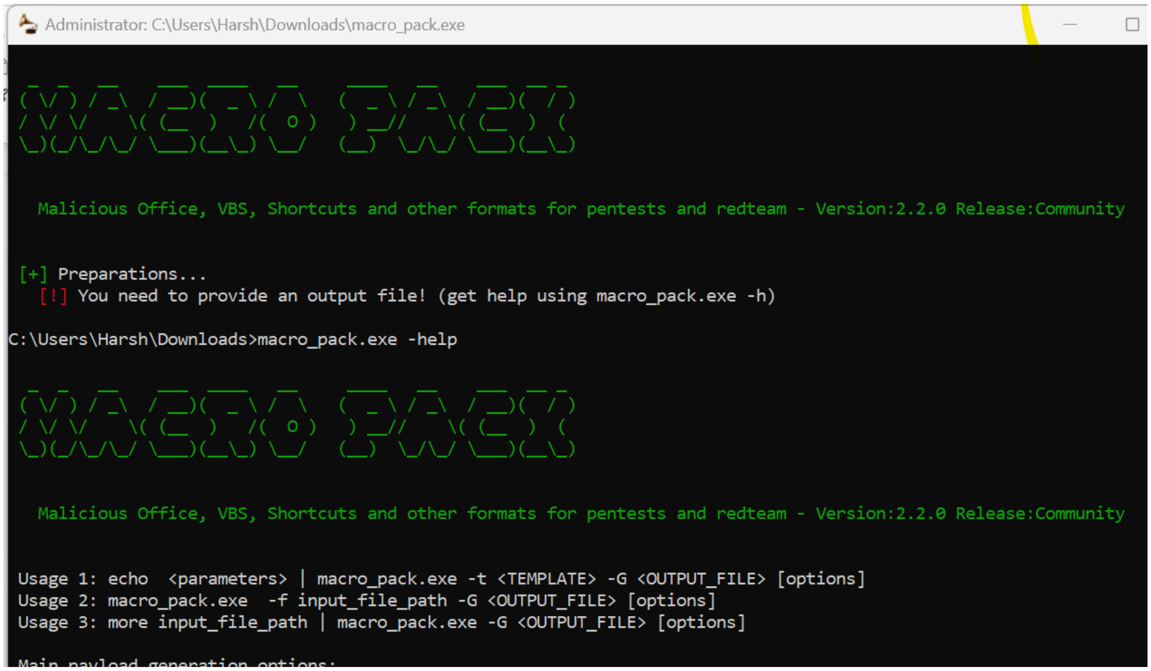
Execrise -3

Macropack:

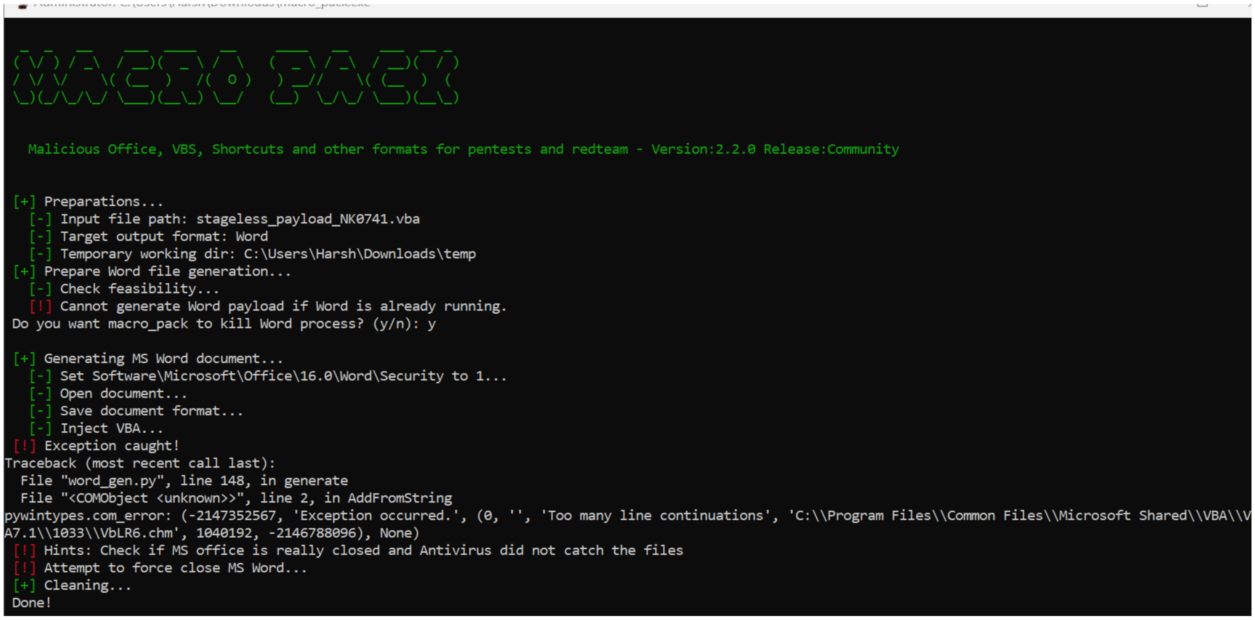
Installing the macropack:



Administrator: C:\Users\Harsh\Downloads\macro_pack.exe

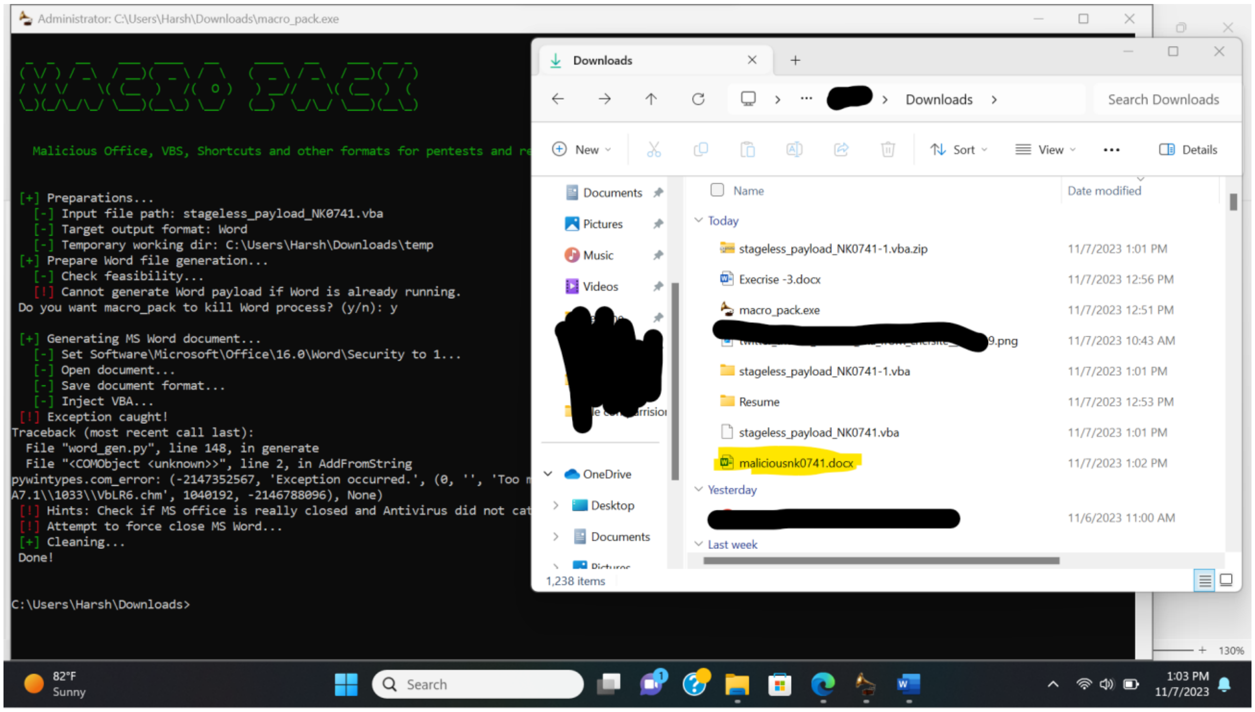
```
  _  _   __   ___  ____   __     ____   __    ___  __ _
 ( \/ ) / _\ / __)(  _ \ /  \   (  _ \ / _\  / __)(  / )
 / \/ \/    \( (__  )   /(  O )   ) __//    \( (__  )  (
 \_)(_/\_/\_/ \___)(__\_) \__/   (__)  \_/\_/ \___)(__\_)


   Malicious Office, VBS, Shortcuts and other formats for pentests and redteam - Version:2.2.0 Release:Community


 [+] Preparations...
   [!] You need to provide an output file! (get help using macro_pack.exe -h)

C:\Users\Harsh\Downloads>macro_pack.exe -help

  _  _   __   ___  ____   __     ____   __    ___  __ _
 ( \/ ) / _\ / __)(  _ \ /  \   (  _ \ / _\  / __)(  / )
 / \/ \/    \( (__  )   /(  O )   ) __//    \( (__  )  (
 \_)(_/\_/\_/ \___)(__\_) \__/   (__)  \_/\_/ \___)(__\_)


   Malicious Office, VBS, Shortcuts and other formats for pentests and redteam - Version:2.2.0 Release:Community


 Usage 1: echo  <parameters> | macro_pack.exe -t <TEMPLATE> -G <OUTPUT_FILE> [options]
 Usage 2: macro_pack.exe  -f input_file_path -G <OUTPUT_FILE> [options]
 Usage 3: more input_file_path | macro_pack.exe -G <OUTPUT_FILE> [options]

 Main payload generation options:
```

Packing the payload:



```
  _  _   __   ___  ____   __     ____   __    ___  __ _
 ( \/ ) / _\ / __)(  _ \ /  \   (  _ \ / _\  / __)(  / )
 / \/ \/    \( (__  )   /(  O )   ) __//    \( (__  )  (
 \_)(_/\_/\_/ \___)(__\_) \__/   (__)  \_/\_/ \___)(__\_)


   Malicious Office, VBS, Shortcuts and other formats for pentests and redteam - Version:2.2.0 Release:Community


 [+] Preparations...
   [-] Input file path: stageless_payload_NK0741.vba
   [-] Target output format: Word
   [-] Temporary working dir: C:\Users\Harsh\Downloads\temp
 [+] Prepare Word file generation...
   [-] Check feasibility...
   [!] Cannot generate Word payload if Word is already running.
 Do you want macro_pack to kill Word process? (y/n): y

 [+] Generating MS Word document...
   [-] Set Software\Microsoft\Office\16.0\Word\Security to 1...
   [-] Open document...
   [-] Save document format...
   [-] Inject VBA...
 [!] Exception caught!
Traceback (most recent call last):
  File "word_gen.py", line 148, in generate
  File "<COMObject <unknown>>", line 2, in AddFromString
pywintypes.com_error: (-2147352567, 'Exception occurred.', (0, '', 'Too many line continuations', 'C:\\Program Files\\Common Files\\Microsoft Shared\\VBA\\V
A7.1\\1033\\VbLR6.chm', 1040192, -2146788096), None)
 [!] Hints: Check if MS office is really closed and Antivirus did not catch the files
 [!] Attempt to force close MS Word...
 [+] Cleaning...
 Done!
```

Full screenshot:



Administrator: C:\Users\Harsh\Downloads\macro_pack.exe

```
  _  _   __    ___  ____   __     ____   __    ___  __ _
 ( \/ ) / _\  / __)(  _ \ /  \   (  _ \ / _\  / __)(  / )
 / \/ \/    \( (__  )   /(  O )   ) __//    \( (__  )  (
 \_)(_/\_/\_/ \___)(__\_) \__/   (__)  \_/\_/ \___)(__\_)


  Malicious Office, VBS, Shortcuts and other formats for pentests and re


 [+] Preparations...
   [-] Input file path: stageless_payload_NK0741.vba
   [-] Target output format: Word
   [-] Temporary working dir: C:\Users\Harsh\Downloads\temp
 [+] Prepare Word file generation...
   [-] Check feasibility...
   [!] Cannot generate Word payload if Word is already running.
 Do you want macro_pack to kill Word process? (y/n): y

 [+] Generating MS Word document...
   [-] Set Software\Microsoft\Office\16.0\Word\Security to 1...
   [-] Open document...
   [-] Save document format...
   [-] Inject VBA...
 [!] Exception caught!
Traceback (most recent call last):
  File "word_gen.py", line 148, in generate
  File "<COMObject <unknown>>", line 2, in AddFromString
pywintypes.com_error: (-2147352567, 'Exception occurred.', (0, '', 'Too m
A7.1\\1033\\VbLR6.chm', 1040192, -2146788096), None)
 [!] Hints: Check if MS office is really closed and Antivirus did not cat
 [!] Attempt to force close MS Word...
 [+] Cleaning...
 Done!


C:\Users\Harsh\Downloads>
```

Downloads

[redacted] > Downloads > Search Downloads

New Sort View Details

Documents
Pictures
Music
Videos
[redacted]
OneDrive
Desktop
Documents
Pictures

Name Date modified

Today

stageless_payload_NK0741-1.vba.zip 11/7/2023 1:01 PM
Exercise -3.docx 11/7/2023 12:56 PM
macro_pack.exe 11/7/2023 12:51 PM
[redacted]9.png 11/7/2023 10:43 AM
stageless_payload_NK0741-1.vba 11/7/2023 1:01 PM
Resume 11/7/2023 12:53 PM
stageless_payload_NK0741.vba 11/7/2023 1:01 PM
maliciousnk0741.docx 11/7/2023 1:02 PM

Yesterday

[redacted] 11/6/2023 11:00 AM

Last week

1,238 items

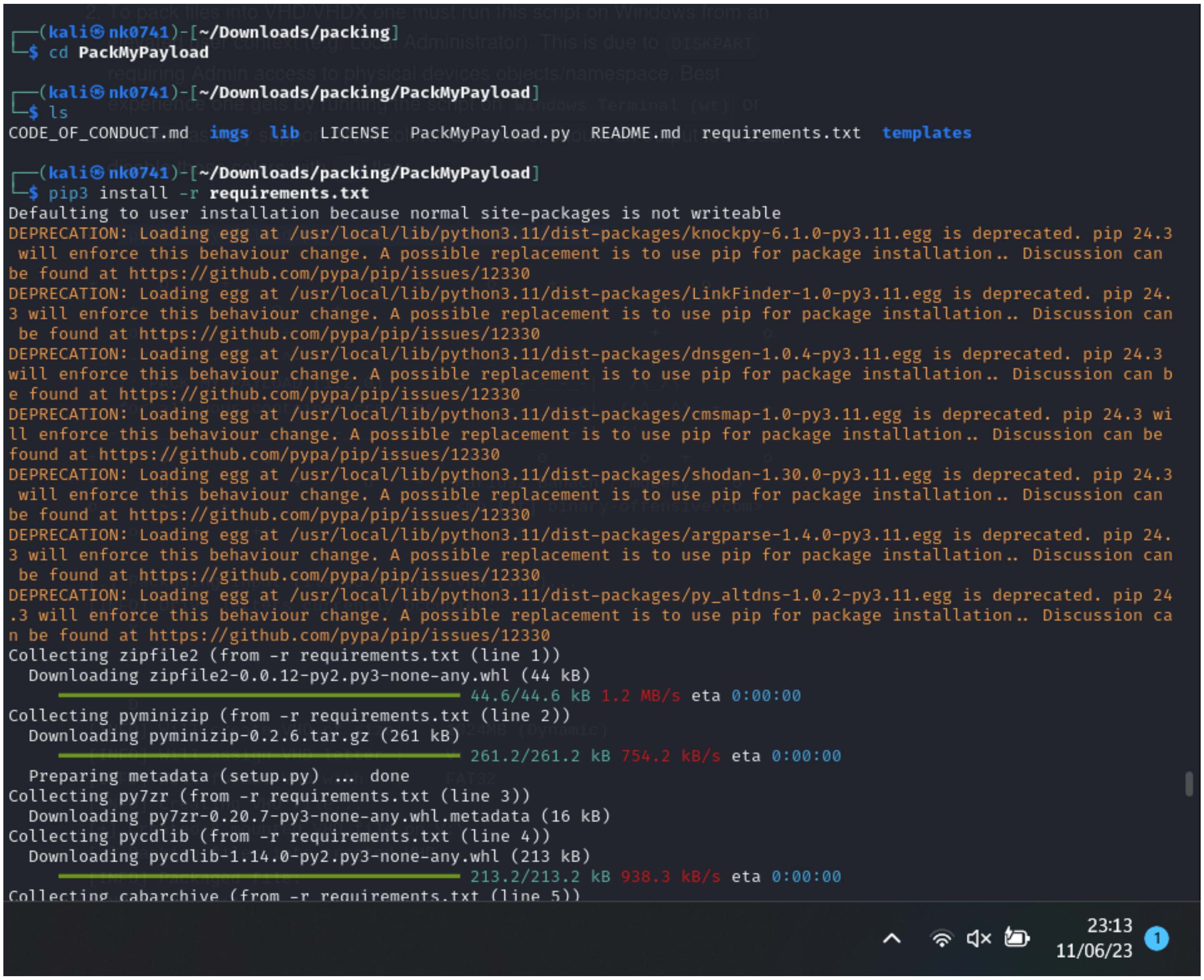
82°F
Sunny

Search

1:03 PM
11/7/2023

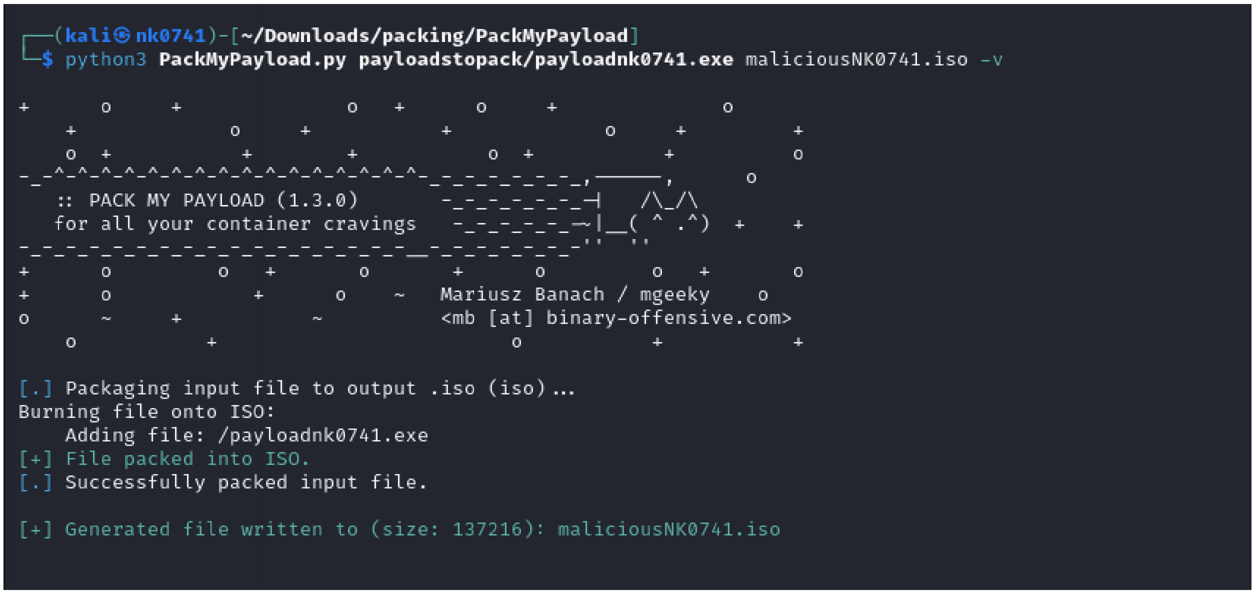
Packmypayload:

Installing the packmypayload:



```
┌──(kali㉿nk0741)-[~/Downloads/packing]
└─$ cd PackMyPayload

┌──(kali㉿nk0741)-[~/Downloads/packing/PackMyPayload]
└─$ ls
CODE_OF_CONDUCT.md  imgs  lib  LICENSE  PackMyPayload.py  README.md  requirements.txt  templates

┌──(kali㉿nk0741)-[~/Downloads/packing/PackMyPayload]
└─$ pip3 install -r requirements.txt
Defaulting to user installation because normal site-packages is not writeable
DEPRECATION: Loading egg at /usr/local/lib/python3.11/dist-packages/knockpy-6.1.0-py3.11.egg is deprecated. pip 24.3
 will enforce this behaviour change. A possible replacement is to use pip for package installation.. Discussion can
be found at https://github.com/pypa/pip/issues/12330
DEPRECATION: Loading egg at /usr/local/lib/python3.11/dist-packages/LinkFinder-1.0-py3.11.egg is deprecated. pip 24.
3 will enforce this behaviour change. A possible replacement is to use pip for package installation.. Discussion can
 be found at https://github.com/pypa/pip/issues/12330
DEPRECATION: Loading egg at /usr/local/lib/python3.11/dist-packages/dnsgen-1.0.4-py3.11.egg is deprecated. pip 24.3
will enforce this behaviour change. A possible replacement is to use pip for package installation.. Discussion can b
e found at https://github.com/pypa/pip/issues/12330
DEPRECATION: Loading egg at /usr/local/lib/python3.11/dist-packages/cmsmap-1.0-py3.11.egg is deprecated. pip 24.3 wi
ll enforce this behaviour change. A possible replacement is to use pip for package installation.. Discussion can be
found at https://github.com/pypa/pip/issues/12330
DEPRECATION: Loading egg at /usr/local/lib/python3.11/dist-packages/shodan-1.30.0-py3.11.egg is deprecated. pip 24.3
 will enforce this behaviour change. A possible replacement is to use pip for package installation.. Discussion can
be found at https://github.com/pypa/pip/issues/12330
DEPRECATION: Loading egg at /usr/local/lib/python3.11/dist-packages/argparse-1.4.0-py3.11.egg is deprecated. pip 24.
3 will enforce this behaviour change. A possible replacement is to use pip for package installation.. Discussion can
 be found at https://github.com/pypa/pip/issues/12330
DEPRECATION: Loading egg at /usr/local/lib/python3.11/dist-packages/py_altdns-1.0.2-py3.11.egg is deprecated. pip 24
.3 will enforce this behaviour change. A possible replacement is to use pip for package installation.. Discussion ca
n be found at https://github.com/pypa/pip/issues/12330
Collecting zipfile2 (from -r requirements.txt (line 1))
  Downloading zipfile2-0.0.12-py2.py3-none-any.whl (44 kB)
     ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 44.6/44.6 kB 1.2 MB/s eta 0:00:00
Collecting pyminizip (from -r requirements.txt (line 2))
  Downloading pyminizip-0.2.6.tar.gz (261 kB)
     ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 261.2/261.2 kB 754.2 kB/s eta 0:00:00
  Preparing metadata (setup.py) ... done
Collecting py7zr (from -r requirements.txt (line 3))
  Downloading py7zr-0.20.7-py3-none-any.whl.metadata (16 kB)
Collecting pycdlib (from -r requirements.txt (line 4))
  Downloading pycdlib-1.14.0-py2.py3-none-any.whl (213 kB)
     ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 213.2/213.2 kB 938.3 kB/s eta 0:00:00
Collecting cabarchive (from -r requirements.txt (line 5))
```

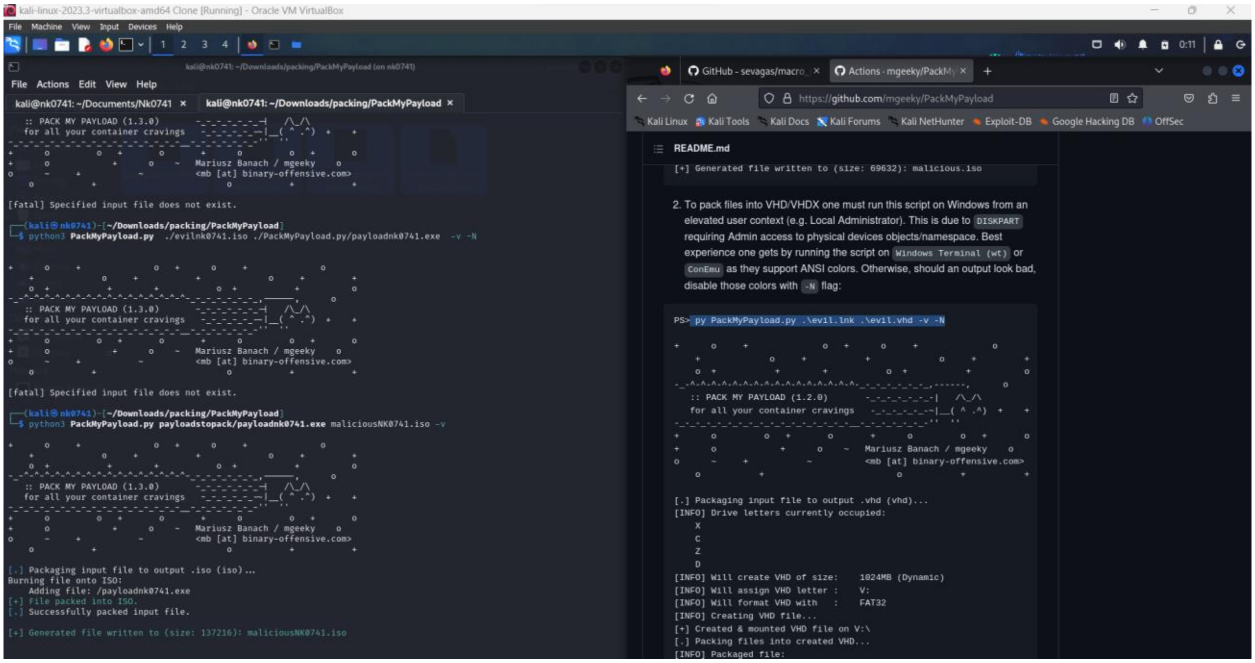
23:13
11/06/23



```
┌──(kali㉿nk0741)-[~/Downloads/packing/PackMyPayload]
└─$ python3 PackMyPayload.py payloadstopack/payloadnk0741.exe maliciousNK0741.iso -v

+      o     +              o   +      o     +              o
    +             o     +           +             o     +         +
    o  +           +        +           o  +           +          o
-_-^-^-^-^-^-^-^-^-^-^-^-^-^-^-^-^-_-_-_-_-_-_-_,______,      o
   :: PACK MY PAYLOAD (1.3.0)       -_-_-_-_-_-_-┤   /\_/\
   for all your container cravings   -_-_-_-_-_-~|__( ^ .^)  +    +
-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-__-_-_-_-_-_-_-''  ''
+      o         o   +       o       +      o         o   +      o
+      o            +      o    ~   Mariusz Banach / mgeeky    o
o      ~     +           ~          <mb [at] binary-offensive.com>
    o           +                         o          +           +

[.] Packaging input file to output .iso (iso)...
Burning file onto ISO:
    Adding file: /payloadnk0741.exe
[+] File packed into ISO.
[.] Successfully packed input file.

[+] Generated file written to (size: 137216): maliciousNK0741.iso
```

Successfully created the payload using packmypayload in .iso format.

Full screenshot with time:


kali-linux-2023.3-virtualbox-amd64 Clone [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
0:11
kali@nk0741: ~/Downloads/packing/PackMyPayload (on nk0741)
File Actions Edit View Help
kali@nk0741: ~/Documents/Nk0741
kali@nk0741: ~/Downloads/packing/PackMyPayload
GitHub - sevagas/macro_
Actions · mgeeky/PackMy
https://github.com/mgeeky/PackMyPayload
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
README.md

```
   :: PACK MY PAYLOAD (1.3.0)       -_-_-_-_-_-_-┤   /\_/\
   for all your container cravings   -_-_-_-_-_-~|__( ^ .^)  +    +
-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-''  ''
+      o         o   +       o       +      o         o   +       o
+      o             +      o    ~   Mariusz Banach / mgeeky    o
o      ~     +           ~           <mb [at] binary-offensive.com>
    o           +                         o           +           +

[fatal] Specified input file does not exist.

┌──(kali㉿nk0741)-[~/Downloads/packing/PackMyPayload]
└─$ python3 PackMyPayload.py  ./evilnk0741.iso ./PackMyPayload.py/payloadnk0741.exe  -v -N


+      o     +              o   +      o     +              o
    +              o     +           +           o     +         +
    o  +           +         +           o  +           +        o
-_-^-^-^-^-^-^-^-^-^-^-^-^-^-^-^-^-^-^-_-_-_-_-_-_-_-_-,------,      o
   :: PACK MY PAYLOAD (1.3.0)       -_-_-_-_-_-_-┤   /\_/\
   for all your container cravings   -_-_-_-_-_-~|__( ^ .^)  +    +
-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-''  ''
+      o         o   +       o       +      o         o   +       o
+      o             +      o    ~   Mariusz Banach / mgeeky    o
o      ~     +           ~           <mb [at] binary-offensive.com>
    o           +                         o           +           +

[fatal] Specified input file does not exist.

┌──(kali㉿nk0741)-[~/Downloads/packing/PackMyPayload]
└─$ python3 PackMyPayload.py payloadstopack/payloadnk0741.exe maliciousNK0741.iso -v

+      o     +              o   +      o     +              o
    +              o     +           +           o     +         +
    o  +           +         +           o  +           +        o
-_-^-^-^-^-^-^-^-^-^-^-^-^-^-^-^-^-^-^-_-_-_-_-_-_-_-_-,------,      o
   :: PACK MY PAYLOAD (1.3.0)       -_-_-_-_-_-_-┤   /\_/\
   for all your container cravings   -_-_-_-_-_-~|__( ^ .^)  +    +
-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-''  ''
+      o         o   +       o       +      o         o   +       o
+      o             +      o    ~   Mariusz Banach / mgeeky    o
o      ~     +           ~           <mb [at] binary-offensive.com>
    o           +                         o           +           +

[.] Packaging input file to output .iso (iso)...
Burning file onto ISO:
    Adding file: /payloadnk0741.exe
[+] File packed into ISO.
[.] Successfully packed input file.

[+] Generated file written to (size: 137216): maliciousNK0741.iso
```

```
[+] Generated file written to (size: 69632): malicious.iso
```

2. To pack files into VHD/VHDX one must run this script on Windows from an elevated user context (e.g. Local Administrator). This is due to `DISKPART` requiring Admin access to physical devices objects/namespace. Best experience one gets by running the script on `Windows Terminal (wt)` or `ConEmu` as they support ANSI colors. Otherwise, should an output look bad, disable those colors with `-N` flag:

```
PS> py PackMyPayload.py .\evil.lnk .\evil.vhd -v -N

+      o     +              o   +      o     +              o
    +              o     +           +           o     +         +
    o  +           +         +           o  +           +        o
-_-^-^-^-^-^-^-^-^-^-^-^-^-^-^-^-^-^-^-_-_-_-_-_-_-_-_-,------,      o
   :: PACK MY PAYLOAD (1.2.0)       -_-_-_-_-_-_-|   /\_/\
   for all your container cravings   -_-_-_-_-_-~|__( ^ .^)  +    +
-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-''  ''
+      o         o   +       o       +      o         o   +       o
+      o             +      o    ~   Mariusz Banach / mgeeky    o
o      ~     +           ~           <mb [at] binary-offensive.com>
    o           +                         o           +           +

[.] Packaging input file to output .vhd (vhd)...
[INFO] Drive letters currently occupied:
    X
    C
    Z
    D
[INFO] Will create VHD of size:    1024MB (Dynamic)
[INFO] Will assign VHD letter :    V:
[INFO] Will format VHD with   :    FAT32
[INFO] Creating VHD file...
[+] Created & mounted VHD file on V:\
[.] Packing files into created VHD...
[INFO] Packaged file:
```

I have attached the packed payload as well.

For macropack we packed it into .docx format and for packmypayload we used .iso formats