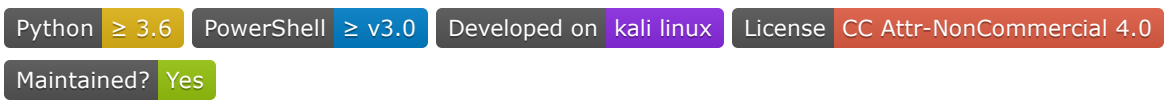
Villain



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 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

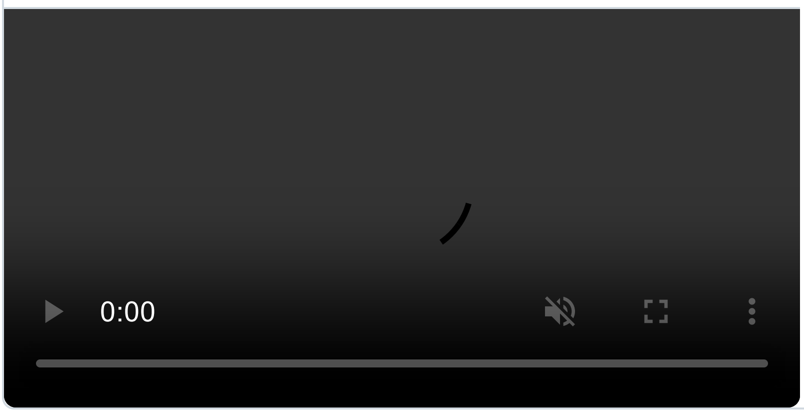
There's no up-to-date presentation of Villain with its latest features, but these videos give a good overview of its functionality.
[2022-11-30] John Hammond showcased the tool in this incredible video -> youtube.com/watch?v=pTUggbSCqA0

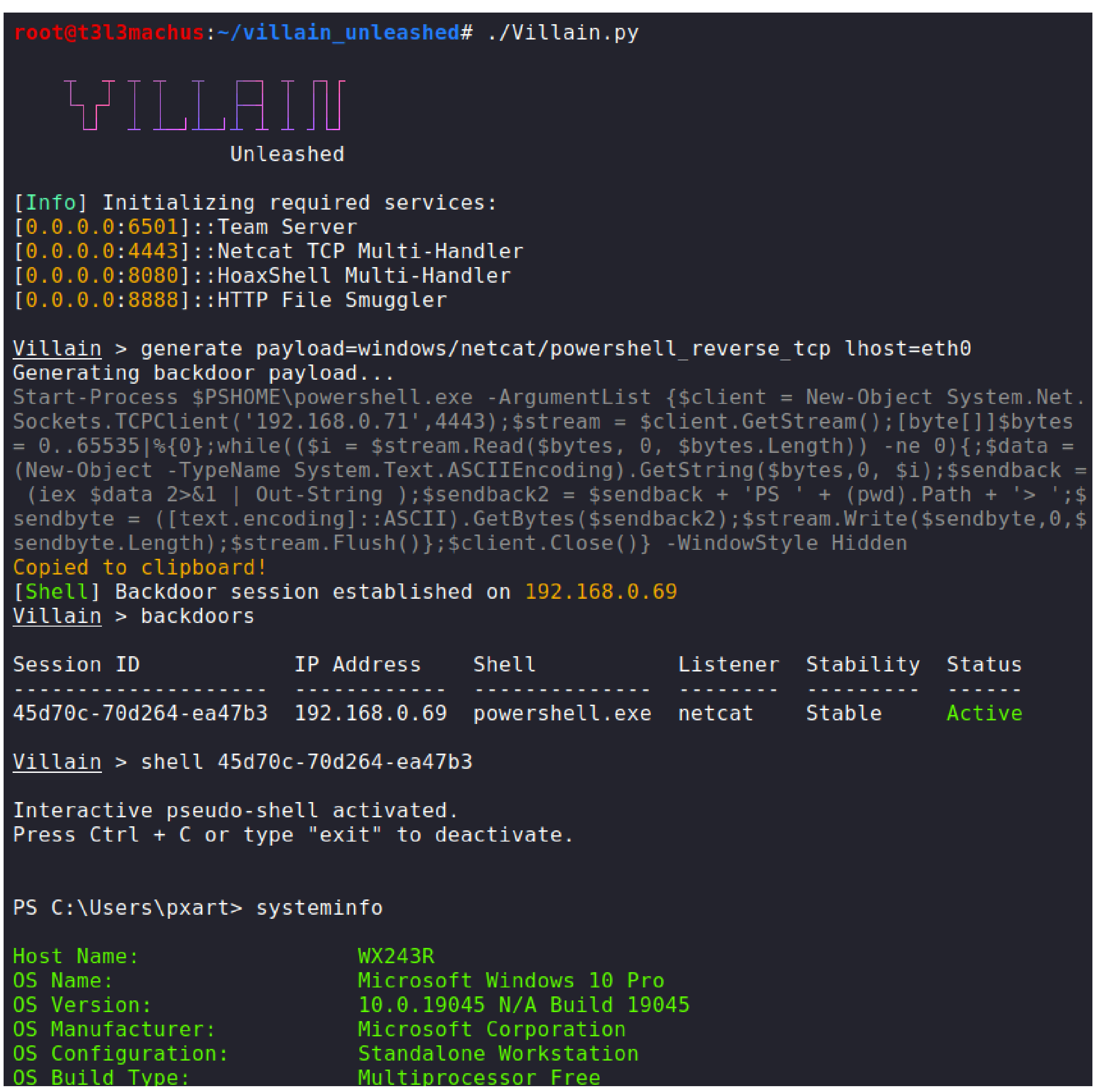
[2023-03-30] Version 2.0.0 release demo, made by me -> youtube.com/watch?v=NqZEmBsLCvQ

❗ 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.

Preview

villain.mp4





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-terminal
```

Usage

You should run as root:

```
villain [-h] [-p PORT] [-x HOAX_PORT] [-n NETCAT_PORT] [-f FILE_SMUG(
```

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 similar already in the making,