**FakeImageExploiter v1.4 - backdoor images.jpg[.ps1]**

CodeName: Metamorphosis

Version release: v1.4 (Stable)

Author: pedro ubuntu [ r00t-3xp10it ]

Distros Supported : Linux Ubuntu, Kali, Mint, Parrot OS Suspicious-Shell-Activity (SSA) RedTeam develop [@2017](mailto:@2017)

**Legal Disclamer:**

The author does not hold any responsibility for the bad use of this tool,

remember that attacking targets without prior consent is illegal and punished by law.

**Description:**

This module takes one existing image.jpg and one payload.ps1 (input by user) and builds a new payload (agent.jpg.exe) that if executed it will trigger the download of the 2 previous files stored into apache2 (image.jpg + payload.ps1) and execute them.

This module also changes the agent.exe Icon to match one file.jpg Then uses the spoof

'Hide extensions for known file types' method to hidde the agent.exe extension.

All payloads (user input) will be downloaded from our apache2 webserver and executed into target RAM. The only extension (payload input by user) that requires to write payload to disk are .exe binaries.

**Exploitation:**

FakeImageExploiter stores all files in apache2 webroot, zips (.zip) the agent, starts apache2 and metasploit services(handler), and provides a URL to send to target (triggers agent.zip download). As soon as the victim runs our executable, our picture will be downloaded and opened in the default picture viewer, our malicious payload will be executed, and we will get a meterpreter session.

But it also stores the agent (not ziped) into FakeImageExploiter/output folder if we wish to deliver agent.jpg.exe using another diferent attack vector.

'This tool also builds a cleaner.rc file to delete payloads left in target'

**Payloads accepted (user input):**

payload.ps1 (default) | payload.bat | payload.txt | payload.exe [Metasploit] "Edit 'settings' file before runing tool to use other extensions"

**Pictures accepted (user input):**

All pictures with .jpg (default) | .jpeg | .png extensions (all sizes) "Edit 'settings' file before runing tool to use other extensions"

**Dependencies/Limitations:**

xterm, zenity, apache2, mingw32[64], ResourceHacker(wine)

'Auto-Installs ResourceHacker.exe under ../.wine/Program Files/.. directorys'

WARNING: To change icon manually (resource hacker bypass) edit 'settings' file. WARNING: Only under windows systems the 2º extension will be hidden (so zip it) WARNING: The agent.jpg.exe requires the inputed files to be in apache2 (local lan hack)

WARNING: The agent.jpg.exe uses the powershell interpreter (does not work againts wine).

WARNING: This tool will not accept payload (user input) arguments (eg nc.exe -lvp

127.0.0.1 555)

WARNING: The ResourceHacker provided by this tool requires WINE to be set to windows

7

**Another senarios:**

If you wish to use your own binary (user input - not metasploit payloads) then:

1º - Edit 'settings' file before runing tool and select 'NON\_MSF\_PAYLOADS=YES' 2º

- Select the binary extension to use **'Remmenber to save settings file before continue'** ..

3º - Run FakeImageExploiter to metamorphosis your binary (auto-storage all files in apache) .. 4º - Open new terminal and execute your binary handler to recibe

connection. **HINT: This funtion will NOT build a cleaner.rc**

**The noob friendly funtion:**

Bypass the need to input your payload.ps1, And let FakeImageExploiter take

care of building the required payload.ps1 + agent.jpg.exe and config the handler. "With this funtion active, you only need to input your picture.jpg :D"

Select the binary extension to use **HINT: This funtion allow users to build**

**(ps1|bat|txt) payloads**

**HINT: This funtion will NOT build .exe binaries**

**"WINE is not owned by you":**

If you get this message it means that you are executing FakeImageExploiter as sudo and your wine installation belongs to user (is not owned by you) to bypass this issue just execute FakeImageExploiter as the wine owner. EXAMPLE: If wine its owned by spirited\_wolf, execute tool without sudo EXAMPLE: If wine its owned by root, execute tool as sudo

**Download/Install/Config:**

1º - Download framework from github

git clone https://github.com/r00t-3xp10it/FakeImageExploiter.git

2º - Set files execution permitions cd FakeImageExploiter

sudo chmod +x \*.sh

3º - Config FakeImageExploiter settings nano settings

4º - Run main tool

sudo ./FakeImageExploiter.sh

**Framework Banner**

**settings file**

**Agent(s) in windows systems**