2023

Hackeando la Dark Web con Neo4j

Ahí no hay cuchara, solo nodos…

Alfredo Abarca

CDMX 2023

BSIDES CDMX

> whoami _

ALFREDO ABARCA

@aabarcab

- **Dev/Endpoint Security Manager/Purple Team Player/Ciberinteligencia**
- **SecOps Manager**

- **Old School Gamer**

BSIDES CDMX

AGENDA

- Contexto de la investigación
- Metodología de trabajo
- Resultados
- Análisis de la información
- Integración de Neo4j
- DEMO (Poniendo todo Junto)

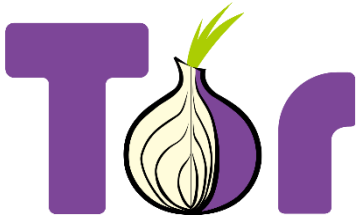
Hackeando la Dark Web con Neo4j

Ahí no hay cuchara, solo nodos…

BSIDES CDMX

Hackeando la Dark Web con Neo4j

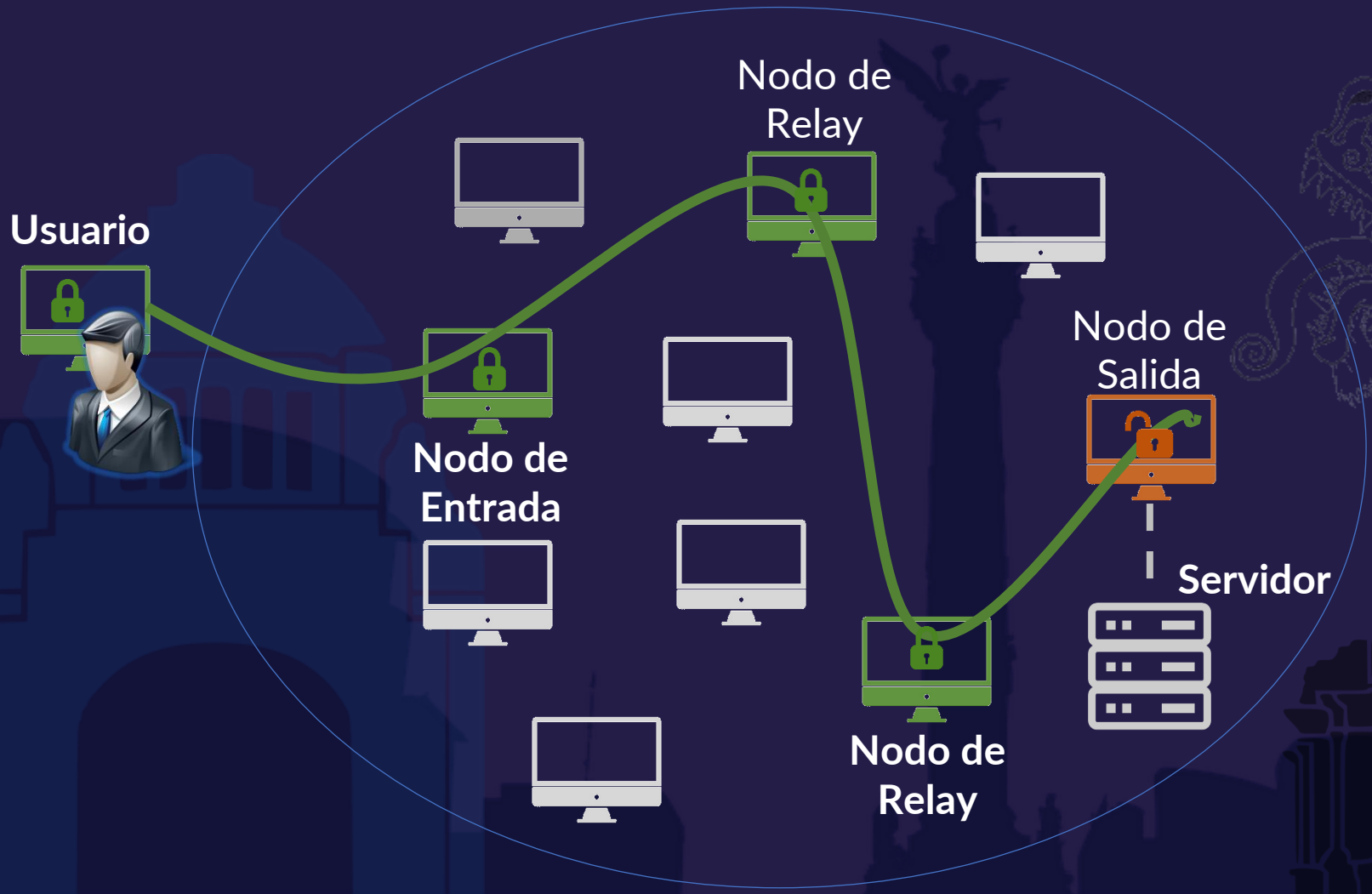
Ahí no hay cuchara, solo nodos…

			
The Onion Router	Invisible Internet Project	ZeroNet	Freenet
• Los datos son enrutados a través de nodos conocidos como relays. • Es posible publicar accesos de forma híbrida. • El anonimato se da por medio de servidores proxy o nodos de entrada.	• Una red que basa su anonimato a través de redes peer to peer (P2P). • El ruteo se realiza por medio de túneles unidireccionales. • Lenta transferencia de datos por diseño.	• El contenido de un sitio se ofrece de forma descentralizada y basándose en redes P2P. (BitTorrent) • Para anonimato emplean TOR.	• Los usuarios comparten porciones de su ancho de banda y almacenamiento. • Las redes son comunidades de redes “amigas” y por medio de P2P.
https://www.torproject.org	https://geti2p.net/en/	https://zeronet.io/	https://freenetproject.org

Hackeando la Dark Web con Neo4j

Ahí no hay cuchara, solo nodos…

¿Cómo funciona la red TOR?



Un servicio oculto es un sitio web u otro tipo de servicio (ftp, smtp, irc, etc…) que utiliza la tecnología de TOR para dar cierto nivel de anonimato y ….. Seguridad?

Hackeando la Dark Web con Neo4j

Ahí no hay cuchara, solo nodos…

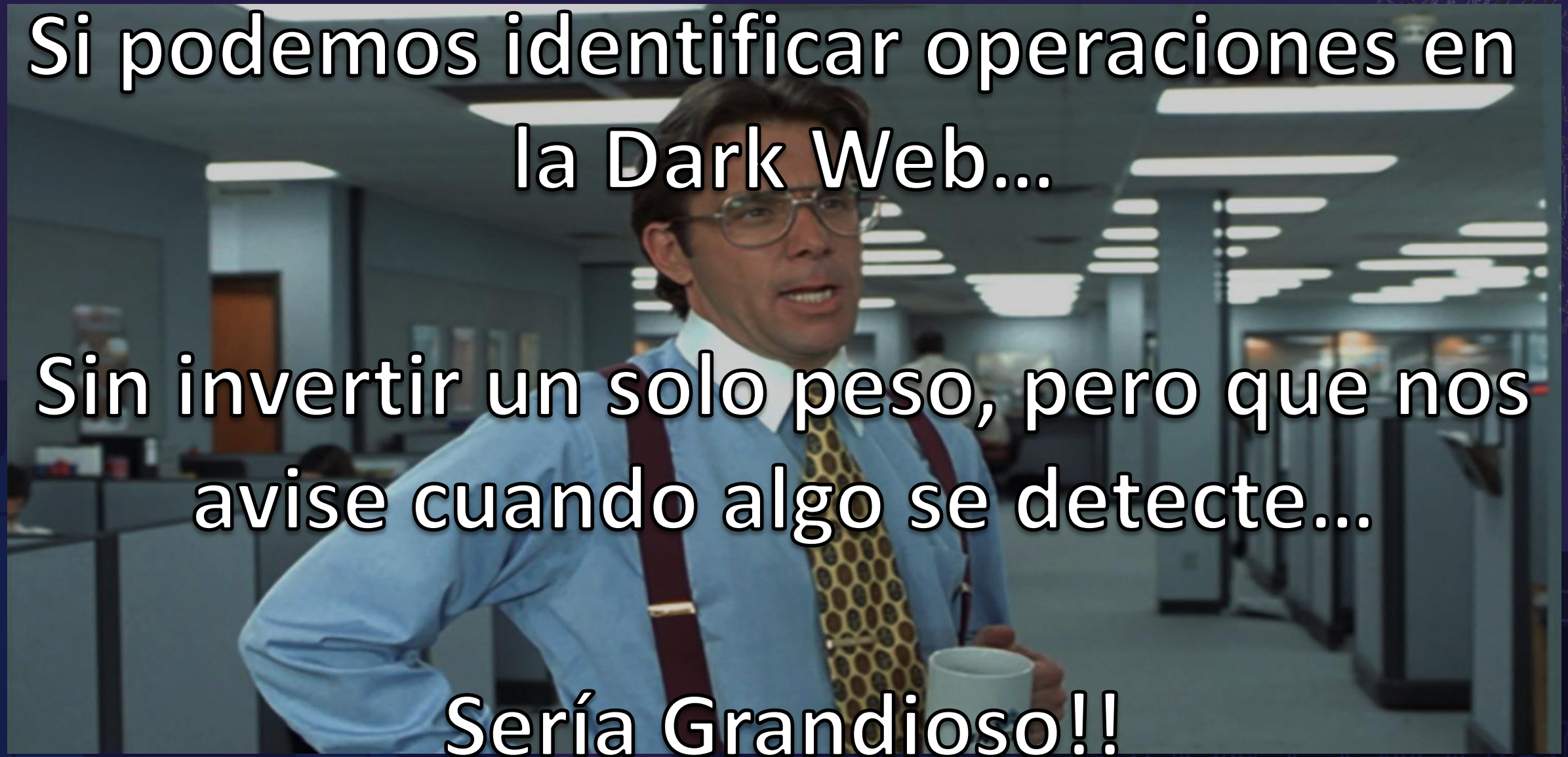
- No existe una relación de IP-Dominio.
- No hay una Base de datos de los dominios existentes.
- No hay una forma simple de realizar la identificación de dominios.

VS

DARK WEB

- Existen una relación de IP-Dominio-ASN
- Existe un registro de Dominios con algún proveedor.
- Diversas bases de datos de reputación.
- Mayores controles de vigilancia y regulación.

CLEAR WEB

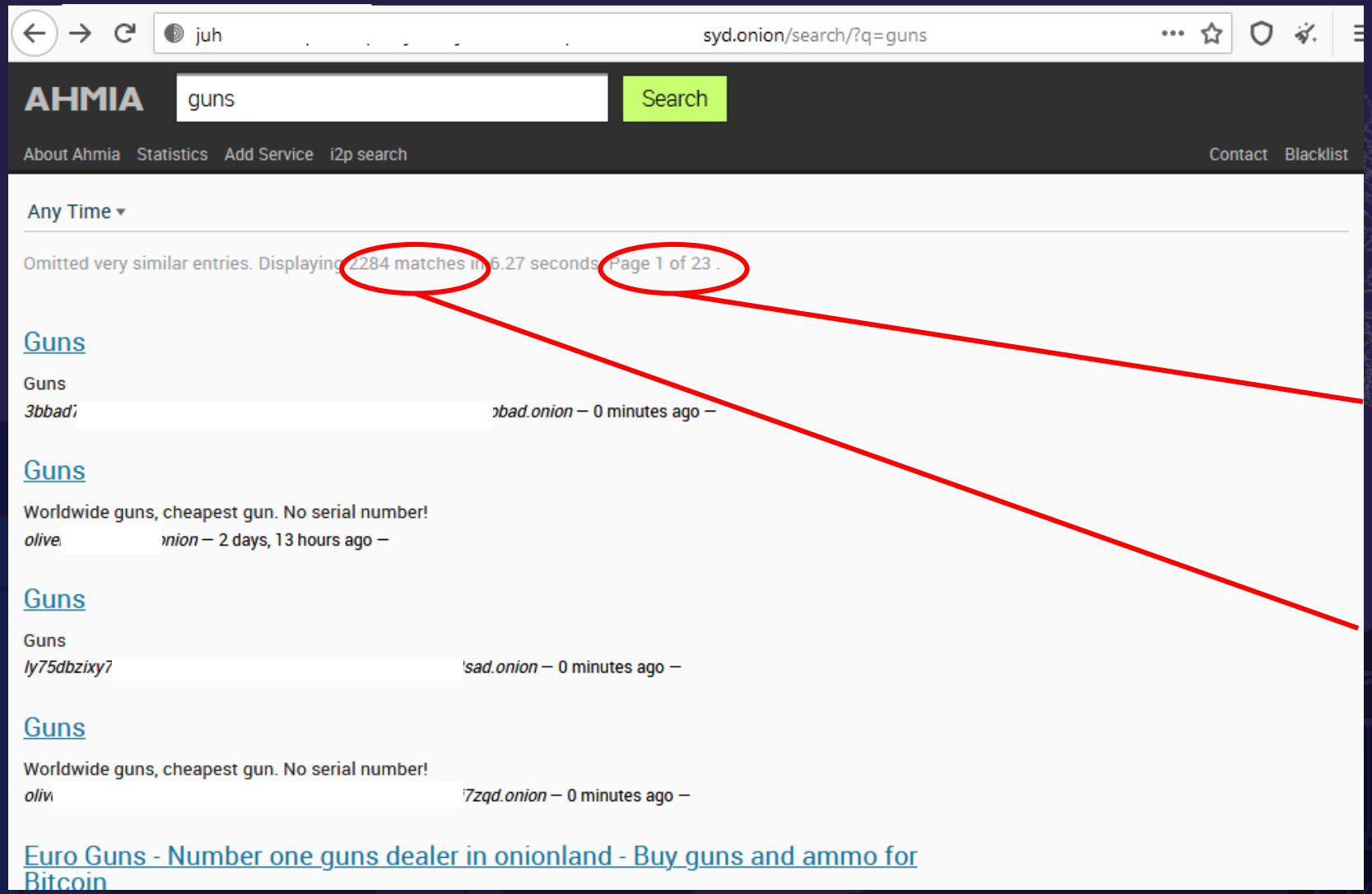

Si podemos identificar operaciones en la Dark Web…
Sin invertir un solo peso, pero que nos avise cuando algo se detecte…
Sería Grandioso!!

Hackeando la Dark Web con Neo4j

Ahí no hay cuchara, solo nodos…

Hackeando la Dark Web con Neo4j

Ahí no hay cuchara, solo nodos…



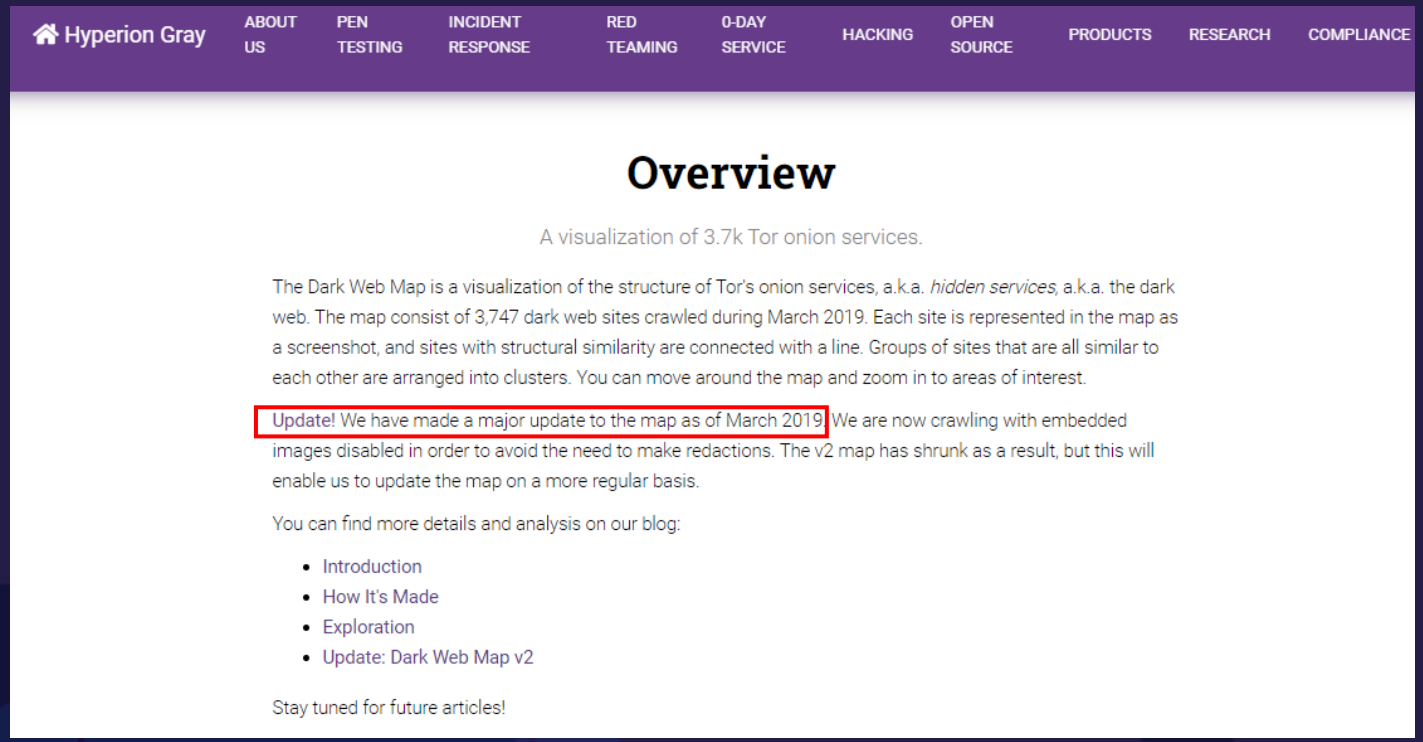
Son buenos pero…

- Muchos resultados
- Salida no procesable de forma simple.

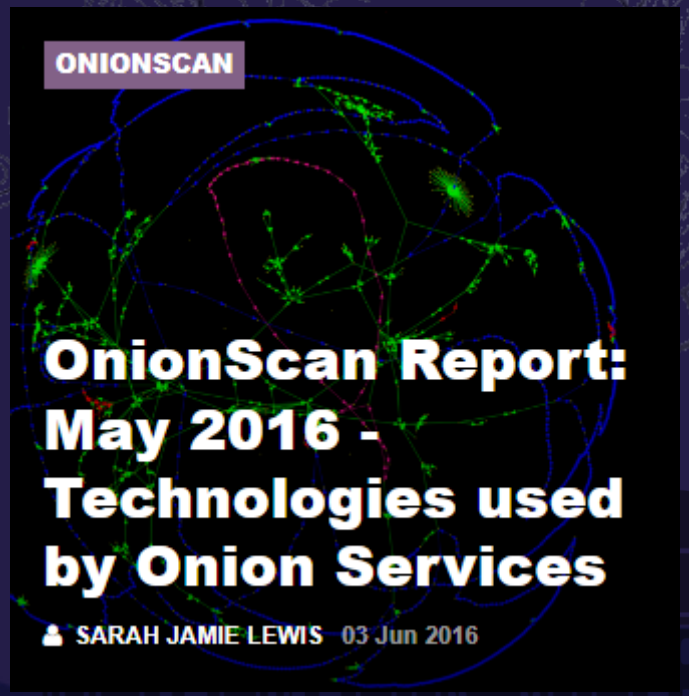
- Un solo buscador no tiene todo el contenido indexado.
- Existen buscadores con contenido focalizado.
- Ligas a sitios no existentes o inservibles.

Hackeando la Dark Web con Neo4j

Ahí no hay cuchara, solo nodos…



Hyperion Gray – Dark Web Map
https://www.hyperiongray.com/dark-web-map



Onion Scan Report
https://mascherari.press/onionscan-report-may-2016-technologies-used-by-onion-services/

Hackeando la Dark Web con Neo4j

Ahí no hay cuchara, solo nodos…

SPLASH SERVER

Es una utilería que nos permite de manera desatendida obtener el contenido de una página web, así como un screenshot de su home page.

https://splash.readthedocs.io/en/stable/api.html

PAGE COMPARE

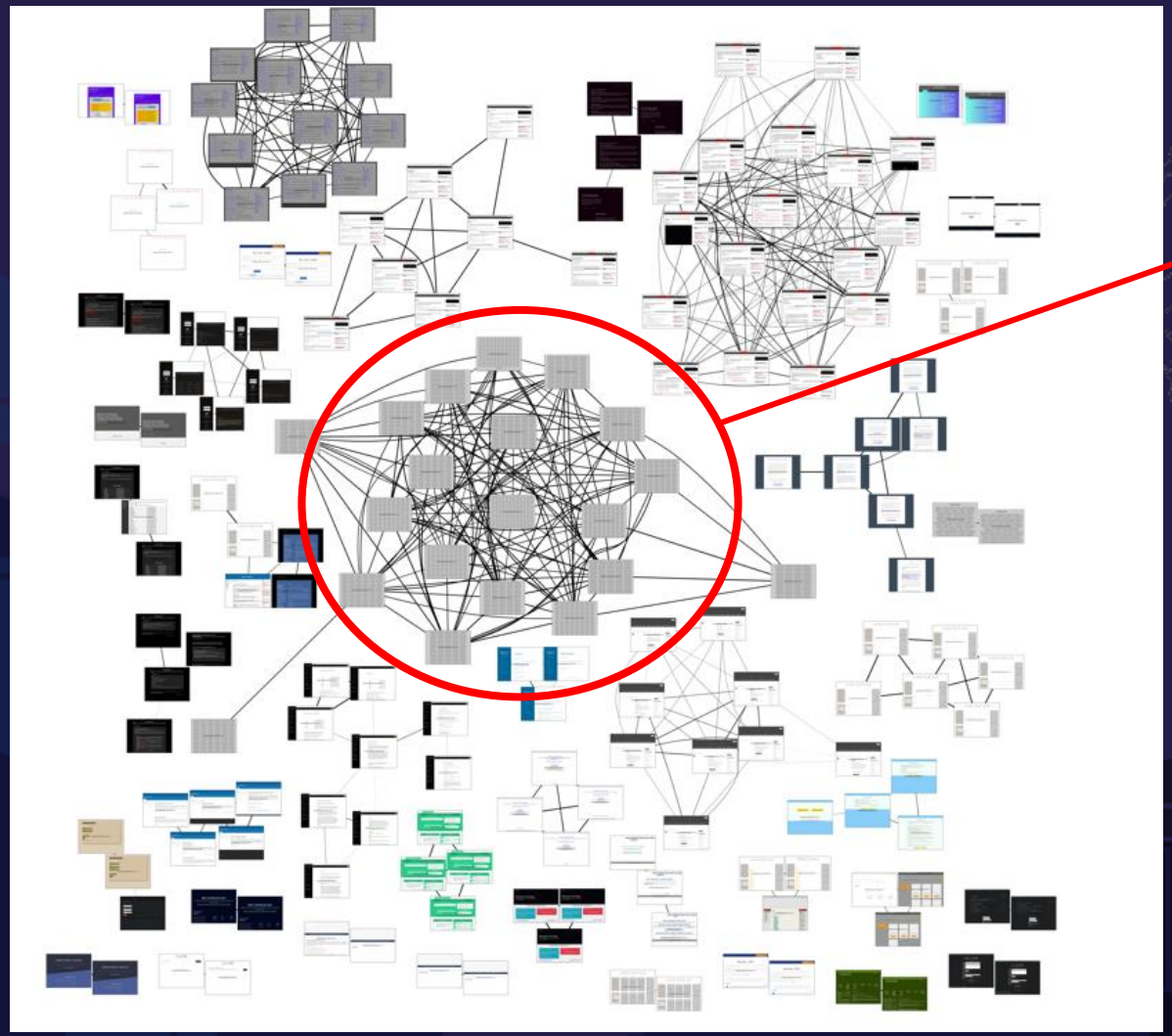
Es una herramienta que realiza comparaciones entre el contenido html de una página web contra otra y con ello permite realizar diagramas de relación entre ellas.

https://github.com/TeamHG-Memex/page-compare.git

BSIDES CDMX

Hackeando la Dark Web con Neo4j

Ahí no hay cuchara, solo nodos…

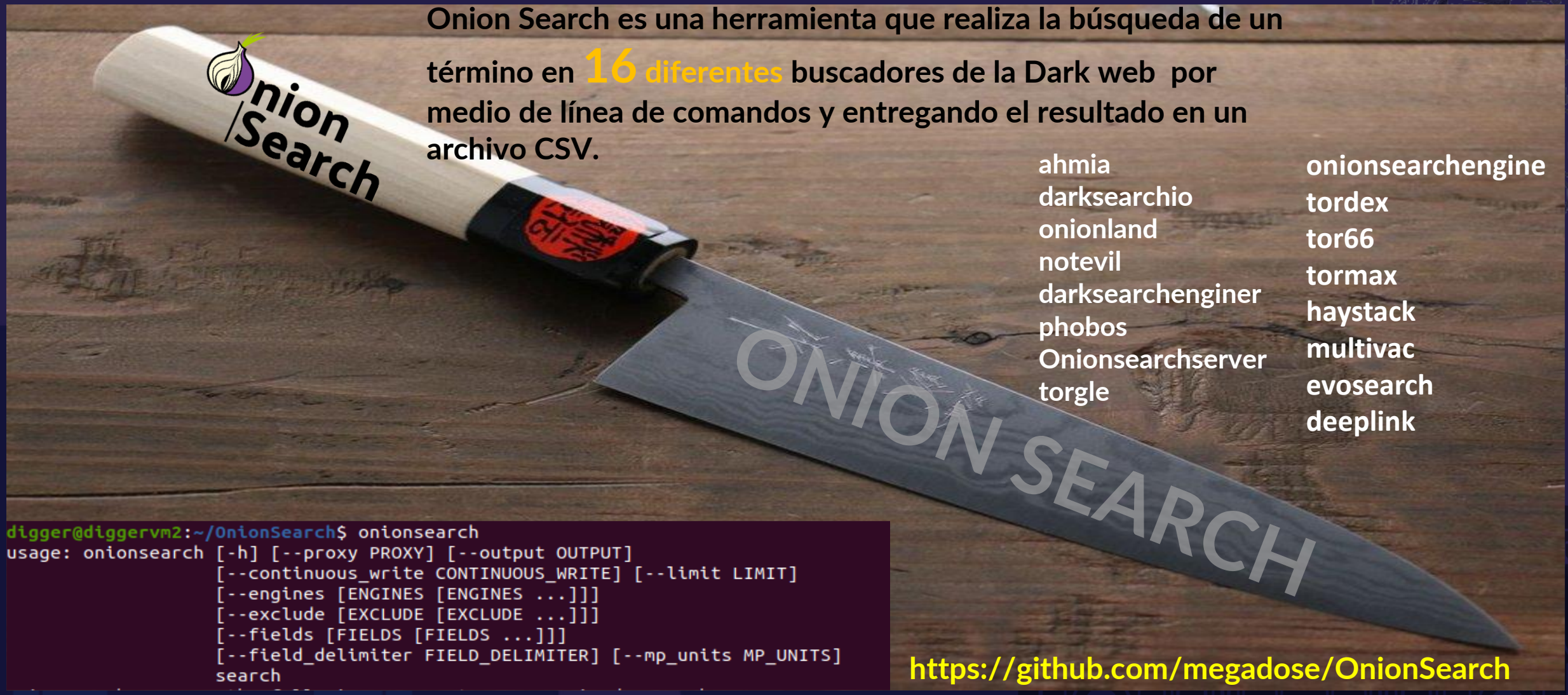


Infraestructura de un sitio web en la Dark Web

Los resultados son bastante buenos, sin embargo, sólo puedes hacer zoom de cada una de las imágenes obtenidas…

Hackeando la Dark Web con Neo4j

Ahí no hay cuchara, solo nodos…



Onion Search es una herramienta que realiza la búsqueda de un término en 16 diferentes buscadores de la Dark web por medio de línea de comandos y entregando el resultado en un archivo CSV.

- ahmia
- darksearchio
- onionland
- notevil
- darksearchenginer
- phobos
- Onionsearchserver
- torgle
- onionsearchengine
- tordex
- tor66
- tormax
- haystack
- multivac
- evosearch
- deeplink

```
digger@diggervm2:~/OnionSearch$ onionsearch
usage: onionsearch [-h] [--proxy PROXY] [--output OUTPUT]
                   [--continuous_write CONTINUOUS_WRITE] [--limit LIMIT]
                   [--engines [ENGINES [ENGINES ...]]]
                   [--exclude [EXCLUDE [EXCLUDE ...]]]
                   [--fields [FIELDS [FIELDS ...]]]
                   [--field_delimiter FIELD_DELIMITER] [--mp_units MP_UNITS]
                   search
```

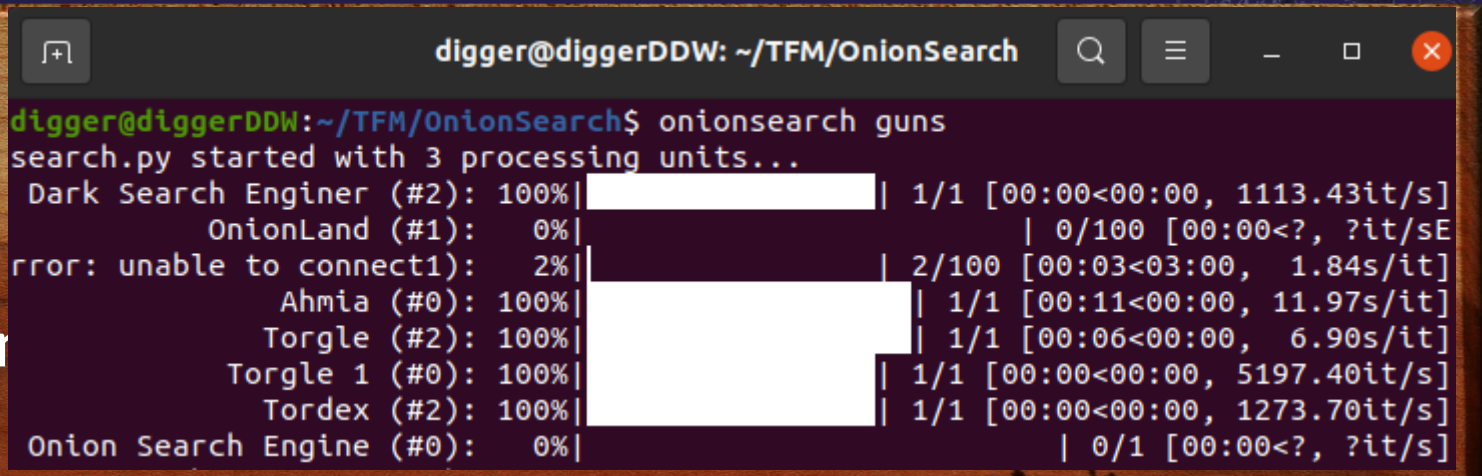
https://github.com/megadose/OnionSearch

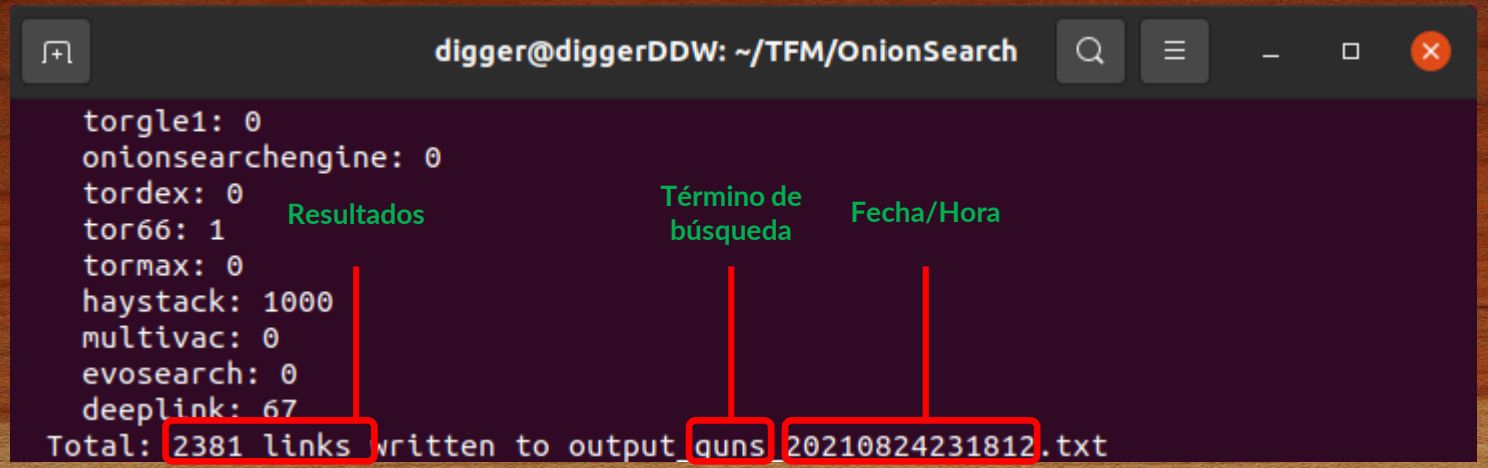
BSIDES CDMX

Hackeando la Dark Web con Neo4j

Ahí no hay cuchara, solo nodos…

Al igual que los buscadores tradicionales, Onion search devuelve diversos resultados en un archivo de tipo CSV.





Hackeando la Dark Web con Neo4j

Ahí no hay cuchara, solo nodos…

digger@diggerDDW: ~

```
"deeplink","BITCARDS - Prepaid cards","http://7[redacted].onion/"
"deeplink","BESTSHOP - Reliable Electronics Discounter","http://B[redacted].onion/"
"deeplink","[redacted]A.ONION | High Volume Bitcoin Mixer","http://[redacted]za.onion/"
"deeplink","btcmix - Bitcoin mixer","http://[redacted]x.onion/"
"deeplink","ChipMixer - Bitcoin tumbler","http://C[redacted].onion/"
```

Archivos

La estructura de este archivo está estructurado de la siguiente forma:

| Nombre del Buscador | Descripción del sitio | URL |

Además, es importante tener en cuenta que para cada término de búsqueda se genera un archivo de salida.

Hackeando la Dark Web con Neo4j

Ahí no hay cuchara, solo nodos…

```
digger@diggerDDW:~/TFM/OnionSearch$ cat RunAll2.sh
#!/bin/bash

onionsearch bank --continuous_write True
onionsearch financial --continuous_write True
onionsearch atm --continuous_write True
onionsearch cashout --continuous_write True
onionsearch ammo --continuous_write True
onionsearch gun --continuous_write True
onionsearch hitman --continuous_write True
onionsearch bitcoin --continuous_write True
onionsearch litecoin --continuous_write True
onionsearch leak --continuous_write True
onionsearch hack --continuous_write True
onionsearch hire --continuous_write True
onionsearch "credit card" --continuous_write True
onionsearch exploit --continuous_write True
onionsearch "zero day" --continuous_write True
onionsearch passport --continuous_write True
onionsearch pasaporte --continuous_write True
onionsearch cvv2 --continuous_write True
onionsearch cvv --continuous_write True
onionsearch mobile --continuous_write True
```

#for file in `ls -tr *.txt`; do cat $file;done > all_sites.list

Una investigación normalmente involucra diversos términos alrededor de una temática determinada.

```
digger@diggerDDW: ~/TFM/OnionSearch
digger@diggerDDW:~/TFM/OnionSearch$ for file in `ls -tr *.txt`; do cat $file;done > all_sites.list
digger@diggerDDW:~/TFM/OnionSearch$ cat all_sites.list  | wc -l
1949796
```

1.9 Millones de Sitios

BSIDES CDMX

Hackeando la Dark Web con Neo4j

Ahí no hay cuchara, solo nodos…

Obteniendo los hostnames

```
digger@diggerDDW:~/TFM/OnionSearch$ head -n 5 all_sites.list
"ahmia","Computer program - The Hidden Wiki","http://zqktlwi4fecvo6ri.onion/wiki/Computer_program"
"ahmia","Hacking Services - Computer- Social Media","http://ly75dbzixy7hlp663j32xo4dtoiikm6bxb53jvivq
kpo6jwppptx3sad.onion/index.php?route=product/product&path=101_107&product_id=160"
"ahmia","Debian -- Computer vendors that pre-install Debian","http://sejnfjrq6szgca7v.onion/distrib/p
re-installed"
"ahmia","Selling Modified and Weaponized Computer Virus - BlackHats Lounge","http://32orihrbrhpk5x6o.
onion?product=selling-modified-and-weaponized-computer-virus"
"ahmia","Does using Tor Browser protect other applications on my computer? | Tor Project | Support","
http://4bflp2c4tnynnbes.onion/tbb/tbb-13/"
```

```
cat all_sites.list | sed -r 's/","/"!"/g' | awk -F'!' '{print $2"*",$3}' | grep "http" | cut -d "/" -f 3 | sed -r 's/www.//g' | sed -r 's/\"//g' | grep ".onion$" | uniq > all_hosts_name.list
```

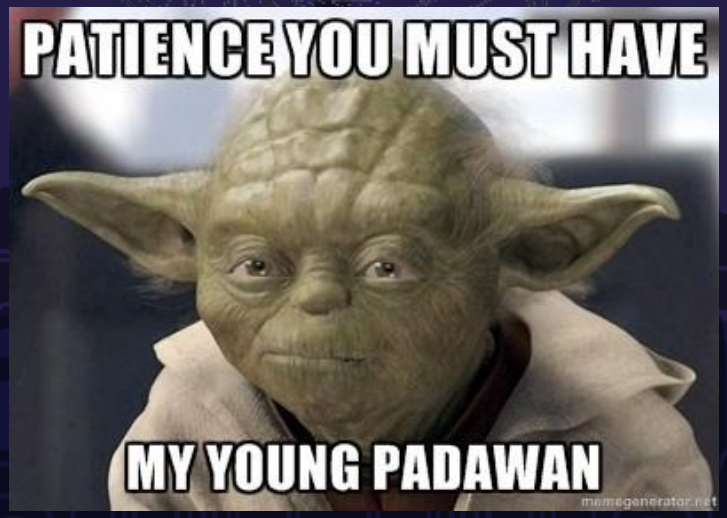
```
digger@diggerDDW: ~/TFM/OnionSearch
digger@diggerDDW:~/TFM/OnionSearch$ cat all_sites.list | sed -r 's/","/"!"/g' | awk -F'!' '{print $2"
*",$3}' | grep "http" | cut -d "/" -f 3 | sed -r 's/www.//g' | sed -r 's/\"//g' | grep ".onion$" | un
iq > all_hosts_name.list
digger@diggerDDW:~/TFM/OnionSearch$ head -n 5 all_hosts_name.list
zqktlwi4fecvo6ri.onion
ly75dbzixy7hlp663j32xo4dtoiikm6bxb53jvivqkpo6jwppptx3sad.onion
sejnfjrq6szgca7v.onion
4bflp2c4tnynnbes.onion
quantum2l7xnxwtb.onion
```

Hackeando la Dark Web con Neo4j

Ahí no hay cuchara, solo nodos…

```
digger@diggerDDW:~/TFM/OnionSearch$ proxychains4 nmap -Pn -sV -v -p 22,21,80,443,25,6667,11009,4050,5
5080 -oX scan_results_full.xml -iL all_hosts_name.list
[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-30 17:20 CST
NSE: Loaded 45 scripts for scanning.
Initiating Parallel DNS resolution of 4096 hosts. at 17:20
Completed Parallel DNS resolution of 4096 hosts. at 17:21, 21.55s elapsed
Initiating Connect Scan at 17:21
Scanning 113 hosts [9 ports/host]
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  ly75dbzixy7hlp663j32xo4dtoiikm6bxb53jvivqkpo6jw
ppptx3sad.onion:443 <--socket error or timeout!
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  quantum2l7xnxwtb.onion:443
```

```
# proxychains4 nmap -Pn -sV -v -p
22,21,80,443,25,6667,11009,4050,55080 -oX
scan_results_full.xml -iL all_hosts_name.list
```



BSIDES CDMX

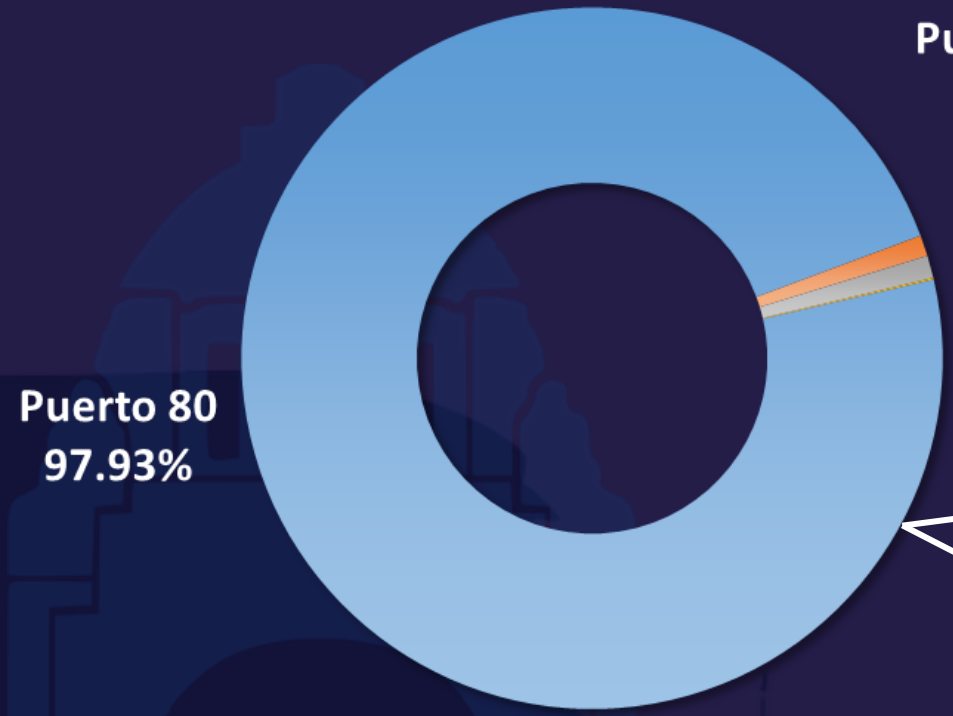
Normalizando la información obtenida

python3 nmap_xml_parser.py -f scan_results_full.xml -csv Scan_Table.csv

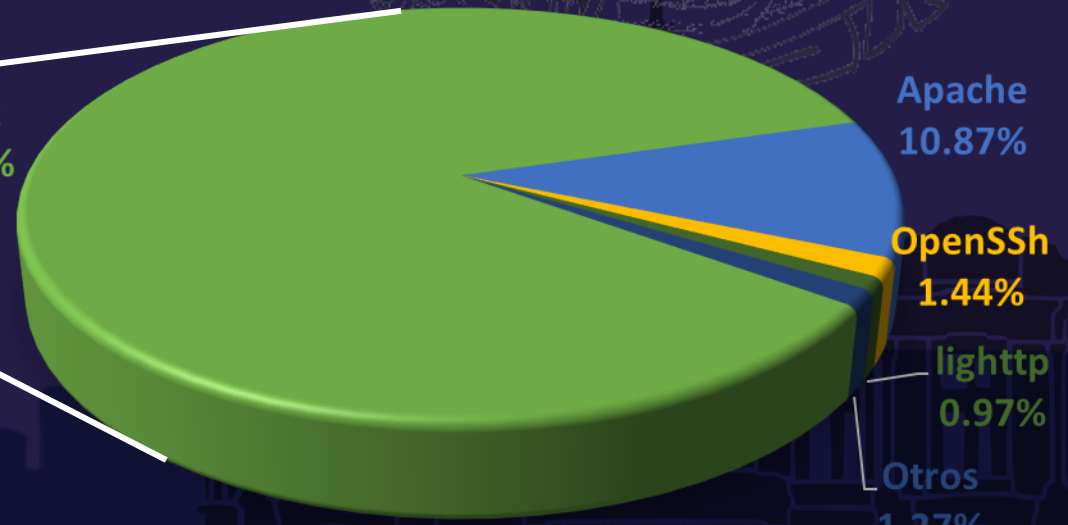
```
digger@diggerDDW:~/TFM/Nmap-Scan-to-CSV$ python3 nmap_xml_parser.py -f scan_results_full.xml -csv Scan_
Table.csv

[+] The file Scan_Table.csv does not exist. New file created!

digger@diggerDDW:~/TFM/Nmap-Scan-to-CSV$ head -n 5 Scan_Table.csv
IP,Host,OS,Proto,Port,Service,Product,Service FP,NSE Script ID,NSE Script Output,Notes
224.0.0.1,zqktlwi4fecvo6ri.onion,,tcp,80,http,nginx,,,
224.0.0.2,sejnfjrq6szgca7v.onion,,tcp,80,http,Apache httpd,,,
224.0.0.4,bn6kma5cpxill4pe.onion,,tcp,80,http,Apache httpd,,,
224.0.0.5,rvy6qmlqfstv6rlz.onion,,tcp,80,http,lighttpd,,,
digger@diggerDDW:~/TFM/Nmap-Scan-to-CSV$
```

https://github.com/laconicwolf/Nmap-Scan-to-CSV.git

Algunos números que resultaron…



Distribución de Hidden Services por tecnología




DESENMASCARANDO
HIDDEN SERVICES

Un servidor en la Dark Web es igual a cualquier otro en varios aspectos:

- Sistema Operativo
- Aplicaciones
- Puertos estándar
- Protocolos inseguros
- Vulnerabilidades

Un servidor en la Dark Web es igual a cualquier otro en varios aspectos:

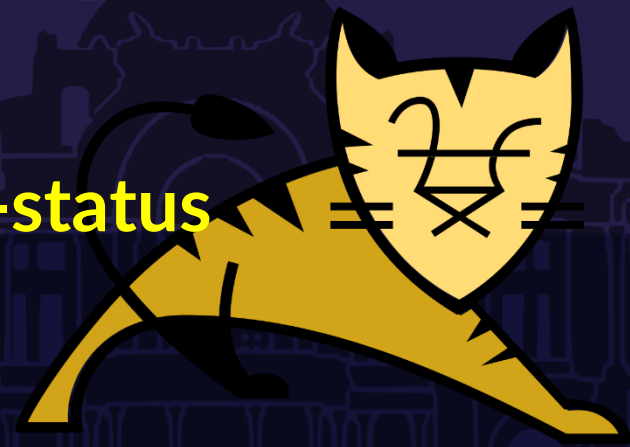
- Sistema Operativo
- Aplicaciones
- Puertos estándar
- Protocolos inseguros
- **Vulnerabilidades**

Elegir a nuestro target….

MOD_SERVER_STATUS

Es una mala configuración en los servidores apache, habilitada en el servidor, permite obtener métricas de uso e inclusive la ip del servidor….

http(s)://server_address/server-status



Hackeando la Dark Web con Neo4j

Ahí no hay cuchara, solo nodos…

cwu f.onion/server-status

Apache Server Status for cw zf.onion
(via)

Server Version: Apache/2.4.7 (Ubuntu) PHP/5.5.9-1ubuntu4.21 OpenSSL/1.0.1f
Server MPM: prefork
Server Built: Jul 27 2017 15:20:24

Current Time: Friday, 27-Aug-2021 15:02:16 UTC
Restart Time: Saturday, 06-Mar-2021 01:36:15 UTC
Parent Server Config. Generation: 30
Parent Server MPM Generation: 29
Server uptime: 174 days 13 hours 26 minutes
Server load: 0.00 0.01 0.05
l accesses: 599609 - Total Traffic: 218.8 GB
CPU Usage: u19.75 s1.05 cu.19 cs.02 - .000139% CPU load
equests/sec - 15.2 kB/second - 382.6 kB/request
quests currently being processed, 9 idle workers

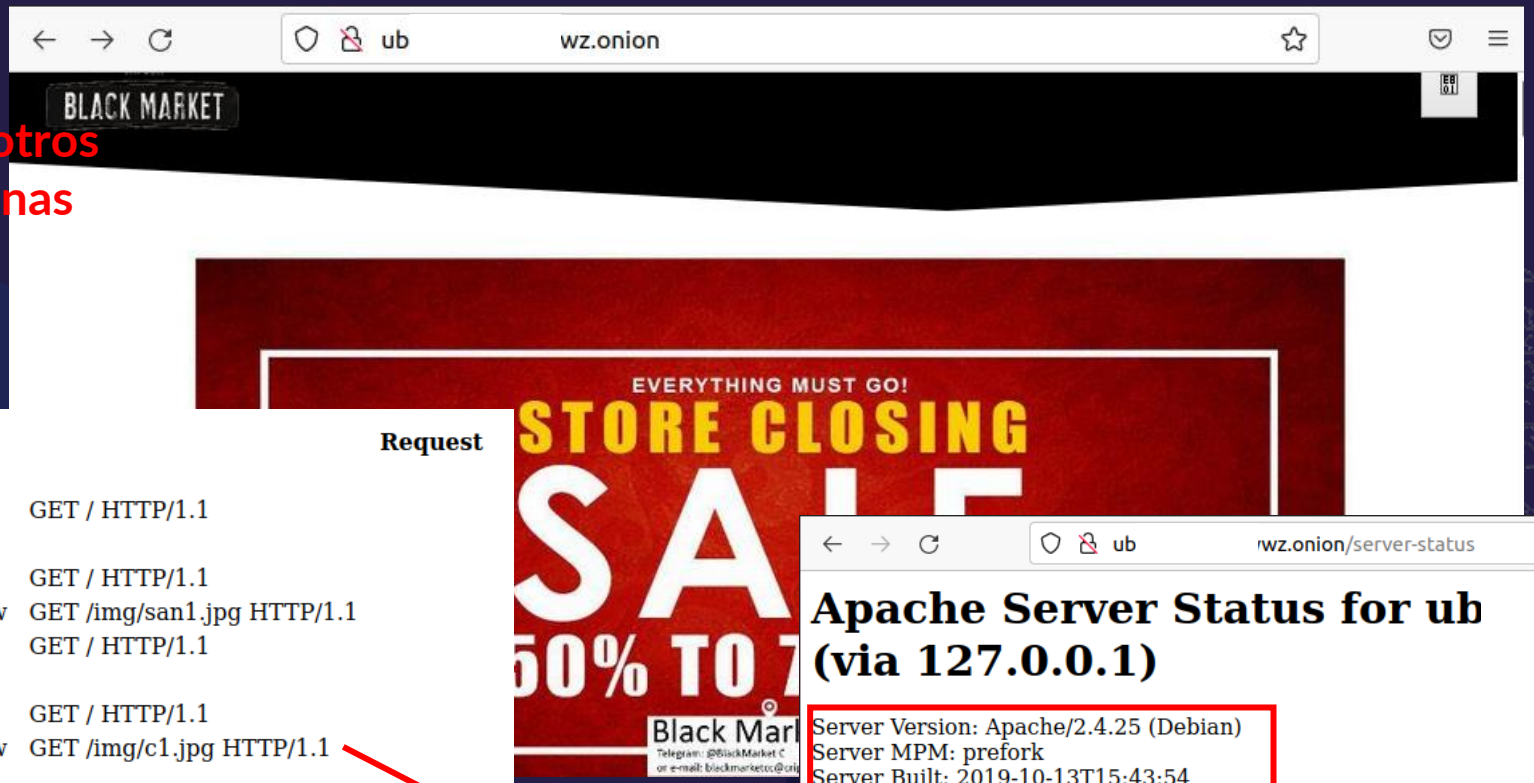
Versión del S.O.

Datos relevantes

Hackeando la Dark Web con Neo4j

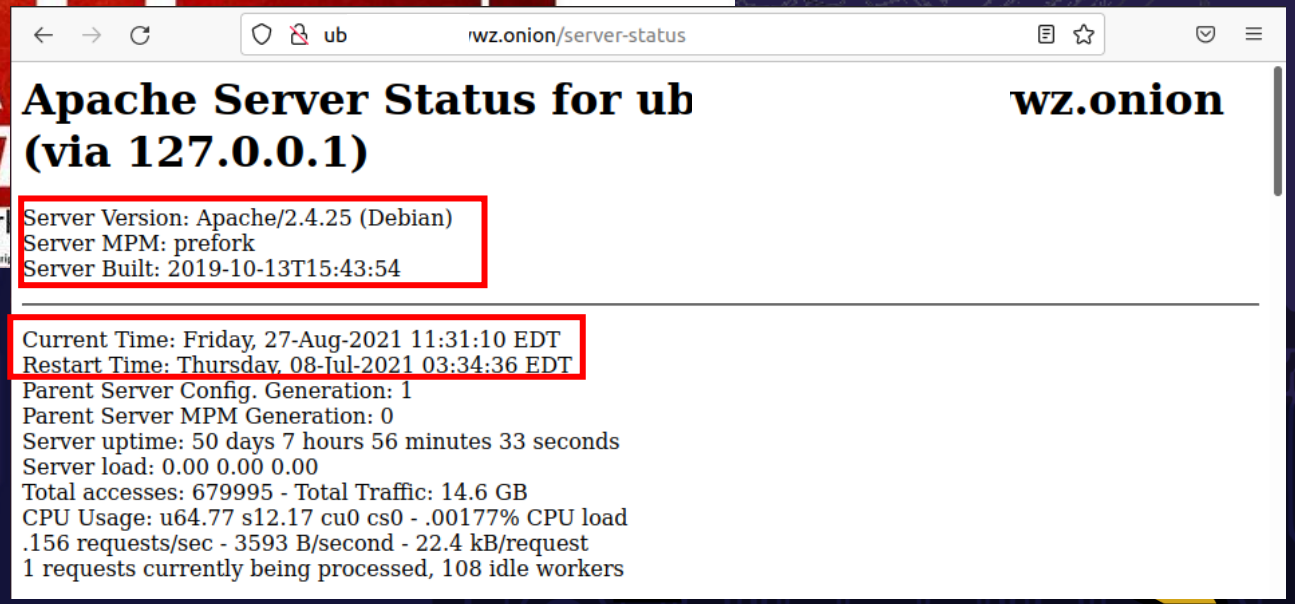
Ahí no hay cuchara, solo nodos…

Relación con otros servicios/páginas



VHost	Request
niq.onion:80	GET / HTTP/1.1
niq.onion:80	GET / HTTP/1.1
bdjupg4rptjzcaruqw	GET /img/san1.jpg HTTP/1.1
niq.onion:80	GET / HTTP/1.1
ız6.onion:80	GET / HTTP/1.1
bdjupg4rptjzcaruqw	GET /img/c1.jpg HTTP/1.1
bdjupg4rptjzcaruqw	GET /img/7.png HTTP/1.1
wn.onion:80	GET / HTTP/1.1
wn.onion:80	GET / HTTP/1.1
bdjupg4rptjzcaruqw	GET /img/22.png HTTP/1.1
niq.onion:80	GET / HTTP/1.1
bdjupg4rptjzcaruqw	GET /Main/css HTTP/1.1
wn.onion:80	GET / HTTP/1.1

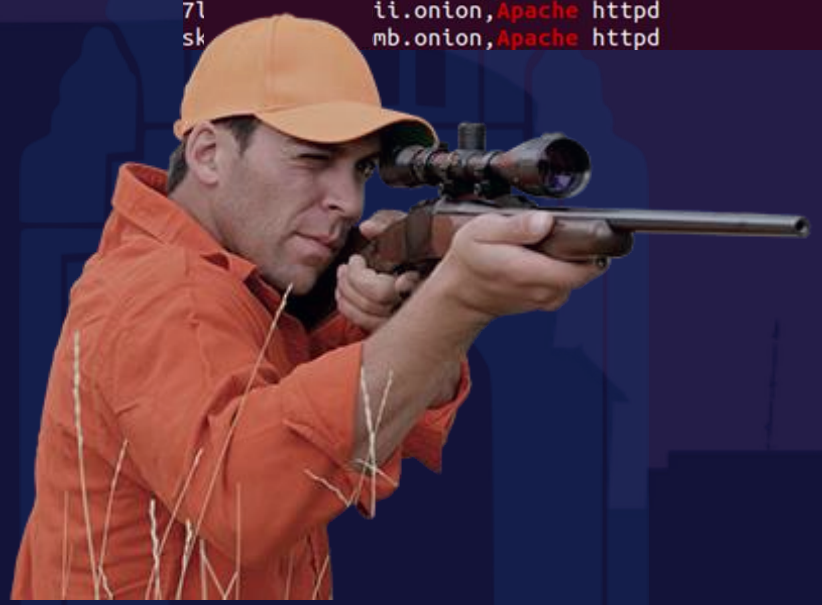
Directorios/Archivos solicitados



Hackeando la Dark Web con Neo4j

Ahí no hay cuchara, solo nodos…

```
digger@diggerDDW:~/TFM/Nmap-Scan-to-CSV$ cat Scan_Table.csv | cut -d "," -f 2,7 | grep Apache
se            7v.onion,Apache httpd
br            pe.onion,Apache httpd
ha            5q.onion,Apache httpd
7p            ha.onion,Apache httpd
f7            ne.onion,Apache httpd
jc            gk.onion,Apache httpd
e4            yt.onion,Apache
cw            zf.onion,Apache/2.4.7 (Ubuntu)
py            rd.onion,Apache/2.4.46 (Debian)
vy            lf.onion,Apache
ug            az.onion,Apache
pa            kp.onion,Apache
pa            kp.onion,Apache
rc            dq.onion,Apache httpd
5s            wz.onion,Apache httpd
ph            yr.onion,Apache httpd
7l            ii.onion,Apache httpd
7l            ii.onion,Apache httpd
sk            mb.onion,Apache httpd
```



Entrada

```
#!/bin/bash

for page in `cat Sites_With_Apache.list`
do
  filename="${page}.html"
  touch $filename
  curl "${page}/server-status" > $filename
done
```

```
GetAll_SS.sh
gr            wjl.onion.html
gr            pda.onion.html
gr            ois.onion.html
gu            rre.onion.html
gv            x3k.onion.html
ha            75q.onion.html
ha            qzq.onion.html
ha            e2b.onion.html
ha            h42n5o7gbzrewxee3
nd            iwk.onion.html
ng            6db.onion.html
ni            6km.onion.html
ni            yzr.onion.html
ni            2ed.onion.html
nl            7wr.onion.html
no            gku.onion
```

Salida

Desenmascarando el hidden service

#grep -rnw '.' -e "ip" | uniq

Tenemos una IP!!

```
digger@diggerDDW:~/TFM/Get_All_Server_Status$ grep -rnw '.' -e "ip" | uniq
./[redacted]gku.onion.html:63:          "ip":"",
./cw[redacted]f.onion.html:44:</td><td>143.110.[redacted]</td><td nowrap>ip-172-31[redacted]s-west-2.comp
u</td><td nowrap>POST /wordpress//xmlrpc.php HTTP/1.1</td></tr>
./c[redacted]f.onion.html:48:</td><td>143.110.[redacted]</td><td nowrap>ip-172-31[redacted]s-west-2.comp
u</td><td nowrap>POST /wordpress//xmlrpc.php HTTP/1.1</td></tr>
./cwu[redacted]nion.html:52:</td><td>143.110.[redacted]</td><td nowrap>ip-172-31[redacted]s-west-2.comp
u</td><td nowrap>POST /wordpress//xmlrpc.php HTTP/1.1</td></tr>
```

WHOIS IP Lookup Tool

The IPWHOIS Lookup tool finds contact information for the owner of a specified IP address.

Enter a host name or an IP address:

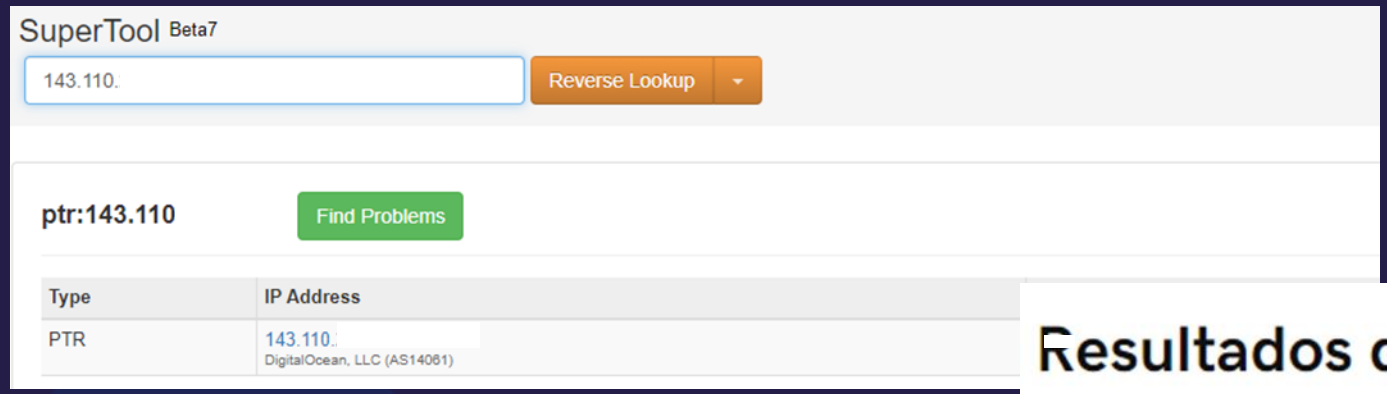
143.110.[redacted] Go »

Related Tools: DNS Traversal Traceroute Vector Trace Ping WHOIS Lookup

```
            Source: whois.arin.net
        IP Address: 143.110.[redacted]
              Name: DIGITALOCEAN-143-110-128-0
            Handle: NET-143-110-[redacted]
  Registration Date: 17/01/20
             Range: 143.110.[redacted]  255.255
               Org: DigitalOcean, LLC
```

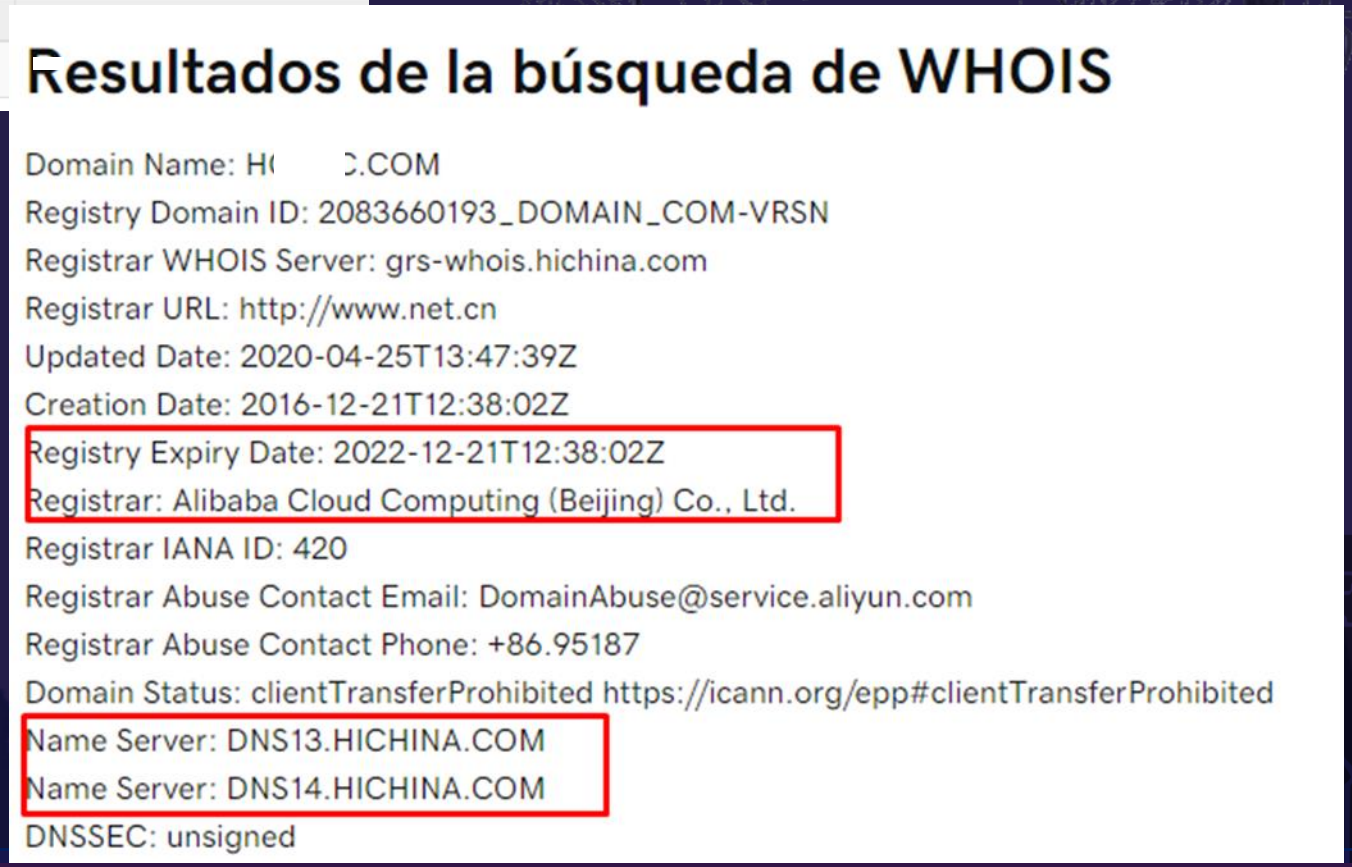
Hackeando la Dark Web con Neo4j

Ahí no hay cuchara, solo nodos…



OSINT:

- Cuentas de correo asociadas al dominio.
- Videos
- Chats
- Waybackmachine
- Etc…



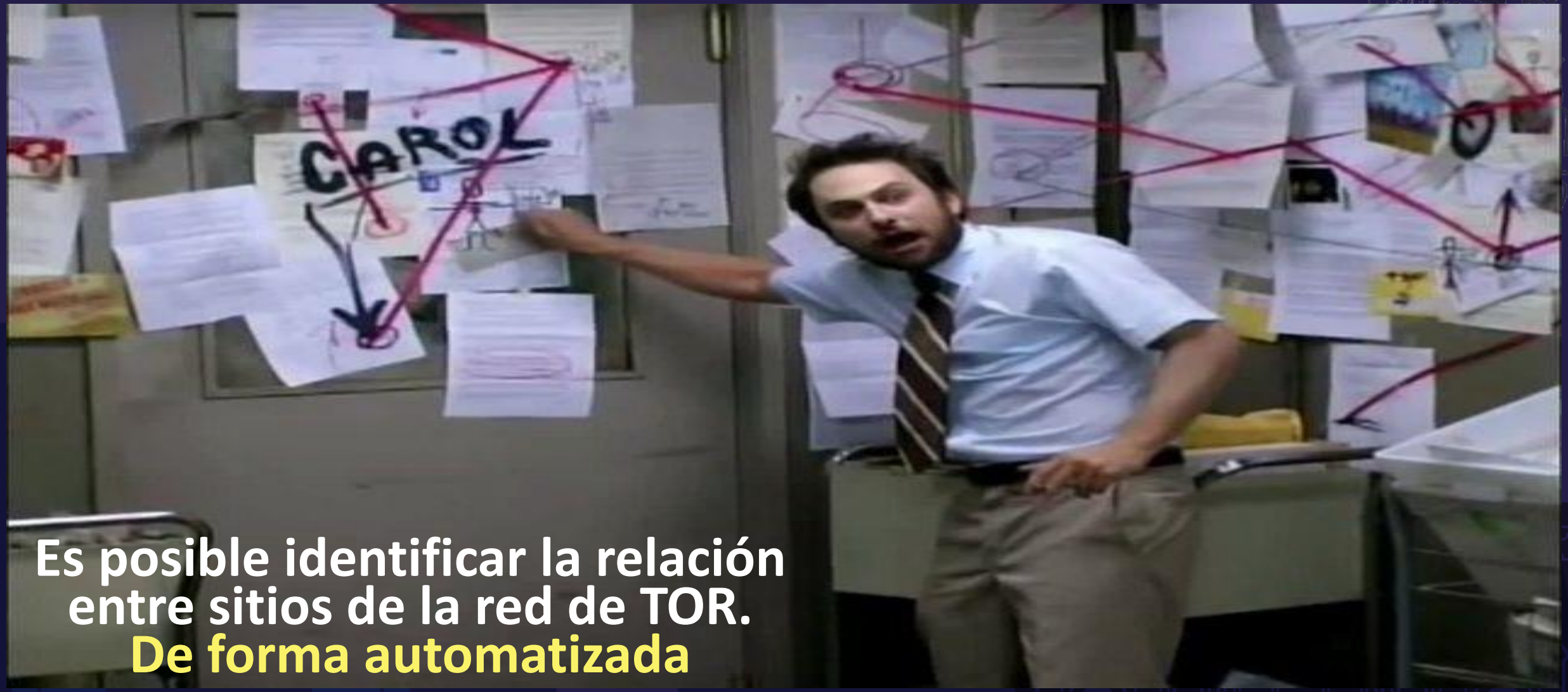
nginx.conf

```
upstream big_server_com {
  server 127.0.0.3:8000 weight=5;
  server 127.0.0.3:8001 weight=5;
  server 192.168.0.1:8000;
  server 192.168.0.1:8001;
}

server { # simple load balancing
  listen          80;
  server_name     big.server.com;
  access_log      logs/big.server.access.log main;

  location / {
    proxy_pass      http://big_server_com;
```

ALGUIEN DIJO ..... NGINX®

Hackeando la Dark Web con Neo4j

Ahí no hay cuchara, solo nodos…



Hackeando la Dark Web con Neo4j

Ahí no hay cuchara, solo nodos…

Hagamos una demostración…

Mas referencias y descripción del proyecto…

https://github.com/AlfredoAbarca/DiggerDDW

@aabarcab

alfredo-abarca

bl4sphem

GRACIAS!!

2023