

5+1 passos para uma contingência **Black Hat**



HYPE 2022 - @blackrat.ads

© Copyright - Todos os Direitos Reservados.

De forma alguma é legal reproduzir, duplicar ou transmitir qualquer parte deste documento em meios eletrônicos ou em formato impresso. A gravação desta publicação é estritamente proibida e qualquer armazenamento deste documento não é permitido, a menos que com permissão por escrito da editora. Todos os direitos reservados.

As informações aqui fornecidas são declaradas verdadeiras e consistentes, na medida em que qualquer responsabilidade, em termos de desatenção ou de outra forma, por qualquer uso ou abuso de quaisquer políticas, processos ou instruções contidas neste documento é de responsabilidade solitária e total do leitor destinatário. Sob nenhuma circunstância qualquer responsabilidade legal ou culpa será imputada à editora por qualquer reparação, dano ou perda monetária devido as informações aqui contidas, direta ou indiretamente.

Os respectivos autores possuem todos os direitos autorais não detidos pela editora:

Black Rat @blackrat.ads

Aviso legal

Esta apresentação é protegido por direitos autorais. Isto significa que ela deve ser usada apenas para fins pessoais. Você não pode alterar, distribuir, vender, usar, citar ou parafrasear qualquer parte do conteúdo deste livro sem o consentimento do autor ou do proprietário dos direitos autorais. Ação legal será prosseguida se isto for violado.

Aviso de isenção de responsabilidade

Favor observar que as informações contidas neste documento são apenas para fins educacionais. Todas as tentativas foram feitas para fornecer informações completas e precisas, atualizadas e confiáveis. Nenhuma garantia de qualquer tipo é expressa ou implícita. Os leitores reconhecem que o autor não está envolvido na prestação de aconselhamento legal, financeiro, médico ou profissional.

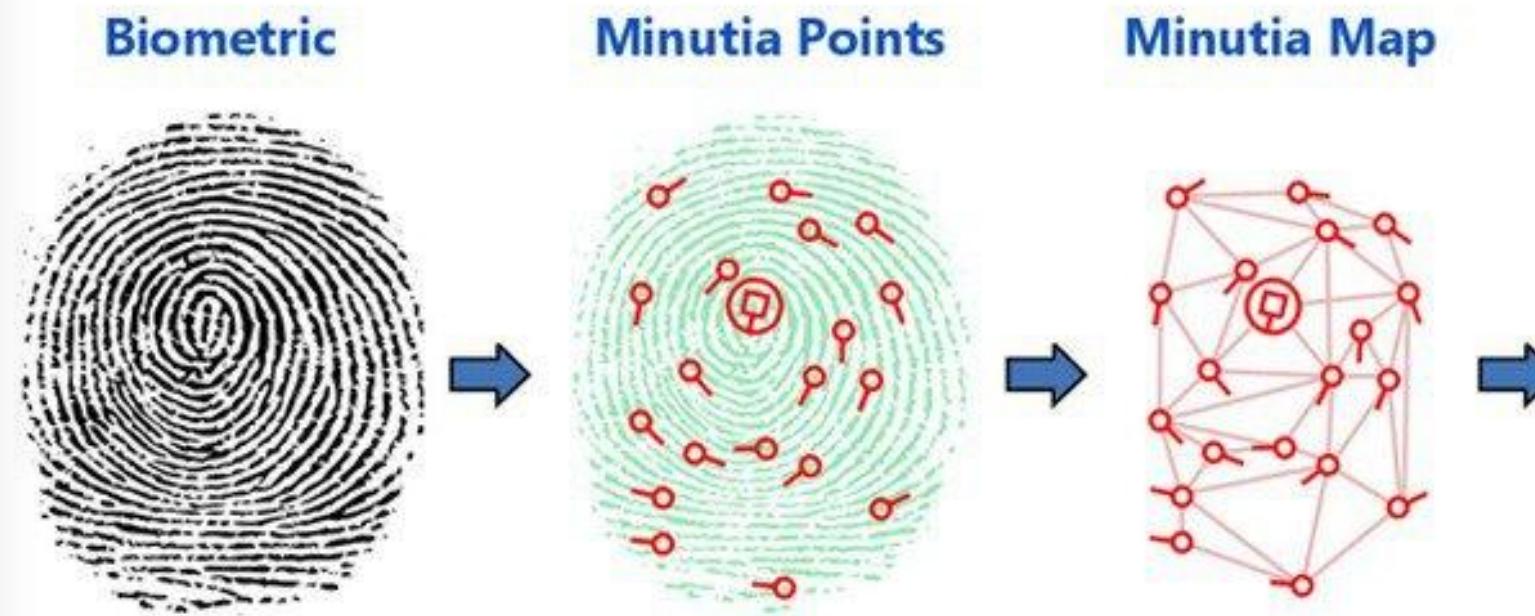
Ao ler este documento, o leitor concorda que, sob nenhuma circunstância, sejamos responsáveis por quaisquer prejuízos, diretos ou indiretos, incorridos como resultado do uso das informações contidas neste documento, incluindo, mas não se limitando a erros, omissões ou imprecisões.

PASSO 1

Fingerprint

Fingerprint

na vida real

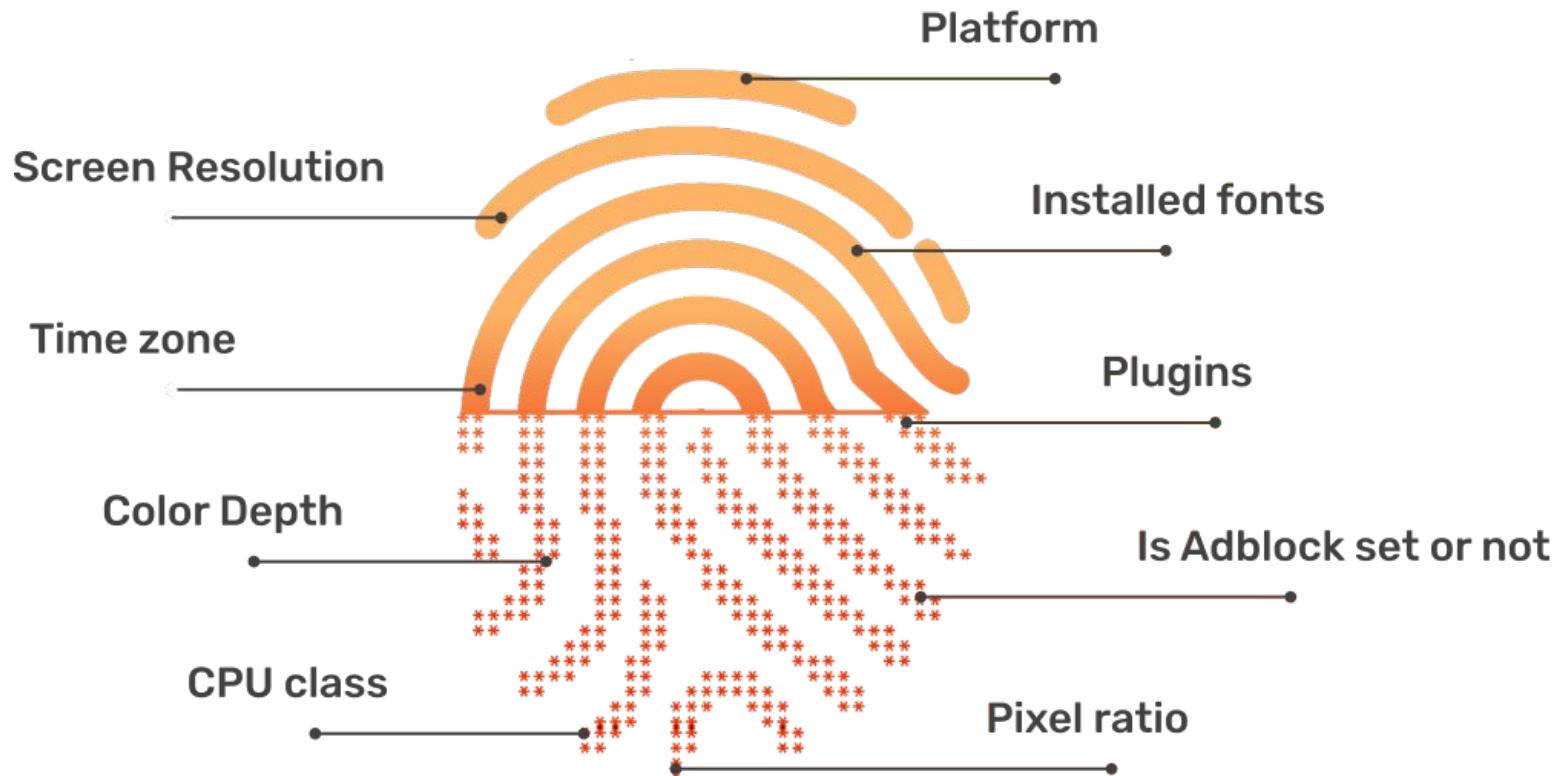


```
0101010001101000011010  
0101110011001000000110  
100101110011001000000011  
1011100110111101110100  
0010000001100001011000  
1101110100011101010110  
0001011011000110110001  
1110010010000001100110  
0110100101101110011001  
1101100101011100100111  
0000011100100110100101  
1011100111010000100000  
0110010001100001011101  
0001100001001011000010
```

Fingerprint

em tecnologia

São as informações que compõem o seu device e que qualquer site pode coletar sobre você.



Fingerprint

em tecnologia

Usando estes dados, qualquer site pode “linkar” suas contas ou encontrar irregularidades (red flags) no seu comportamento, tal como usar máquinas virtuais.

Sendo assim, é importante que cada conta possua uma fingerprint.



Dolphin{anty}

PASSO 2

Internet Protocol (IP)

Internet Protocol (IP)

O que é um IP?

Um IP é o seu “endereço digital”

Avenida Paulista, 100
197.25.34.108/24

Rede

Máscara



* Máscara = Número dessa máquina dentro dessa rede

Internet Protocol (IP)

3 tipos de IP

- IP mobile
- IP residencial
- IP data center

Por que o IP mobile é “melhor” que os outros?

Internet Protocol (IP)

É preciso ter um IP e Fingerprint alinhados

Se você esconde o seu IP usando uma VPN, por exemplo. Facebook e Google ainda são capazes de saber onde você realmente está, usando alguns dos parâmetros de Fingerprint, como:

- Timezone
- Geolocation API
- WebRTC Public IP Leak

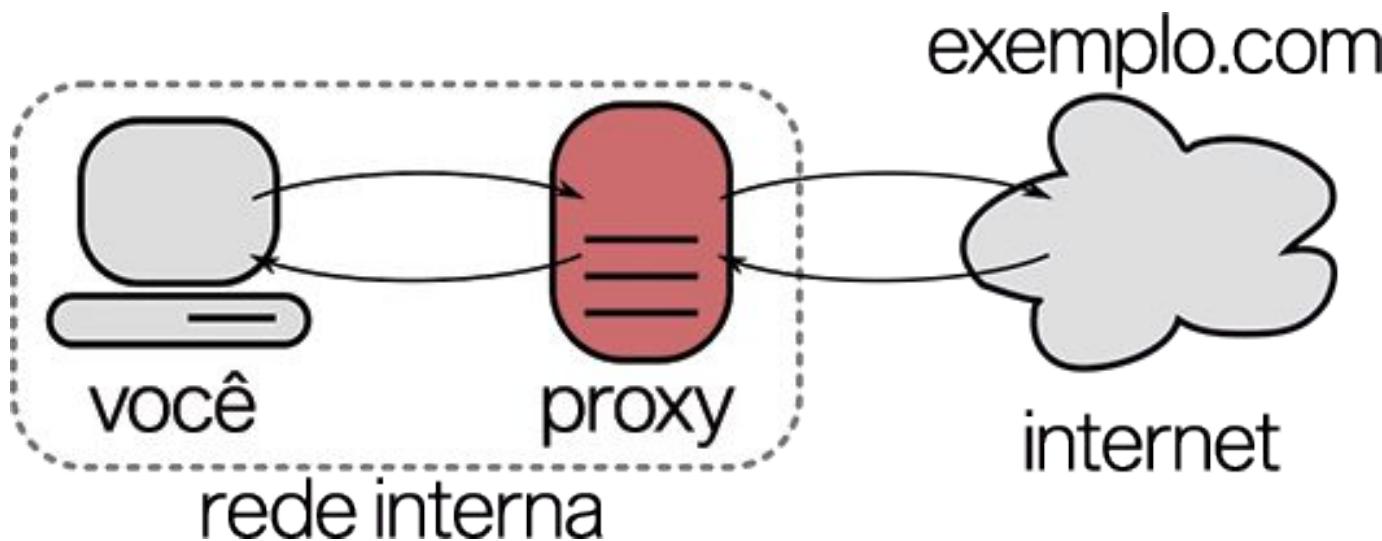
PASSO 3

Proxy

Proxy

O que é, como usar, onde comprar, protocolos...

Um proxy é um intermediário entre um dispositivo e os serviços de internet que ele acessa.



Proxy

O que é, como usar, onde comprar, protocolos...

Ele direciona o tráfego por uma rota específica, a partir das configurações do usuário. Desse modo, é possível bloquear sites, gerar mais privacidade para a navegação e evitar situações de risco, por exemplo.

199.18.99.071:1008:blackrat:abc123

HOST

PORTA

LOGIN

SENHA

Proxy

O que é, como usar, onde comprar, protocolos...

O que diferencia um proxy bom de um ruim, de forma muito simplória, é o seu **protocolo**.

Existem vários protocolos, em proxys os mais famosos são HTTP, HTTPS, SOCKS4, SOCKS5 e SHADOWSOCKS.

Proxy

O que é, como usar, onde comprar, protocolos...

	HTTP	HTTPS	SOCKS4	SOCKS5	SHADOW SOCKS
ocultar o IP verdadeiro	✓	✓	✓	✓	✓
suporte SSL	✗	✓	✓	✓	✓
esconde que é um proxy	✗	✗	✓	✓	✓
não muda os cabeçalhos	✗	✗	✓	✓	✓
suporte UDP	✗	✗	✗	✓	✓
endereçamento IPV6	✗	✗	✗	✓	✓
disfarce de tráfego	✗	✗	✗	✗	✓
proteção DPI	✗	✗	✗	✗	✓

** Alguns itens têm valores variáveis que dependem das configurações*

PASSO 4

Portas TCP/UDP

Portas TCP/UDP

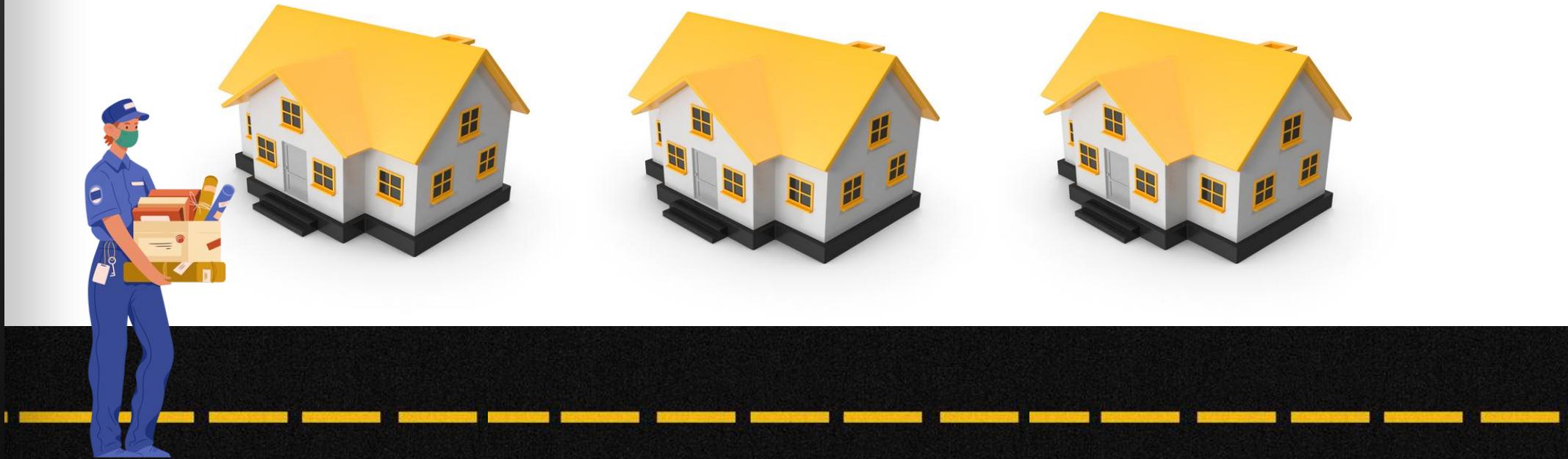
Imagina que um carteiro precisa fazer uma entrega em uma casa e tem a rua e o número desta casa...

**Carteiro = Levar informações
em bytes (imagem, texto,
vídeo) de um lugar para o
outro**



Portas TCP/UDP

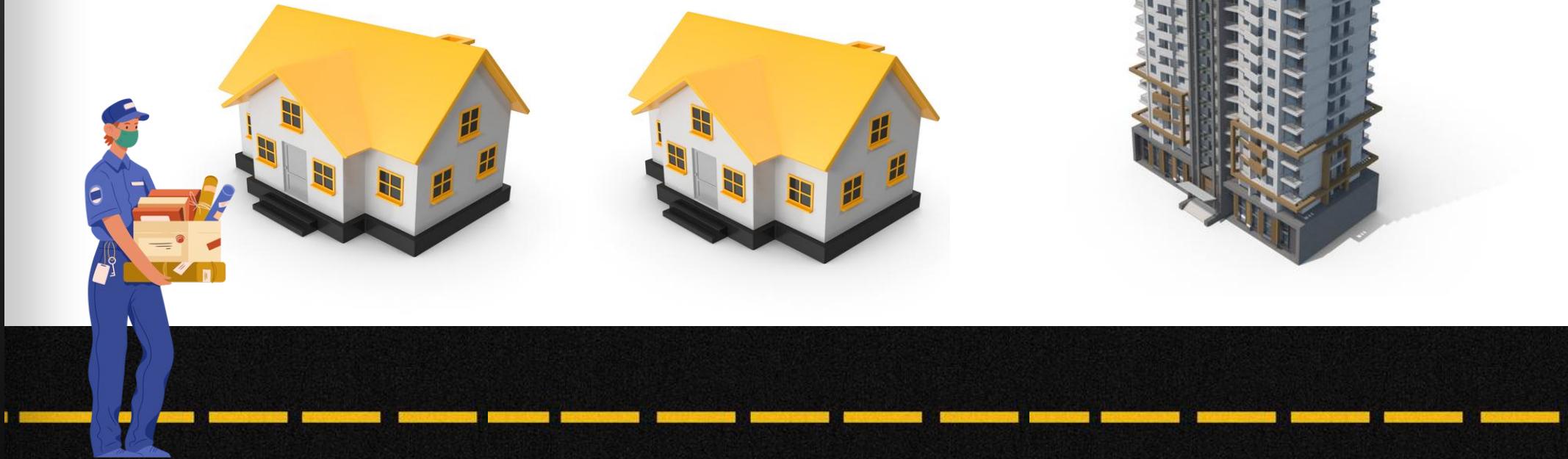
Imagina que o carteiro precisa fazer uma entrega em uma casa e tem a rua e o número da casa...



Avenida Paulista, 100
197.25.34.108/24

Portas TCP/UDP

Imagina que o carteiro precisa fazer uma entrega no prédio e tem a rua e o número da casa...



**Avenida Paulista, 100 - Apto 87
197.25.34.108/24 PORTA 5938**

Portas TCP/UDP

O seu notebook é como se fosse o prédio



197.25.34.108/24

PORTA 5938



Avenida Paulista, 100

Apto 87

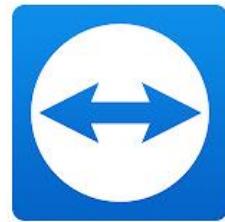
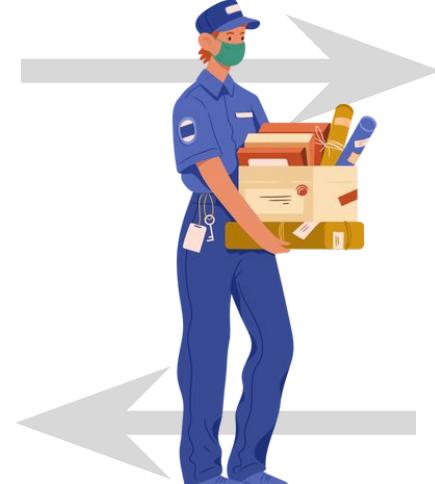
Portas TCP/UDP

Um “prédio” enviando informações para outro “prédio” em uma mesma porta



197.25.34.108/24

PORTA 5938



TeamViewer

203.110.1.32/11

PORTA 5938

Portas TCP/UDP

**Sites podem escanear seu browser
atrás de portas abertas usando um
método chamado websockets.**

Assim, os sites conseguem descobrir
qualquer programa que você esteja
usando naquele exato momento.

```
Array(3)
  ▼ 0: Array(6)
    ▶ 0: (3) ["63333", "REF", f]
    ▶ 1: (3) ["5900", "VNC", f]
    ▶ 2: (3) ["5901", "VNC", f]
    ▶ 3: (3) ["5902", "VNC", f]
    ▶ 4: (3) ["5903", "VNC", f]
    ▶ 5: (3) ["3389", "RDP", f]
      length: 6
    ▶ __proto__: Array(0)
  ▼ 1: Array(6)
    ▶ 0: (3) ["5950", "ARO", f]
    ▶ 1: (3) ["5931", "AMY", f]
    ▶ 2: (3) ["5939", "TV0", f]
    ▶ 3: (3) ["6039", "TV1", f]
```

Portas TCP/UDP

O Facebook, por exemplo, sabe quando você está compartilhando sua tela com outras pessoas. E isso é claramente um comportamento que ele detesta

Portanto, você precisa se proteger disso
Multilogin e Dolphin Anty

```
Array(3)
└ 0: Array(6)
  └ 0: (3) ["63333", "REF", f]
  └ 1: (3) ["5900", "VNC", f]
  └ 2: (3) ["5901", "VNC", f]
  └ 3: (3) ["5902", "VNC", f]
  └ 4: (3) ["5903", "VNC", f]
  └ 5: (3) ["3389", "RDP", f]
    length: 6
    └ __proto__: Array(0)
└ 1: Array(6)
  └ 0: (3) ["5950", "ARO", f]
  └ 1: (3) ["5931", "AMY", f]
  └ 2: (3) ["5939", "TV0", f]
  └ 3: (3) ["6039", "TV1", f]
```

PASSO 5

Mouse movements e
Typing Patterns

Typing Patterns

User Identification

Se você digitar em um computador e depois digitar em outro, ainda será possível identificar você por padrões



TOUR TECHNOLOGY TRY OUT PRICING SUPPORT DEVELOPERS SIGN IN

Keyboard biometrics made simple for you

Identify people based on keystroke dynamics. KeyTrac works with any existing keyboard and doesn't require any special hardware.



Mouse Movements

User Identification

Automatizações, se feitas de forma errada, são ruins.

Prefira manualmente.

The screenshot shows the India Today news website. At the top, there is a navigation bar with links for NEWS, LIVE TV, and APP. Below the navigation bar is a sub-navigation bar with links for HOME, MY FEED (highlighted in yellow), ELECTIONS, CORONA, INDIA, BUSINESS, WORLD, TECH, MOVIES, and HAPPINESS. A banner for 'Assembly Election 2022' is visible. The main content area features a news article with the following text:

News / Technology / News / Facebook confirms that it tracks how you move mouse on the computer screen

Facebook confirms that it tracks how you move mouse on the computer screen

Facebook admitted that it collects information from and about computers, phones, and connected devices, including mouse, to give users a personalised content.

The article is attributed to Shweta Ganjoo, New Delhi, with a publication date of June 12, 2018, and an update date of June 13, 2018, 19:43 IST. There are social sharing icons for YouTube, Facebook, Twitter, WhatsApp, and others at the bottom of the article.

O ÚLTIMO PASSO
PARA O SUCESSO!

PASSO 5+1

User Behavior

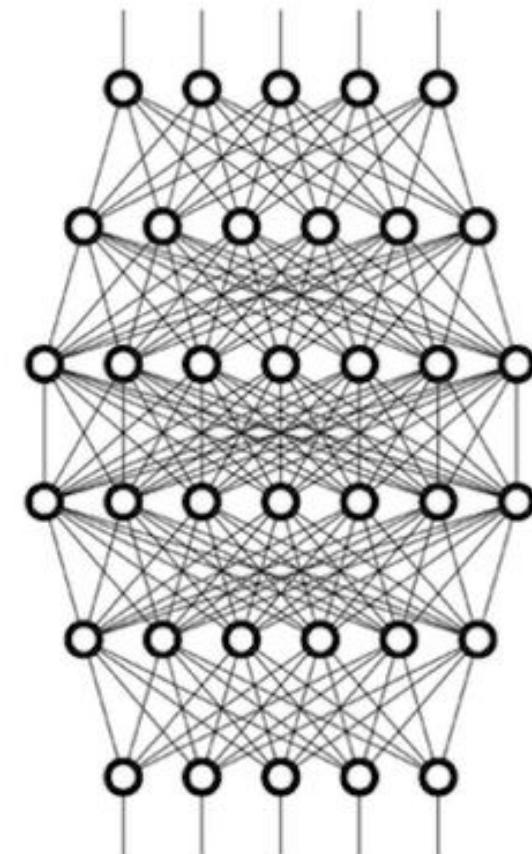
User Behavior

Como as redes usam isso a seu favor

Elas estão cada vez mais indo para o Behavior Analysis

User Behavior: quanto rápido você cria uma conta de anúncio, de onde você está logando, que ads você está usando...

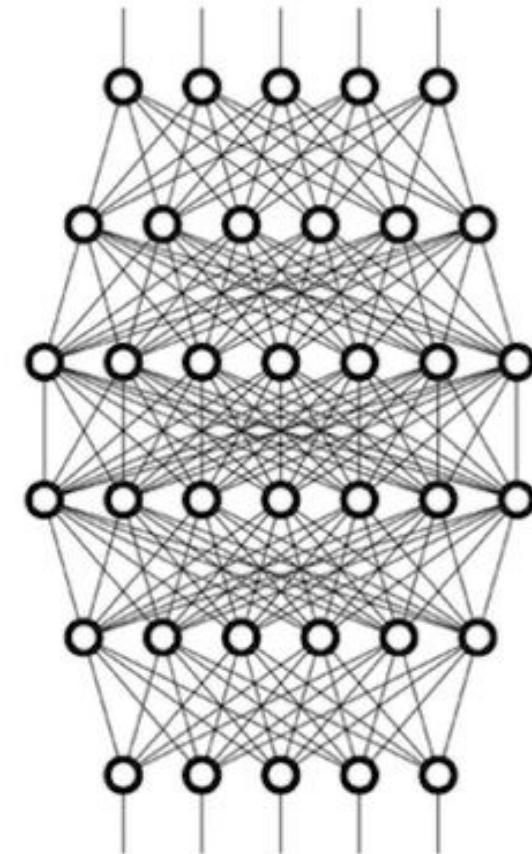
- Facebook e Google já possuem muitos desses tipos de dados (**é muito fácil para eles usarem isso para criar modelos preditivos muito eficazes**)



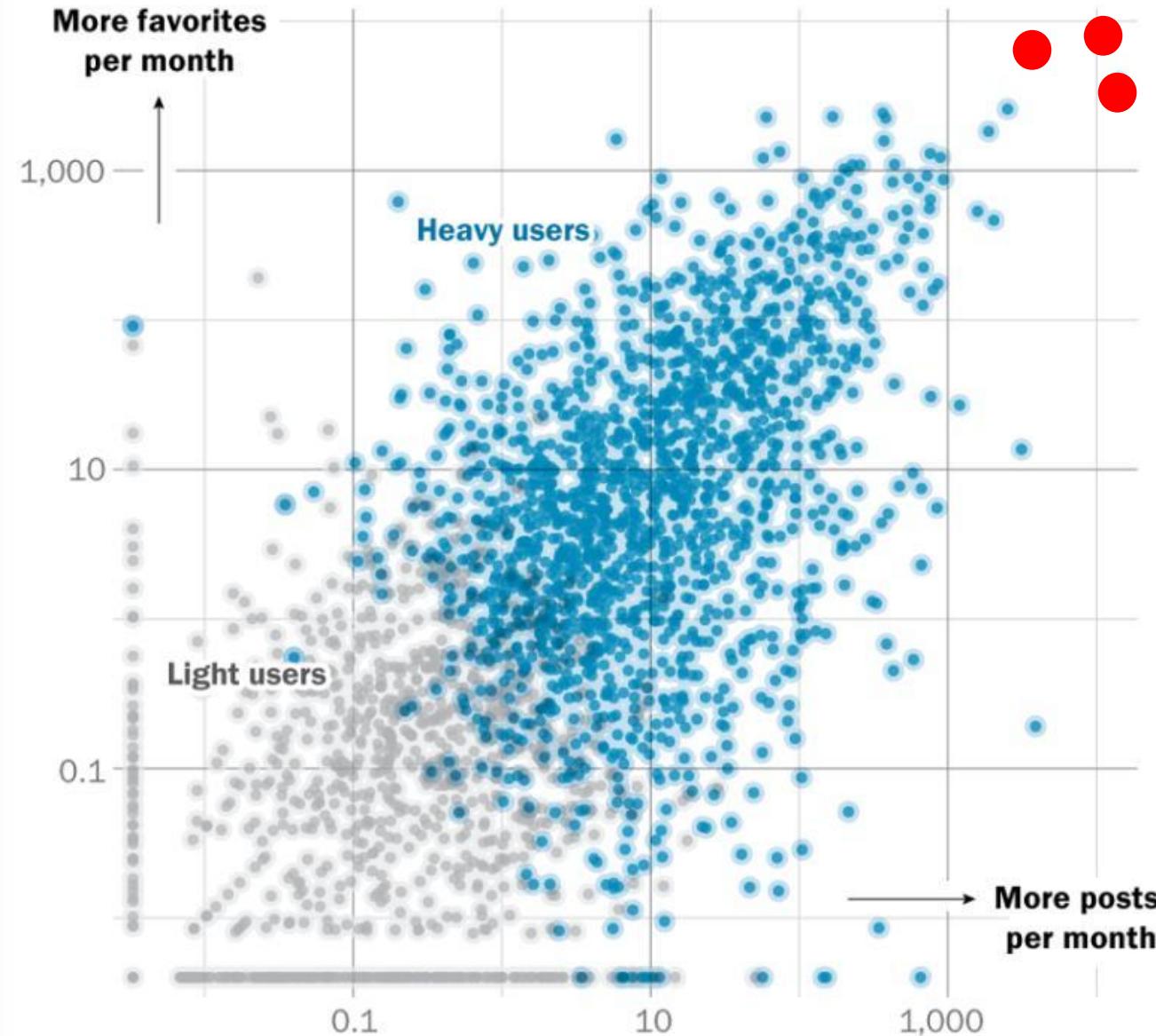
User Behavior

Os usuários aprenderam a mascarar os parâmetros de uma Fingerprint e o Facebook e Google sabem disso...

Isso faz com que a forma com que as nossas ações sejam muito mais importantes, pois ele detecta com facilidade um usuário comum de um anunciante padrão.



Cluster analysis of Twitter behavior shows distinct groups in terms of posting, favoriting behavior



Você com sua esteira
postando 50x por dia

User Behavior

Frase para lembrar sempre!

**Se misture na
multidão, mas na
multidão certa!**

**Não seja o cara
com uma melancia
no pescoço.**



Obrigado!

[Clica aqui e me segue](#)

[@blackrat.ads](#)