EuskalHack Security Congress VI

> whoami

- Raúl Caro Teixidó (aka **Secu**)
- **Offensive Security Engineer en Telefónica Tech**
- Co-desarrollador de **Mística** (canales encubiertos)
- Me recordarán de otras charlas como…
  - **H-c0n 2023**
  - **Navaja Negra 2022**
  - **BlackHat Arsenal USA 2020**
  - **Bitup Alicante 2020**

•Twitter: **@secu_x11**
•Linkedin: **raul-caro-teixido**
•Blog: **https://makemalware.com**

¿Cuál es el objetivo del taller?

- Conocer la **estructura interna** de Kraken.
- Aprender a utilizar Kraken de forma **práctica**.
- Entender la necesidad de realizar una **explotación segura**.
- Conocer la importancia de un **diseño** que permita:
  - Mejorar en la **Escalabilidad y Modularidad**
  - Mentalidad de elaboración de un **Arsenal**
  - Construcción de herramientas complejas que nos simplifique la vida.

¿Qué es Kraken?

- Un Orquestador de Webshells (**PHP, JSP, ASPX**)
- Un Framework para post-explotación vía Web
- Un proyecto centrado en la Evasión de Defensas
- Una herramienta escalable y customizable
- Link: https://github.com/kraken-ng/Kraken

Características principales

- Se evita la **ejecución de comandos del sistema**
  - La reimplementación de los comandos a partir de módulos en el lenguaje nativo.
  - Los módulos son piezas de código que buscan replicar la misma funcionalidad que realiza el comando o permite obtener información similar.
- **Multi-lenguaje** (soporta PHP, JAVA y NET).
- **Multi-versión** (se centra en la retrocompatibilidad).
- Carga dinámica y compilación sin dependencias.

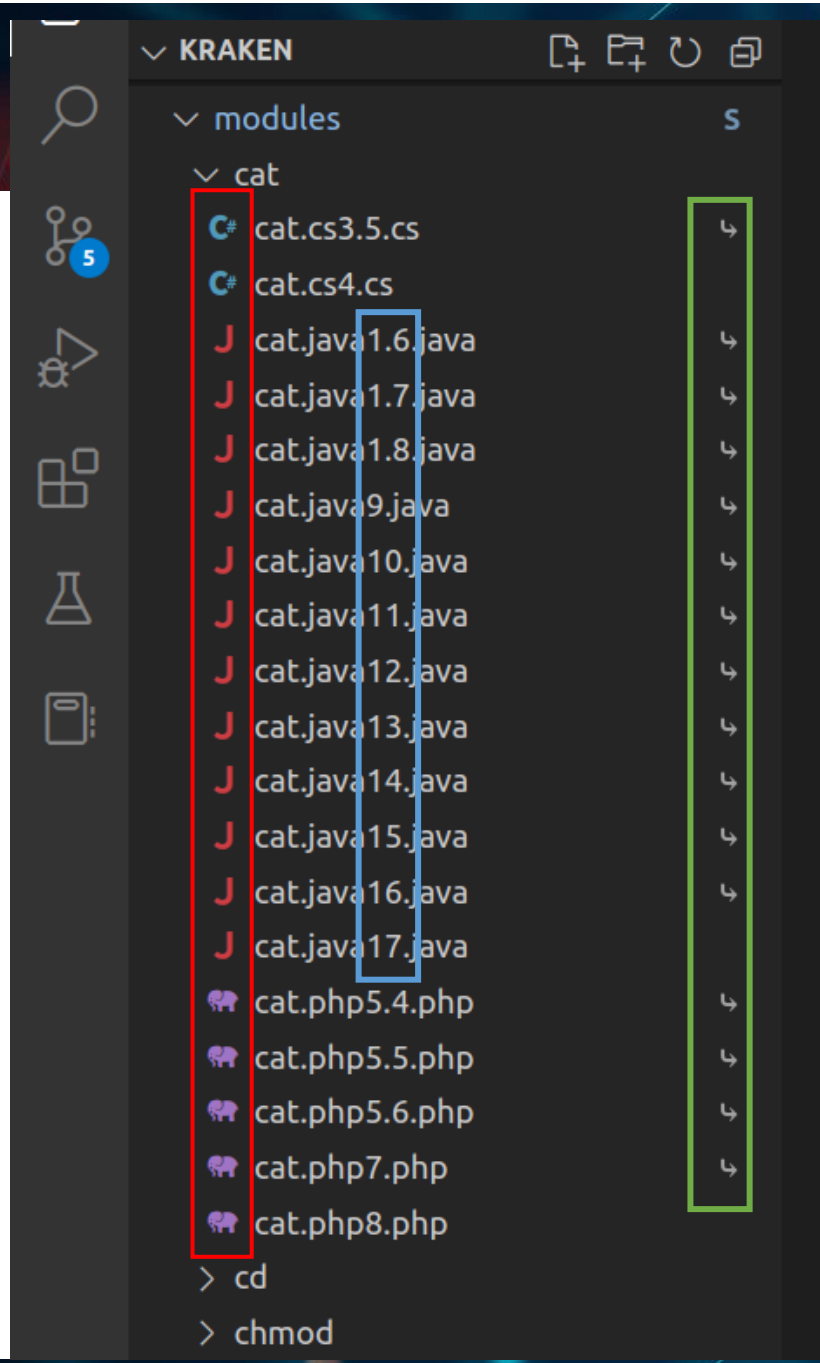
¿Por qué es útil para un Pentester?

- Permite evadir políticas de bloqueo (AppLocker, Disabled functions, etc)
- Permite evadir soluciones de seguridad (AV, EDRs, etc)
- Permite al operador ejecutar código pero también comandos
- Soporte para versiones antiguas o muy concretas
- TTY completito y cómodo (tabs, suggest, history, searches, etc)
- Histórico de comandos (modo simple o modo extendido)

¿Por qué es útil para un Red Teamer?

- Permite realizar un primer contacto con el sistema comprometido sin ejecutar ningún comando (útil de cara a no ser detectado)
- Minimizar el uso de herramientas sobre la máquina víctima
- Posibilidad de elevar y mantener el contexto privilegiado
- Realizar técnicas de descubrimiento, acceso a credenciales y mov. lateral
- <ctrl+c> pentester <ctrl+v>

MÓDULOS DE KRAKEN



Soporte Multi-lenguaje

Multi-version

Uso de enlaces simbólicos para evitar duplicados

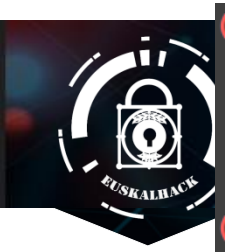
Ejemplos de ejecución:

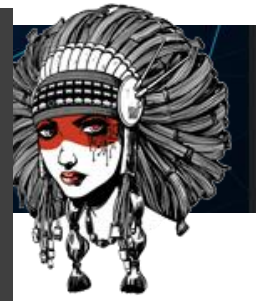
```
(ST) www-data@edc536a611dc:/var/www/html$ ls

 drwxrwxrwx  1      www-data  www-data  4096   2023/01/10 11:26:48  .
 drwxr-xr-x  1      root      root      4096   2022/11/15 04:13:21  ..
 -rwxrwxr-x  1      1000      1000      21909  2023/01/10 13:58:35  agent_c2.php
 -rwxrwxr-x  1      1000      1000      12899  2022/12/19 14:11:56  agent_st.php
 -rwxrwxr-x  1      1000      1000      17     2022/12/19 14:11:56  index.php
 -rwxrwxr-x  1      1000      1000      2915   2022/12/26 14:59:07  test.php

(ST) www-data@edc536a611dc:/var/www/html$
```

Kraken "ls" module

```
root@edc536a611dc:/var/www/html# ls -la
total 60
drwxrwxrwx 1 www-data www-data  4096 Jan 10 11:26 .
drwxr-xr-x 1 root     root      4096 Nov 15 04:13 ..
-rwxrwxr-x 1     1000     1000 21909 Jan 10 13:58 agent_c2.php
-rwxrwxr-x 1     1000     1000 12899 Dec 19 14:11 agent_st.php
-rwxrwxr-x 1     1000     1000    17 Dec 19 14:11 index.php
-rwxrwxr-x 1     1000     1000  2915 Dec 26 14:59 test.php
root@edc536a611dc:/var/www/html#
```

Unix "ls" command





```
(ST) IIS APPPOOL\DefaultAppPool@DESKTOP-DH3LRI4:C:/inetpub/wwwroot$ whoami

  USERNAME                    SID

  IIS APPPOOL\DefaultAppPool  S-1-5-82-3006700770-424185619-1745488364-794895919-4004696415

(ST) IIS APPPOOL\DefaultAppPool@DESKTOP-DH3LRI4:C:/inetpub/wwwroot$ whoami -p

  PRIVILEGE NAME                STATUS

  SeAssignPrimaryTokenPrivilege  Disabled
  SeIncreaseQuotaPrivilege       Disabled
  SeShutdownPrivilege            Disabled
  SeAuditPrivilege               Disabled
  SeChangeNotifyPrivilege        Enabled
  SeUndockPrivilege              Disabled
  SeImpersonatePrivilege         Enabled
  SeCreateGlobalPrivilege        Enabled
  SeIncreaseWorkingSetPrivilege  Disabled
  SeTimeZonePrivilege            Disabled

(ST) IIS APPPOOL\DefaultAppPool@DESKTOP-DH3LRI4:C:/inetpub/wwwroot$ netstat -l

  PROTOCOL  LOCAL ADDRESS                         REMOTE ADDRESS        STATE

  tcp       0.0.0.0:80                            DESKTOP-DH3LRI4:0     Listen
  tcp       0.0.0.0:135                           DESKTOP-DH3LRI4:0     Listen
  tcp       0.0.0.0:445                           DESKTOP-DH3LRI4:0     Listen
  tcp       0.0.0.0:5040                          DESKTOP-DH3LRI4:0     Listen
  tcp       0.0.0.0:7680                          DESKTOP-DH3LRI4:0     Listen
  tcp       0.0.0.0:49664                         DESKTOP-DH3LRI4:0     Listen
  tcp       0.0.0.0:49665                         DESKTOP-DH3LRI4:0     Listen
  tcp       0.0.0.0:49666                         DESKTOP-DH3LRI4:0     Listen
  tcp       0.0.0.0:49667                         DESKTOP-DH3LRI4:0     Listen
  tcp       0.0.0.0:49668                         DESKTOP-DH3LRI4:0     Listen
  tcp       0.0.0.0:49671                         DESKTOP-DH3LRI4:0     Listen
  tcp       127.0.0.1:6788                        DESKTOP-DH3LRI4:0     Listen
  tcp       127.0.0.1:6789                        DESKTOP-DH3LRI4:0     Listen
  tcp       192.168.30.128:139                    DESKTOP-DH3LRI4:0     Listen
  tcp       192.168.30.131:139                    DESKTOP-DH3LRI4:0     Listen
  tcp       [::]:80                               DESKTOP-DH3LRI4:0     Listen
  tcp       [::]:135                              DESKTOP-DH3LRI4:0     Listen
```

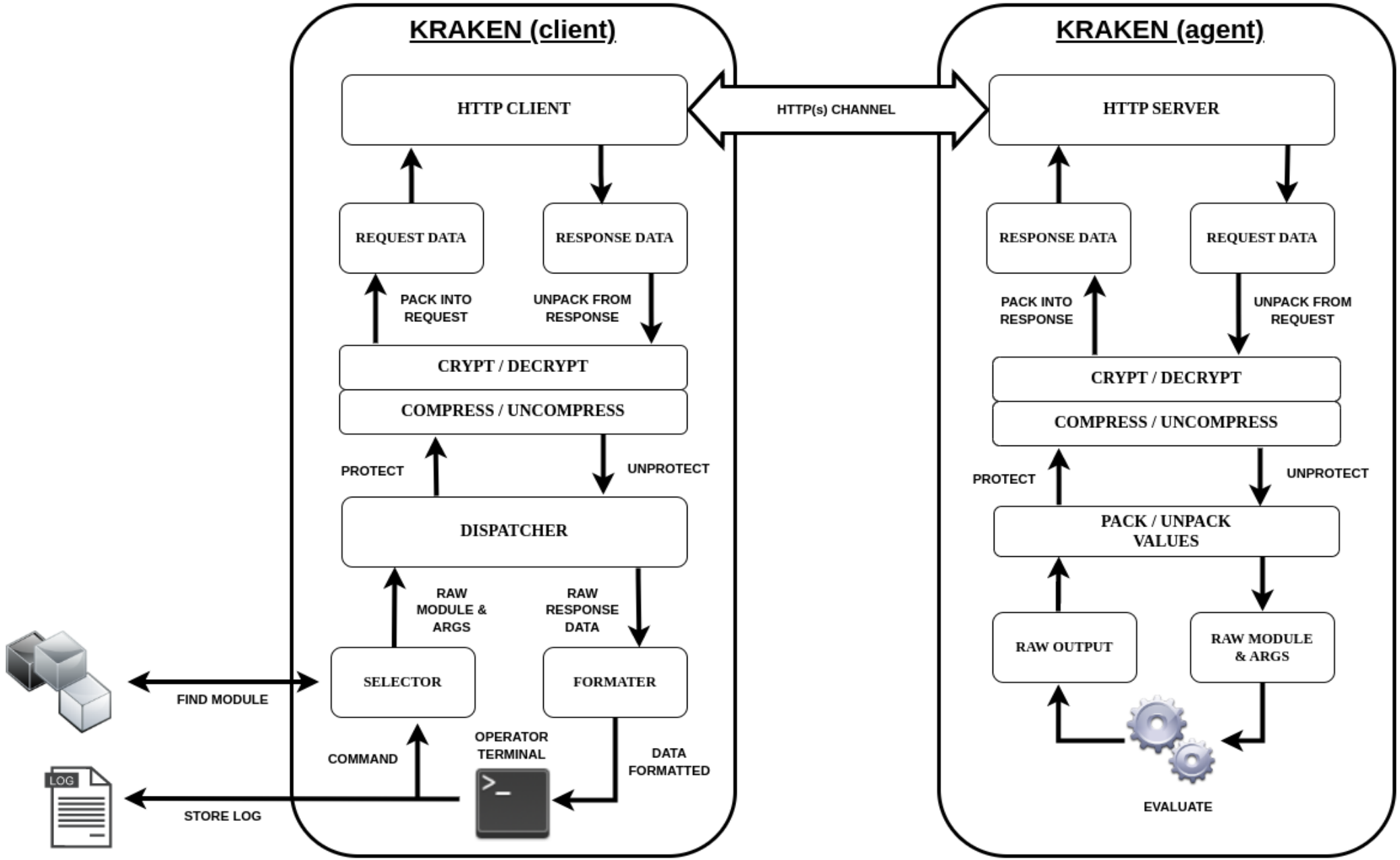
Linux

Modules	PHP >=5.4	PHP 7	PHP 8	JAVA 6	7 >= JAVA <= 17
cat	✓	✓	✓	✓	✓
cd	✓	✓	✓	✓	✓
chmod	✓	✓	✓	✗	✗
cp	✓	✓	✓	✗	✓
download	✓	✓	✓	✓	✓
execute	✓	✓	✓	✓	✓
find	✓	✓	✓	✗	✗
grep	✓	✓	✓	✗	✗
id	✓	✓	✓	✓	✓
ls	✓	✓	✓	✗	✓
mkdir	✓	✓	✓	✓	✓
netstat	✓	✓	✓	✗	✗
ps	✓	✓	✓	✗	✗
pspy	✓	✓	✓	✗	✗
rm	✓	✓	✓	✓	✓
sysinfo	✓	✓	✓	✓	✓
tcpconnect	✓	✓	✓	✓	✓
touch	✓	✓	✓	✗	✓
upload	✓	✓	✓	✓	✓
webinfo	✓	✓	✓	✗	✗

Windows

Modules	PHP >=5.4	PHP 7	PHP 8	JAVA 6	7 >= JAVA <= 17	NET 3.5	NET 4.0
cat	✓	✓	✓	✓	✓	✓	✓
cd	✓	✓	✓	✓	✓	✓	✓
cp	✓	✓	✓	✗	✓	✓	✓
download	✓	✓	✓	✓	✓	✓	✓
driveinfo	–	–	–	–	–	✓	✓
dump_iis_secrets	–	–	–	–	–	✓	✓
dup_token	–	–	–	–	–	✓	✓
execute	✓	✓	✓	✓	✓	✓	✓
execute_assembly	–	–	–	–	–	✓	✓
execute_with_token	–	–	–	–	–	✓	✓
find	✗	✗	✗	✗	✗	✗	✗
grep	✗	✗	✗	✗	✗	✗	✗
id	–	–	–	–	–	✓	✓
impersonate	–	–	–	–	–	✓	✓
list_tokens	–	–	–	–	–	✗	✓
ls	✓	✓	✓	✗	✓	✓	✓
mkdir	✓	✓	✓	✓	✓	✓	✓
netstat	–	–	–	–	–	✗	✗
powerpick	–	–	–	–	–	✓	✓
ps	–	–	–	–	–	✓	✓
pspy	–	–	–	–	–	✗	✗
rm	✓	✓	✓	✓	✓	✓	✓
sc	–	–	–	–	–	✓	✓
secretsdump	–	–	–	–	–	✓	✓
set_token	–	–	–	–	–	✓	✓
show_integrity	–	–	–	–	–	✓	✓
sysinfo	✓	✓	✓	✓	✓	✓	✓
tcpconnect	✓	✓	✓	✓	✓	✓	✓
touch	✓	✓	✓	✗	✓	✓	✓
upload	✓	✓	✓	✓	✓	✓	✓
whoami	–	–	–	–	–	✓	✓

AGENTES DE KRAKEN


KRAKEN (client)
HTTP CLIENT
REQUEST DATA
RESPONSE DATA
PACK INTO REQUEST
UNPACK FROM RESPONSE
CRYPT / DECRYPT
COMPRESS / UNCOMPRESS
PROTECT
UNPROTECT
DISPATCHER
RAW MODULE & ARGS
RAW RESPONSE DATA
SELECTOR
FORMATER
FIND MODULE
COMMAND
OPERATOR TERMINAL
DATA FORMATTED
LOG
STORE LOG
HTTP(s) CHANNEL
KRAKEN (agent)
HTTP SERVER
RESPONSE DATA
REQUEST DATA
PACK INTO RESPONSE
UNPACK FROM REQUEST
CRYPT / DECRYPT
COMPRESS / UNCOMPRESS
PROTECT
UNPROTECT
PACK / UNPACK VALUES
RAW OUTPUT
RAW MODULE & ARGS
EVALUATE

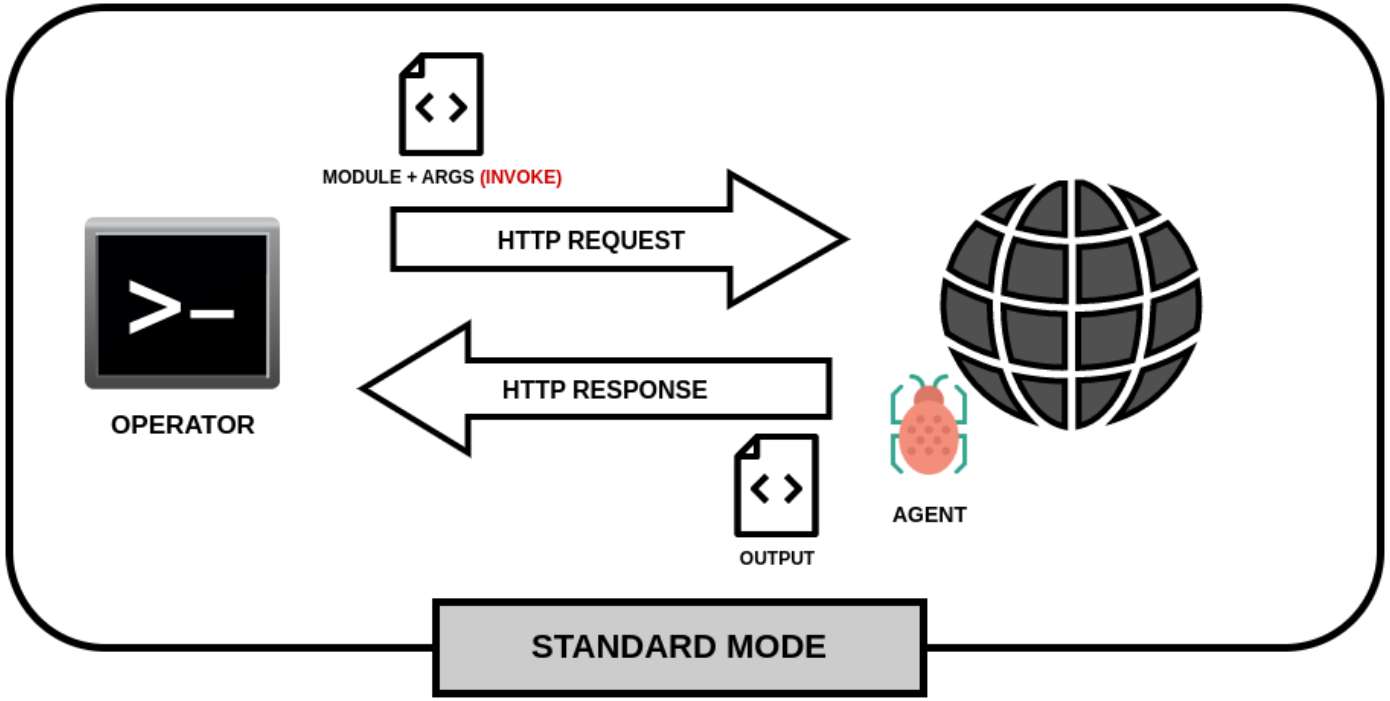
Ejecutores (cargadores disponibles):

Los ejecutores son los encargados de **invocar/evaluar/cargar** los módulos de Kraken. Están limitados a las funcionalidades del propio lenguaje en uso y pueden no estar disponibles en todas las versiones.

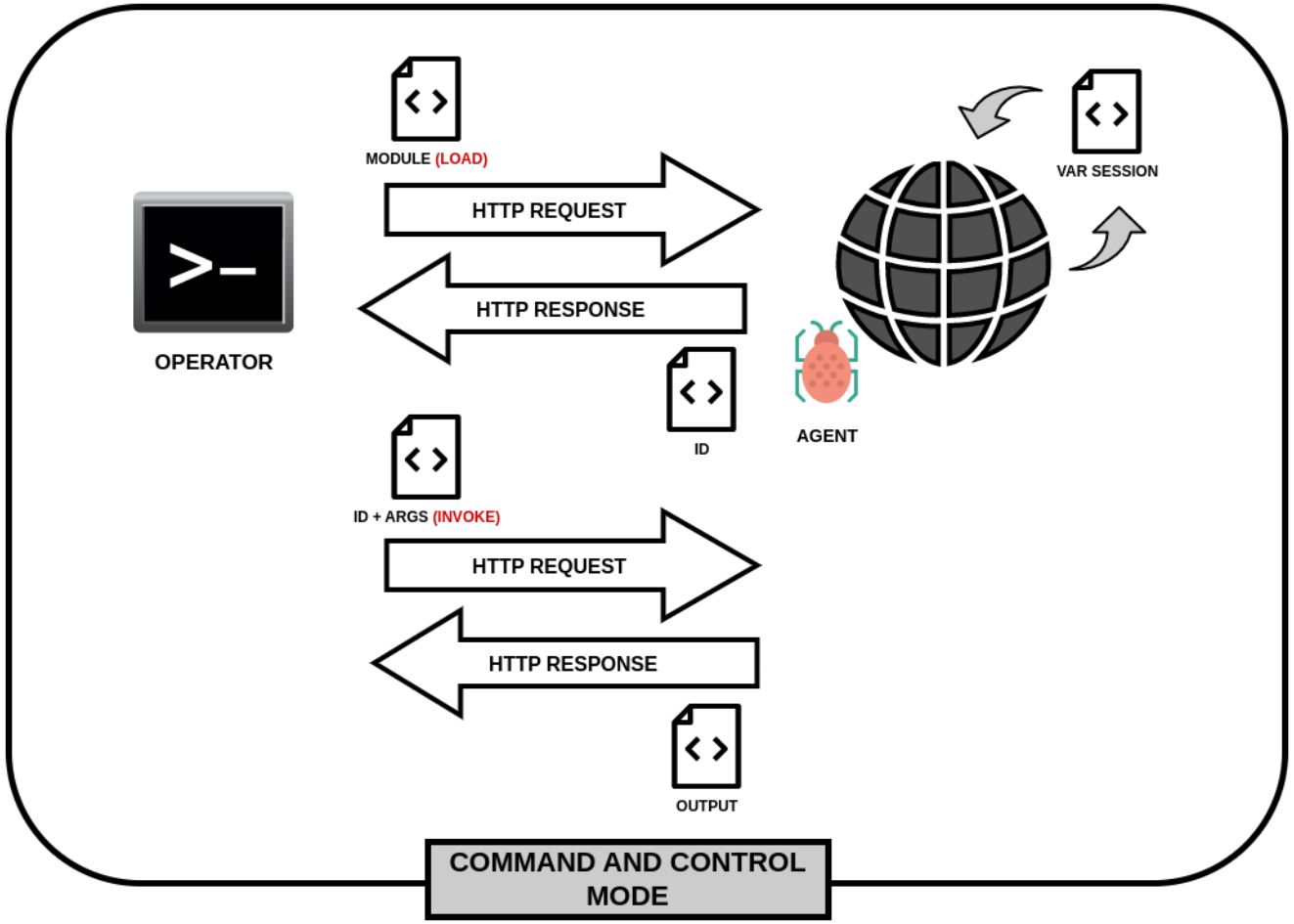
PHP	JSP	ASPX
eval()	ClassLoader	CSharpCodeProvider
create_function()	javax.tools.JavaCompiler	Assembly.Load()
include() / require()		System.Reflection.Emit

Modo Standard (ST):

- Modo tradicional de funcionamiento en webshells.
- Es simple y preciso.
- Tamaño elevado de las peticiones HTTP.
- Información volátil.



Modo Command and Control (C2):



- Modo de funcionamiento similar a un C2 (reflective DLL)
- Complejo y propenso a fallos
- Contenido elevado sólo en la carga, y más ligero en el resto de peticiones.
- Almacenamiento de módulos en variables de sesión (servidor)

Post-Exploitation with Kraken

profile_testing_php_linux_st.json

```
{
    "client" : {
        "url" : "http://localhost:8000/agent_st.php",
        "skip_ssl": false,
        "method" : "POST",
        "headers" : {
            "Host" : "localhost:8000",
            "User-Agent" : "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0"
        },
        "cookies" : {},
        "fields" : {},
        "message" : {
            "secret" : {
                "type" : "COOKIE",
                "key" : "X-Authorization",
                "value" : "P4ssw0rd!"
            },
            "data" : {
                "type" : "FIELD",
                "key" : "data"
            }
        }
    },
    "server" : {
        "type" : "FIELD",
        "key" : "data"
    }
}
```

- Encapsulación
- Autenticación con clave
- Cifrado simétrico

snappify.com

COMPONENTES DE KRAKEN

Dispatchers (resolución de tareas):

- **Default:** utilizado en módulos de ejecución directa o lógica simple.
  - ls, cd, cp, chmod, cat, whoami, ps, find, grep, mv…
- Usados para procesamiento simple de argumentos u otros parámetros.
  - execute, execute_with_token, powerpick, …
- Algunos que interactúan con el sistema de archivos local.
  - upload, download, reg_dump_trans, …
- Caso de lógica más compleja o multi-request.
  - tcpconnect

Compilers (and) Formaters:

- **Compilers:** encapsulan los módulos en función del ejecutor utilizado:
  - Código en raw (eval, CsharpCodeProvider)
  - Código compilado (ClassLoader, Assembly.Load, System.Reflection.Emit)
    - Compilación con contenedor de Docker (Java)
    - Compilación local con CSC (.NET)

- **Formaters:** procesan las respuestas de los módulos y les dan el formato adecuado.
  - Default, columns, columns_header, pspy

Post-Exploitation with Kraken

Post-Exploitation with Kraken

¡MUCHAS GRACIAS!

ESKERRIK ASKO!