidden directories:

```
stinson@kali:~/Downloads/devol/a6b1de8184a7e560cea461b0e05d4136d0068b35c12c0889c4036d177e331a83 (1)/attachments/Attachments/2023$ exiftool Attachments.Lnk
ExifTool Version Number      : 12.42
File Name                    : Attachments.Lnk
Directory                   :
File Size                    : 1352 bytes
File Modification Date/Time  : 2023:10:30 01:27:40+02:00
File Access Date/Time       : 0000:00:00 00:00:00
File Inode change Date/Time  : 2023:10:31 11:25:41+02:00
File Permissions             : -rw-rw-r--
File Type                    : LNK
File Type Extension         : lnk
MIME Type                    : application/octet-stream
Flags                        : IDList, RelativePath, CommandArgs, IconFile, Unicode
File Attributes              : (none)
Target File Size             : 0
Icon Index                   : 4
Run Window                   : Show Minimized No Activate
Hot Key                      : Control-Alt-R
Target File DOS Name         : conhost.exe
Relative Path                 : ..\..\..\..\..\Windows\System32\conhost.exe
Command Line Arguments       : --headless "Windows.Diagnostic.Document\Diagnostic.exe"
```

Figure 4: LNK command line arguments

The file “Diagnostic.exe” has been used in both archives Deep Instinct observed. The purpose of this file is to execute another executable called “Windows.Diagnostic.Document.EXE,” which is located in the hidden directory named “.end” under a “Windows.Diagnostic.Document” hidden directory.

The file named “Windows.Diagnostic.Document.EXE” is a signed, legitimate installer for “Advanced Monitoring Agent.”

In addition to executing the remote administration tool, “Diagnostic.exe” also opens a new Windows Explorer window of the hidden “Document” folder. This is done to fool the victim that opened the LNK file into thinking that it was indeed a folder.

The decoy document is an official memo from the Israeli Civil Service Commission, which can be publicly downloaded from their [website](#).

The memo describes what to do in case a government worker expresses opinions against the Israeli state on social networks:



כ"ו בתשרי תשפ"ד
11 באוקטובר 2023

סימוכין:
0491-0013-2023-031170

לכבוד
מנכ"לים במשרדי הממשלה וביחידות הסמך
מנכ"לים בתאגידים הסטטוטוריים
מנהלי בתי החולים הממשלתיים

שלום רב,

הנדון: טיפול משמעתי בהתבטאויות כנגד מדינת ישראל בעת מלחמה

- 1) בימים אלו נמצאת מדינת ישראל במלחמה מול ארגון הטרור חמאס לאחר שטרוריסטים פעילי החמאס חדרו לישראל וביצעו מעשי טרור אכזריים ביישובי הדרום.
- 2) על רקע מצב מלחמה זה אנו נתקלים במקרים בודדים של התבטאויות פסולות של עובדי מדינה ברשתות החברתיות אשר הביעו תמיכה בפעולות הטרור הנפשעות הללו וכנגד מדינת ישראל.
- 3) כידוע, על עובדי מדינה חלות מגבלות שונות, לרבות בכל הנוגע לאופן התבטאותם. הגבלות אלו חלות גם על התבטאויות במסגרת הפרטית וברשתות החברתיות¹.
- 4) התבטאויות מסוג זה של עובדי מדינה ושל עובדי הגופים הכפופים לחוק שירות המדינה (משמע), תשכ"ג – 1963 מהוות לכאורה עבירת משמעת חמורה, במיוחד במצב מלחמה בו אנו מצויים כיום, והן מחייבות טיפול משמעתי תקיף ומהיר.
- 5) לפיכך, בכל מקרה בו הנכם נתקלים בהתבטאויות מסוג זה, בין במקום העבודה ובין מחוצה לו, יש לפנות אלינו באופן מיידי לקבלת הנחיות לרבות לקידום השעיה דחופה, חקירה, העמדה לדין ובחינת פיטורים.

Figure 5: Decoy document

Conclusion

MuddyWater continues to attack Israeli targets in various ongoing campaigns.

In this campaign, MuddyWater employs updated TTPs. These include a new public hosting service, employing a LNK file to initiate the infection, and utilizing intermediate malware that mimics the opening of a directory while executing a new remote administration tool.

After the victim has been infected, the MuddyWater operator will connect to the infected host using the legitimate remote administration tool and will start doing reconnaissance on the target.

After the reconnaissance phase, the operator will likely execute PowerShell code which will cause the infected host to beacon to a custom C2 server.

MuddyWater has used PhonyC2 in the past. However, Deep Instinct recently observed MuddyWater using a new C2 framework named MuddyC2Go – a detailed blog will be published soon, stay tuned.

IOCs:

File

| MD5 | Description |
|----------------------------------|-------------------------------------|
| 37c3f5b3c814e2c014abc1210e8e69a2 | Archive containing Atera Agent |
| 16923d827a440161217fb66a04e8b40a | Atera Agent Installer |
| 7568062ad4b22963f3930205d1a14df7 | Archive containing Atera Agent |
| 39eea24572c14910b67242a16e24b768 | Archive containing Atera Agent |
| 2e09e53135376258a03b7d793706b70f | Atera Agent Installer |
| 1f0b9aed4b2c8d958a9b396852a62c9d | Archive containing SimpleHelp |
| 065f0871b6025b8e61f35a188bca1d5c | SimpleHelp Installer |
| 146cc3a1a68be349e70b79f9115c496b | defense-video.zip |
| dd247ccd7cc3a13e1c72bb01cf3a816d | Attachments.Ink |
| 8d2199fa11c6a8d95c1c2b4add70373a | Diagnostic.exe |
| 04afff1465a223a806774104b652a4f0 | Advanced Monitoring Agent Installer |

| MD5 | Description |
|----------------------------------|------------------------------------|
| 6167f03c8b2734c20eb02d406d3ba651 | Decoy Document (defense-video.zip) |
| e8f3ecc0456fcbbb029b1c27dc1faad0 | attachments.zip |
| 952cc4e278051e349e870aa80babc755 | Decoy Document (attachments.zip) |

Network

| IP or URL | Description |
|---|---|
| ws.onehub[.]com/files/7f9dxtt6 | URL to Archive of Atera Agent |
| a.storyblok[.]com/f/253959/x/b92ea48421/form.zip | URL to Archive of Atera Agent |
| a.storyblok[.]com/f/255988/x/5e0186f61d/questionnaire.zip | URL to Archive of Atera Agent |
| a.storyblok[.]com/f/259791/x/94f59e378f/questionnaire.zip | URL to Archive of SimpleHelp |
| 146.70.149[.]61 | MuddyWater's SimpleHelp server |
| 146.70.124[.]102 | <u>Suspected MuddyWater's SimpleHelp server</u> |
| 37.120.237[.]204 | Suspected MuddyWater's SimpleHelp server |
| 37.120.237[.]248 | Suspected MuddyWater's SimpleHelp server |
| a.storyblok[.]com/f/259837/x/21e6a04837/defense-video.zip | URL to Archive of Advanced Monitoring Agent |

IP or URL**Description**

a.storyblok[.]com/f/259791/x/91e2f5fa2f/attachments.zip

URL to Archive of Advanced Monitoring Agent

Additional IOCs regarding MuddyWater can be found in our GitHub page:

<https://github.com/deepinstinct/Israel-Cyber-Warfare-Threat-Actors>

[Back To Blog](#)