



1



2



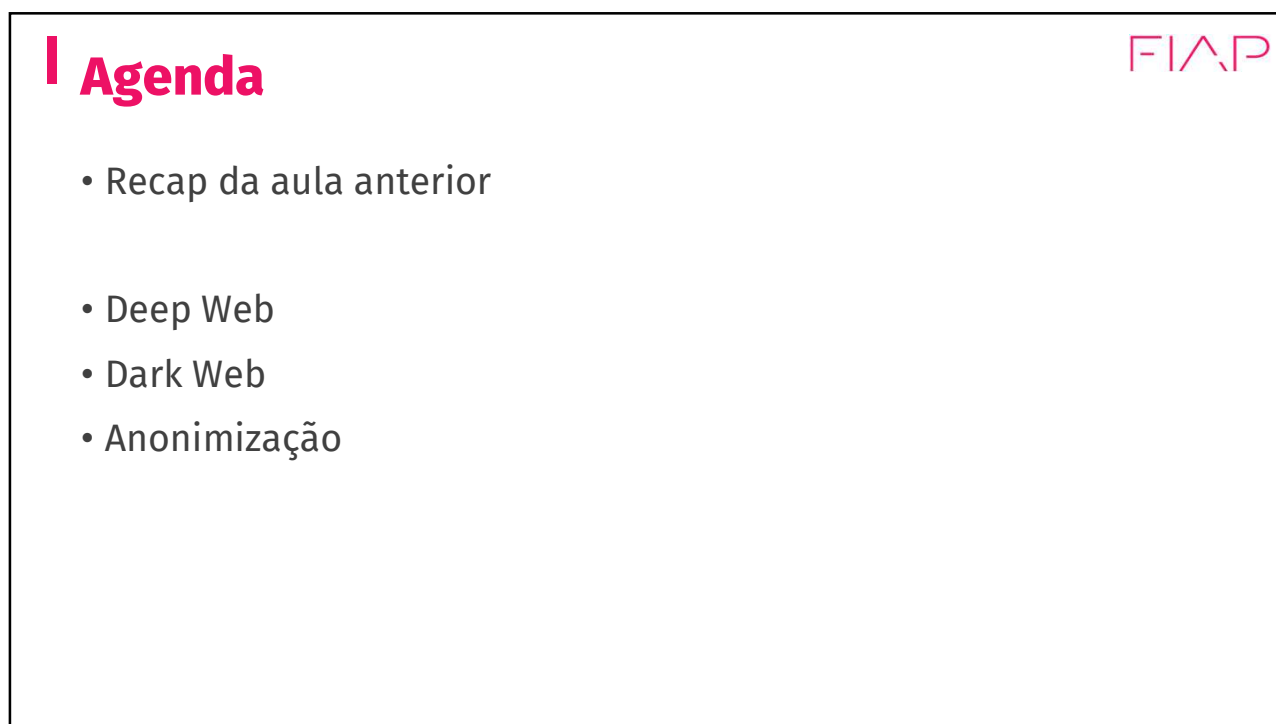
FIAP GRADUAÇÃO

Cognitive Cybersecurity

Prof. Leonardo Orabona
E-mail: profleonardo.orabona@fiap.com.br

Prof. Dr. Noris Junior
E-mail: profnoris.junior@fiap.com.br

3



I Agenda

- Recap da aula anterior
- Deep Web
- Dark Web
- Anonimização

4



DEEP and DARK WEB

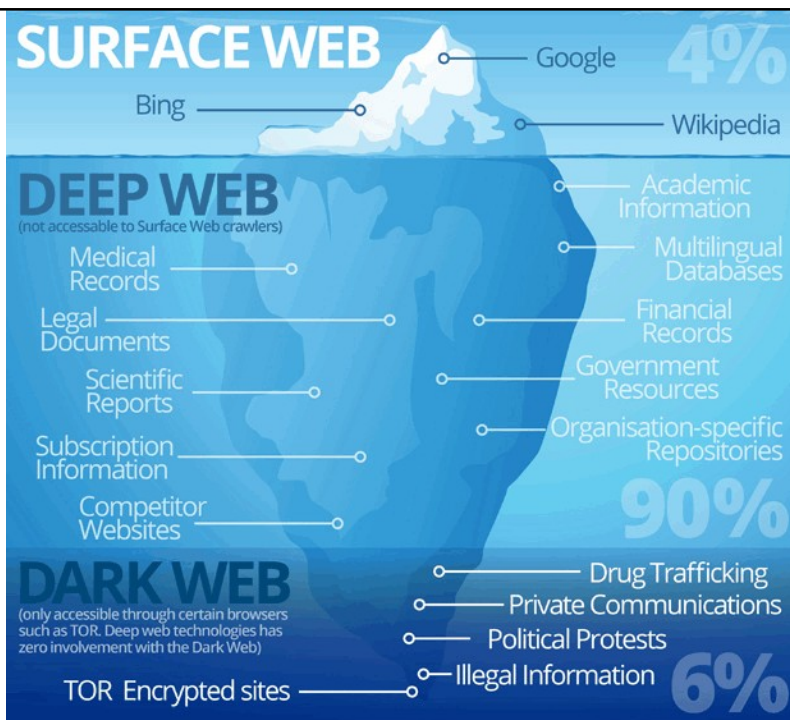
5

I Web

O “iceberg” da Web

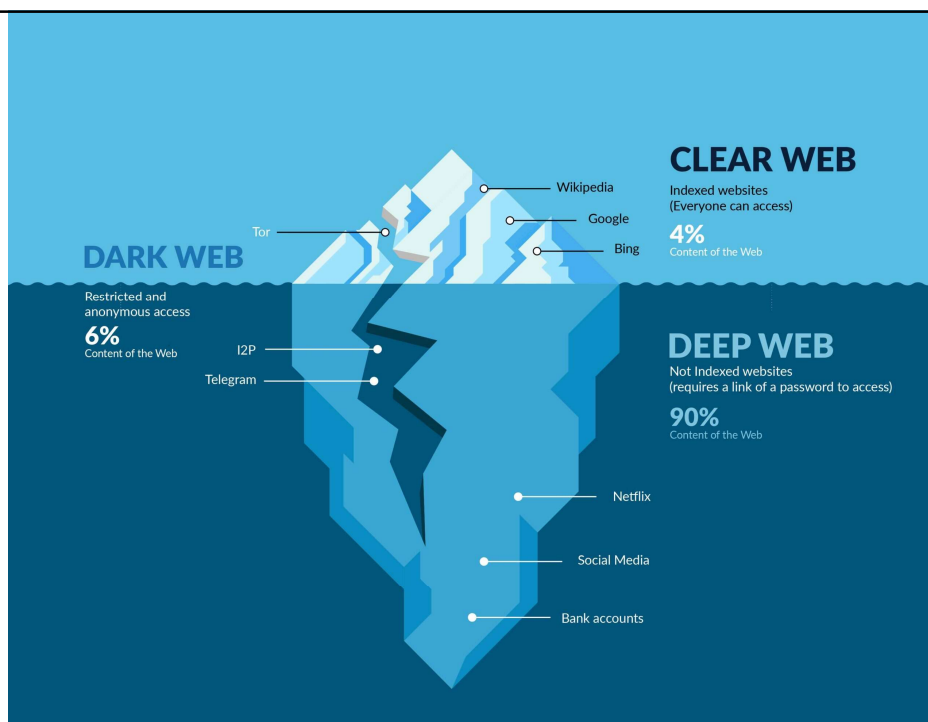
Se mais de 90% da Web está escondida, o que vemos?

- Crawlers: indexação de páginas para serem encontradas - e as que não querem? São a Deep Web



6

I Web



7

I Surface, Deep & Dark Web

FIAP

- A **camada superficial**, também conhecida como web visível, é a camada da internet acessível por meio dos motores de busca comuns, como Google, Bing e Yahoo. Essa camada é composta por sites que podem ser facilmente encontrados por meio de uma pesquisa simples.
- A **camada profunda (deep web)**, por sua vez, é a camada que não é indexada pelos motores de busca comuns, sendo composta por sites que exigem um acesso específico, como bancos de dados de pesquisa, redes corporativas, sistemas governamentais, entre outros. Essa camada não é acessível por meio de uma pesquisa comum, exigindo um conhecimento específico para se encontrar e acessar.
- A **camada escondida (dark web)** é a camada mais profunda da internet. Essa camada é composta por sites que estão escondidos deliberadamente e que exigem um acesso específico, como o uso de softwares de anonimato, como o Tor. A camada escondida é frequentemente associada a atividades ilegais, como tráfico de drogas, terrorismo, entre outros.

8

I Deep & Dark Web

FIAP

- Podem requerer software específico
- Conexão peer-to-peer das máquinas que utilizam o mesmo software

9

I Deep & Dark Web

FIAP

- Para acessar a **Deep Web**, é necessário usar um navegador que possa acessar sites que usam o protocolo Tor (**The Onion Router**). O Tor é um software de código aberto que foi criado com o objetivo de proteger a privacidade dos usuários da internet.
- A **rede onion**, é uma rede de computadores que permite navegar na internet de forma anônima e segura. O funcionamento da rede onion é baseado em uma série de servidores espalhados pelo mundo, que se comunicam de forma criptografada para proteger a identidade e a privacidade dos usuários.
- Ao usar a rede onion, o tráfego de internet é enviado através de uma série de servidores chamados de "nós de cebola" (**onion nodes**), que **criptografam** e **descriptografam** as informações em cada nó, antes de encaminhá-las para o próximo nó na rota. Cada nó na rede onion só sabe a identidade do nó anterior e do próximo nó na rota, o que torna quase impossível para um observador externo rastrear a origem do tráfego ou identificar o usuário final.

10

I TOR

FIAP

Imagine que você quer enviar uma carta anônima. Você a coloca dentro de um envelope, dentro de outro envelope, e assim por diante.

Cada vez que a carta passa por alguém (nó), um envelope é removido, até que ela chegue ao destino, sem que ninguém saiba quem a enviou.

11

I TOR

FIAP

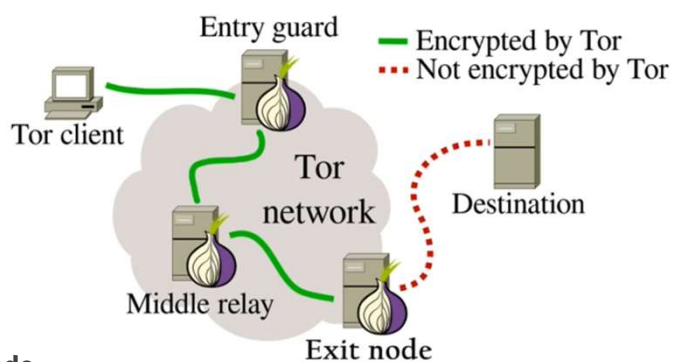
- Onion routing
- Entry node/guard
- Middle relay
- Exit node
- End-to-end encryption
 - Entre cliente e nó de saída, não até o destino final

12

I TOR

FIAP

THE ONION ROUTER



Entry guard = Guard node

Middle relay = Middle node

13

I TOR

FIAP

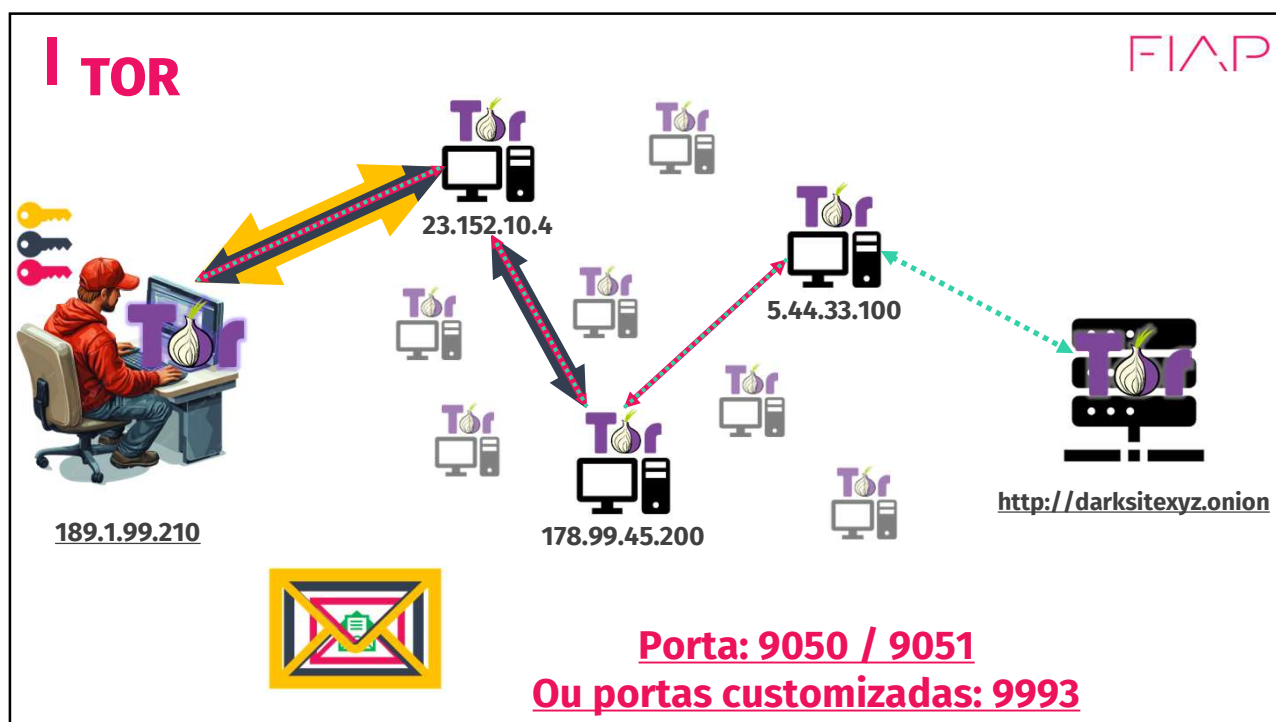


189.1.99.210



<http://darksitexyz.onion>

14



15



16

I TOR

FIAP

- Navegador:
 - <https://www.torproject.org/download/>
- Verificar navegação:
 - <https://check.torproject.org>
- IP de navegação:
 - <https://whatismyipaddress.com>
- Observar circuito

17

I TOR

FIAP

Sites

- The CIA:** <http://ciadotgov4sjwlzihbgbxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion/>
- ProtonMail:** <https://protonmailrmez3lotccipshtkleetolb73fuirgi7r4o4vfu7ozyd.onion/>
- VPN Mullvad:** <http://o54hon2e2vj6c7m3aqq6uyece65by3vgoxhqlsvkmacw6a7m7kiad.onion/>
- ProPublica:** <http://p53lf57qovyuvwsc6xnrppyply3vtqm7l6pcobkmyqsiofyezfnfu5uqd.onion/>
- BBC:** <https://www.bbcnewsd73hkzno2ini43t4gblxvycyac5aw4gnv7t2rccijh7745uqd.onion/>
- Bellingcat (OSINT):** <http://www.bellcatmbguthn3age23lrbseln2lryzv3mt7whis7ktjw4qrestbzad.onion/>
- Psychonaut Wiki:** http://vvedndyt433kopnhv6vejxnut54y5752vpshjaqmj7ftwiu6quiv2ad.onion/wiki/Main_Page
- Bible4u:** <https://bible4u2lvhacg4b3to2e2veqpwmrc2c3tjf2wuuqiz332vlwmr4xbad.onion/>
- tor.taxi:** <http://tortaxi2dev6xjwbaydqzla77rrnth7yn2oqzjfmuiwn5h6vsk2a4syd.onion/>

18

I TOR

FIAP

Ahmia: <http://juhanurmihxlp77nkq76byazcldy2hlmovfu2epvl5ankdibsot4csyd.onion/>

Ransomware Group Sites: <http://ransomwr3tsydeii4q43vazm7wofla5ujdajquitomtd47cxjtfgywyd.onion/>

The Hidden Wiki: <http://s4k4ceiapwwgcm3mkb6e4diqecpo7kvdnfr5gg7sph7jppqkvwwqtyd.onion>

RelateList (vazamentos): <http://relateoak2hkvdty6ldp7x67hys7pzaeax3hwhidbqkjzva3223jpxqd.onion>

19

I TOR

FIAP

O que muda na experiência de navegação quando usamos o Tor em vez do navegador comum?

20



ANONIMIZAÇÃO

21

I TOR

- Ainda posso ser rastreado?
 - Sim
- Quais os riscos?
- Como ficar totalmente anônimo (e mesmo que achem a máquina não seria possível ver o conteúdo)?
 - Tails

22

I Tails = TOR no pendrive ;)

FIAP

- Não armazena nada local
- Memória RAM é apagada quando o computador desligar
- Minimiza os rastros

23

I Tails

FIAP

- <https://tails.net/>

24

I Anonimização

FIAP

- A privacidade online é uma questão cada vez mais importante nos dias de hoje.
- Com a crescente quantidade de dados pessoais que são coletados e compartilhados online, é essencial ter a capacidade de proteger sua privacidade e anonimato online.
- Dark Web: fonte valiosa de informações
 - Porém, também é conhecida por ser um lugar onde atividades ilegais, como o tráfico de drogas e armas, podem ocorrer.
 - Riscos de malware, phishing e outros tipos de ameaças online.

25

I Anonimização

FIAP

- Para se manter anônimo não adianta usar o e-mail convencional!
- Protonmail, exemplo
- Onde mais podemos usar a anonimização?
 - Google Dorks
 - Shodan.io
- Qual a motivação de usar Shodan e Dorks anonimizado?



26

I Quiz relâmpago

FIAP

- Qual é a camada da web acessível por mecanismos de busca convencionais?
- O que é onion routing?
- A rede Tor garante 100% de anonimato?
- O que são nós de saída no Tor?

27

I Mapa mental

FIAP

- Recap da aula

28

