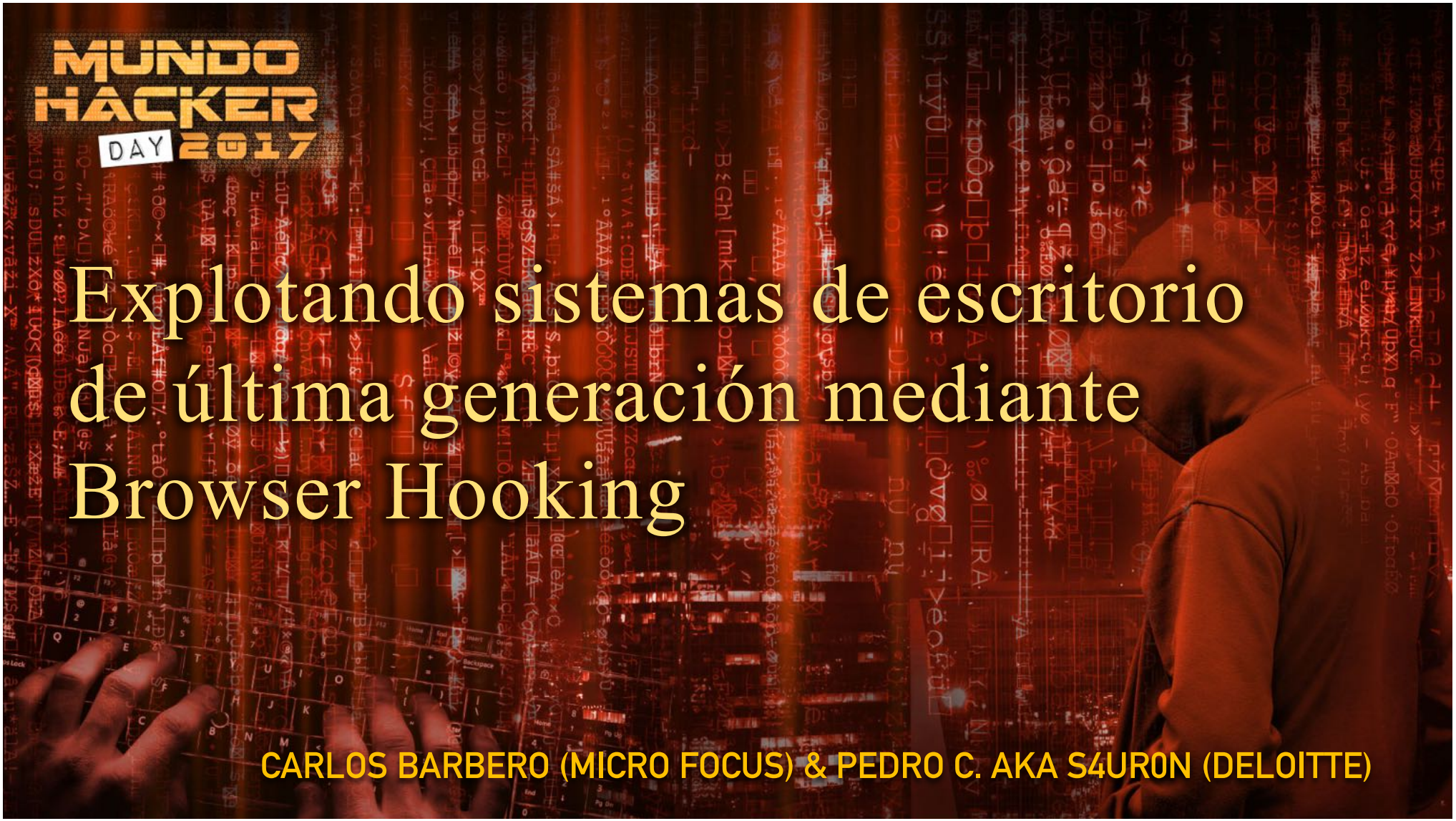


Explotando sistemas de escritorio de última generación mediante Browser Hooking

CARLOS BARBERO (MICRO FOCUS) & PEDRO C. AKA S4UR0N (DELOITTE)

Whoami

```
class PedroC:
    def __init__(self):
        self.name =     'Pedro Candel'
        self.role =     'Deloitte CyberSOC Academy'
        self.email =    'pcandel@cybersoc.deloitte.es'
        self.nickname = '@NN2ed_s4ur0n'
        self.website =  'https://s4ur0n.com'
        self.interest = [ 'Malware', 'RE', 'Exploiting', 'Offensive Security' ]
        self.member_of = [ 'mlw.re', 'OWASP', 'NetXploit', '...' ]
```

Deloitte. CyberSOC Academy

Whoami

Carlos A. Barbero Muñoz (@Nevnaur)

Identity, Access and Security - Sales Engineer

MundoHacker Team, colaborador en Radio y TV

Libros de seguridad informática y hacking ético

Pr0n Cheerleader

¿Qué es BeEF?

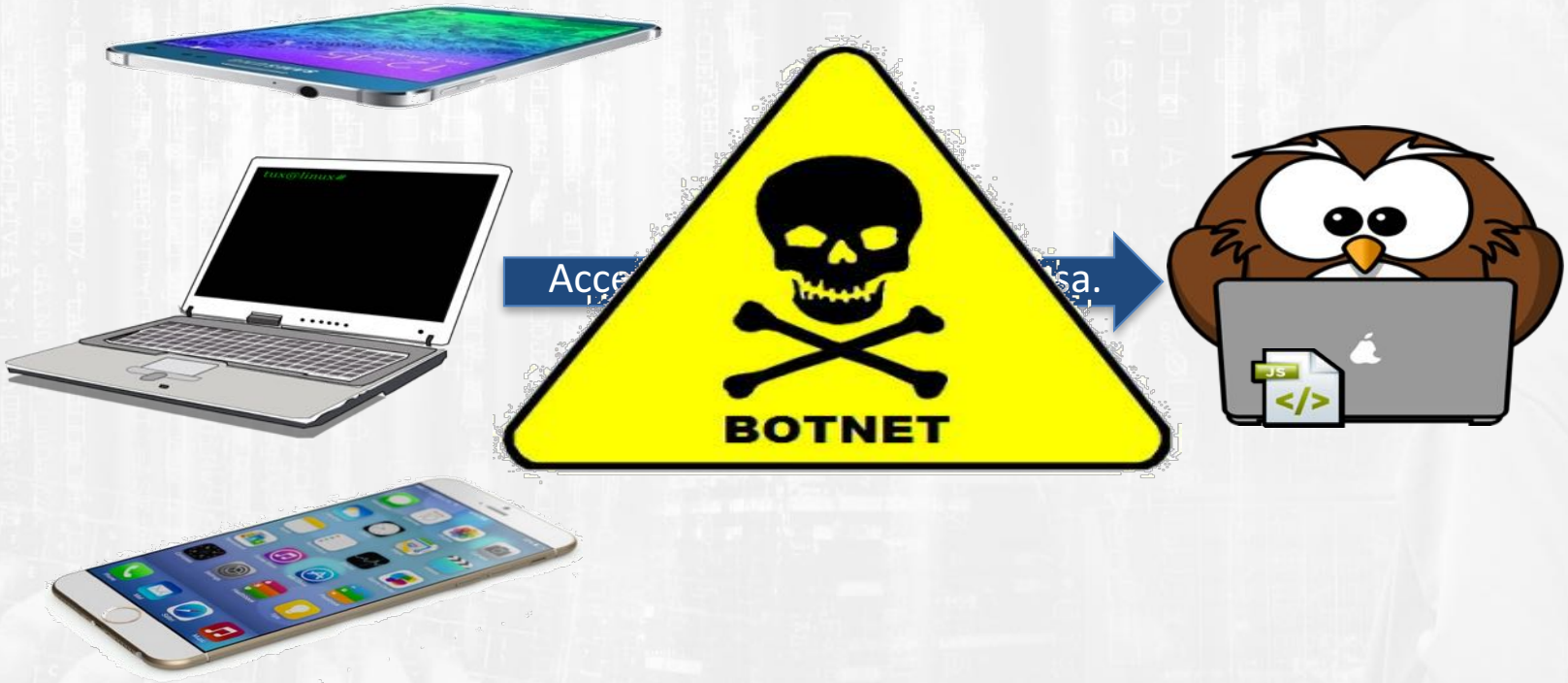
- **Beef project** **(The browser exploitation framework)**
- http://beefproject.com
- Framework de pentesting, que permite desafiar la seguridad de los navegadores.
- Software de acceso publico, que permite realizar **acciones maliciosas "a medida"** en navegadores.
- Se incluye en Kali Linux out of the box.

Algunas características…

- Infección **últimas versiones de iOS** (iPhone, iPad).
- Infección de las **últimas versiones de Android**.
- Infección de **navegadores en sus últimas versiones**. (Internet Explorer, Chrome, Firefox, Opera, Safari…).
- Ejecución **"silenciosa"** de un **fichero en javascript** (hook.js) al visitar la página web maliciosa.
- **Persistencia** con una "**cookie**" (BEEFHOOK).
- Utiliza un equipo infectado como un Proxy.

Mecanismos clásicos de infección…

Funcionamiento de la herramienta.



Man in the Browser: escenarios típicos

Panel de control Web de BeEF.

Category: Browser (7 Items)

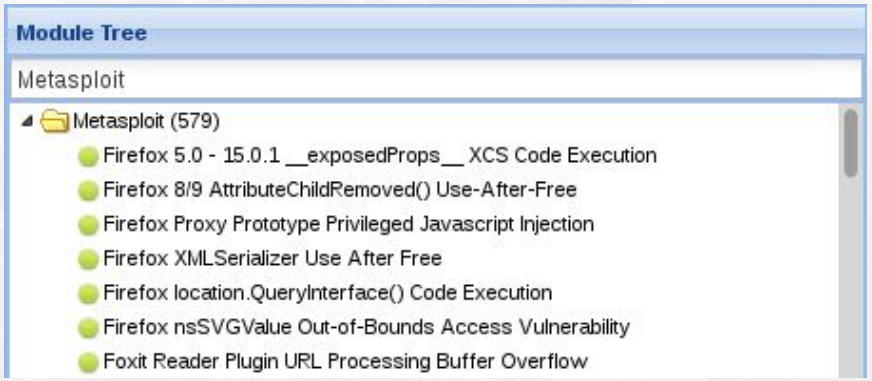
Browser Name: Firefox
Browser Version: 18
Browser UA String: Mozilla/5.0 (X11; Linux x86_64; rv:18.0) Gecko/20100101 Firefox/18.0
Browser Language: en-US
Browser Platform: Linux x86_64
Browser Plugins: GNOME Shell Integration-v.,IcedTea-Web Plugin (using IcedTea-Web 1.6.2 (1.6.2-3))-v.
Window Size: Width: 1661, Height: 1214

Category: Browser Components (12 Items)

Flash: Yes
VBScript: No
PhoneGap: No
Google Gears: No
Web Sockets: Yes
QuickTime: No
RealPlayer: No
Windows Media Player: No

Integración con metasploit®

- Permite utilizar los exploits de metasploit desde la interfaz web de BeEF.
- Si no quieres complicarte… también funciona con un Iframe y Browser Autopwn.

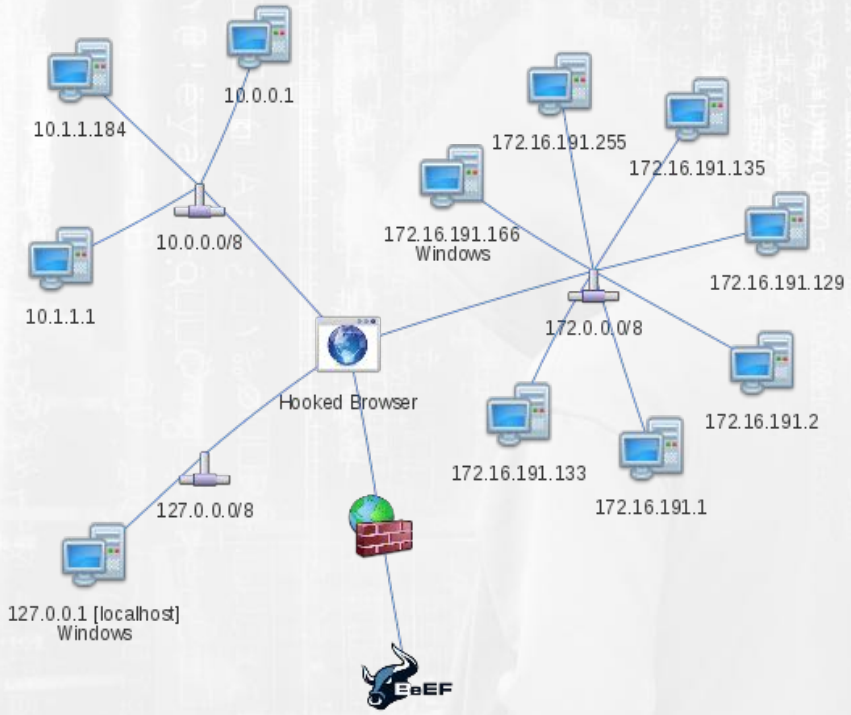


Análisis de la red del equipo infectado.

Details | Logs | Commands | Rider | XssRays | Ipec | **Network** | WebRTC

Map | Hosts | **Services**

IP Address	Port	Protocol	Type
10.1.1.1	80	http	HTTP Server
10.1.1.184	80	http	HTTP Server (CORS)
10.1.1.184	8080	http	HTTP Server (CORS)
10.1.1.184	80	http	HTTP Server
10.1.1.184	8080	http	HTTP Server
172.16.191.129	80	http	Apache
172.16.191.129	80	http	Apache 2.x
172.16.191.133	80	http	HTTP Server (Flash)
172.16.191.133	80	http	Apache
172.16.191.133	80	http	Apache 2.x

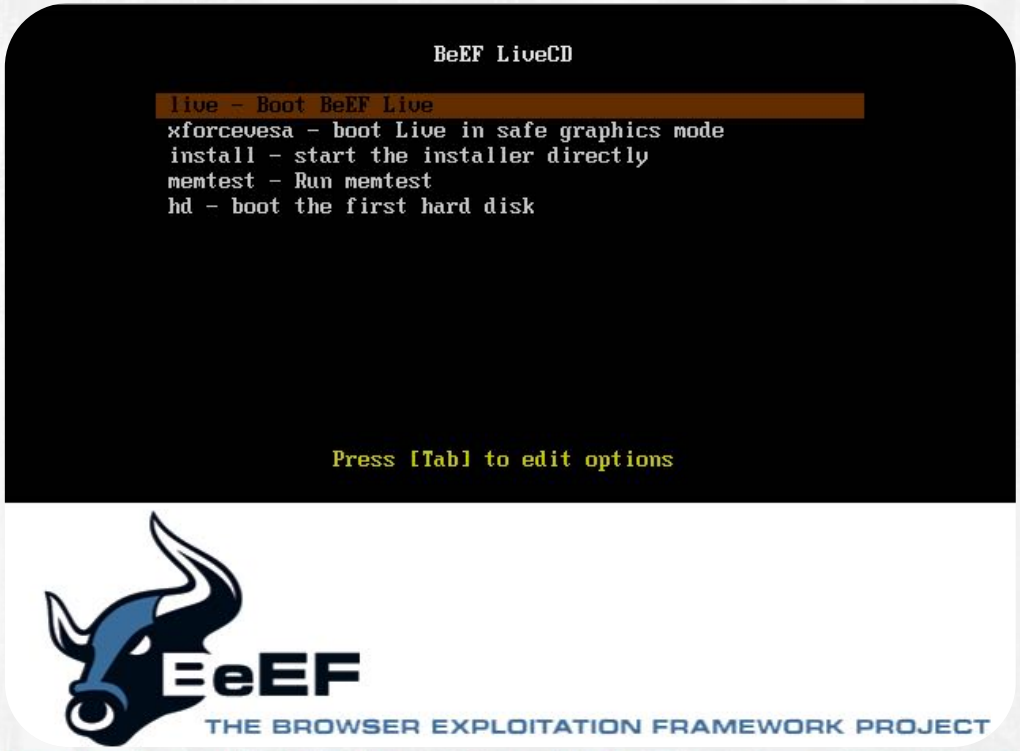


Automatización de tareas.

- Es posible definir una serie de tareas que se realizaran de forma automática cuando un usuario sea hookeado.
- Editando el fichero autorun.rb es posible definir los módulos que se ejecutaran de forma automática.

```
24  $stdout.sync = true
25  # RESTful API root endpoints
26  ATTACK_DOMAIN = "127.0.0.1"
27  RESTAPI_HOOKS = "http://" + ATTACK_DOMAIN + ":3000/api/hooks"
28  RESTAPI_LOGS = "http://" + ATTACK_DOMAIN + ":3000/api/logs"
29  RESTAPI_MODULES = "http://" + ATTACK_DOMAIN + ":3000/api/modules"
30  RESTAPI_ADMIN = "http://" + ATTACK_DOMAIN + ":3000/api/admin"
31
32  BEEF_USER = "beef"
33  BEEF_PASSWD = "beef"
```

BeEF Live CD

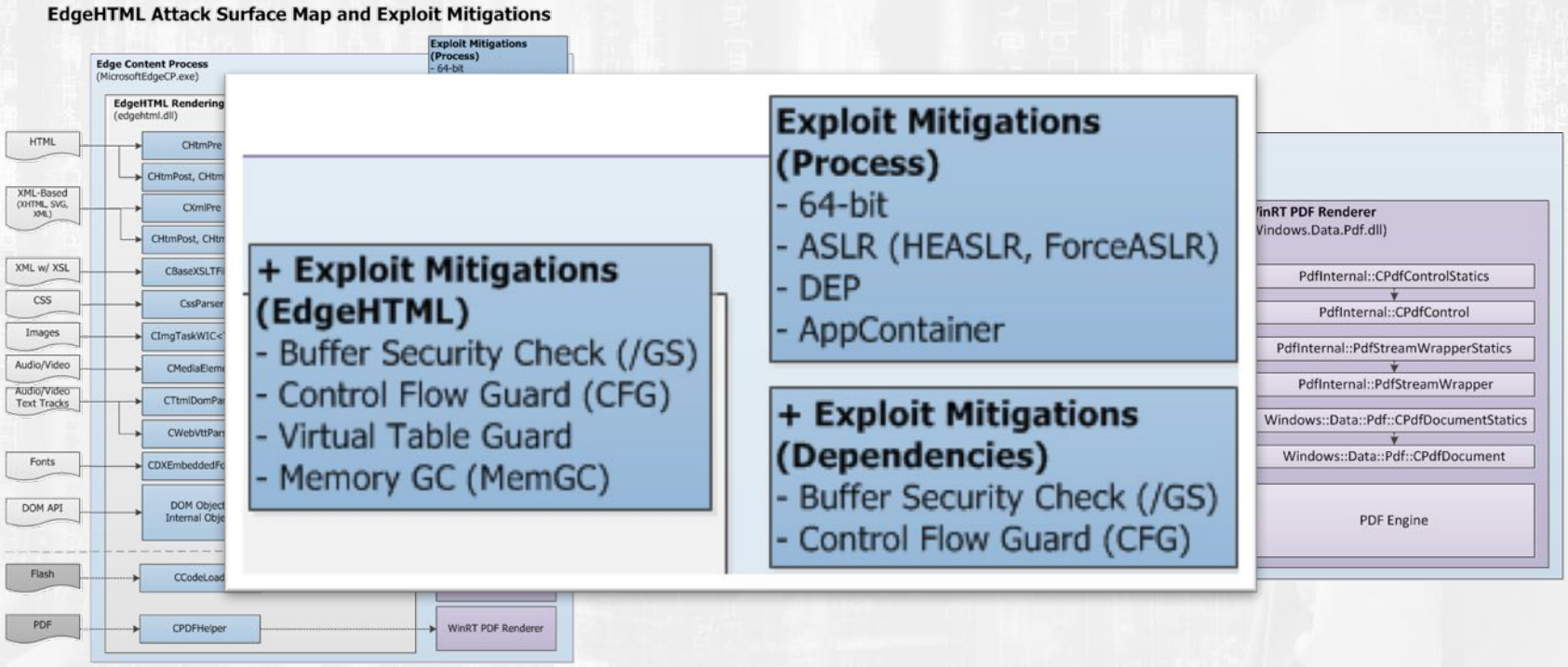

BeEF LiveCD
live - Boot BeEF Live
xforcevesa - boot Live in safe graphics mode
install - start the installer directly
memtest - Run memtest
hd - boot the first hard disk
Press [Tab] to edit options
BeEF
THE BROWSER EXPLOITATION FRAMEWORK PROJECT


DEMO

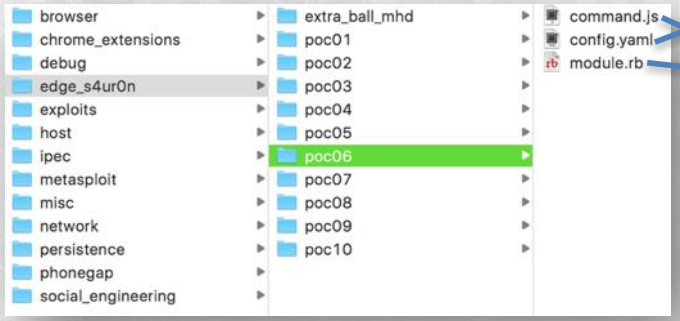
Disclaimer

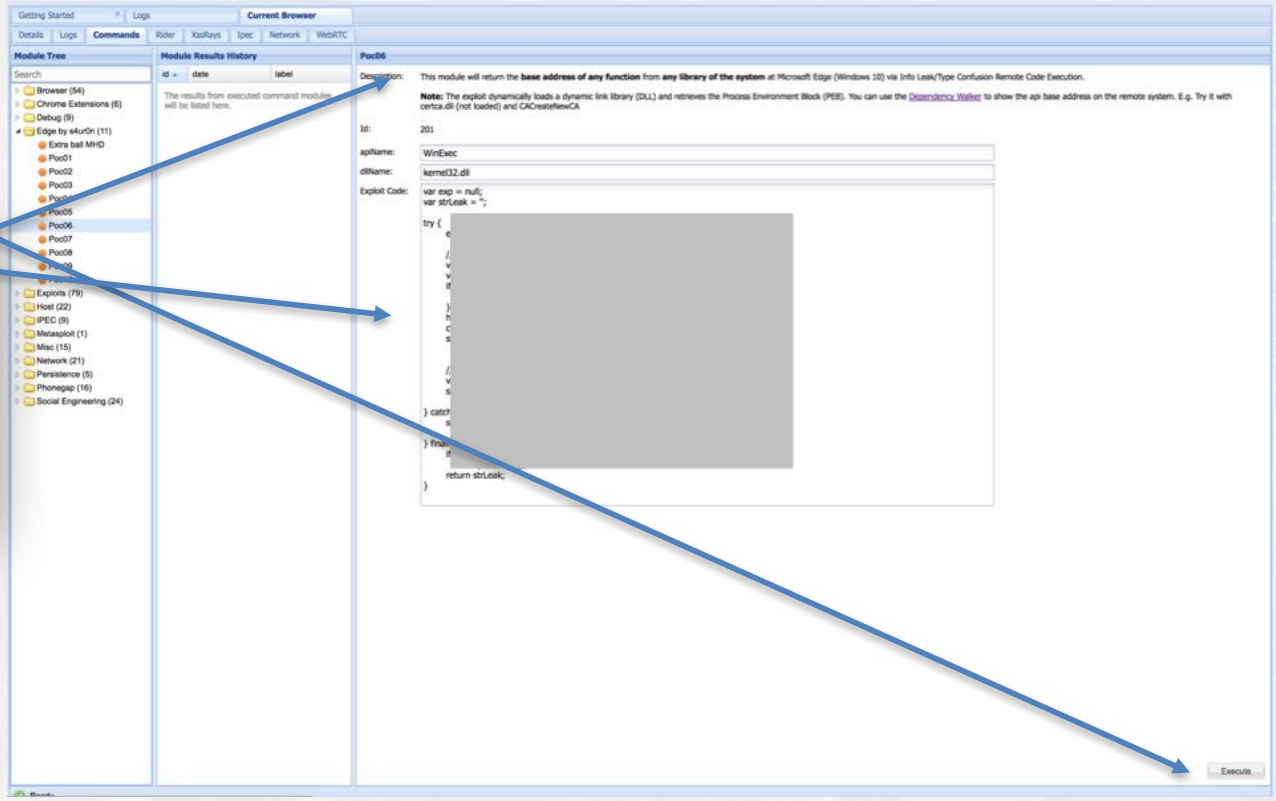

urchase Technology
ara: s4ur0n@s4ur0n.com,
esponder a: Vulntech
ello, S4uron, I`m interested in purchasing 0day ex
ooking forward to your reply.
egards,
oman.
you have interest to sell it?
itter: @vulntech2
ternative Email: vulntech2@vulntech.com
portant: We purchase products strictly in research purposes. As we do not understand th
olations of law from your side.
All of our actions are conforming to the local law and we are not responsible for
they see me trollin'
they hatin'

Security enhancements for Microsoft Edge



Beef Modules






DEMO

Thanks


EXTRA BALL
LIT


MUCHAS GRACIAS POR
VUESTRA ATENCIÓN
memegen.es