

ANONIMATO E SUAS FACETAS

25/04/2022



UNIDADE 37
SEGURANÇA CIBERNÉTICA

FIAP

\$ CAT .AGENDA

- ❖ Disclaimer && whoami && objetivo
- ❖ O que é o Anonimato?
- ❖ Open-Source Intelligence (OSINT)
- ❖ Operations Security (OPSEC)
- ❖ Anonimato na Prática
- ❖ De-Anonimização
- ❖ Recursos e Referências

./AVISO LEGAL

- ❖ A apresentação a seguir não expressa de **nenhuma maneira a opinião**, ou faz referência de nenhuma natureza ao **meu empregador**.
- ❖ Todas as ideias e pontos de vistas apresentadas aqui são de minha inteira responsabilidade;
- ❖ Todos os documentos externos, imagens e artigos aqui referenciados, estão indexados em “Referências”.
- ❖ Um grande agradecimento aos profissionais de segurança e suas pesquisas!



MORE ~/.PROFILE

- ❖ Real Name: Felippe Foppa
- ❖ Area de atuação: Redteamer, Pentester and Security Researcher
- ❖ Current Role:
 - ❖ Founder | Chief Executive Officer – Unidade 37 Segurança Cibernética Ofensiva
 - ❖ Especialista de Segurança Ofensiva - GlobalHitss
- ❖ Certifications: LPI1, LPI2, OSCP, CRTP, eWPTXv2, eCPTXv2, ISO27k, ITILv4
- ❖ CVE's: CVE-2021-39375, CVE-2021-39376
- ❖ Material apresentado estará disponível no repositório:
 - ❖ <https://github.com/d34dfr4m3/Contributions/>
- ❖ Blog: <https://diesec.home.blog/>
- ❖ Linkedin: <https://www.linkedin.com/in/felippe-foppa-6b1434108/>
- ❖ Github: <https://github.com/d34dfr4m3>



echo \$OBJETIVO

- ❖ A expectativa no pouco tempo de duração de agenda é expor as facetas do anonimato e sua importância, não só no contexto positivo da liberdade de expressão, equipes de segurança ofensiva e inteligência, mas também em como é utilizado por criminosos cibernéticos e ativistas.

O que é o Anonimato?

Entendendo a Origem

Origem

- ❖ Com o advento das mensagens por telecomunicações e, em particular, pela Internet, designa o ato de manter uma identidade escondida de terceiros;
- ❖ Mas o anonimato também pode ser entendido como um instrumento que conserva a privacidade e a segurança na internet e, de certa forma, auxilia o exercício da liberdade de expressão;
- ❖ Anonimato e Privacidade?

Privacidade vs Anonimato

- ❖ Apesar da proximidade, anonimato e privacidade não têm o mesmo significado;
- ❖ Principalmente porque a privacidade, que é um direito constitucional no Brasil, não dispensa a identificação do usuário, mas exige a proteção a informações pessoais;
- ❖ Segundo pontua a **Constituição Federal** em seu **Art. 5º, inciso X:**
 - ❖ “**São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação.**”
- ❖ Assim, podemos concluir que a privacidade se refere ao direito de controlar a divulgação de dados e informações a respeito de nós mesmos, enquanto o anonimato é o ato de não divulgar a identidade.



Criptoanarquismo

- ❖ O cripto-anarquismo é uma tática anarquista de ação-direta alternativa e tem como principal preocupação garantir a privacidade e a liberdade extra estatal, por meio da utilização de criptografia;
- ❖ Uma das motivações dos cripto-anarquistas é a defesa contra a vigilância de redes de comunicação de computadores. Cripto-anarquistas tentam proteger-se contra a retenção de dados de telecomunicações, a polêmica vigilância sem mandado, entre outras coisas;
- ❖ Cripto-anarquistas consideram o desenvolvimento e uso de criptografia como a principal defesa contra tais problemas, em oposição à ação política. A segunda preocupação é **a fuga da censura, especialmente a censura na Internet, em razão da liberdade de expressão**. Os programas utilizados pelos cripto-anarquistas muitas vezes tornam possível publicar e ler informações anonimamente que estão "inacessíveis" na internet ou outras redes de computadores.



Criptoanarquismo

- ❖ Tor, I2P, Freenet e muitas redes similares permitem páginas "escondidas" acessíveis apenas por usuários destes programas. Isso ajuda denunciantes e a oposição política em nações opressoras a espalhar suas informações. Uma terceira razão é desenvolver e participar da **contra-economia**;
- ❖ **Cripto-moedas** como **Bitcoin** e serviços como **Silk Road** tornam possível o comércio de bens e serviços com pouca interferência da lei. Além disso, o desafio técnico no desenvolvimento destes sistemas criptográficos é enorme, o que interessa a alguns programadores trabalharem em conjunto nos projetos.

Como alcançar o Anonimato?

- ❖ Personas (Profiles)
 - ❖ Nomes de usuários, personalidades etc.
- ❖ Metadados
 - ❖ Informações em Arquivos;
 - ❖ Ex: Geolocalização, Owner, etc.
- ❖ Tráfego de Rede
 - ❖ Endereços (IP Address) de origem;
 - ❖ DNS leakage;
- ❖ Padrão Comportamental Online
 - ❖ Textos, emojis etc.

CriptoMoedas

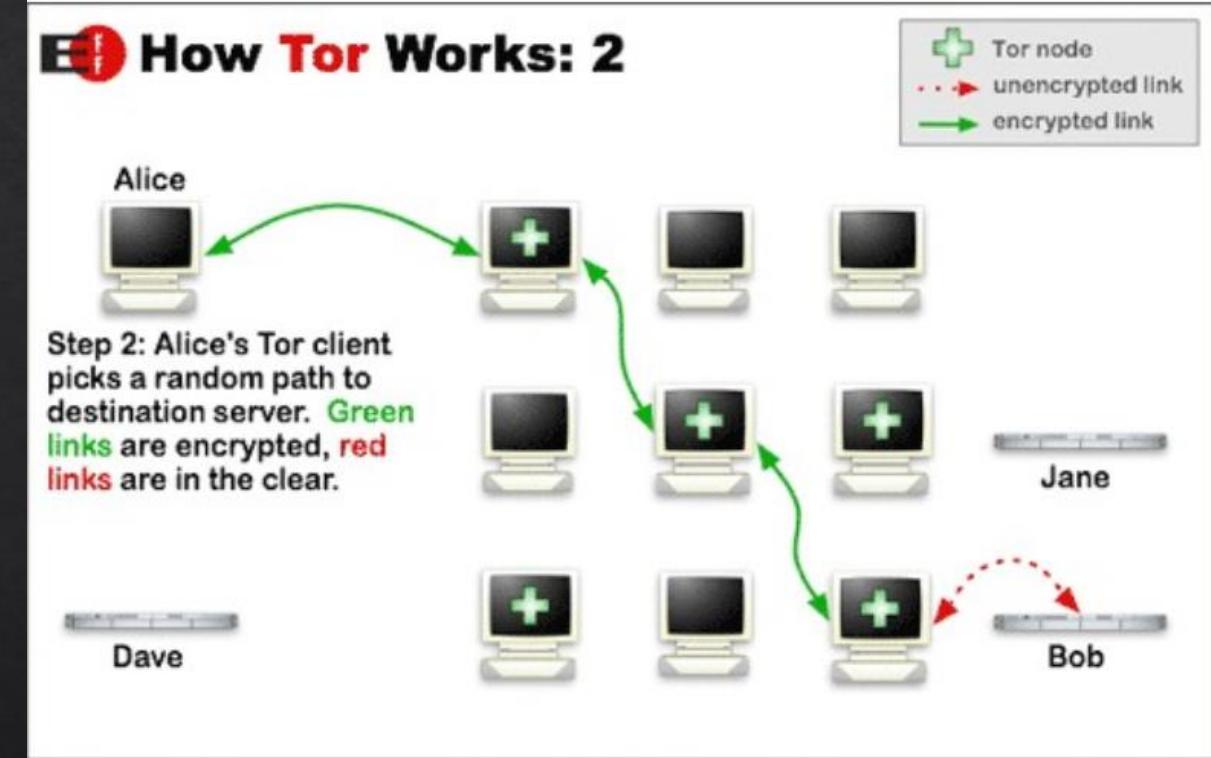
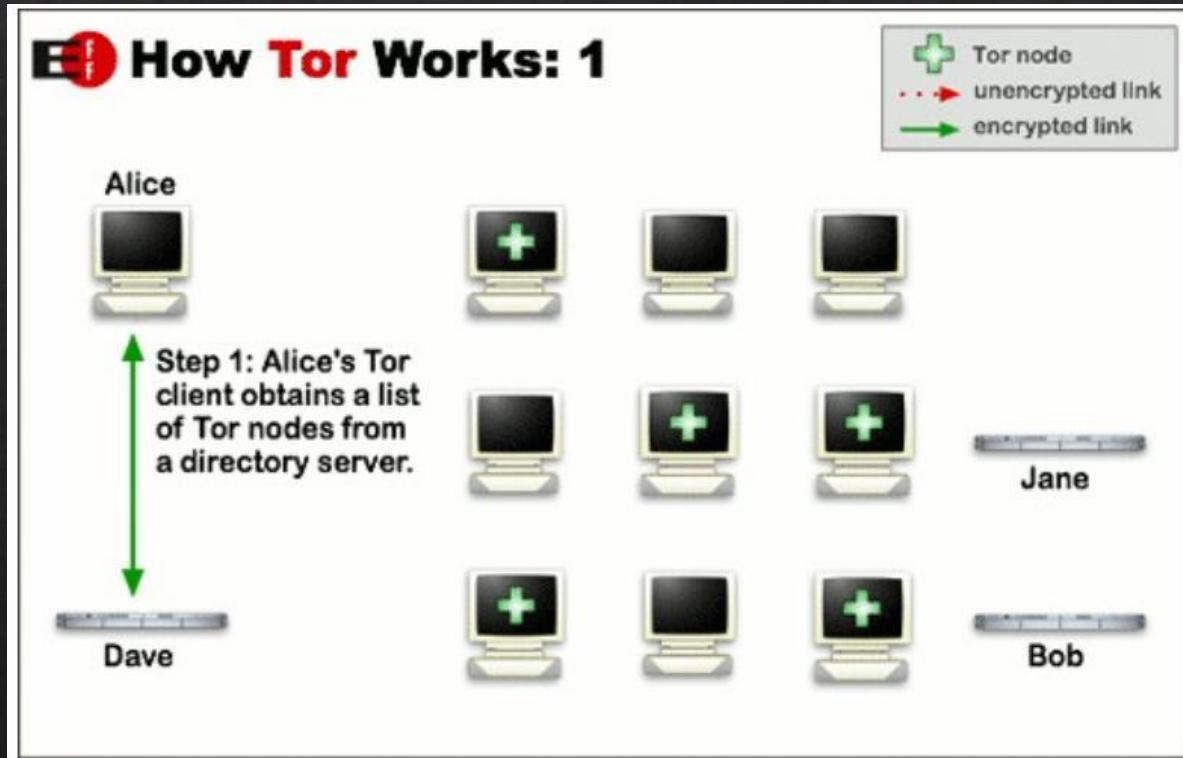




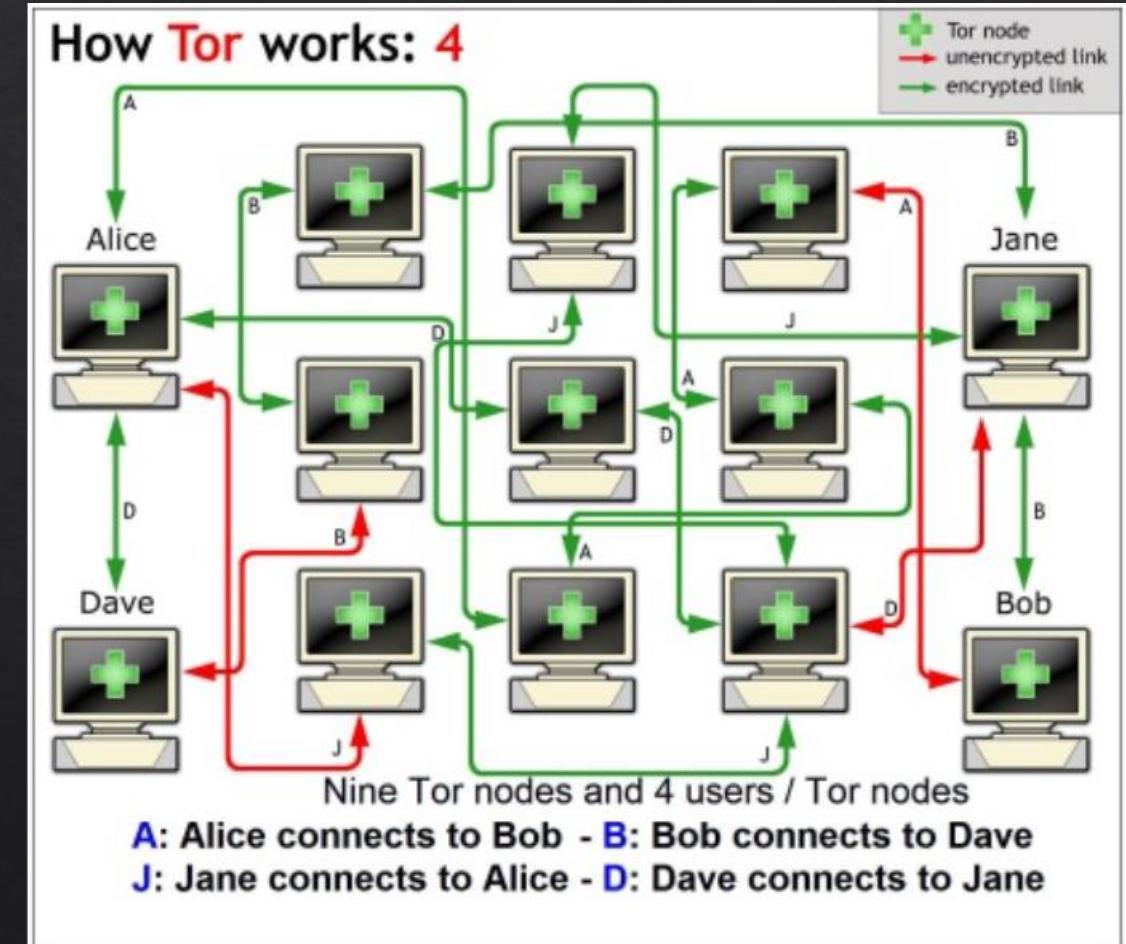
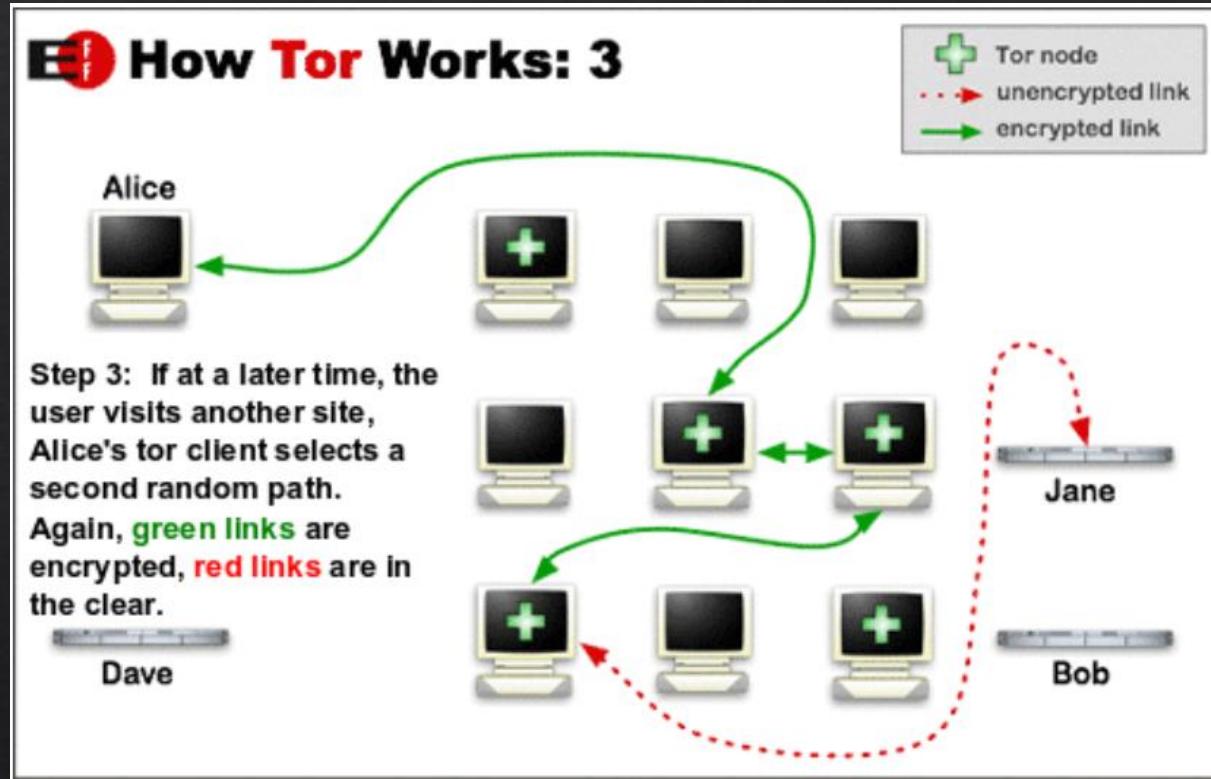
The Tor Project

- ❖ “We believe everyone should be able to explore the internet with privacy. We are the Tor Project, a US nonprofit. We advance human rights and defend your privacy online through free software and open networks.” – Tor Project;
- ❖ Block Trackers;
- ❖ Defesa contra Surveillance;
- ❖ Resist Fingerprinting;
- ❖ Multi-Layered Encryption;
- ❖ Browse Freely.

The Tor Project



The Tor Project



APPs



Signal



ProtonMail

Case - WannaCry hero

- ❖ Marcus Hutchin aka MalwareTech;
- ❖ Preso em Agosto de 2017 pelo FBI em Las Vegas aos 23 anos acusado de vender Malware bancário conhecido como Kronos;
- ❖ Pesquisa de DNS pelo nome Marcus Hutchins retorna alguns domínios relacionados a ele:
 - ❖ surfa1day2day@hotmail.co.uk – Mesmo endereço utilizado pelo residente do Reino Unido (Marcus Hutchin);
 - ❖ Gh0sth0sting[dot]com – Serviço de Hospedagem relacionado com o HackForums.net;
 - ❖ O endereço surfa1day2day@hotmail.co.uk vinculado aos registros iniciais de registro de domínio da Gh0sth0sting também foi usado para registrar uma conta do Skype chamada **Iarkey** que listava seu alias como “**Marcus**”. Uma conta no Twitter registrada em 2009 sob o apelido “**Iarkey**” aponta para Gh0sth0sting[ponto]com;
- ❖ Para mais infos sobre a exposição, consulte:
 - ❖ <https://krebsonsecurity.com/2017/09/who-is-marcus-hutchins/>

Case - WannaCry hero

Plaintiff,

v.

[REDACTED]
[REDACTED] and
MARCUS HUTCHINS,
aka "Malwaretech,"

Defendants.

Case No. **17-CR-124**

[Title 18, United States Code,
Sections 371, 1030(a)(5)(A),
2511(a)(1), and 2512(1)(a), (b), and
(c)(i)]

- a. Defendant MARCUS HUTCHINS created the Kronos malware.
- b. On or about July 13, 2014, a video showing the functionality of the "Kronos Banking trojan" was posted to a publically available website. Defendant [REDACTED] used the video to demonstrate how Kronos worked.
- c. In or around August 2014, on an internet forum, defendant [REDACTED] offered to sell the "Kronos Banking trojan" for \$3,000.
- d. In or around February 2015, defendants MARCUS HUTCHINS and [REDACTED] updated the Kronos malware.
- e. On or about April 29, 2015, defendant [REDACTED], using the name [REDACTED] advertised the availability of the Kronos malware on the AlphaBay market forum.
- f. On or about June 11, 2015, defendant [REDACTED] sold a version of the Kronos malware in exchange for approximately \$2,000 in digital currency.
- g. On or about July 17, 2015, defendant [REDACTED] offered crytping services for Kronos.

All in violation of Title 18, United States Code, Section 371.

THE GRAND JURY CHARGES:

1. At times material to this indictment:

DEFENDANTS

- a. Defendant [REDACTED]
[REDACTED] used the online aliases [REDACTED]
- b. Defendant MARCUS HUTCHINS was a citizen and resident of the United Kingdom. HUTCHINS used various online aliases, including "Malwaretech."

Case – Ukraine War

- ❖ Metadados de fotos de combatentes na ucrânia subsidiando bombardeios Russos (Não Confirmado);

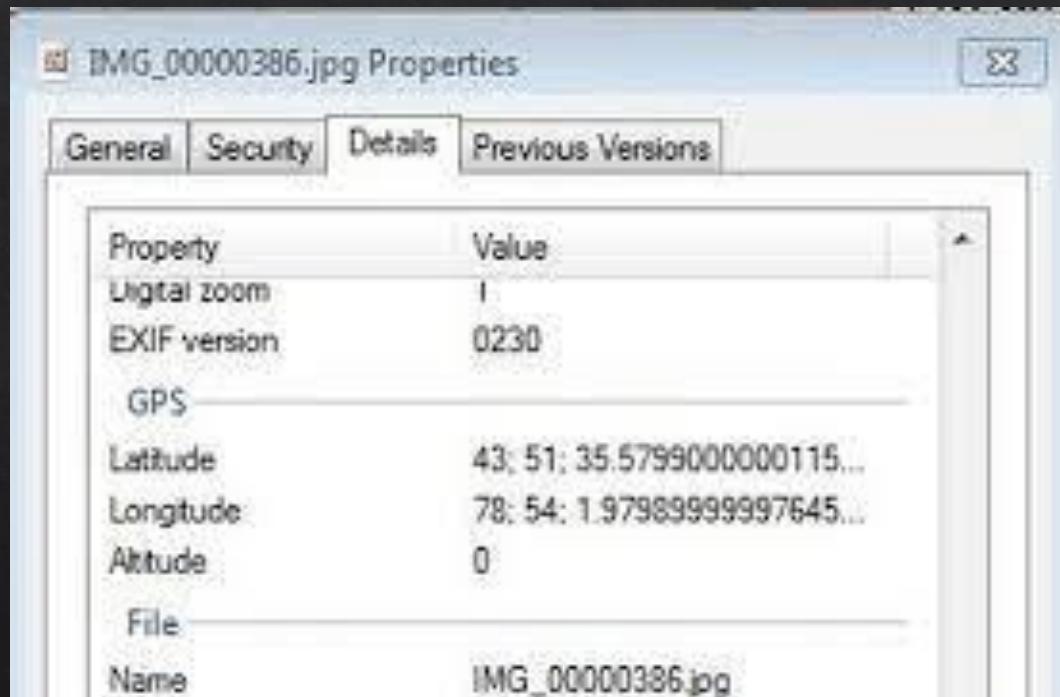
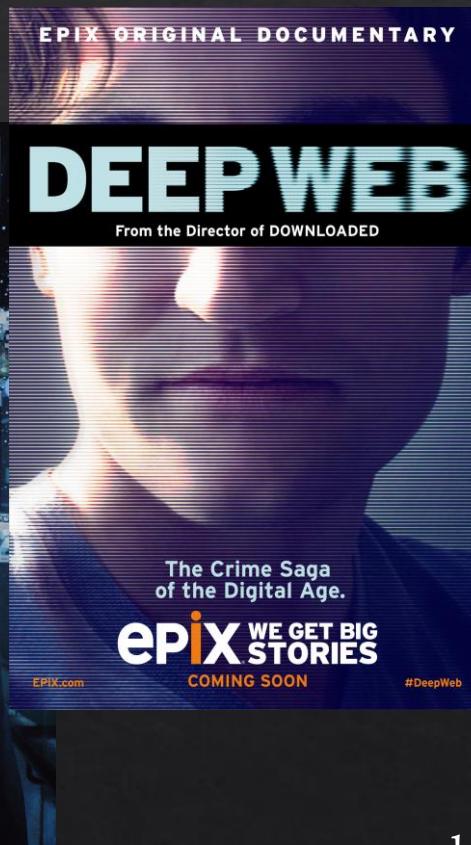


Imagen Ilustrativa

Emprego do Anonimato

- ❖ Anti Censura e Liberdade de Expressão;
- ❖ Inteligencia (Threat Intel) e infiltração;
- ❖ Ativistas (jornalistas etc) e Hacktivistas;
- ❖ ContraEconomia
 - ❖ CritpoMoedas (Monero, Bitcoin etc);
- ❖ CiberCriminosos;
- ❖ RedTeam Remotos.

Sugestão de Conteúdo



CYBERWAR / S2 EP4

A screenshot from the TV show "CYBERWAR". It shows a man with a beard and short hair, wearing a dark jacket, sitting in a car and looking intensely at something off-camera. A timestamp in the bottom left corner reads "22:33".

ACTIVISTS VS. THE SURVEILLANCE STATE

Activists fight against America's growing cyber-surveillance industrial complex

https://www.vicetv.com/en_us/show/cyberwar

Open-Source Intelligence (OSINT)

Find and profile your targets!

Open-Source Intelligence (OSINT)

- ❖ Open Source Intelligence, OSINT, refere-se a todas as informações que podem ser encontradas publicamente, via internet, sem violar quaisquer leis de direitos autorais ou privacidade;
- ❖ É a **coleta, análise e o processamento de informações**. Sob esta definição, uma ampla gama de fontes pode ser considerada parte de OSINT. Por exemplo, **informações publicadas em sites de mídia social, fóruns de discussão, chats em grupo**, basicamente qualquer informação que possa ser **encontrada pesquisando online**;
- ❖ Porém, a maioria dos recursos OSINT não pode ser encontrada usando mecanismos de buscas comuns, como o Google, em cenários onde as informações não são indexadas (dark/deepweb).

Open-Source Intelligence (OSINT)

- ❖ Em ciber segurança, OSINT é extremamente útil para os profissionais de segurança, que utilizam técnicas e ferramentas de pesquisa para descobrir fraquezas em sistemas de TI, para que essas vulnerabilidades possam ser resolvidas antes que criminosos as descubram;
- ❖ As vulnerabilidades comumente encontradas incluem, por exemplo, vazamento acidental de informações confidenciais em sites de mídia social;
- ❖ Por outro lado, cibercriminosos utilizam OSINT dessa mesma forma para encontrar informações sobre suas vítimas, identificar falhas nas redes, e através dessa inteligência conseguir explorar o alvo. Por isso, é considerada uma ferramenta valiosa para auxiliar na realização de ataques de engenharia social, sendo que geralmente, a primeira fase da maioria de um pentest começa com o reconhecimento, ou seja, utilizando OSINT.

DarkWeb e DeepWeb

❖ DeepWeb

- ❖ É a web que não pode ser acessada pelos mecanismos de busca, como dados privados do governo, dados bancários, dados em nuvem etc. Esses dados são confidenciais e privados, portanto, mantidos fora de alcance. Ele é usado para fornecer acesso a um específico para um grupo específico de pessoas. Na dark web, os usuários realmente escondem dados intencionalmente.

❖ DarkWeb

- ❖ A dark web refere-se ao conteúdo on-line criptografado que não é indexado pelos mecanismos de pesquisa convencionais. A Darknet fornece anonimato ao usuário, mas foi introduzido um serviço que permitiu que alguém hospedasse um site na darknet e permanecesse anônimo. Isso atraiu pessoas que fazem coisas ilegais para vender coisas sem serem pegos. Um exemplo é um site chamado silkroad que estava na darknet chamado TOR, usado para vender drogas e foi derrubado pelo FBI.

Open-Source Intelligence (OSINT)

- ❖ Motores de Busca:

- ❖ Google
- ❖ DuckDuckGo
- ❖ Bing
- ❖ etc

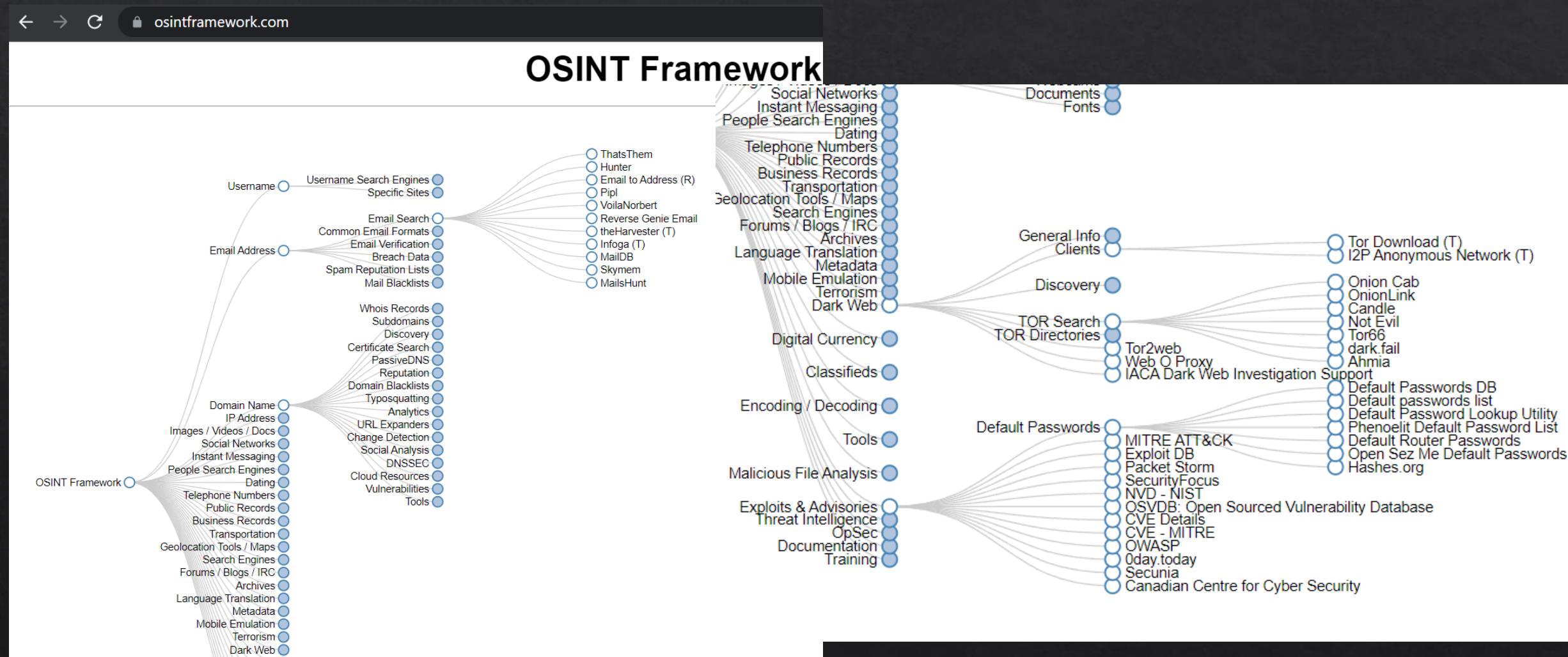
- ❖ Redes Sociais

- ❖ Facebook
- ❖ Instagram
- ❖ Twitter
- ❖ Linkedin
- ❖ etc

- ❖ Sites Gerais

- ❖ Trello
- ❖ Gitlab/Github
- ❖ etc

OSINT Framework



<https://osintframework.com/>

Google Hacking (ou Dorks) - Operadores

Advanced Operators at a Glance

Advanced operators can be combined in some cases.

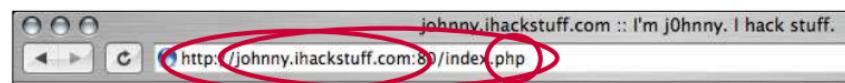
In other cases, mixing should be avoided.

Operator	Purpose	Mixes with other operators?	Can be used alone?	Does search work in			
				Web	Images	Groups	News
intitle	Search page title	yes	yes	yes	yes	yes	yes
allintitle	Search page title	no	yes	yes	yes	yes	yes
inurl	Search URL	yes	yes	yes	yes	not really	like intitle
allinurl	Search URL	no	yes	yes	yes	yes	like intitle
filetype	Search specific files	yes	no	yes	yes	no	not really
allintext	Search text of page only	not really	yes	yes	yes	yes	yes
site	Search specific site	yes	yes	yes	yes	no	not really
link	Search for links to pages	no	yes	yes	no	no	not really
inanchor	Search link anchor text	yes	yes	yes	yes	not really	yes
numrange	Locate number	yes	yes	yes	no	no	not really
daterange	Search in date range	yes	no	yes	not really	not really	not really
author	Group author search	yes	yes	no	no	yes	not really
group	Group name search	not really	yes	no	no	yes	not really
insubject	Group subject search	yes	yes	like intitle	like intitle	yes	like intitle
msgid	Group msgid search	no	yes	not really	not really	yes	not really

Some operators can only be used to search specific areas of Google, as these columns show.

Crash course in advanced operators

Some operators search overlapping areas. Consider site, inurl and filetype.



Site can not search port.

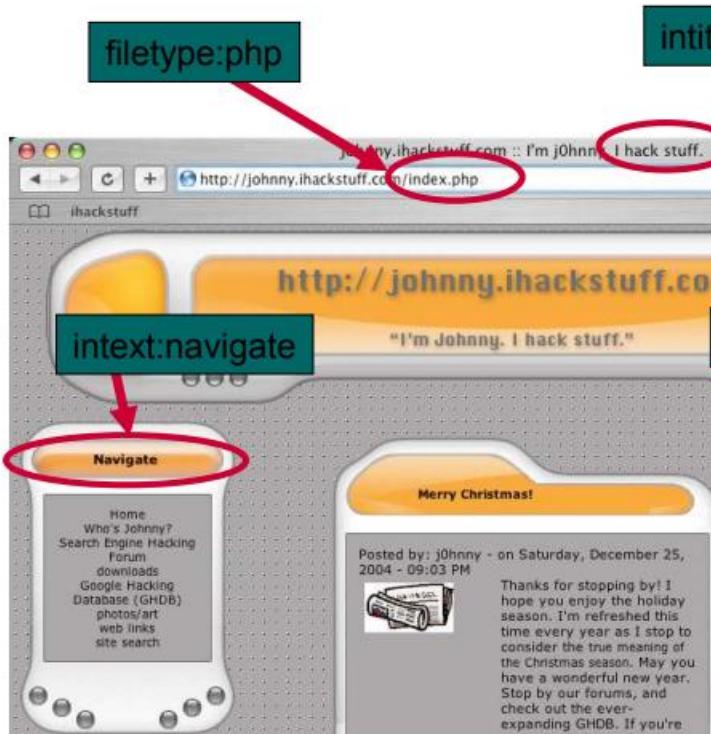
Inurl can search the whole URL, including port and filetype.

Filetype can only search file extension, which may be hard to distinguish in long URLs.

Google Hacking (ou Dorks)

Advanced Google Searching

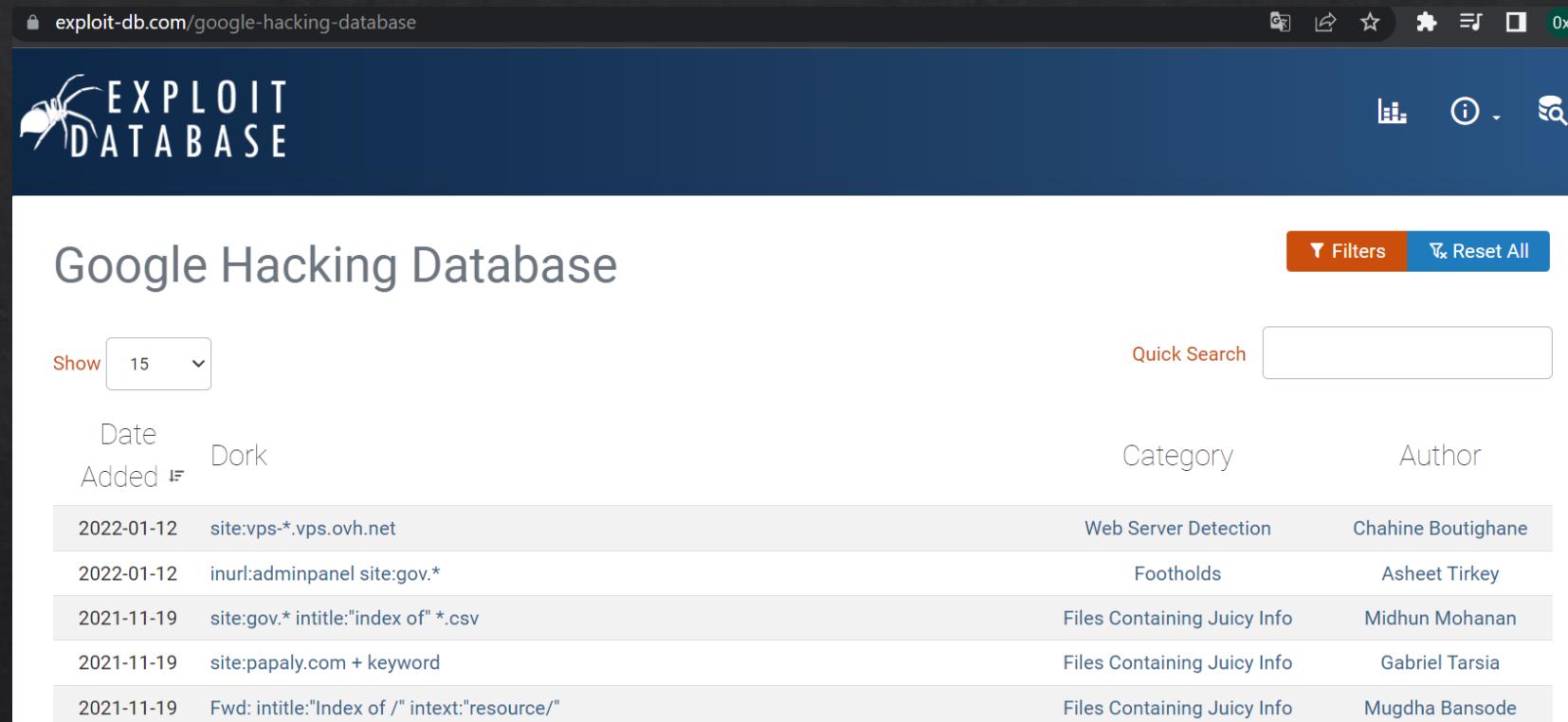
There are many ways to find the same page. These individual queries could all help find the same page.



Advanced Google Searching

The image shows a Google search results page with a single result. The search query is "numrange:99999-100000 intitle:'I hack stuff' filetype:php intext:'navigate'". The result is a link to "johnny.ihackstuff.com :: I'm j0hnny. I hack stuff.". A speech bubble on the right side of the screen says: "Put those individual queries together into one monster query and you only get that one specific result." Another speech bubble at the bottom right says: "Adding advanced operators reduces the number of results adding focus to the search."

Google Hacking (ou Dorks) - GHD



The screenshot shows the Exploit Database Google Hacking Database page. The URL in the browser bar is <https://www.exploit-db.com/google-hacking-database>. The page has a dark blue header with the Exploit Database logo (a stylized spider icon) and the text "EXPLOIT DATABASE". Below the header, there's a search bar with a magnifying glass icon and a "Quick Search" input field. On the right side of the header are icons for filters, reset all, and other navigation. The main content area is titled "Google Hacking Database". It features a table with columns: Date Added, Dork, Category, and Author. The table contains five rows of data:

Date Added	Dork	Category	Author
2022-01-12	site:vps-* .vps.ovh.net	Web Server Detection	Chahine Boutighane
2022-01-12	inurl:adminpanel site:gov.*	Footholds	Asheet Tirkey
2021-11-19	site:gov.* intitle:"index of" *.csv	Files Containing Juicy Info	Midhun Mohanan
2021-11-19	site:papaly.com + keyword	Files Containing Juicy Info	Gabriel Tarsia
2021-11-19	Fwd: intitle:"Index of /" intext:"resource/"	Files Containing Juicy Info	Mugdha Bansode

<https://www.exploit-db.com/google-hacking-database>

DuckDuckGo (ou DDG)

help.duckduckgo.com/duckduckgo-help-pages/results/syntax/ 🔍 ⌂ ⌂ ⌂ ⌂ ⌂

The image shows a web browser window with two tabs open. The left tab is titled "Results" and contains the "DuckDuckGo Search Syntax" page. It features a table of search operators with examples and results. The right tab is titled "github.com/d34dfr4m3/goDuck" and shows a GitHub repository for "d34dfr4m3 / goDuck". The repository is public and has 1 branch and 0 tags. The README.md file has been updated by user "d34dfr4m3" on 11 Jan 2019 with 10 commits. Other files shown include dorklist, goDuck.py, install.sh, and requirements.txt.

Example	Result
<code>cats dogs</code>	Results about cats or dogs
<code>"cats and dogs"</code>	Results for exact term "cats and dogs". If no results are found, try to show related results.
<code>cats -dogs</code>	Fewer dogs in results
<code>cats +dogs</code>	More dogs in results
<code>cats filetype:pdf</code>	PDFs about cats. Supported file types: pdf, doc(x), xls(x), ppt(x)
<code>dogs site:example.com</code>	Pages about dogs from example.com
<code>cats -site:example.com</code>	Pages about cats, excluding example.com
<code>intitle:dogs</code>	Page title includes the word "dogs"
<code>inurl:cats</code>	Page url includes the word "cats"

`d34dfr4m3 / goDuck` Public

Code Issues Pull requests Actions Projects Wiki Security Insights Settings

master 1 branch 0 tags

d34dfr4m3 Update README.md 9231820 On 11 Jan 2019 10 commits

README.md Update README.md 3 years ago

dorklist Create dorklist 3 years ago

goDuck.py Update goDuck.py 3 years ago

install.sh Create install.sh 3 years ago

requirements.txt Create requirements.txt 3 years ago

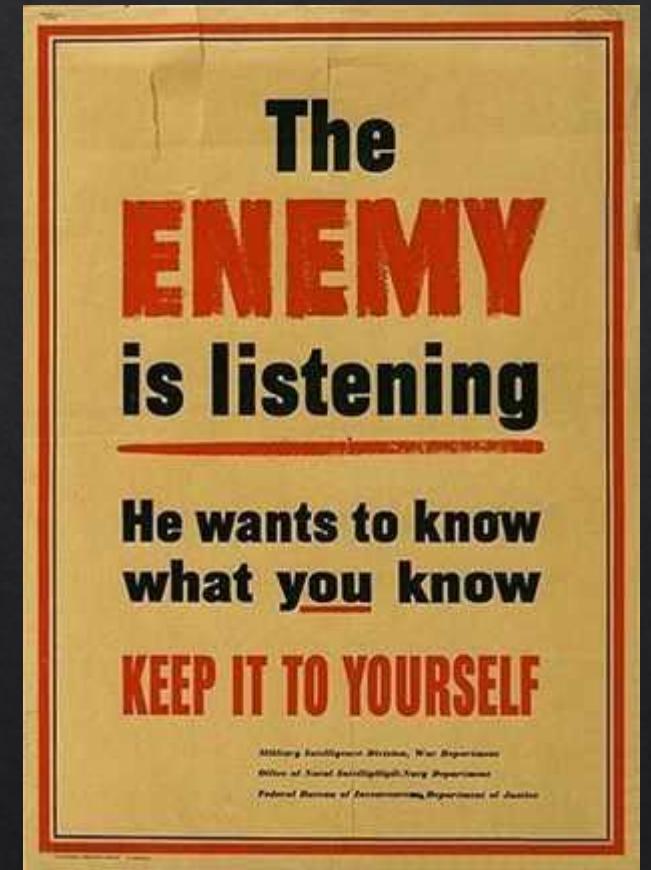
<https://help.duckduckgo.com/duckduckgo-help-pages/results/syntax/>
<https://github.com/d34dfr4m3/goDuck>

Operations Security

OPSEC

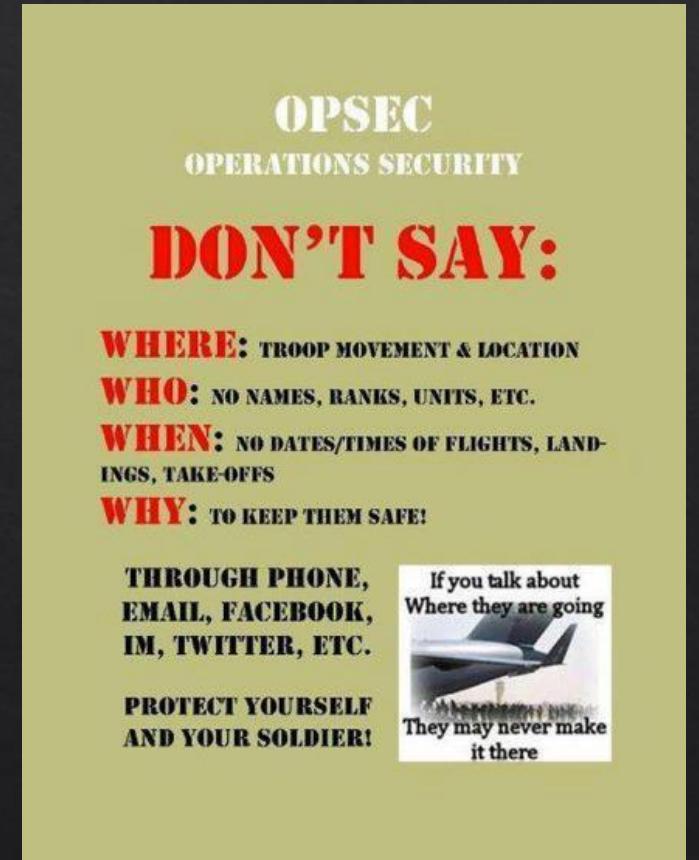
Operations Security (ou OPSEC)

- ❖ É um termo que foi cunhado por militares norte-americanos durante a Guerra do Vietnã;
- ❖ É um processo que identifica informações críticas para determinar se ações amigas conseguem ser observadas pela inteligência inimiga, determina se as informações obtidas pelo adversário podem ser interpretadas como úteis para eles e, em seguida, executa ações selecionadas que eliminam ou reduz a exploração adversa de informações críticas amigas;
- ❖ Visa dar a uma operação militar, por exemplo, o nível apropriado de segurança, negar o conhecimento ao potencial oponente sobre as disposições, capacidades, intenções e vulnerabilidades das forças amigas.



OPSEC em CiberSecurity

- ❖ BlackHats/APTs;
- ❖ RedTeam;
- ❖ Threat Intel.



Cenários

- ❖ BlackHats/APTs
- ❖ RedTeam
- ❖ All the same
 - ❖ Ocultar as operações das equipes de defesa (BlueTeam, Intel etc)
 - ❖ Táticas, Técnicas e Procedimentos
 - ❖ Detecção etc.



O Adversário (BlueTeam)

- ❖ Equipes de BlueTeam com maturidade podem ter diversas fontes para detectar atividades suspeitas:
 - ❖ Logs em sistemas/serviços voltados para a Internet;
 - ❖ Fazer logon em sistemas e conexões que saem do sistema interno/rede (por exemplo, estações de trabalho);
 - ❖ Vários serviços de "inteligência de ameaças" de terceiros;
 - ❖ Análise e correlação de informações coletadas dessas fontes.

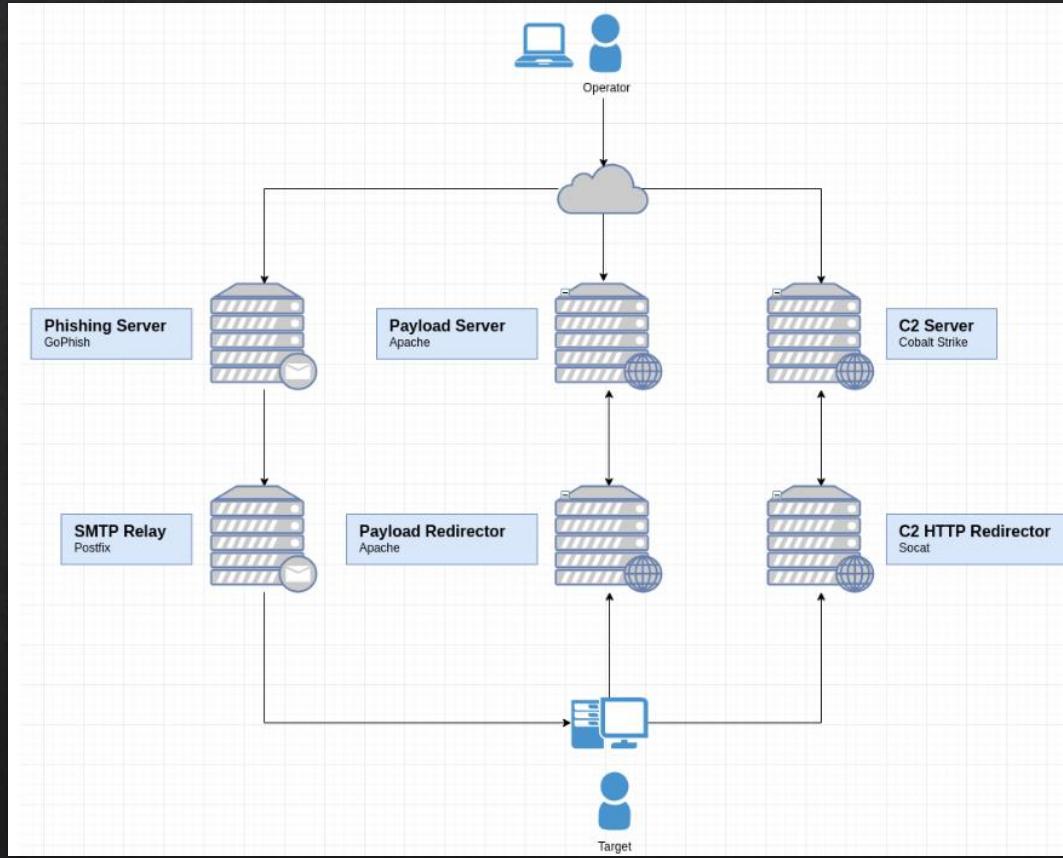
O Adversário (BlueTeam)

- ❖ Cada interação da equipe ofensiva deixa traços para a equipe de BlueTeam;
- ❖ Com traços suficientes, a equipe defensiva pode ligar os pontos, identificando as ferramentas da equipe ofensiva e infraestrutura, podendo prevenir ataques antes que eles ocorram;
- ❖ Se a equipe defensiva identificar a operação da campanha, ela precisará ser queimada, exigindo grande esforço da equipe ofensiva para subir uma nova infraestrutura ou preparer novas ferramentas ou abordagens;
- ❖ É um cenário complicado, uma vez que a interação direta tende a deixar rastros.

Contra Medidas

- ❖ Proteger a Infraestrutura de RedTeam com relays e Http Forwarders;
- ❖ Camuflar o endereço de origem para não levanter suspeitas (endereços do mesmo país etc);
- ❖ Se for deixar rastros, deixe rastros falsos que levem a equipe defensiva para becos sem saídas;
- ❖ Ajustes de ferramentas, removendo metadados etc.

Infraestrutura de RedTeam



Contra Medidas – Metadados de Ferramentas

- Nmap default User-Agent:

```
└$ nmap -p80 --script=default 127.0.0.1
```

```
GET / HTTP/1.1
Host: localhost
Connection: close
User-Agent: Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)
```

- WPScan default User-Agent:

```
└$ wpscan --url 127.0.0.1
```

```
Accept-Encoding: gzip, deflate
User-Agent: WPScan v3.8.12 (https://wpscan.com/wordpress-security-scanner)
```

Anonimato na Prática

Camuflagem de Endereço IP

Camuflagem de IP

- ❖ Proxies
 - ❖ Proxychains
 - ❖ Reputação de IP
- ❖ VPNs
 - ❖ <https://github.com/d34dfr4m3/Jumper>
- ❖ Tor Network, darknets
 - ❖ Splitter – Publicado na H2HC 2018 (<https://dieseclivehome.blog/2018/12/07/h2hc-2018/>)
 - ❖ <https://github.com/h2hconference/2018/blob/master/H2HC%20University%20-%20Rener%20Silva%20-%20Splitter%20Paper%20%26%20Slides.zip>
 - ❖ <https://dieseclivehome.blog/2018/12/07/h2hc-2018/>
 - ❖ Bloqueio de Nodes de saída tor (<https://check.torproject.org/torbulkexitlist>)

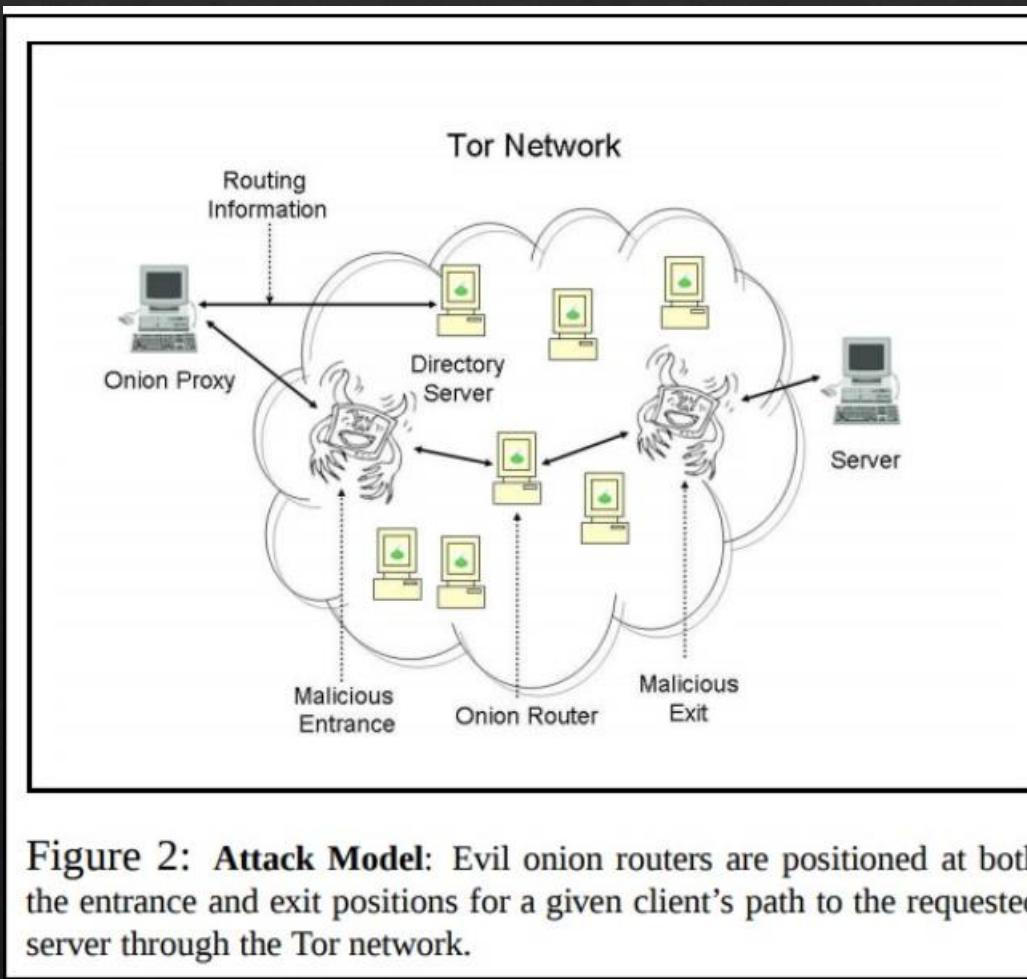
De-Anonimização

Abordagens para De-Anonimizar Usuários

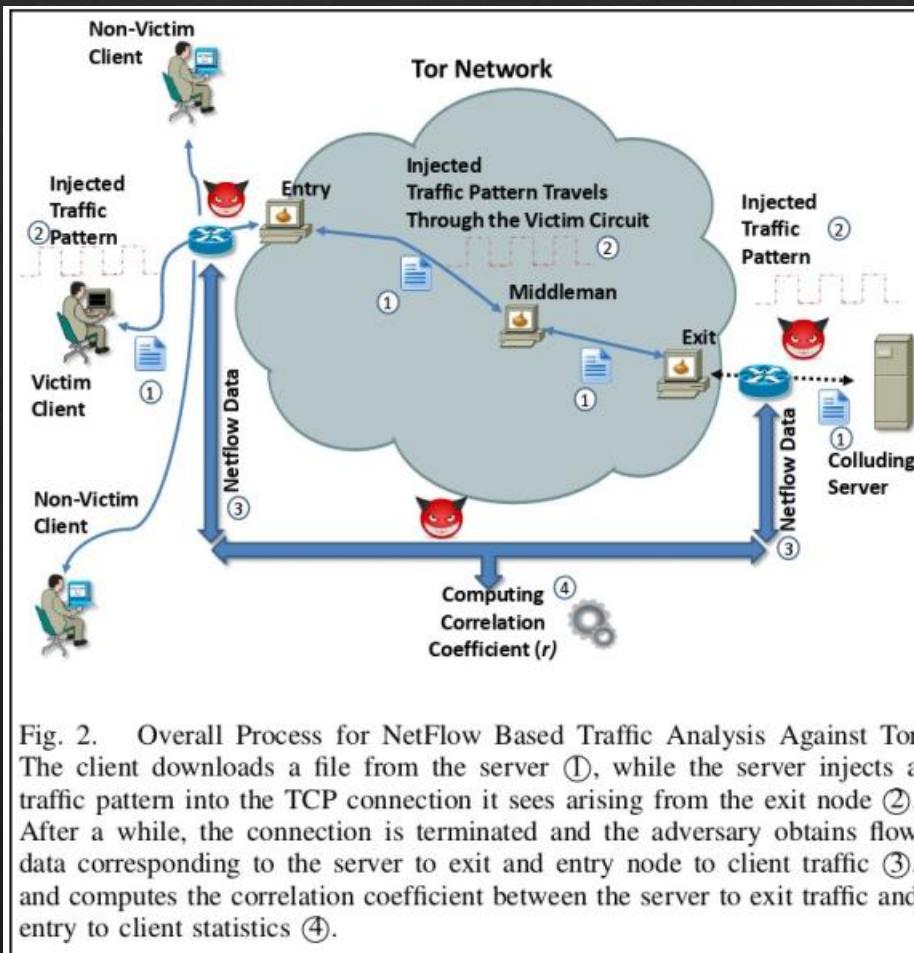
Fragilidades da Anonimização

- ❖ Fator Humano
 - ❖ User Behavior e Metadados
- ❖ Tor De-Anonymization
 - ❖ Low-Resource Routing Attacks Against Anonymous Systems
 - ❖ A Practical Congestion Attack on Tor Using Long Paths
 - ❖ On the Effectiveness of Traffic Analysis Against Anonymity Networks Using Flow Records
 - ❖ How Much Anonymity does Network Latency Leak?

Low-Resource Routing Attacks Against Anonymous Systems



On the Effectiveness of Traffic Analysis Against Anonymity Networks Using Flow Records



Others

- ❖ How Much Anonymity does Network Latency Leak?
 - ❖ <https://www-users.cs.umn.edu/~hoppernj/tissec-latency-leak.pdf>

Common Weakness from De-anonymization Techniques

- ❖ The majority of De-anonymization Techniques rely that victim will use:
 - ❖ The same TOR circuit to transfer the injected pattern.
 - ❖ The same global network path from the compromised web server or compromised EXIT NODE to the client.
 - ❖ The same TCP STREAM or the same global path to transfer a cert amount of data necessary to transmit a specific pattern during a specific time frame.
 - ❖ The victim will exchange a minimum amount of data with the server.

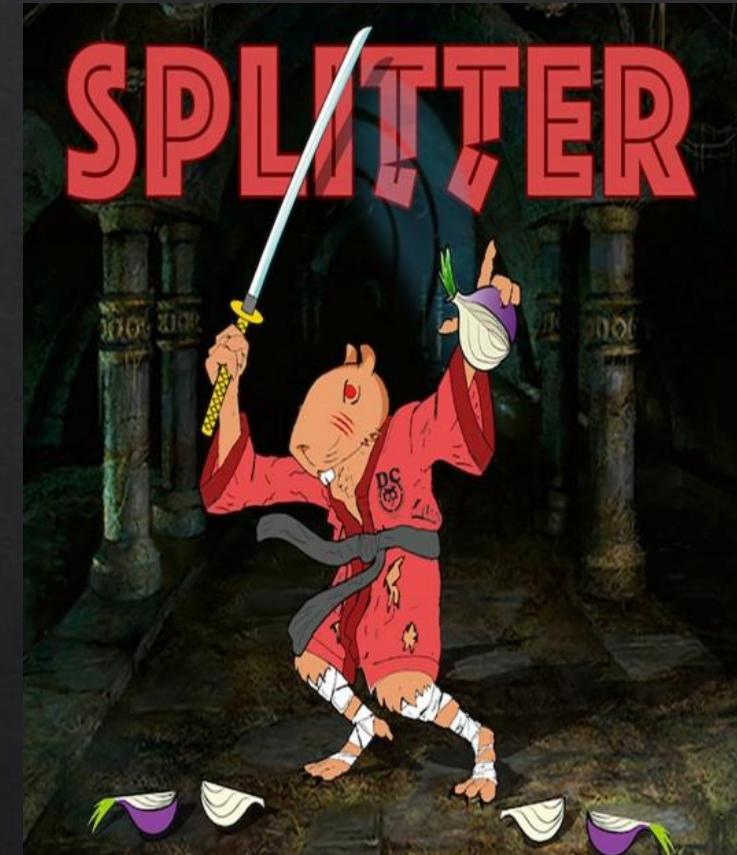
Common Weakness from De-anonymization Techniques

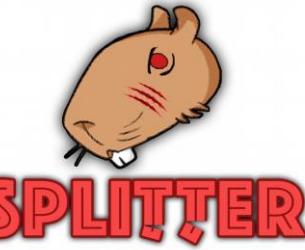
- ❖ The majority of De-anonymization Techniques could fail if the anonymous network user can affect the adversary ability of:
 - ❖ Collect the minimum amount of data to analyze and correlate
 - ❖ Create time related disturbs to difficulty the time correlation of intercepted packets
 - ❖ Identify the injected pattern among the intercepted packets

SPLITTER

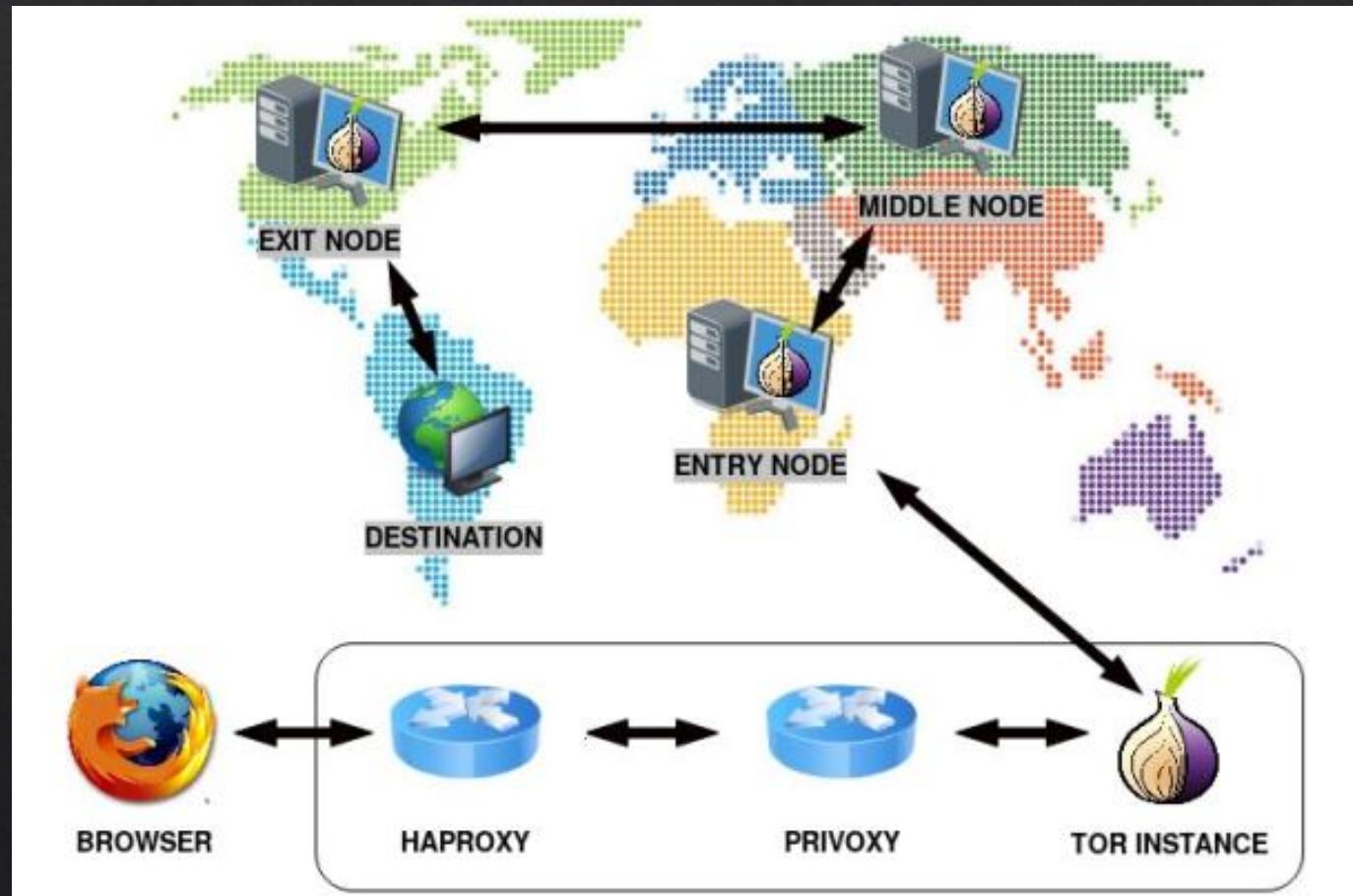
- ❖ Pontos Resolvidos pelo Splitter

- ❖ A different TOR circuit from the previous TCP stream. It means, ensures that the ENTRY NODE or the EXIT NODE will be different from the previous TCP stream.
- ❖ A different global network path for packets traveling from his machine, crossing the TOR network and arriving in the final destination server.
- ❖ Control or disturb the time which TOR could generate the same compromised TOR CIRCUIT again.
- ❖ Disturb the TCP stream lifetime, interrupting the transmission if the stream is being used for more than “X” minutes.

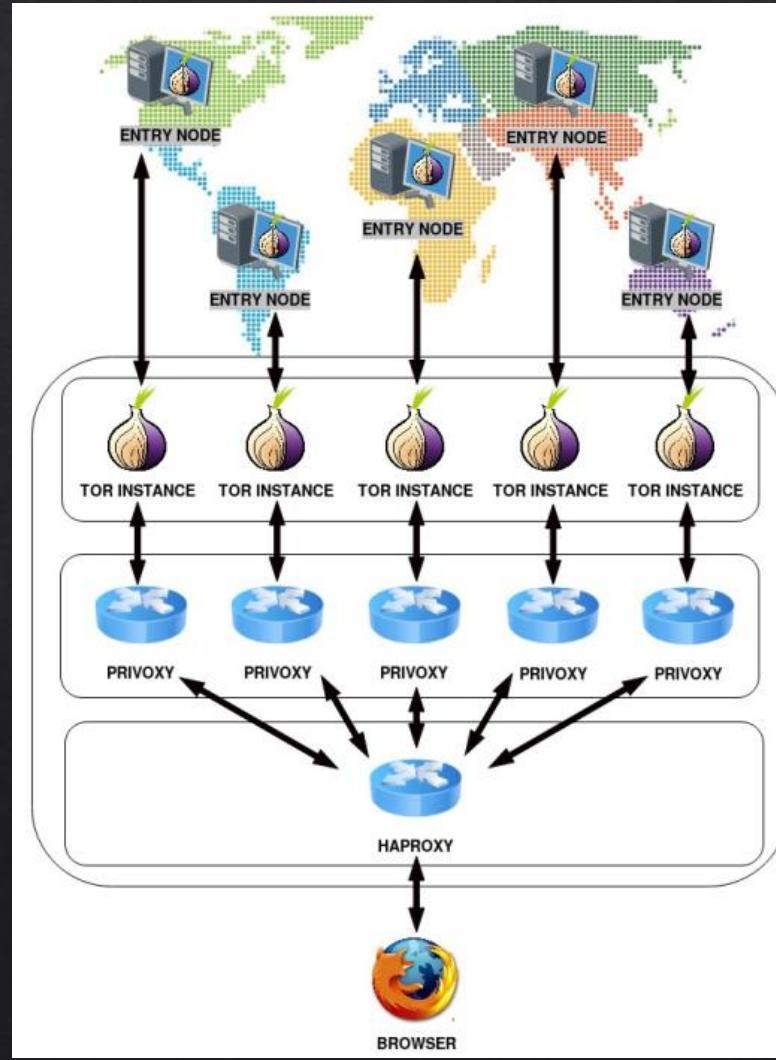




SPLITTER



SPLITTER



SPLITTER



```
docker run -it -p 63537:63537 -p 63536:63536 --name splitterport gr1nchdc/splitter:v.0.0.1 /bin/bash  
cd splitter_v.0.0.1/  
/bin/bash splitter.sh -i 2 -c 5 -re exit
```

SPLITTER



```
grinch@dclabs:~$ time for c in $(seq 1 10000) ; do [148/2008$  
ne2>&1 | grep ":"  
02:32:16; 185.220.101.3  
02:32:16; 37.187.94.86  
02:32:16; 171.25.193.78  
02:32:16; 185.220.102.6  
02:32:16; 185.220.102.7  
02:32:16; 5.9.158.75  
02:32:16; 176.10.99.200
```

→ TOR EXIT node IP address.

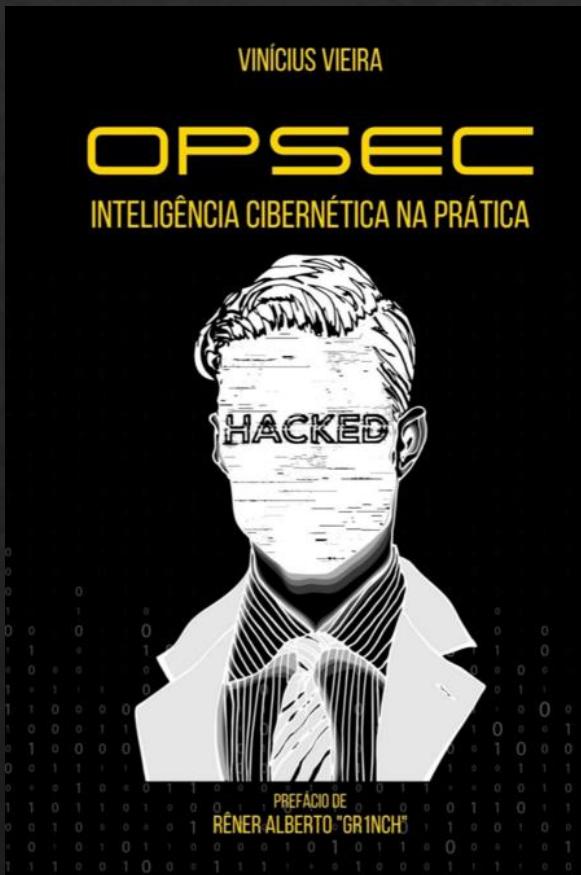
Recursos e Referências

Quer aprender mais?

Papers e Recursos

- ❖ https://www.blackhat.com/presentations/bh-europe-05/BH_EU_05-Long.pdf
- ❖ <https://sansorg.egnyte.com/dl/f4TCYNMgN6>
- ❖ <https://www.exploit-db.com/google-hacking-database>
- ❖ <https://moz.com/learn/seo/search-operators>
- ❖ <https://www.einvestigator.com/google-search-commands/>
- ❖ <https://www.semrush.com/blog/google-search-operators/>
- ❖ https://github.com/id3s3c/bhis-pdfs/blob/master/SLIDES_OPSECFundamentalsforRemoteRedTeams.pdf
- ❖ <https://github.com/h2hconference/2018/blob/master/H2HC%20University%20-%20Rener%20Silva%20-%20Splitter%20Paper%20%26%20Slides.zip>
- ❖ <https://dieseclab.home.blog/2018/11/02/anti-tor-de-anonymization-and-tor-load-balance/>
- ❖ <https://www.ired.team/offensive-security/red-team-infrastructure/automating-red-team-infrastructure-with-terraform>
- ❖ https://www.youtube.com/watch?v=E4SYtCOYzQM&ab_channel=CATx003

Livros





Dúvidas?

Muito Obrigado!