Malware Analysis - Lumma Stealer

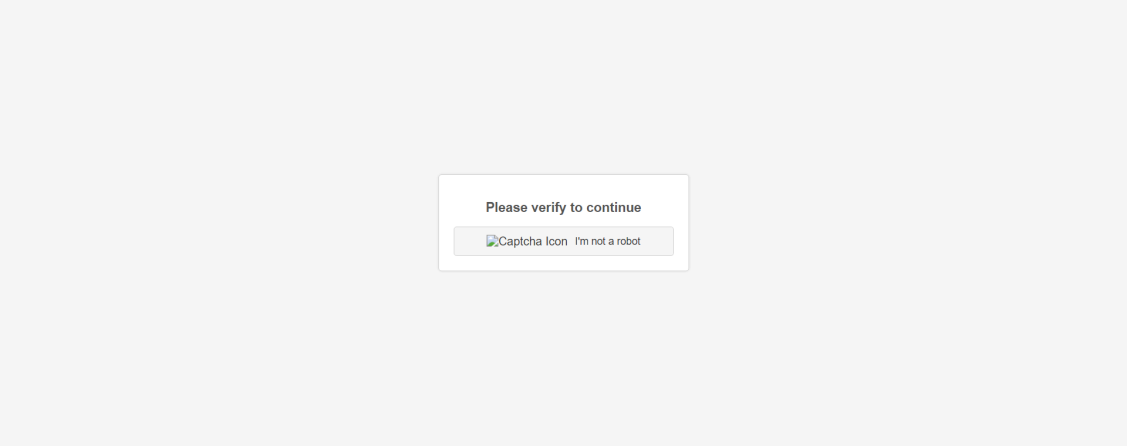
By Mandar Naik

Published: 2024-10-04 · Archived: 2026-04-05 21:13:38 UTC

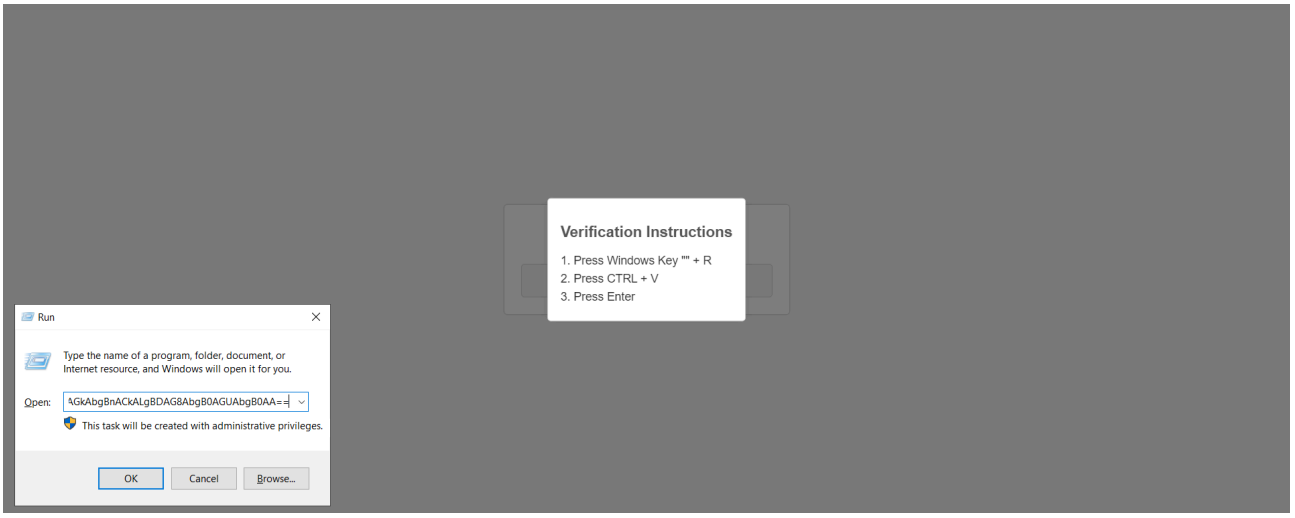
In this post, we will analyze malware and reverse engineer a sample called **lumma stealer**.

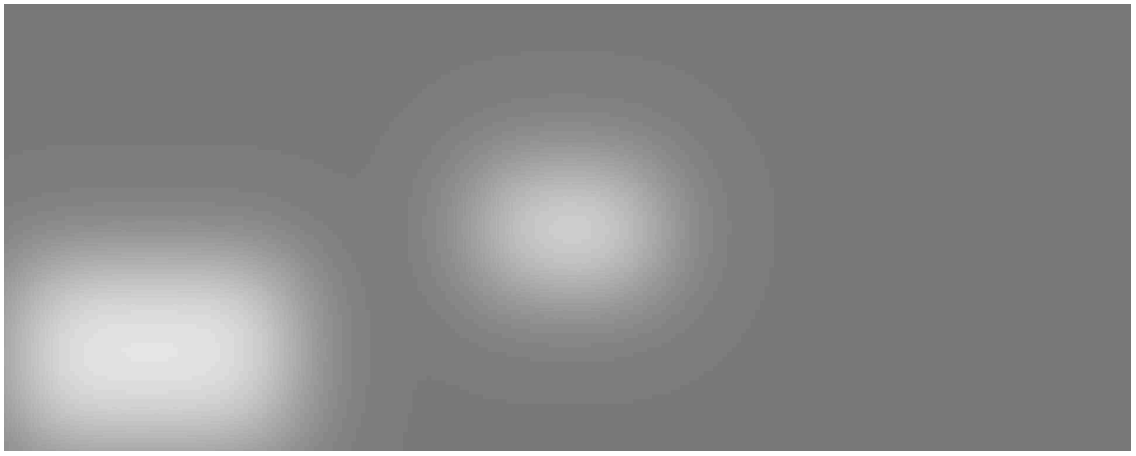
A web-based attack vector has a captcha page that asks the users to perform the task for verification.

The user is presented with a captcha page as shown below,

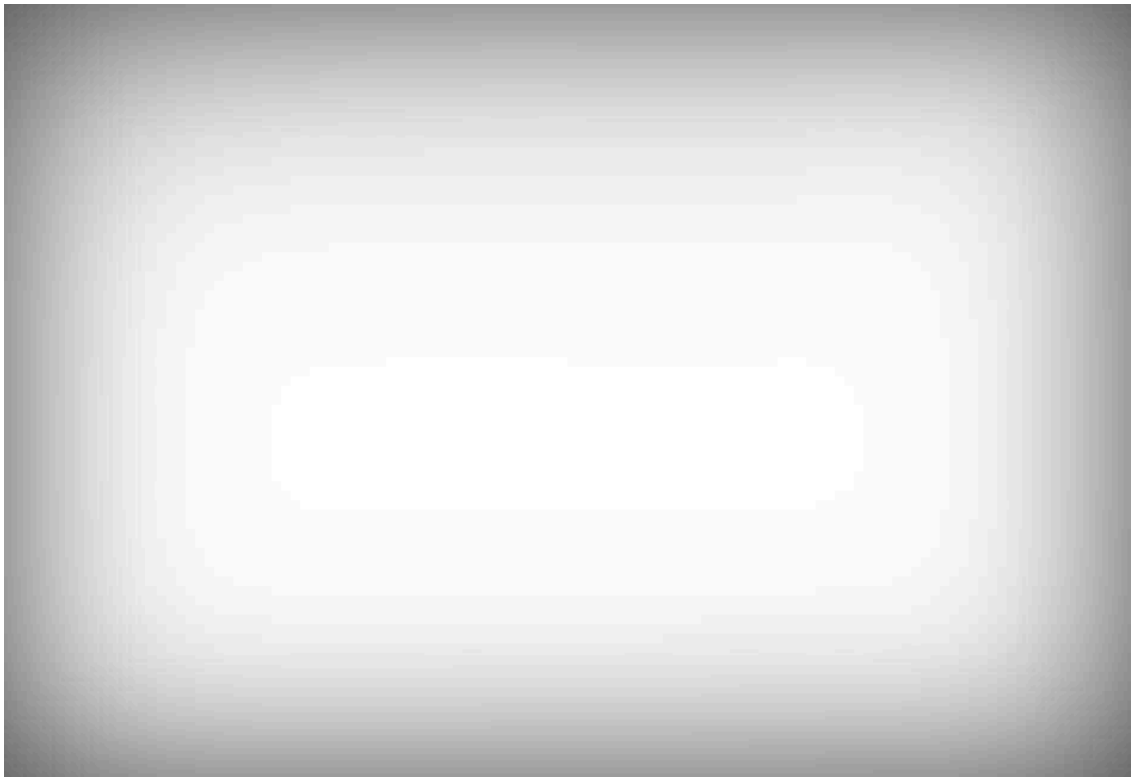


On a legitimate page, the user will be asked to select some boxes that contain this or that object, but here the users are asked to run a PowerShell script for verification that is **automatically copied to the system clipboard** once the user clicks on “I am not a robot” as shown below,





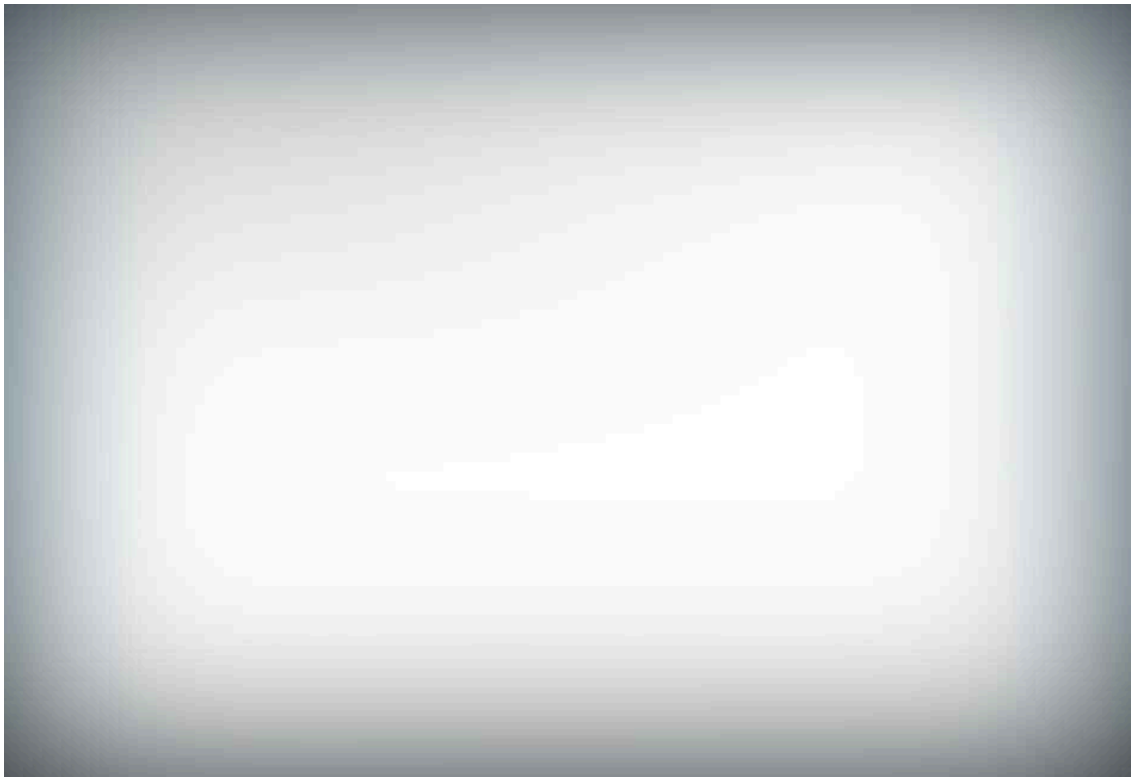
We will use the automatically copied PowerShell script for investigation, the script contains a base64 encoded text being executed with a hidden window.



After decoding the base64 text we get the following data, The decoded text contains another PowerShell command to execute the content of a file called *a.txt* stored at a remote location.

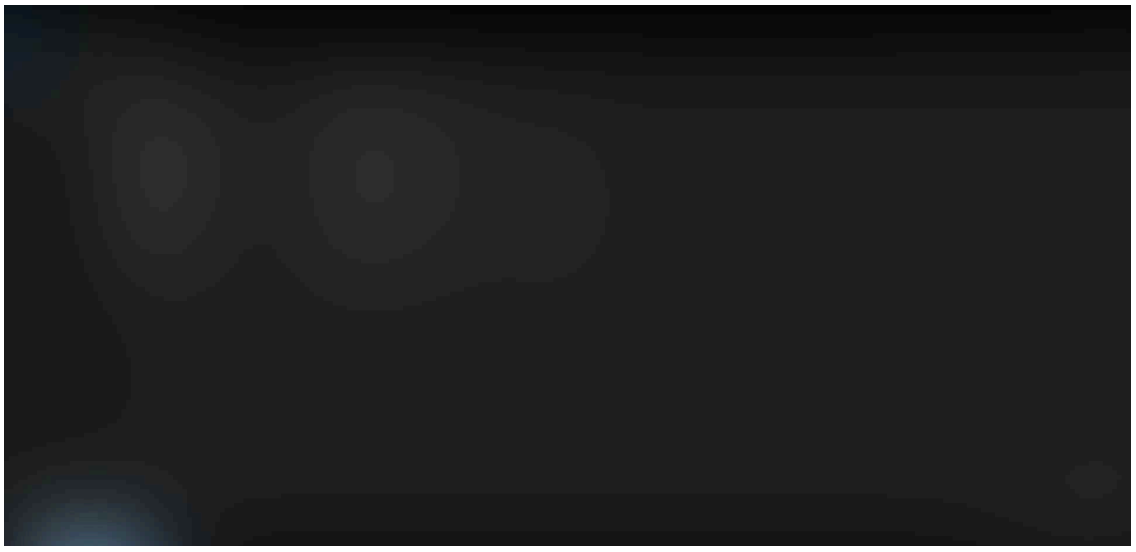
We download the *a.txt* file for further examination.

The *a.txt* contains,



The file in turn contains another PowerShell command that downloads the file called *malt.zip* from a remote location and stores that file with a different name *pg1.zip* in a temp location, it then extracts the *pg1.zip* content into the folder called *file* then executes the *set-up.exe* from that path.

After unzipping *malt.zip* the directory content is,



The interesting thing to note, the file *set-up.exe* has a resemblance to the **Iobit uninstaller**. A normal user would see the copyright of the file to be Iobit and might consider the file as Legitimate.

Apart from *set-up.exe*, we do not find any executable in the directory but after we check the file type of every file we can see that most of the files with *.bpl* extension are executable.

We ran floss on *madbasic_.bpl*, *maddisAsm_.bpl*, *madexcept_.bpl* and *Set-up.exe*,

The strings inside *madbasic_.bpl* seems pretty interesting they include text like Encrypt, Decrypt, Encode, and Decode.

The file *maddisAsm_.bpl* has a reference to the previous file *madbasic_.bpl*.

The file *madexcept_.bpl* contains text like HTTP account, password, SMTP account, password, etc.

At last, the *Set-up.exe* contains text like sending mail, sending attachments, etc.

Let’s do a dynamic analysis to get more insight.

After we execute the file we use **procom** to get the activity performed by *Set-up.exe* file.

The file did perform a lot of activity but the most interesting are **CreateFile**, **WriteFile**, and **CreateProcess**.

The process tree gave us more insight i.e. the *Set-up.exe* file created a subprocess called *more.com* which executes from the SYSWOW64 folder in turn creating two subprocesses of *conhost.exe* and *Launcher.exe* executing from the AppData folder.

We use x32Dbg for debugging the *Set-up.exe* file. We set the following breakpoints which we got from the file activity in procmon.

We hit an interesting CreateFile breakpoint,

It created a file called *pla.dll* in the SYSWOW64 folder.

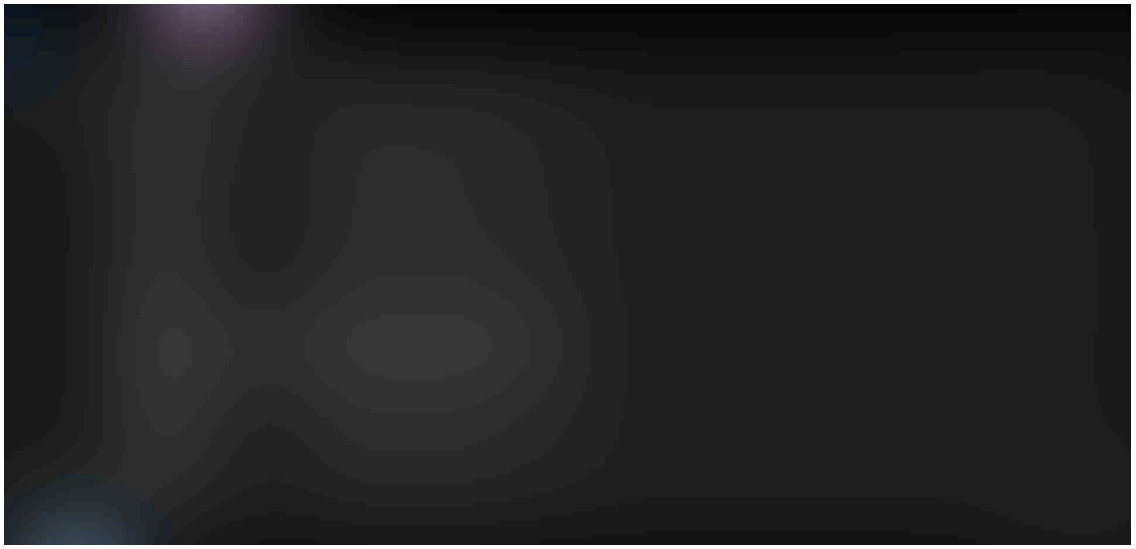
Simultaneously it also created the *Launcher.exe* in the AppData folder.

We hit another breakpoint of CreateProcess, it is creating a process of *IUservice* from the roaming folder,

Unfortunately, we do not see any executable in that folder, although it copied itself in that folder for **persistence**.

Another breakpoint of CreateProcess was hit, it is creating a process of *more.com* from the SYSWOW64 folder,

We can also see *more.com* in the SYSWOW64 folder.



In parallel we were also monitoring the network connections, The *Set-up.exe* tried to communicate with the following URL,

```
 hittybanndwk[.]shop
racedsuitreow[.]shop
defenddsouneuw[.]shop
deallyharvenw[.]shop
priooozekw[.]shop
pumpkinkwquo[.]shop
abortinoiwiam[.]shop
surroundeocw[.]shop
covvercilverow[.]shop
steamcommunity[.]com
```

IOCs

1. IPs

```
 165[.]227[.]121[.]41
```

2. URLs

```
 downcheck[.]nyc3[.]cdn[.]digitaloceanspaces[.]com
hittybanndwk[.]shop
racedsuitreow[.]shop
defenddsouneuw[.]shop
deallyharvenw[.]shop
priooozekw[.]shop
pumpkinkwquo[.]shop
abortinoiwiam[.]shop
surroundeocw[.]shop
covvercilverow[.]shop
steamcommunity[.]com
```

3. Hashes

```
 36a942a4e3308d47dfecbce2cd9c85ed316f877dbb85706f413cddcf04960a56
36c0dba42123f1bda46e4526af9a6fe2ceca755470703a45e90d5c0515c0044c
038511fc64801be03d8472a2f7a6ba8a27e0398cf876be1427c1463cf9190c80
11e3568f497c40331ee4a9e9973967e61b224e19204e09ed7451da3b74bd2ff5
fb64a5954b726d2d0f0bc26113a36dc8a86c469af994ceeaf2e2609743a0a557
80ae800e8b3a8091249d7e8b25a81788a3fe1ab5ece122bf0bd7ac458bc2f315
11d0f55c105883d203137a87a610ba793299dc4774fd6d8b3a86666a2c337041
6b2174db9f76580e59ff9fa91247491ce3da49172afe415ff8deb2a3fc7b97dc
d5a6714ab95caa92ef1a712465a44c1827122b971bdb28ffa33221e07651d6f7
```

```
a65d00beae117d1421b28ec9e6fe03893586eb7c96cd2089644901088129e24f
ccccadde7393f1b624cde32b38274e60bbe65b1769d614d129babdaeef9a6715
d4e5b7223d06cd464df898c6cf569ca00743e5e79e64009056602b09927d9bfe
95c8afbac49a7554453bfe509b11919a4e25742f292a11bac0ac467ec78b517a
92a918a88da8b8413381acad73ac093162d5237eedb1ef41c7c5aa604d3206ed
c3f6f6f1c310d0d61c2d07950fb2bd23d2b8a979e52d94cb623435aaed30ec60
fe65540f70c1a4c7d9625f8dc8f81fc47bacd0ffb65cb4b147e20b27a7d5d709
c2a5838937954785565 73db3a020ee607fabe7e37473d094d825f96c4912c43d
118de01fb498e81eab4ade980a621af43b52265a9fcbae5dedc492cdf8889f35
```

Source: https://mandarnaik016.in/blog/2024-10-05-malware-analysis-lumma-stealer/