CYBERGUARD

INTEGRAL · INFORMATION · IMPROVEMENT

aces
ASSOCIACIÓ CATALANA
D'ENTITATS DE SALUT

CIBERSEGURETAT
una recomanació del nou reglament

¿Què cal fer si som víctimes d'un robatori d'informació?

Classificació de vulnerabilitats:

Atacs
d'origen extern

Atacs
d'origen interns

Riscos associats
al mal ús

Hola!

Joel Gámez

Director tècnic de CYBERGUARD

info@cyberguard.es

Escenari actual del món de la ciberdelinqüència

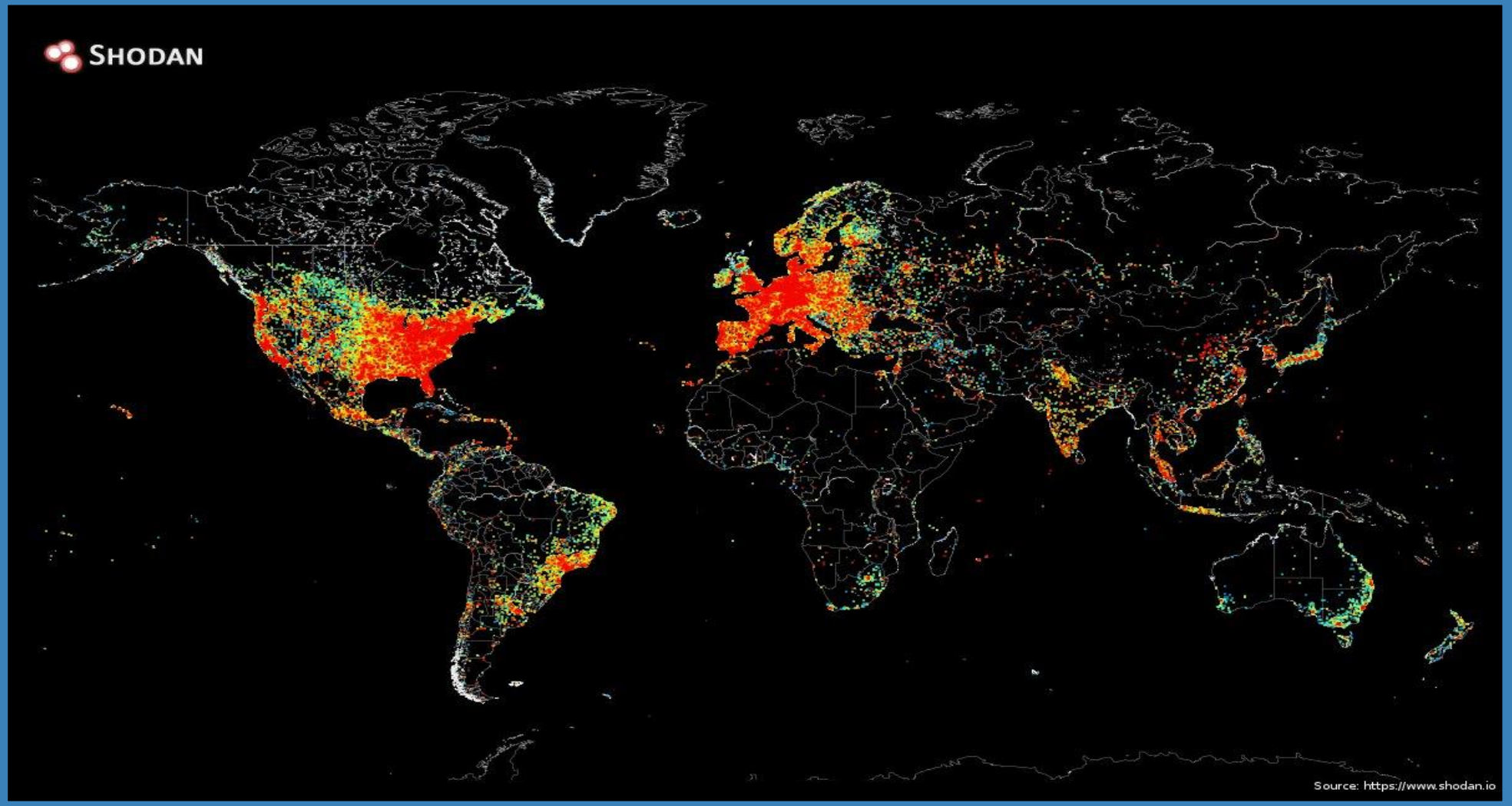
Introducció a l'automatització de processos fets servir pels cibercriminals

Atacs massius a servidors d'accés públic amb Shodan, Censys o Zoomeye

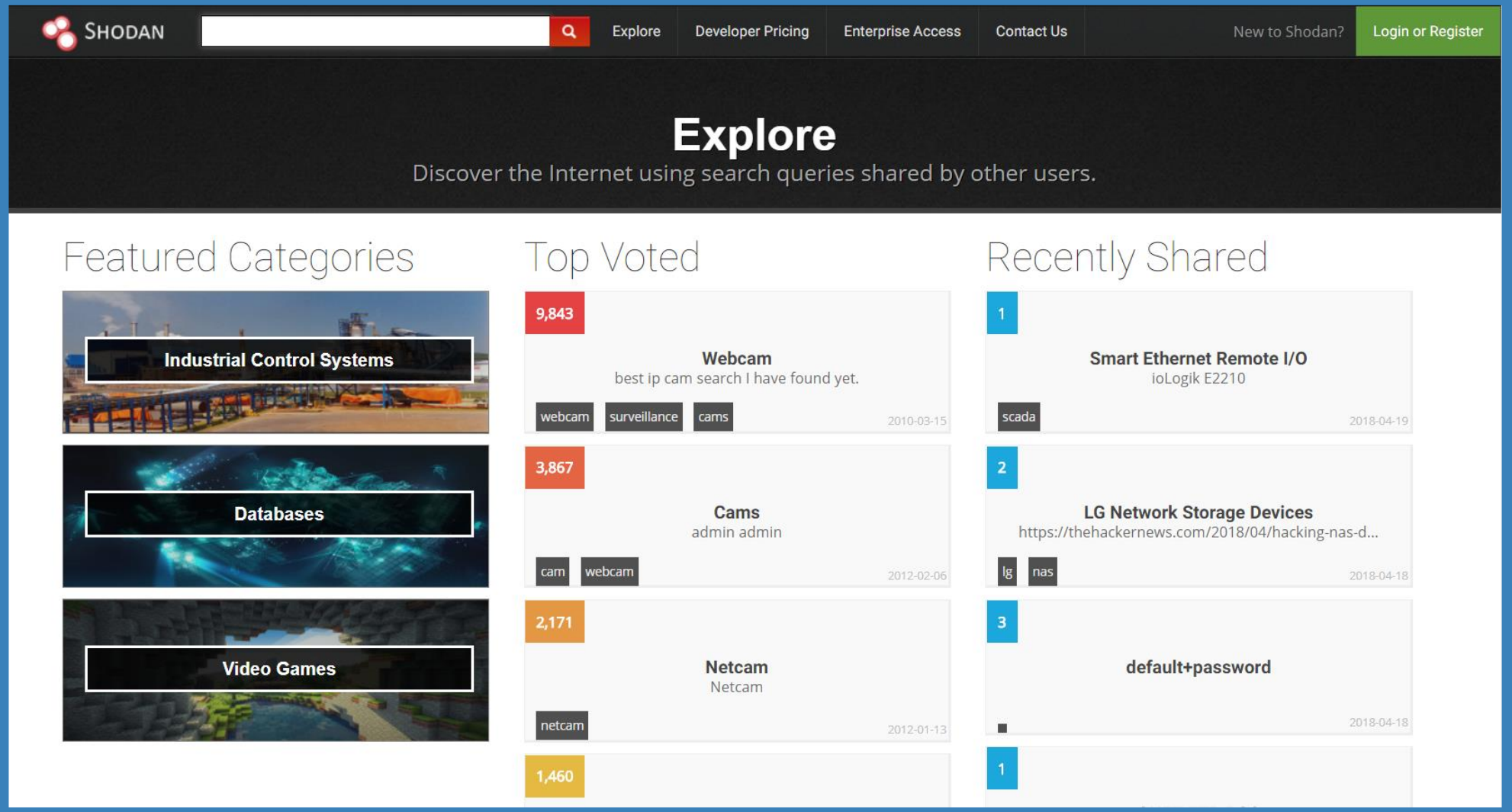
Atacs dirigits o focalitzats (SpearPhising)

Infraestructures de Ransomware

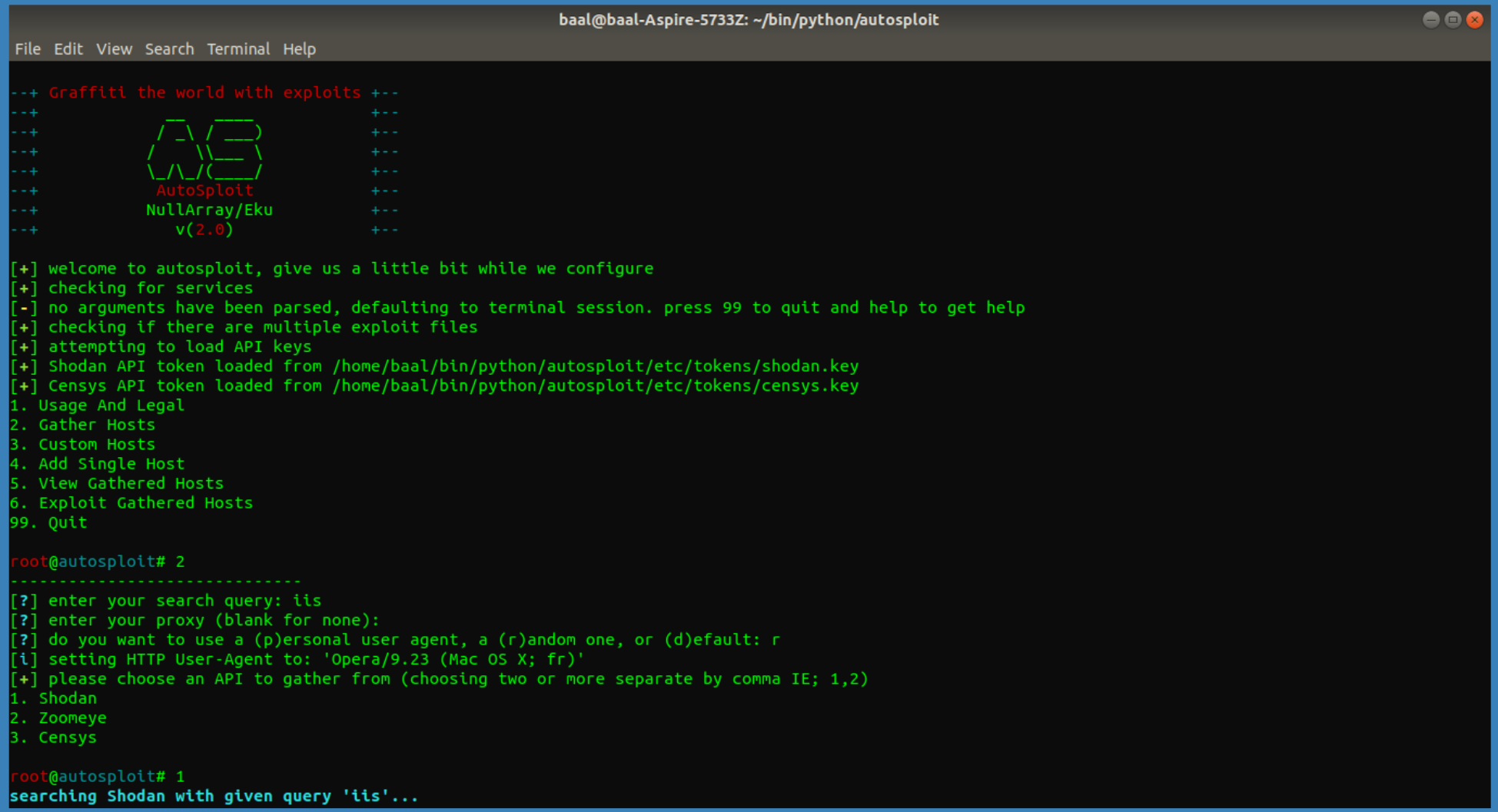
Atacs massius a servidors d'accés públic



Atacs massius a servidors d'accés públic



Atacs massius a servidors d'accés públic



Atacs dirigits o focalitzats (SpearPishing)

Atacs dirigits o focalitzats (SpearPishing)

Atacs dirigits o focalitzats (SpearPishing)

Infraestructures de Ransomware

Infraestructures de Ransomware

WannaCry

WannaCry, también conocido como **WanaCrypt0r 2.0**,[1] es un *programa dañino* de tipo *ransomware*.

Índice [ocultar]

Ciberataque global [editar]

El 12 de mayo de 2017 entre las 8 y las 17:08 horas UTC[2] se registró un ataque a escala mundial que afectó a las empresas Telefónica, Iberdrola y Gas Natural, entre otras compañías en España,[3] así como al servicio de salud británico, como confirmó el Centro Nacional de Inteligencia.[4 5 6 7 8] La prensa digital informaba aquel día que al menos 141 000 computadores habían sido atacados en todo el mundo.[9 10 11]

Los expertos sostienen que WannaCry usó la vulnerabilidad EternalBlue, desarrollada por la Agencia de Seguridad Nacional estadounidense y filtrada por el grupo The Shadow Brokers, que permite atacar computadores con el sistema operativo Microsoft Windows[1] no actualizados debidamente. La compañía Microsoft había comenzado a distribuir actualizaciones de seguridad al día siguiente de conocerse esta vulnerabilidad, el 10 de marzo de 2017,[12] a través de Windows Update, pero sólamente para las versiones de Windows posteriores a Windows Vista. El 13 de mayo de 2017, ante la supuesta gravedad del ataque, publicó un parche separado para Windows 8, Server 2003 y XP.[13] Muchos computadores que no tenían aplicadas las actualizaciones de seguridad MS17-010 de marzo de 2017 quedaron gravemente afectados,[10] con sus archivos cifrados y mostrando un mensaje en pantalla que exigía un rescate de 300 dólares en bitcoins a cambio de descifrar los archivos.

En realidad, un experto de Reino Unido evitó en gran medida la expansión del ciberataque global. El autor del blog MalwareTech estaba estudiando el programa dañino cuando se dio cuenta de que el mismo intentaba conectarse a un dominio no registrado: si no lo lograba, cifraba el equipo; si lo lograba, se detenía.[2] Una vez que este experto en seguridad registró el dominio, a las 17:08 UTC del 12 de mayo, cesó el ataque. Todas las medidas urgentes que se tomaron a partir de esa hora fueron prácticamente innecesarias.

Un análisis del *malware* ha sido publicado por Microsoft.[14]

WannaCry

Países afectados por el ciberataque.

Información	
Nombre técnico	WanaCrypt0r 2.0
Alias	Wannadecryptor
Clasificación	Gusano informático
Tipo	ransomware
Sistema operativo	Windows XP, Windows 7, Windows 8.1, Windows 10 y Windows Server 2008

[editar datos en Wikidata]

Atacs, infeccions i vulnerabilitats més comunes

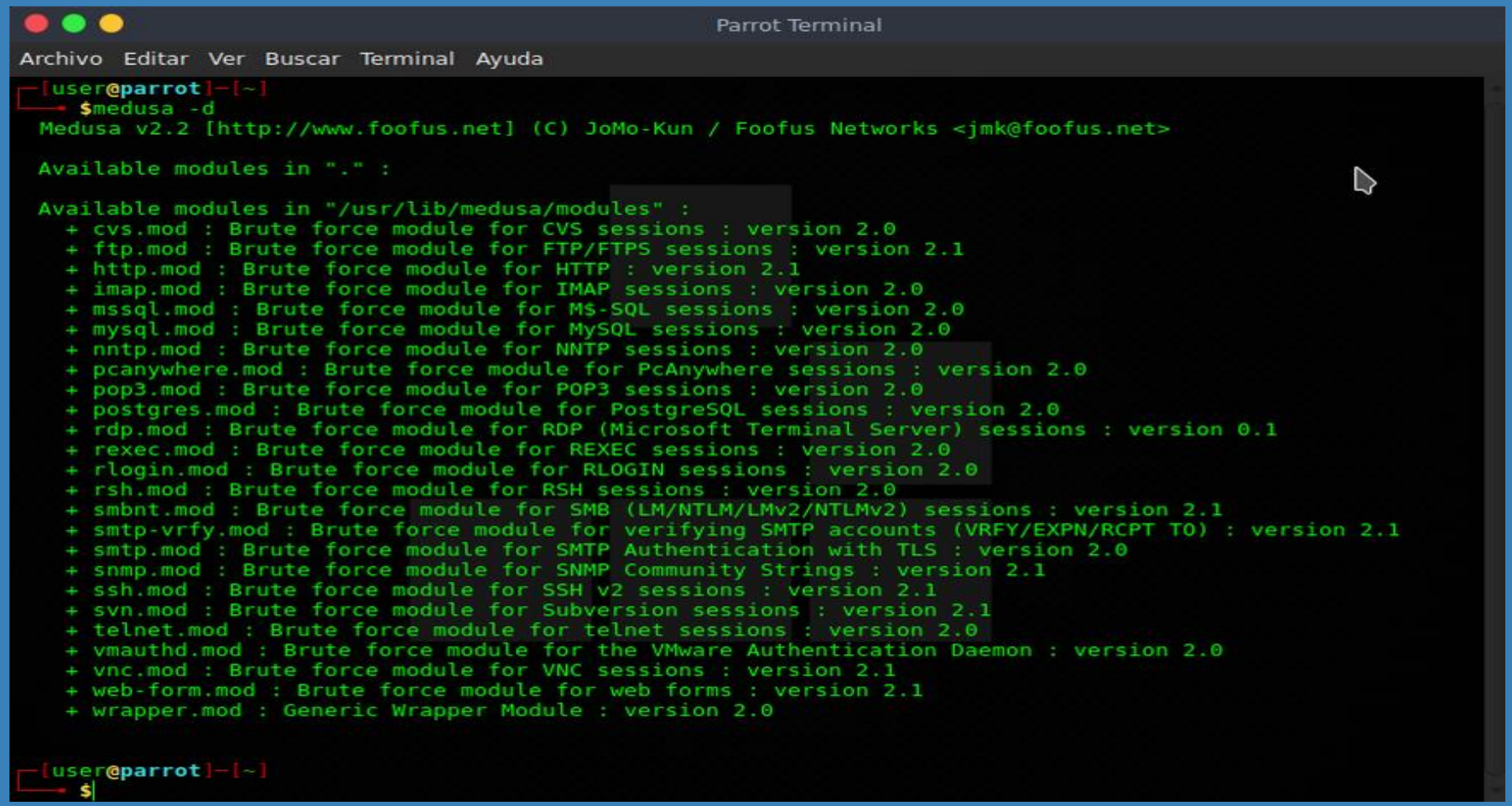
Atacs externs per força bruta i malware

Atacs interns a través de xarxes sense fils, backdoors i eines de hacking

Exfiltració i mala praxis d'us de les dades

Atacs externs per força bruta, malware i vulnerabilitats web

Atacs externs per força bruta, malware i vulnerabilitats web



Atacs externs per força bruta, malware i vulnerabilitats web

Atacs externs per força bruta i malware

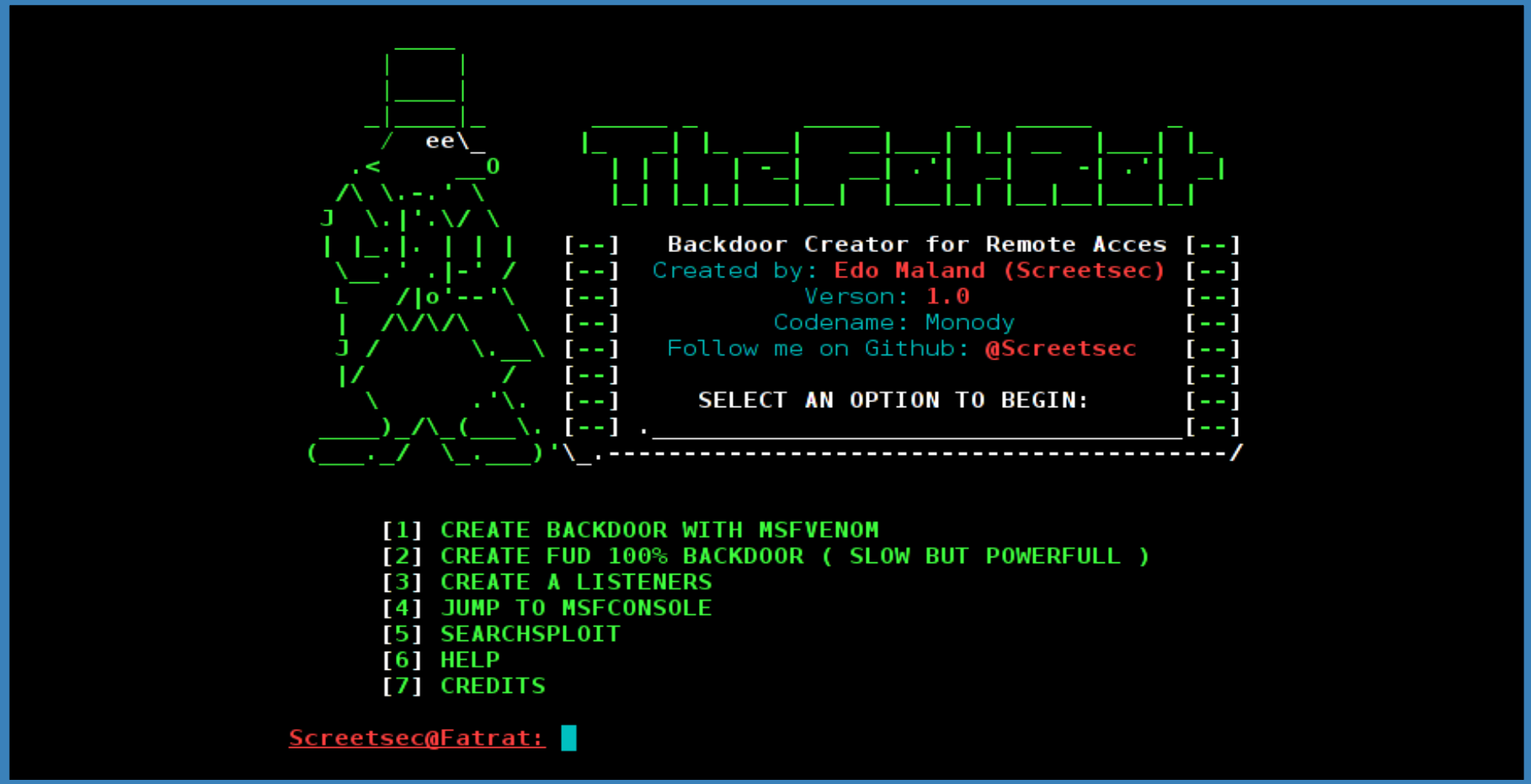
Atacs interns a través de xarxes sense fils, backdoors i eines de hacking

Atacs interns a través de xarxes sense fils, backdoors i eines de hacking

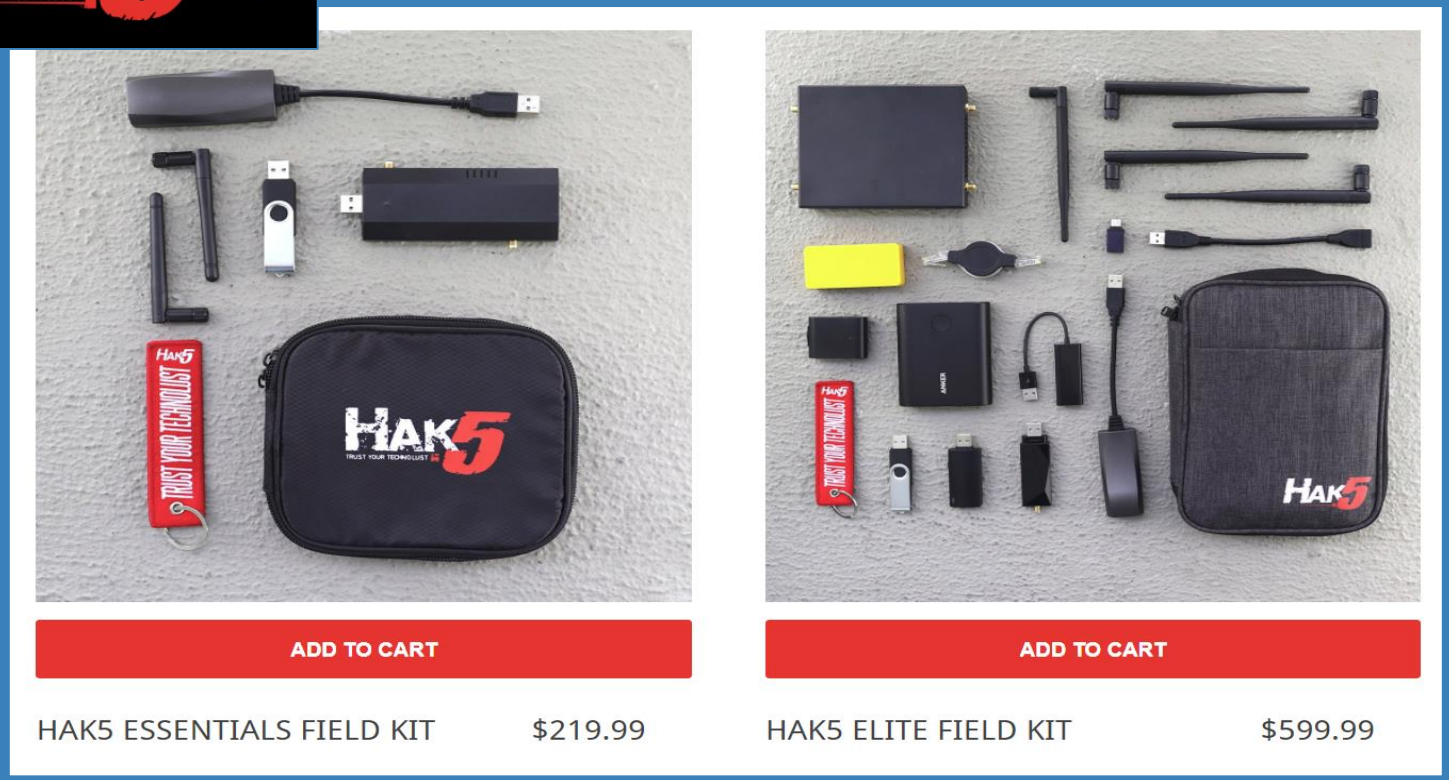
Atacs interns a través de xarxes sense fils, backdoors i eines de hacking

Atacs interns a través de xarxes sense fils, backdoors i eines de hacking

Atacs interns a través de xarxes sense fils, backdoors i eines de hacking



Atacs interns a través de xarxes sense fils, backdoors i eines de hacking



Exfiltració i mala praxis d'us de les dades

Copia de dades en dispositius externs

Enviament d'informació per correu electrónic

Enviament informació per altres medis
(WeTransfer, Dropbox o Google Drive)

Dramatització i recreació de les tècniques aquí descrites

Primera passa...

AUDITAR

Segona passa...
ACTUAR

Tercera passa...
MANTENIR/ACTUALITZAR

Firewall

Atacs
d'origen extern

Atacs
d'origen interns

Riscos associats
al mal ús

IPS
Intercept X
XG Firewall

Aturi les amenaces a la porta

- ✓ Aturi el malware i el ransomware.
- ✓ Aturi els atacs de robatori de dades al perímetre de la xarxa.

Secure WiFi
User & APP Control

Aconsegueixi conexions Wifi segures

- ✓ Wireless gestionat per dispositiu.
- ✓ Polítiques de seguretat sobre els dispositius d'enmagatzement extern.

DLP
Email Appliance
Central Device Encryption

Aturi els errors humans

- ✓ Bloquegi i xifri les dades confidencials als correus.
- ✓ Asseguris de que només les persones autoritzades puguin accedir als arxius confidencials.
- ✓ Mantingui les seves dades protegides si perd els seus dispositius o els hi roben.

Manteniment proactiu i periòdic

- ✓ Actualització dels sistemes de seguretat.
- ✓ Manteniment proactiu dels sistemes.

La nostra oferta de seguretat informàtica per empreses

SOL·LUCIÓ INTEGRAL DE SEGURETAT INFORMÀTICA

1- AUDITORIA INFORMÀTICA BÀSICA DE SEGURETAT

- Per detectar les principals debilitats i amenaces.

inclòs en el preu*

* Possibilitat de realitzar auditories més profundes i presonalitzades. Demana'ns me´s informació.

2- IMPLANTACIÓ FIREWALL I SOLUCIONS DE SEGURETAT

- IPS: Sistema de prevenció d'intrusions.
- Protecció contra amenaces avançades.
- DLP: Protecció contra la filtració de dades.
- Xifrat SPX: Enviament segur de correu electrònic.

desde 1.495 €

3- MANTENIMENT PROACTIU I PERIÒDIC

- Actualització dels sistemes de seguretat.
- Manteniment proactiu dels sistemes.

desde 49 € / mes

CYBERGUARD

INTEGRAL · INFORMATION · IMPROVEMENT

Gràcies!

+34 93 159 59 05
info@cyberguard.es
www.cyberguard.es