5+1 passos para uma contingência Black Hat

HYPE 2022 - @blackrat.ads

Aviso legal

Aviso de isenção de responsabilidade

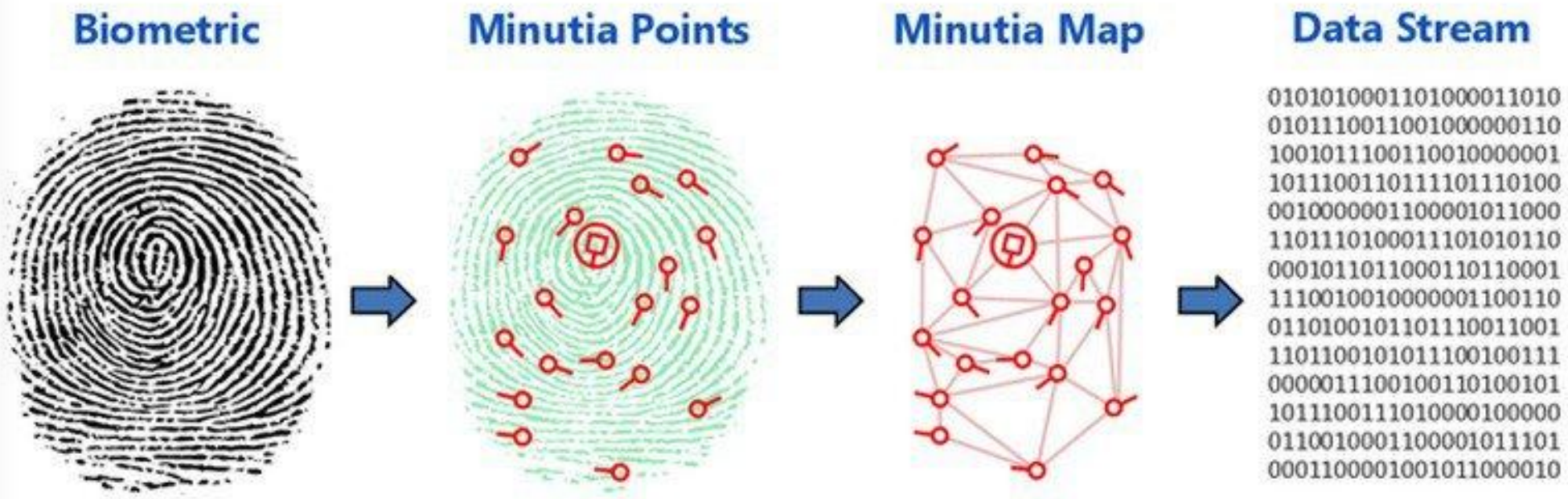
Favor observar que as informações contidas neste documento são apenas para fins educacionais. Todas as tentativas foram feitas para fornecer informações completas e precisas, atualizadas e confiáveis. Nenhuma garantia de qualquer tipo é expressa ou implícita. Os leitores reconhecem que o autor não está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

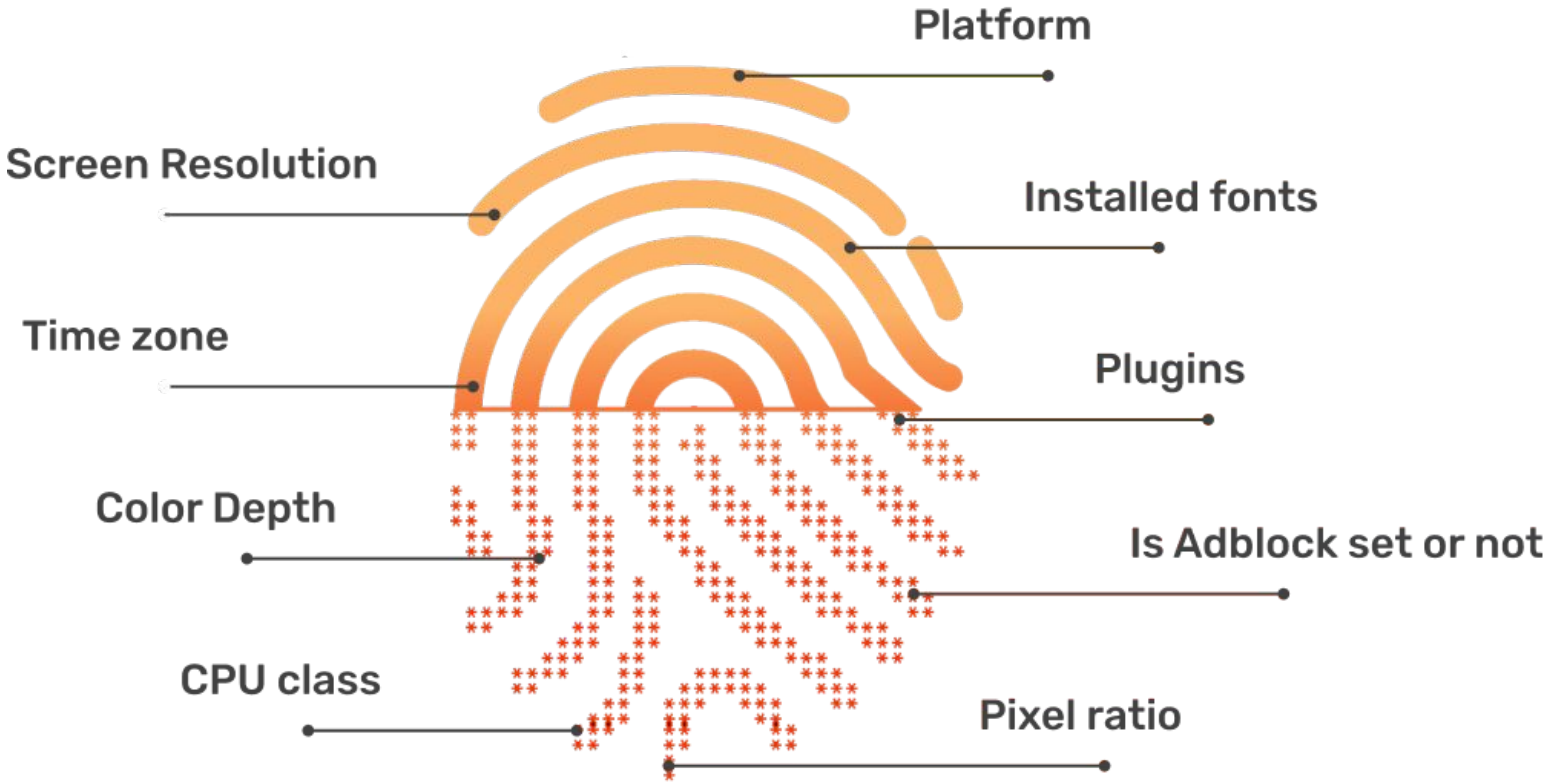
na vida real



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.

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:

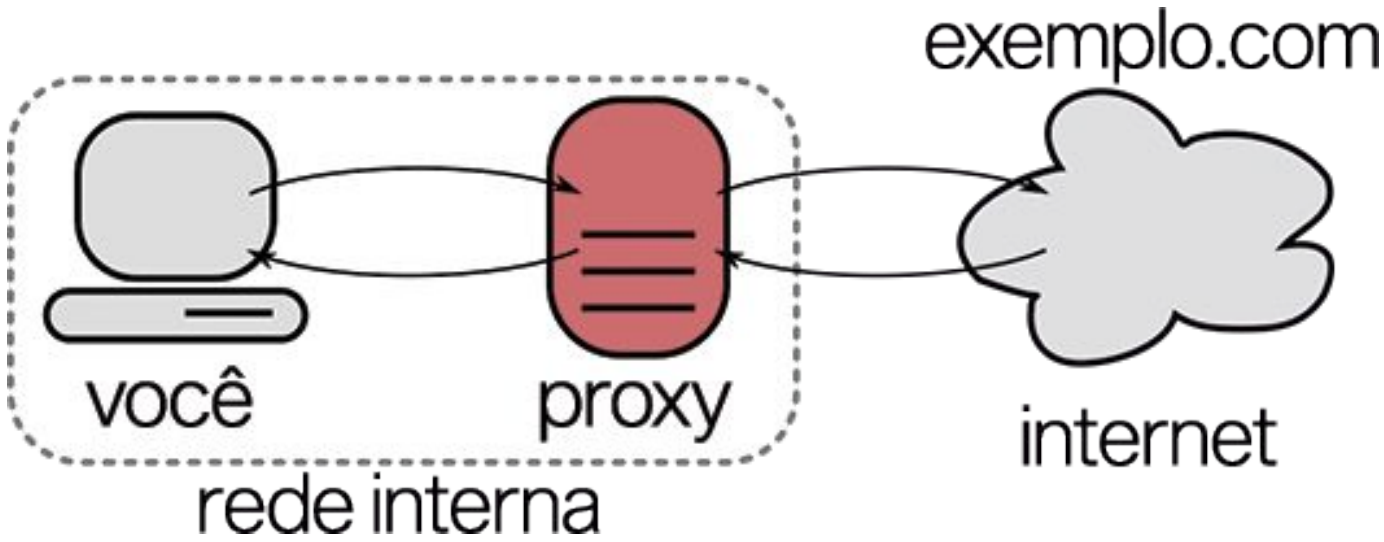
- Timezone
- Geolocation API
- WebRTC Public IP Leak

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

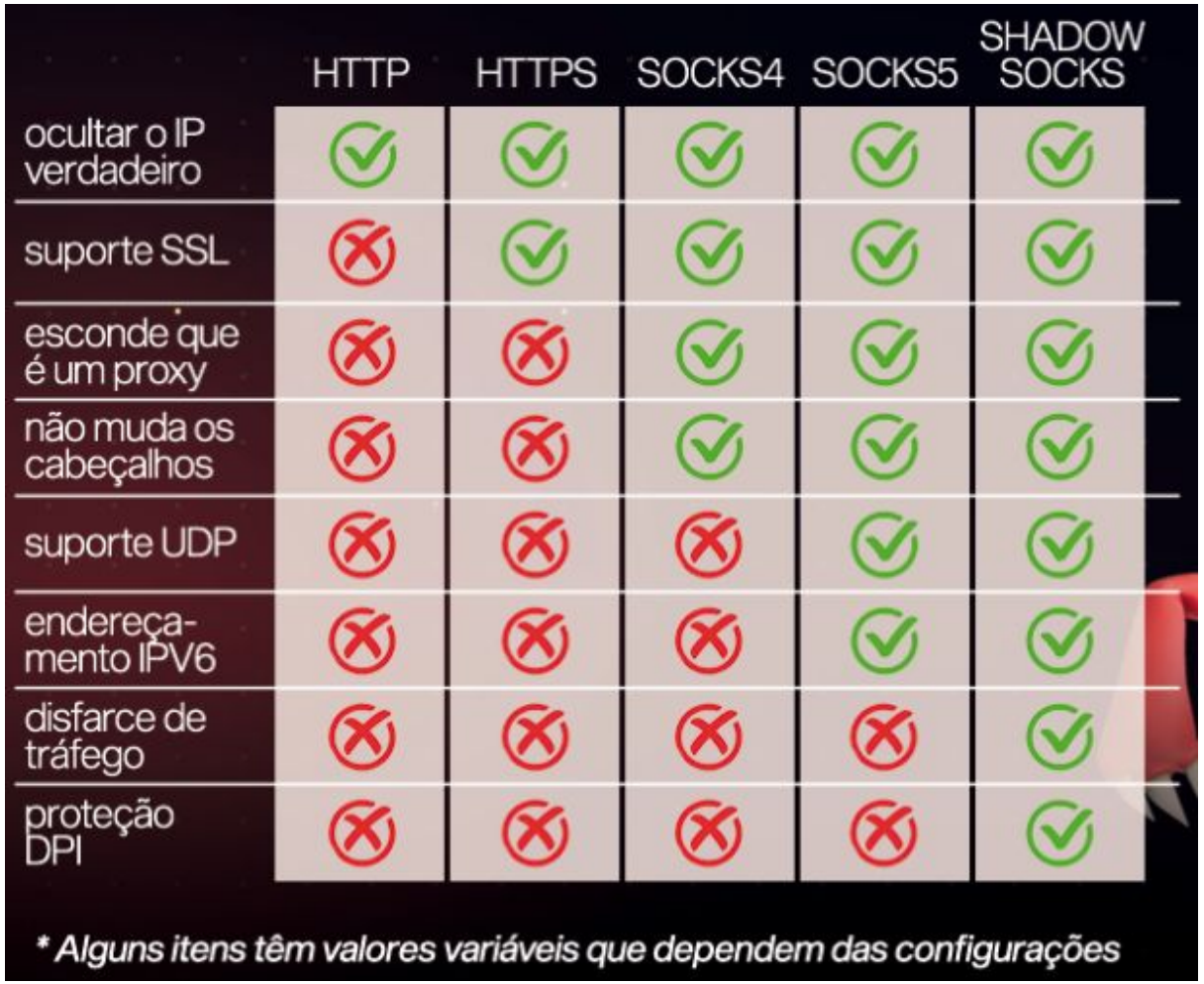
O que é, como usar, onde comprar, protocolos...

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...



PASSO 4
Portas TCP/UDP

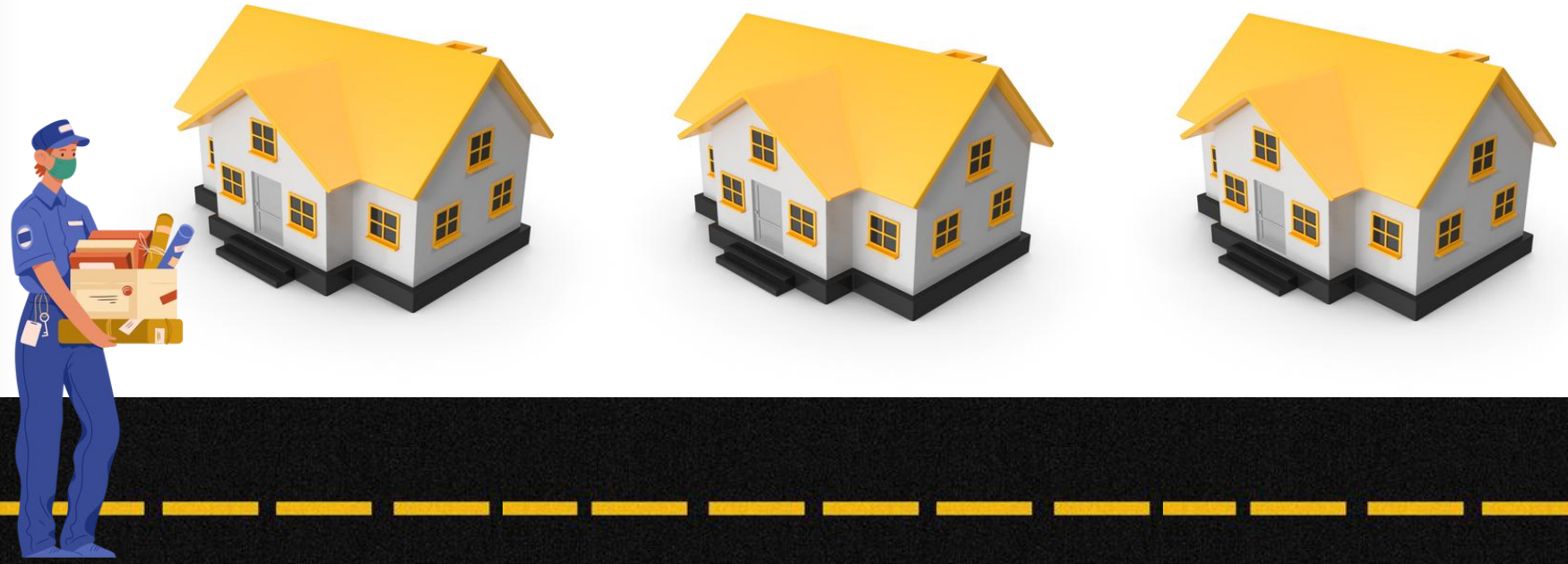
Portas TCP/UDP

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

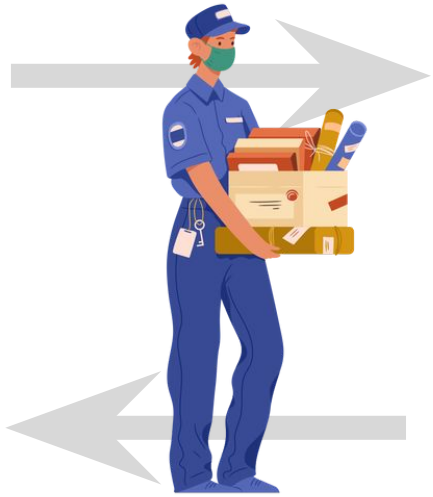
PORTA 5938

Avenida Paulista, 100

Apto 87

Portas TCP/UDP

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



TeamViewer

197.25.34.108/24

PORTA 5938

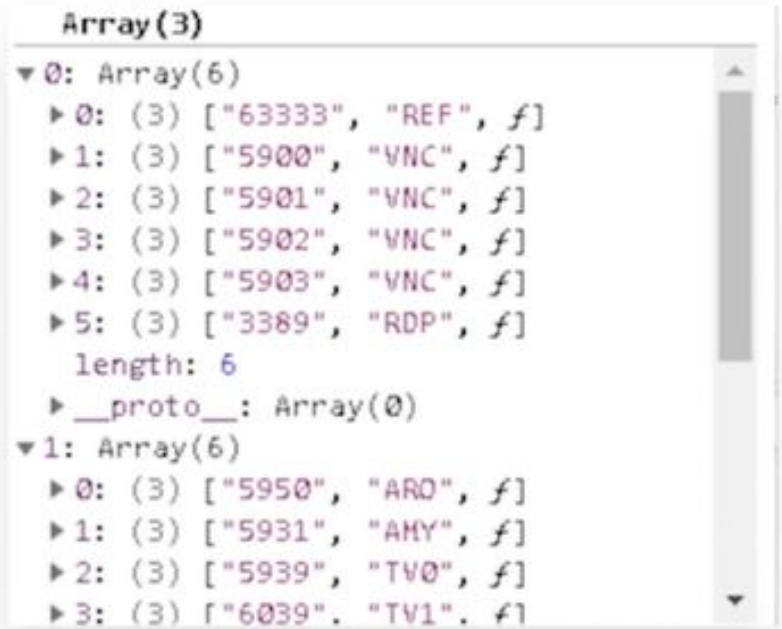
203.110.1.32/11

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.

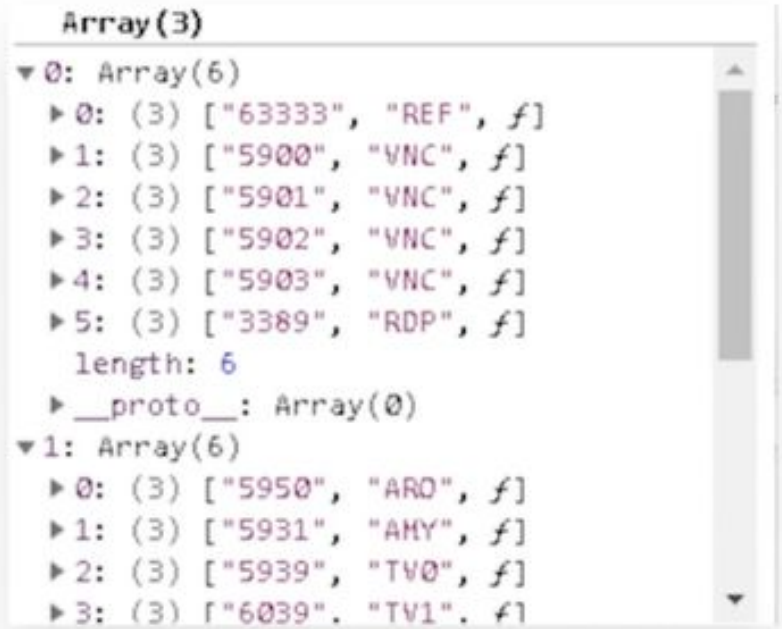


Portas TCP/UDP

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



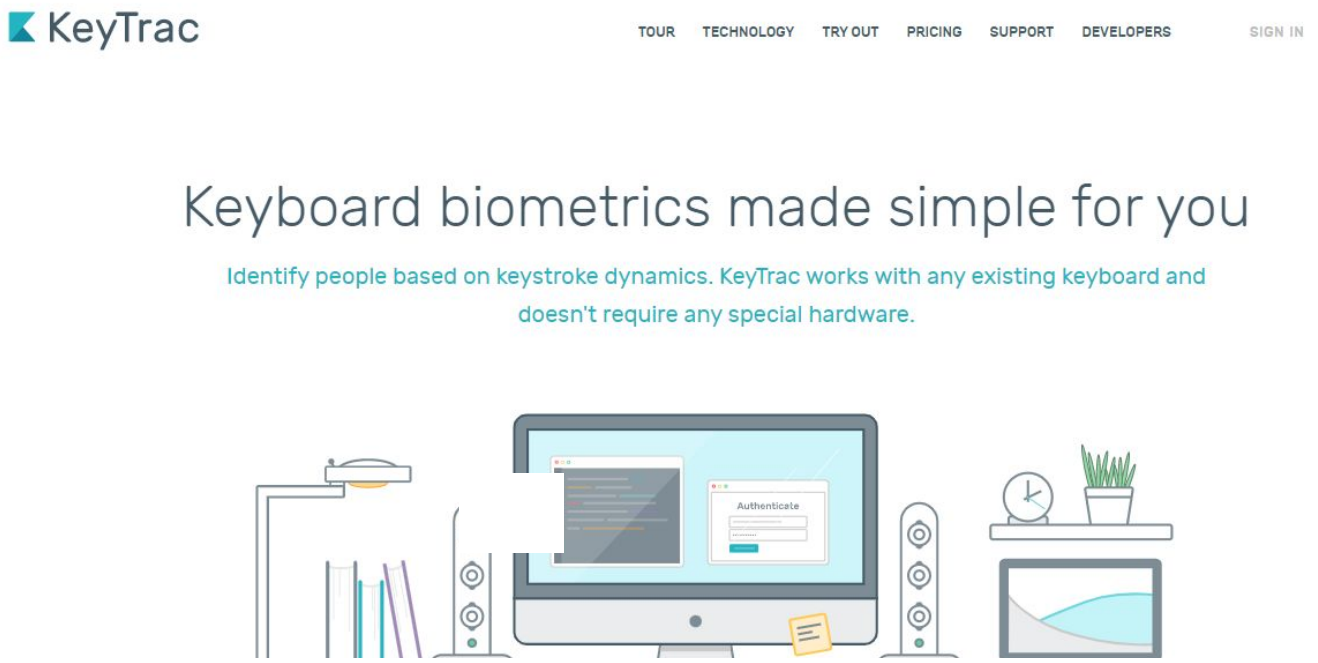
PASSO 5

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



Mouse Movements

User Identification

Automatizações, se feitas de forma errada, são ruins.

Prefira manualmente.

O ÚLTIMO PASSO PARA O SUCESSO!

PASSO 5+1
User Behavior

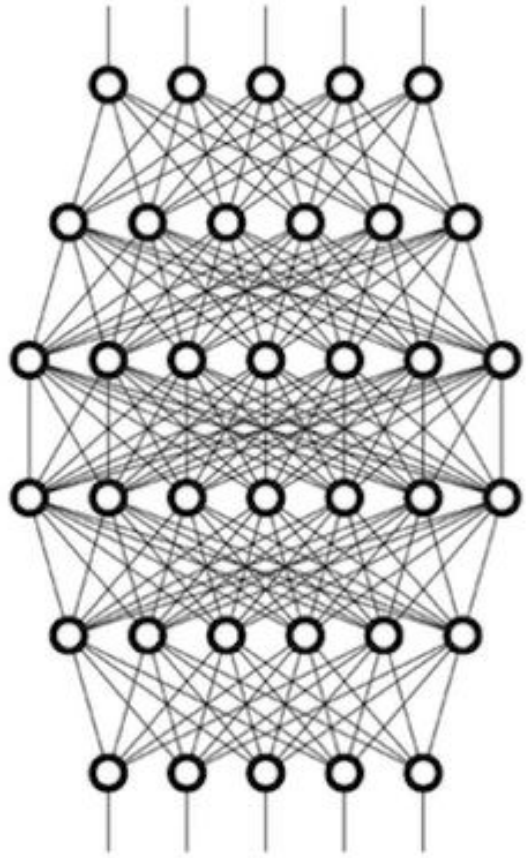
User Behavior

Como as redes usam isso a seu favor

Elas estão cada vez mais indo para o Behavior Analysis

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

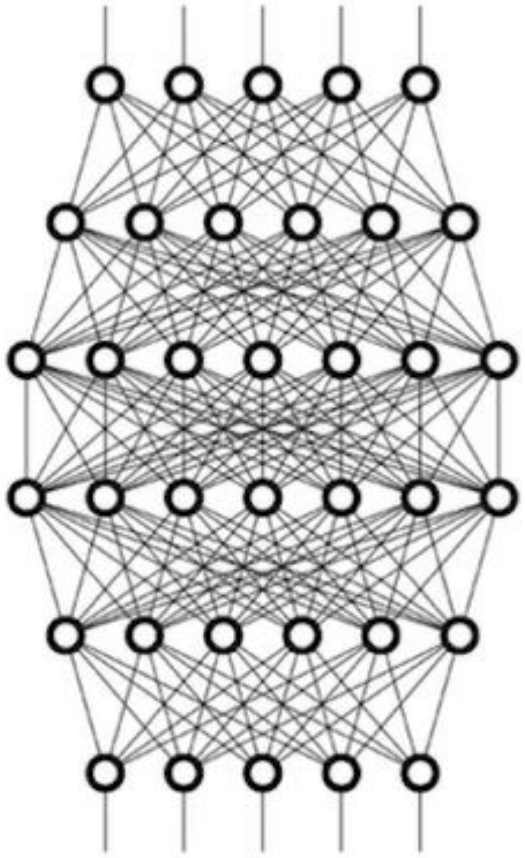
- Facebook e Google já possuem muitos desses tipos de dados **(é muito fácil para eles usarem isso para criar modelos preditivos muito eficazes)**

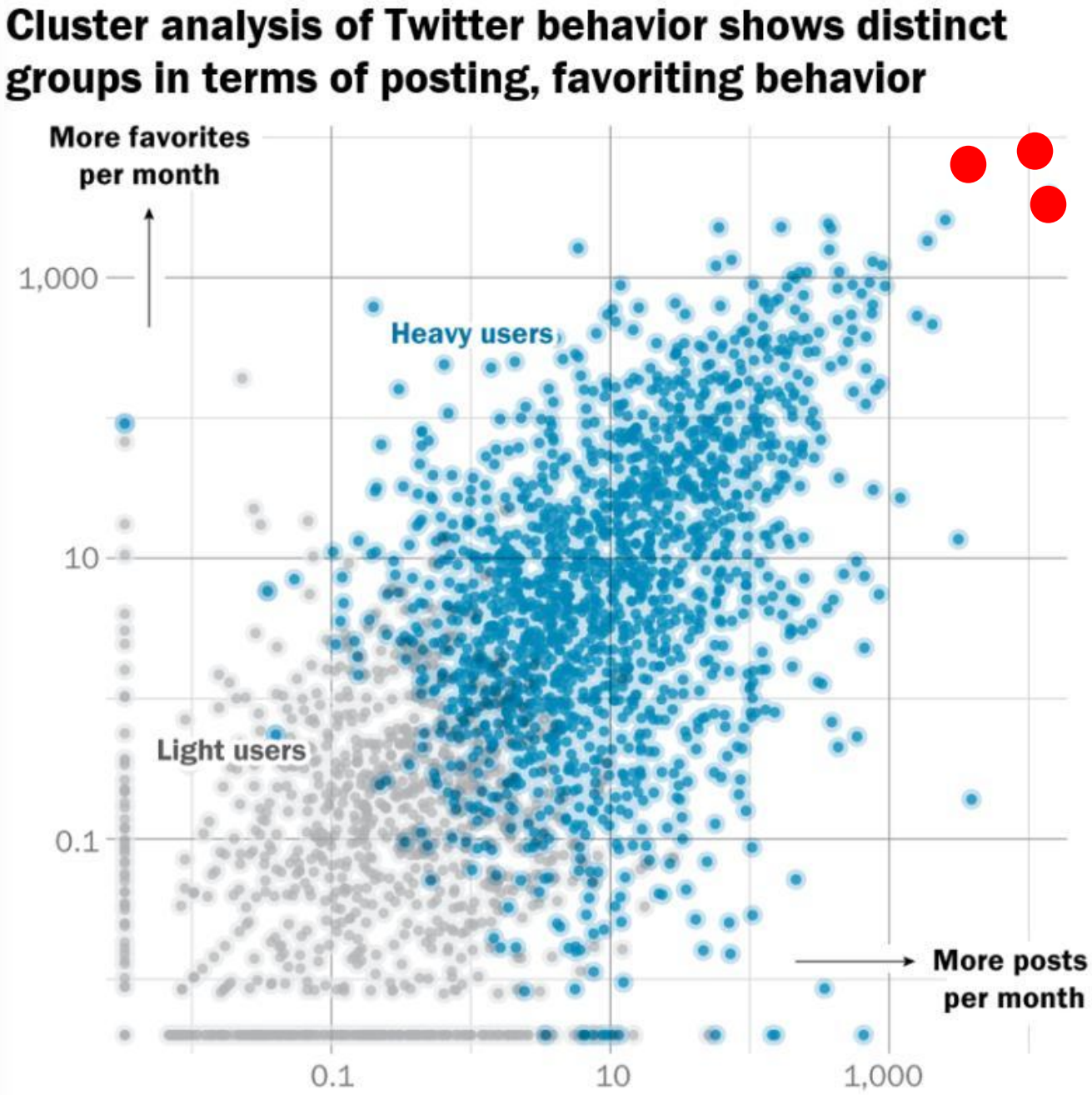


User Behavior

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.





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