

#IntelCon2021



IntelCon
by Ginseg

Cortando la cebolla... (Y no morir en el intento)

Alfredo Abarca

Congreso Online de Ciberinteligencia



> whoami -

ALFREDO ABARCA
@aabarcab

- Ing. Cibernética y Sistemas computacionales.
- Dev/Endpoint Security Manager/Purple Team Player/Ciberinteligencia
- Old School Gamer



<https://github.com/AlfredoAbarca>

DISCLAIMER



#IntelCon2021

* **NO**, No es una clase de cocina...

(Quizá rompamos algo, pero ya veremos mas adelante.)

* Las herramientas y metodologías mostradas en la presentación, son con fines didácticos. Por lo que no se fomenta el mal uso de las mismas.



OBJETIVO



Familiarizarse con el tipo de información que podemos obtener en la Dark Web.

Automatizar el proceso de recolección y análisis de estos sitios.

AGENDA

- Contexto de la investigación
- Requerimientos técnicos
- Metodología de trabajo
- Resultados
- Otros Usos



Deep Web

90%



Surface Web

Todo aquello que puede ser encontrado a través de un buscador como: Google, Yahoo, etc...

8%



Analista de
Ciberinteligencia

- Recursos Gubernamentales
- Registros Médicos
- Repositorios empresariales
- Servicios de Correo
- Servicios de Suscripción

Todo aquello que no está indexado en algún buscador público.



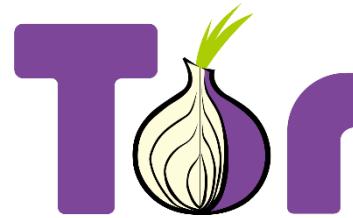
Cliente TOR

Dark Web

- Sitios de protesta política
- Información Ilegal*
- Sitios de la red anónima TOR
- Mercados Ilegales (Drogas, Armas, etc...)

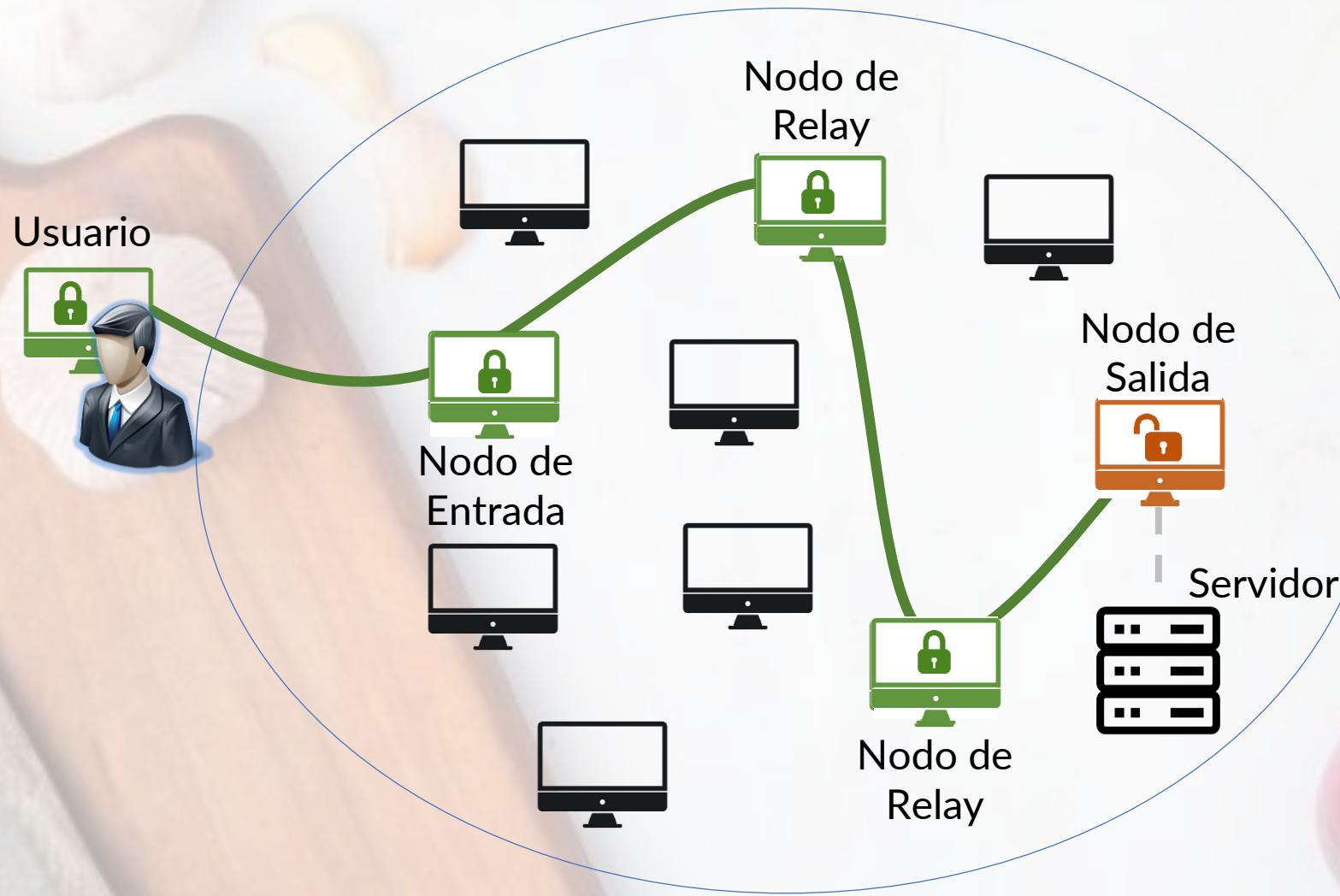
2%

TIPOS DE REDES EN DEEPWEB



The Onion Router	Invisible Internet Project	ZeroNet	Freenet
<ul style="list-style-type: none">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.	<ul style="list-style-type: none">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.	<ul style="list-style-type: none">El contenido de un sitio se ofrece de forma descentralizada y basándose en redes P2P. (BitTorrent)Para anonimato emplean TOR.	<ul style="list-style-type: none">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

¿Cómo funciona la red TOR?



INVESTIGACIONES

- 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.

DARK WEB



VS

CLEAR WEB

- Existe 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.

COME TO THE
DARK ~~WEB~~
WE HAVE COOKIES
SEARCHERS TOO



DuckDuckGo



Candle



GORCH

AHMIA

Tor Anonymity Network Search Engine

A screenshot of the AHMIA search interface. The URL in the address bar is `https://osot4csyd.onion/search/?q=guns`. The search term 'guns' is entered in the search bar, and the 'Search' button is highlighted in green. Below the search bar, there are links for 'About Ahmia', 'Statistics', 'Add Service', and 'i2p search'. On the right side of the header, there are links for 'Contact' and 'Blacklist'. The main content area shows search results for 'Guns'. A red arrow points from the text 'Page 1 of 23' to a bulleted list of observations on the right.

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.

Any Time ▾

Omitted very similar entries. Displaying 2284 matches in 6.27 seconds. Page 1 of 23

Guns

Guns

3bb

[bad.onion](#) – 0 minutes ago –

Guns

Worldwide guns, cheapest gun. No serial number!

oliver [.onion](#) – 2 days, 13 hours ago –

Guns

Guns

ly75a

[sad.onion](#) – 0 minutes ago –

Guns

Worldwide guns, cheapest gun. No serial number!

olivq [akai7zqd.onion](#) – 0 minutes ago –

[Euro Guns - Number one guns dealer in onionland - Buy guns and ammo for Bitcoin](#)



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.



#IntelCon2021

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>

```
digger@diggerDDW:~/TFM/OnionSearch$ onionsearch guns
search.py started with 3 processing units...
Dark Search Enginer (#2): 100%|██████████| 1/1 [00:00<00:00, 1113.43it/s]
    OnionLand (#1): 0%|                | 0/100 [00:00<?, ?it/s]
error: unable to connect1): 2%|                | 2/100 [00:03<03:00, 1.84s/it]
    Ahmia (#0): 100%|██████████| 1/1 [00:11<00:00, 11.97s/it]
    Torgle (#2): 100%|██████████| 1/1 [00:06<00:00, 6.90s/it]
    Torgle 1 (#0): 100%|██████████| 1/1 [00:00<00:00, 5197.40it/s]
    Tordex (#2): 100%|██████████| 1/1 [00:00<00:00, 1273.70it/s]
Onion Search Engine (#0): 0%|                | 0/1 [00:00<?, ?it/s]
```

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

```
digger@diggerDDW:~/TFM/OnionSearch$ onionsearch guns
search.py started with 3 processing units...
Dark Search Enginer (#2): 100%|██████████| 1/1 [00:00<00:00, 1113.43it/s]
    OnionLand (#1): 0%|                | 0/100 [00:00<?, ?it/s]
error: unable to connect1): 2%|                | 2/100 [00:03<03:00, 1.84s/it]
    Ahmia (#0): 100%|██████████| 1/1 [00:11<00:00, 11.97s/it]
    Torgle (#2): 100%|██████████| 1/1 [00:06<00:00, 6.90s/it]
    Torgle 1 (#0): 100%|██████████| 1/1 [00:00<00:00, 5197.40it/s]
    Tordex (#2): 100%|██████████| 1/1 [00:00<00:00, 1273.70it/s]
Onion Search Engine (#0): 0%|                | 0/1 [00:00<?, ?it/s]
```

Término de búsqueda Fecha/Hora

Resultados

torgle1: 0
onionsearchengine: 0
tordex: 0
tor66: 1
tormax: 0
haystack: 1000
multivac: 0
evosearch: 0
deeplink: 67

Total: 2381 links written to output guns 20210824231812.txt



```
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/"
Archivos[REDACTED],"ChipMixer - Bitcoin tumbler","http://C[REDACTED].onion/"
```

La estructura de este archivo esta 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.



```
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

```
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
L949796
```

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



1.9 Millones de
Sitios

Creo que ahora tenemos más
que una sola cebolla...

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**

Obteniendo los hostnames

```
digger@diggerDDW:~/TFM/OnionSearch$ head -n 5 all_sites.list
"ahmia","Computer program - The Hidden Wiki","http://zq          .onion/wiki/Computer_program"
"ahmia","Hacking Services - Computer- Social Media","http://ly7          .km6bx53jvivq
kpo6jwppptx3sad.onion/index.php?route=product/product&path=101_107&product_id=160"
"ahmia","Debian -- Computer vendors that pre-install Debian","http://           ca7v.onion/distrib/p
re-installed"
"ahmia","Selling Modified and Weaponized Computer Virus - BlackHats Lounge","http://           5x6o.
onion?product=selling-modified-and-weaponized-computer-virus"
"ahmia","Does using Tor Browser protect other applications on my computer? | Tor Project | Support","
http://4b           bes.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
```

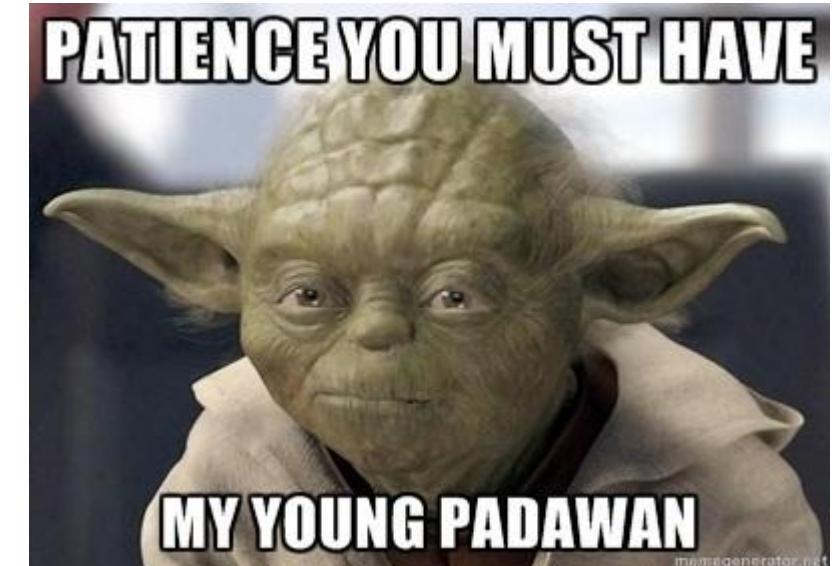


```
digger@diggerDDW: ~/TFM/OnionSearch
digger@diggerDDW:~/TFM/OnionSearch$ cat all_sites.list | sed -r 's/", "/!"/g' | awk -F'!' '{print $2"**",$3}' | grep "http" | cut -d "/" -f 3 | sed -r 's/www//g' | sed -r 's/\//g' | grep ".onion$" | uniq > all_hosts_name.list
digger@diggerDDW:~/TFM/OnionSearch$ head -n 5 all_hosts_name.list
zq          .onion
ly75dbzixy7hlp66 .onion
se          a7v.onion
4b          bes.onion
qua         vtb.onion
```

Escaneo de puertos en Servidores

```
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 ... ly75db 6jw  
ppptx3sad.onion:443 <--socket error or timeout!  
[proxychains] Strict chain ... 127.0.0.1:9050 ... q itb.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
```



Normalizando la información obtenida



#IntelCon2021

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

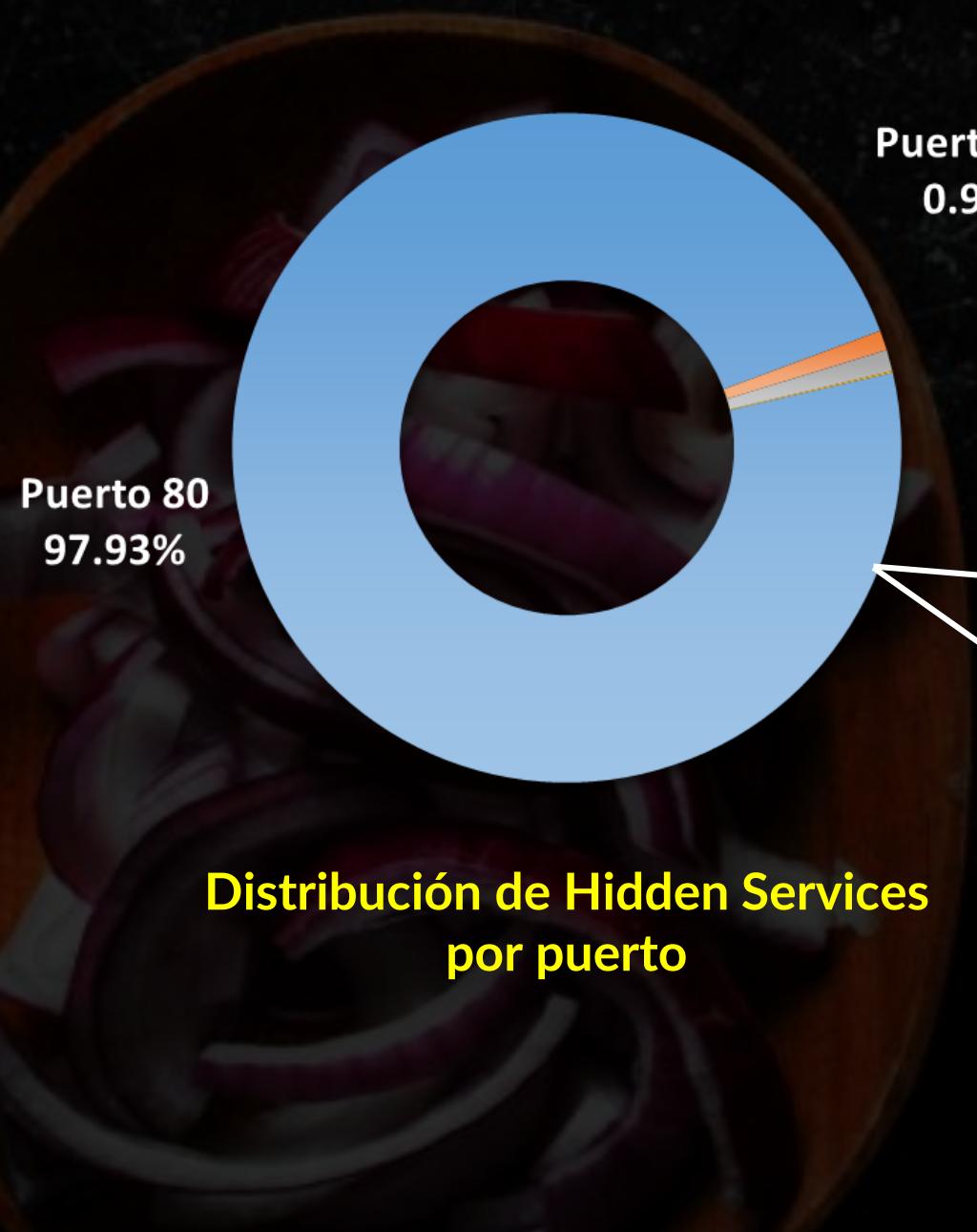
Veo
tecnologías
vulnerables,
Ahooy.

```
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,z0ri.onion,,tcp,80,http,nginx,,
224.0.0.2,s7v.onion,,tcp,80,http,Apache httpd,,
224.0.0.4,bpe.onion,,tcp,80,http,Apache httpd,,
224.0.0.5,rv,lz.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...



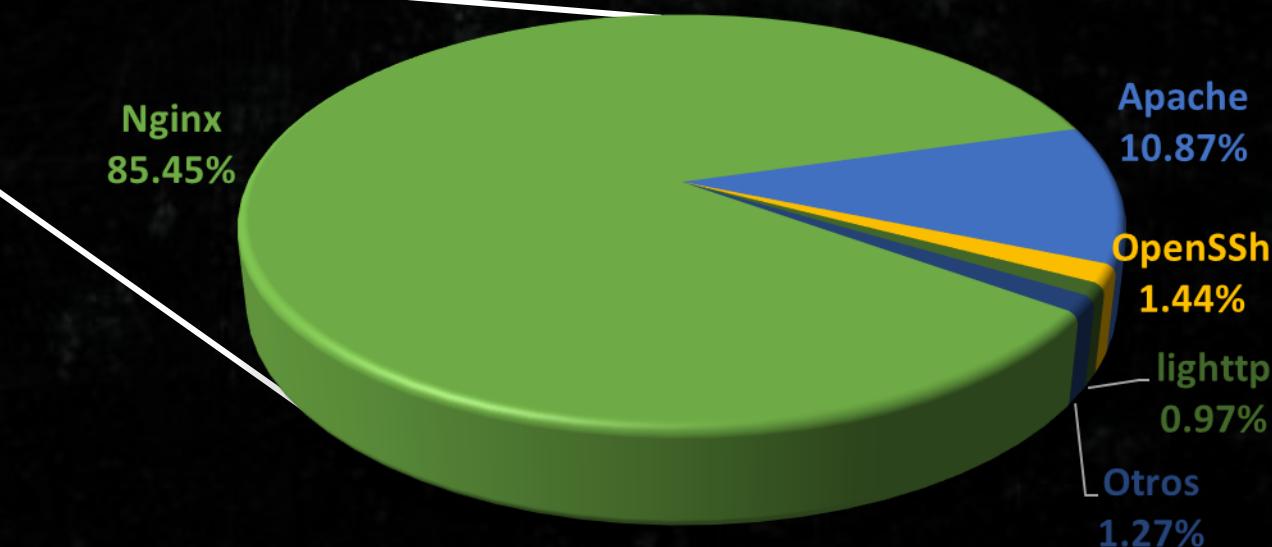
Distribución de Hidden Services
por puerto

Puerto 443
0.96%

Otros
0.07%

Puerto 22
1.04%

Distribución de Hidden Services
por tecnología



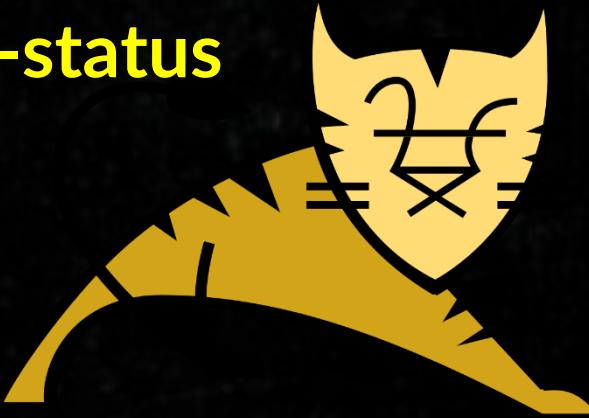
MOD_SERVER_STATUS



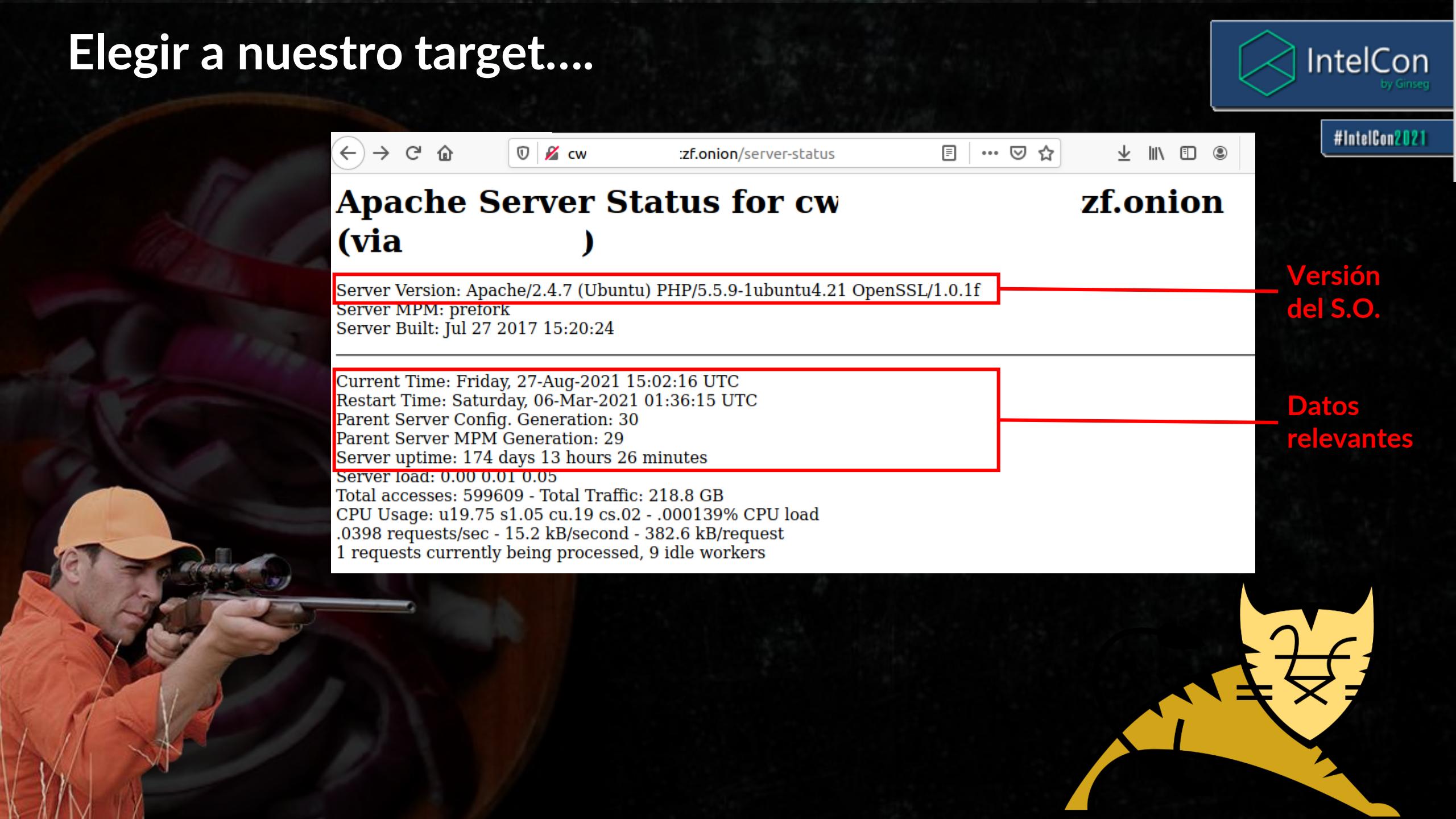
Me pareció
haber visto
un lindo
gatito.

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



Elegir a nuestro target...



Apache Server Status for cw
(via)

zf.onion

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
Total accesses: 599609 - Total Traffic: 218.8 GB
CPU Usage: u19.75 s1.05 cu.19 cs.02 - .000139% CPU load
.0398 requests/sec - 15.2 kB/second - 382.6 kB/request
1 requests currently being processed, 9 idle workers

Versión
del S.O.

Datos
relevantes

Elegir a nuestro target....

Relación con otros servicios/páginas

VHost

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
iz6.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

wz.onion

Apache Server Status for ub (via 127.0.0.1)

Server Version: Apache/2.4.25 (Debian)
Server MPM: prefork
Server Built: 2019-10-13T15:43:54

Current Time: Friday, 27-Aug-2021 11:31:10 EDT
Restart Time: Thursday, 08-Jul-2021 03:34:36 EDT
Parent Server Config. Generation: 1
Parent Server MPM Generation: 0
Server uptime: 50 days 7 hours 56 minutes 33 seconds
Server load: 0.00 0.00 0.00
Total accesses: 679995 - Total Traffic: 14.6 GB
CPU Usage: u64.77 s12.17 cu0 cs0 - .00177% CPU load
.156 requests/sec - 3593 B/second - 22.4 kB/request
1 requests currently being processed, 108 idle workers

Elegir a nuestro target...

```
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
55      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.html
```

Salida



Desenmascarando el hidden service

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

```
digger@diggerDDW:~/TFM/Get_All_Server_Status$ grep -rnw '.' -e "ip" | uniq
./index.html:63:      "ip":"".
./cwe79xx/index.html:44:</td><td>143.110.          </td><td nowrap>ip-172-31      s-west-2.comp
u</td><td nowrap>POST /wordpress//xmlrpc.php HTTP/1.1</td></tr>
./cwe79xx/index.html:48:</td><td>143.110.          </td><td nowrap>ip-172-31      s-west-2.comp
u</td><td nowrap>POST /wordpress//xmlrpc.php HTTP/1.1</td></tr>
./cwe79xx/index.html:52:</td><td>143.110.          </td><td nowrap>ip-172-31      s-west-2.comp
u</td><td nowrap>POST /wordpress//xmlrpc.php HTTP/1.1</td></tr>
```

Tenemos una IP!!

WHOIS IP Lookup Tool

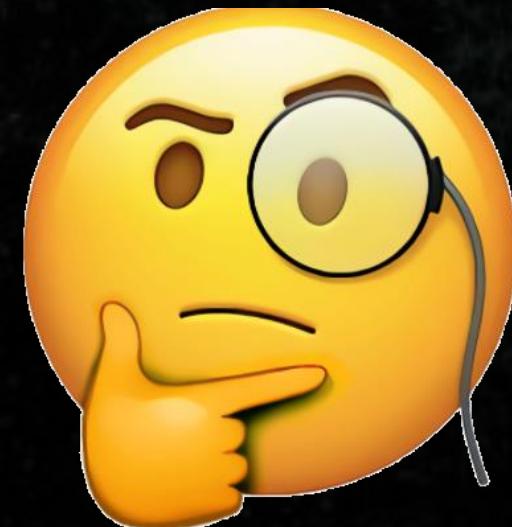
The IPWHOIS Lookup tool finds contact information for the owner of a specified IP address.

Enter a host name or an IP address:

Go »

Related Tools: [DNS Traversal](#) [Traceroute](#) [Vector Trace](#) [Ping](#) [WHOIS Lookup](#)

Source:	whois.arin.net
IP Address:	143.110. .
Name:	DIGITALOCEAN-143-110-
Handle:	NET-143-110-
Registration Date:	17/01/20
Range:	143.110. . 0.255.255
Org:	DigitalOcean, LLC



Desenmascarando el hidden service

SuperTool Beta7

143.110. Reverse Lookup ▾

ptr:143.110 Find Problems

Type	IP Address	Domain Name
PTR	143.110. DigitalOcean, LLC (AS14061)	h c.com

OSINT:

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

Resultados de la búsqueda de WHOIS

Domain Name: H C.COM
Registry Domain ID: 2083660193_DOMAIN_COM-VRSN
Registrar WHOIS Server: grs-whois.hichina.com
Registrar URL: <http://www.net.cn>
Updated Date: 2020-04-25T13:47:39Z
Creation Date: 2016-12-21T12:38:02Z
Registry Expiry Date: 2022-12-21T12:38:02Z
Registrar: Alibaba Cloud Computing (Beijing) Co., Ltd.
Registrar IANA ID: 420
Registrar Abuse Contact Email: DomainAbuse@service.aliyun.com
Registrar Abuse Contact Phone: +86.95187
Domain Status: clientTransferProhibited <https://icann.org/epp#clientTransferProhibited>
Name Server: DNS13.HICHINA.COM
Name Server: DNS14.HICHINA.COM
DNSSEC: unsigned

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®

Requerimientos Técnicos empleados



#IntelCon2021

**VM Ubuntu Desktop
20.04**
12 Gb en RAM
4 Procesadores
40 Gb en Disco Duro



Software Adicionalmente Instalado

- Cliente de TOR (Instalará también el servicio)
- Onion Search
- ProxyChains4
- Nmap
- Splash
- Docker Server
- Page-Compare
- Privoxy
- Curl



Gracias por la atención

Congreso Online de Ciberinteligencia

#IntelCon2021



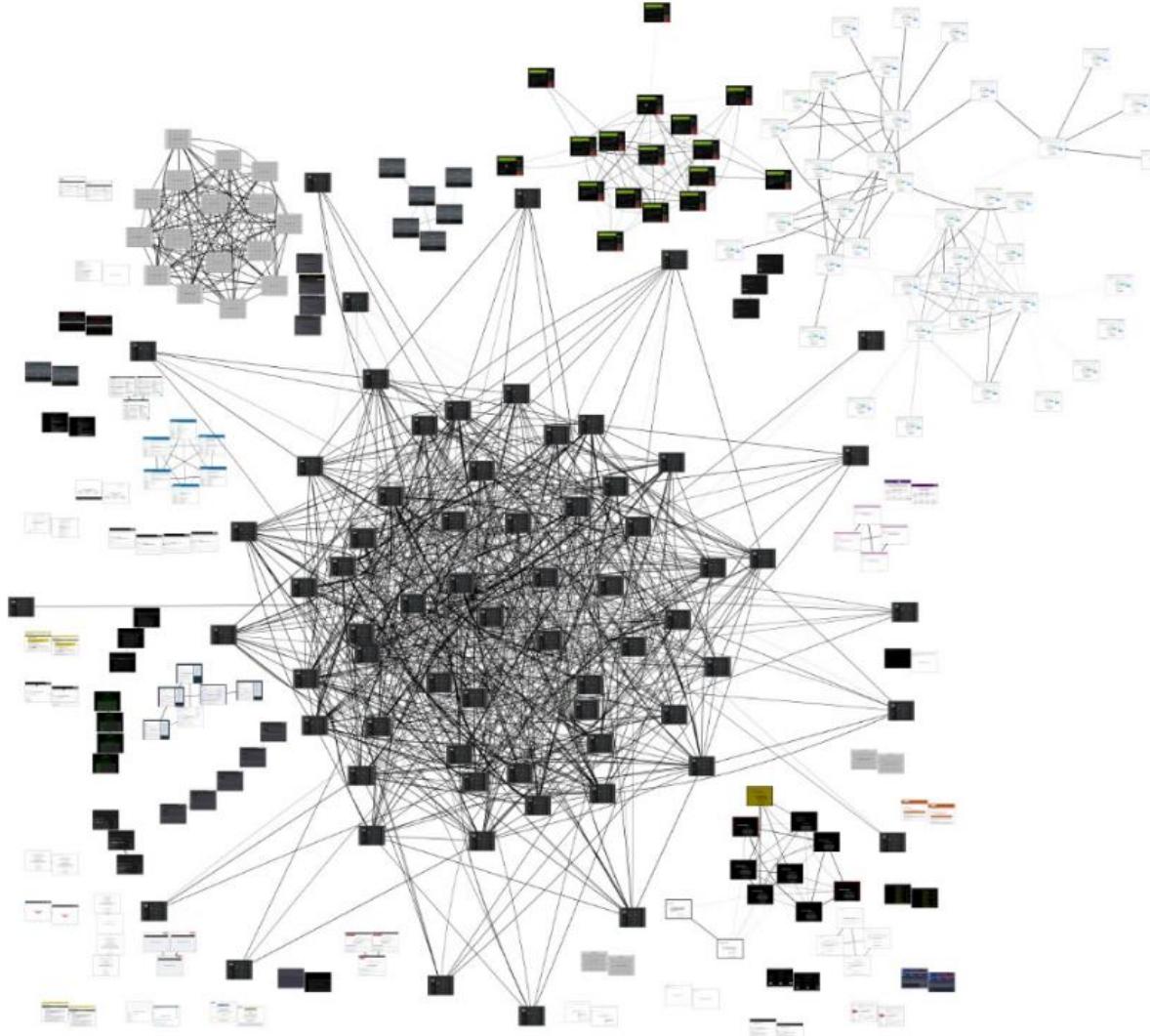
IntelCon
by Ginseg

BONUS STAGE

Gracias por la atención

Congreso Online de Ciberinteligencia

Es posible ubicar la relación entre sitios de la red de TOR.



Es posible ubicar la relación entre sitios de la red de TOR.



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.

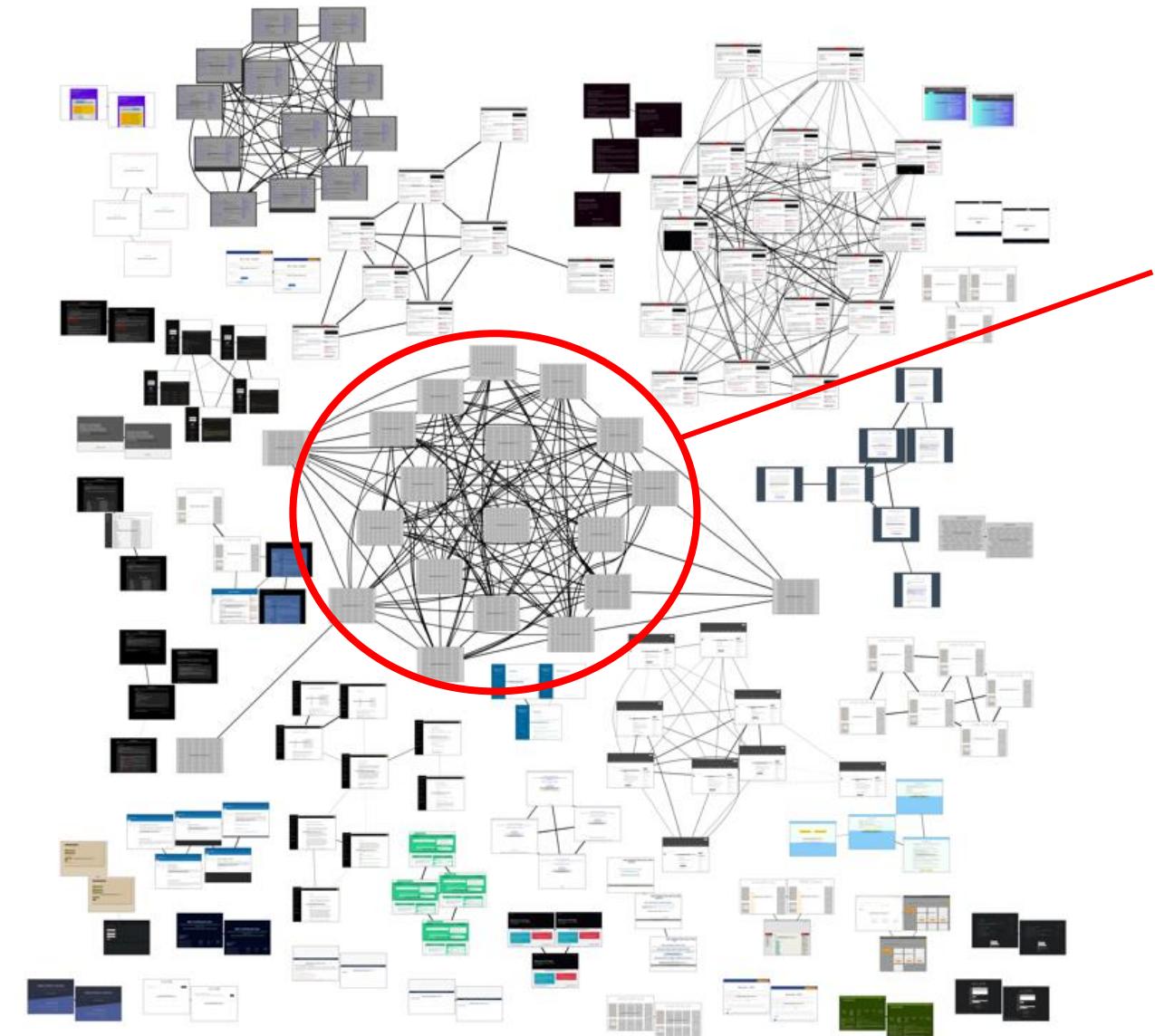
<https://splash.readthedocs.io/en/stable/api.html>

PAGE COMPARE

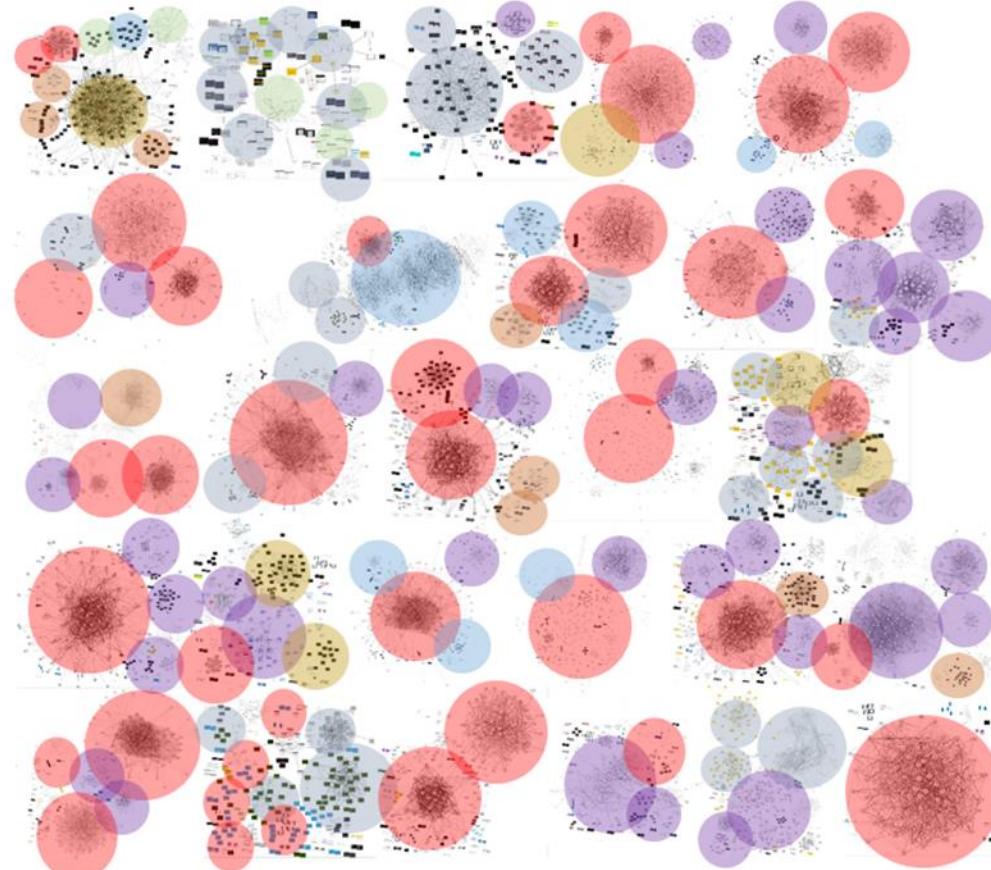
Es una herramienta que realiza comparaciones entre el contenido html de una página web contra otra y con ello permite realizar diagramas de relación entre ellas.

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

Es posible ubicar la relación entre sitios de la red de TOR.



Es posible ubicar la relación entre sitios de la red de TOR.



Gracias por la atención

Congreso Online de Ciberinteligencia