

Princípios básicos para o sucesso no **Black Hat**



Nomenclatura

Black Hat à nível code



White Hat



Grey Hat



Black Hat

Nomenclatura

Black Hat no Marketing Digital

BLACK HAT

- Cloaker
- Fora das políticas



WHITE HAT

- Conteúdo relevante
- Tudo dentro das políticas



Por que nasceu O Black Hat?



1. As pessoas são o maior ativo, logo, ele sempre prioriza a **qualidade do que é anunciado** em detrimento de quem anuncia e põe dinheiro em seu bolso
2. Portanto, tem políticas de anúncios rigorosas
3. Os “Bots” bloqueiam sem piedade
4. Sendo assim, nós (media buyers) precisamos nos preparar para se manter no jogo

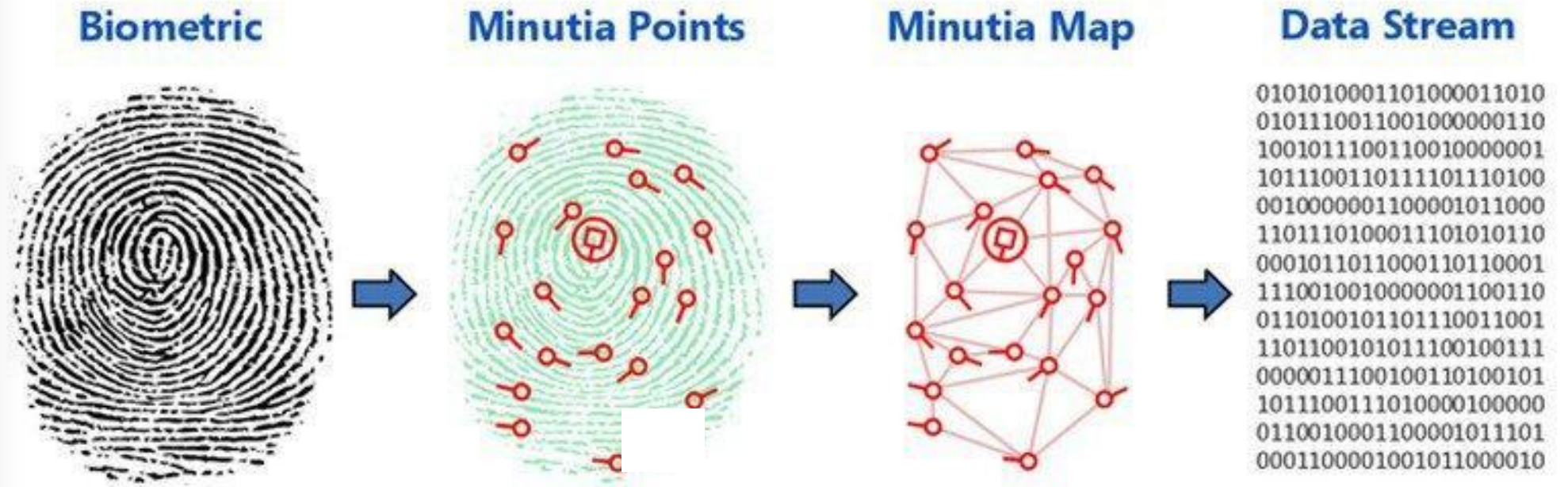
PASSO 1

Fingerprint e Antidetectects

Fingerprint

na vida real

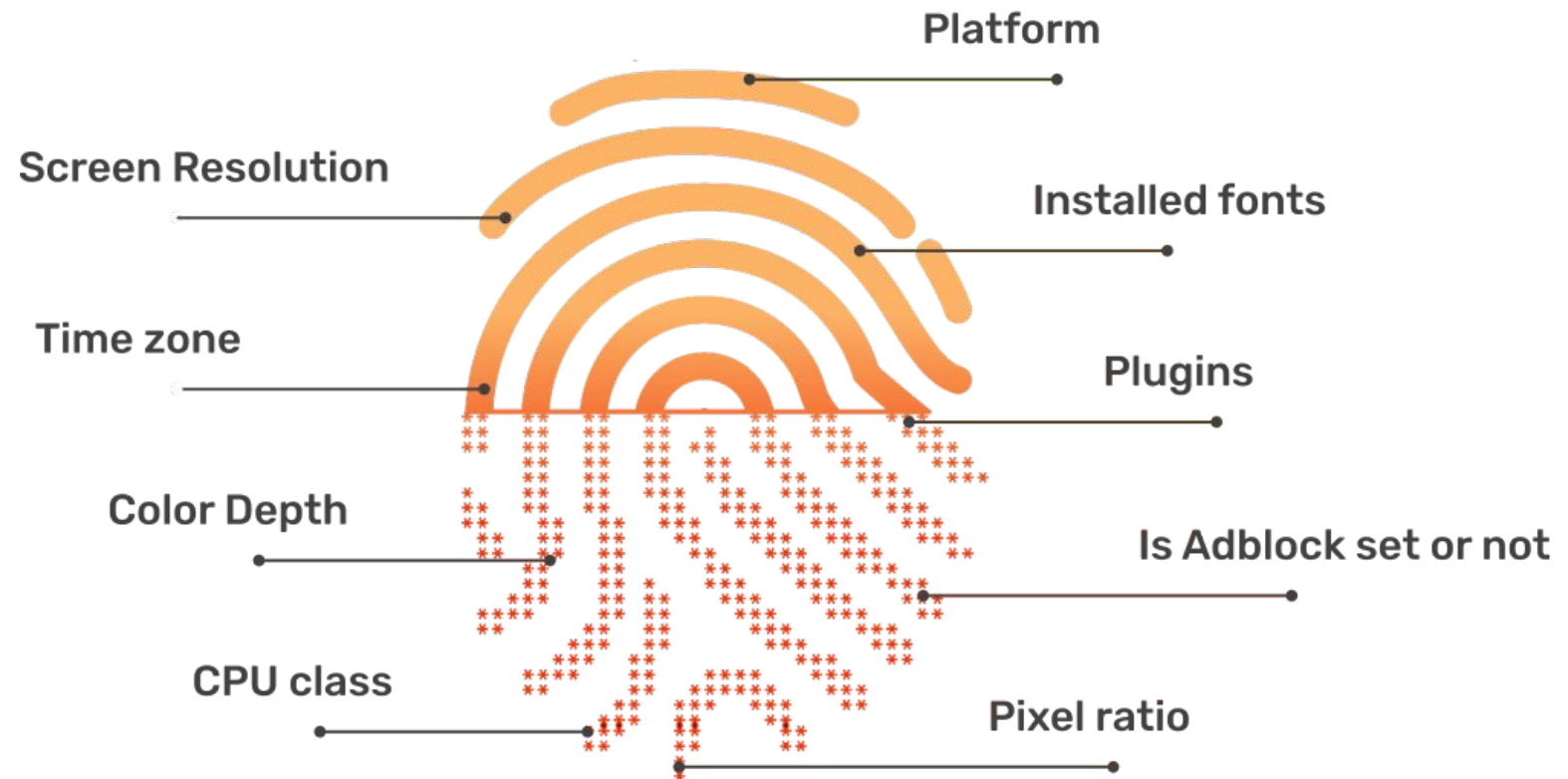
Minutia points: pontos de mudança de linha. Vetores (x,y) em um plano cartesiano.



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)

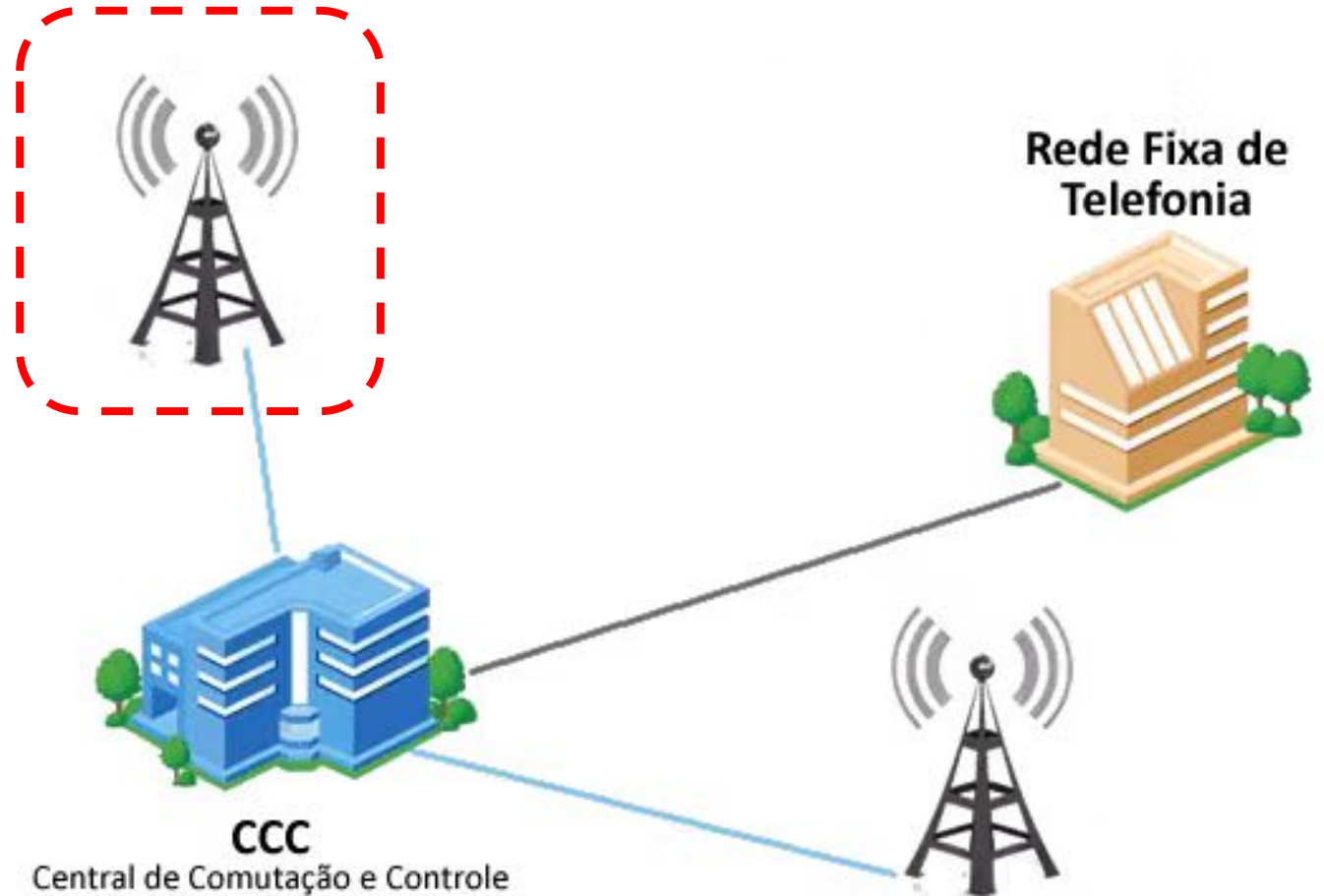
3 tipos de “casas” (IP)

- IP data center
- IP residencial
- IP mobile

Internet Protocol (IP)

Por que IPs mobile são “melhores”?

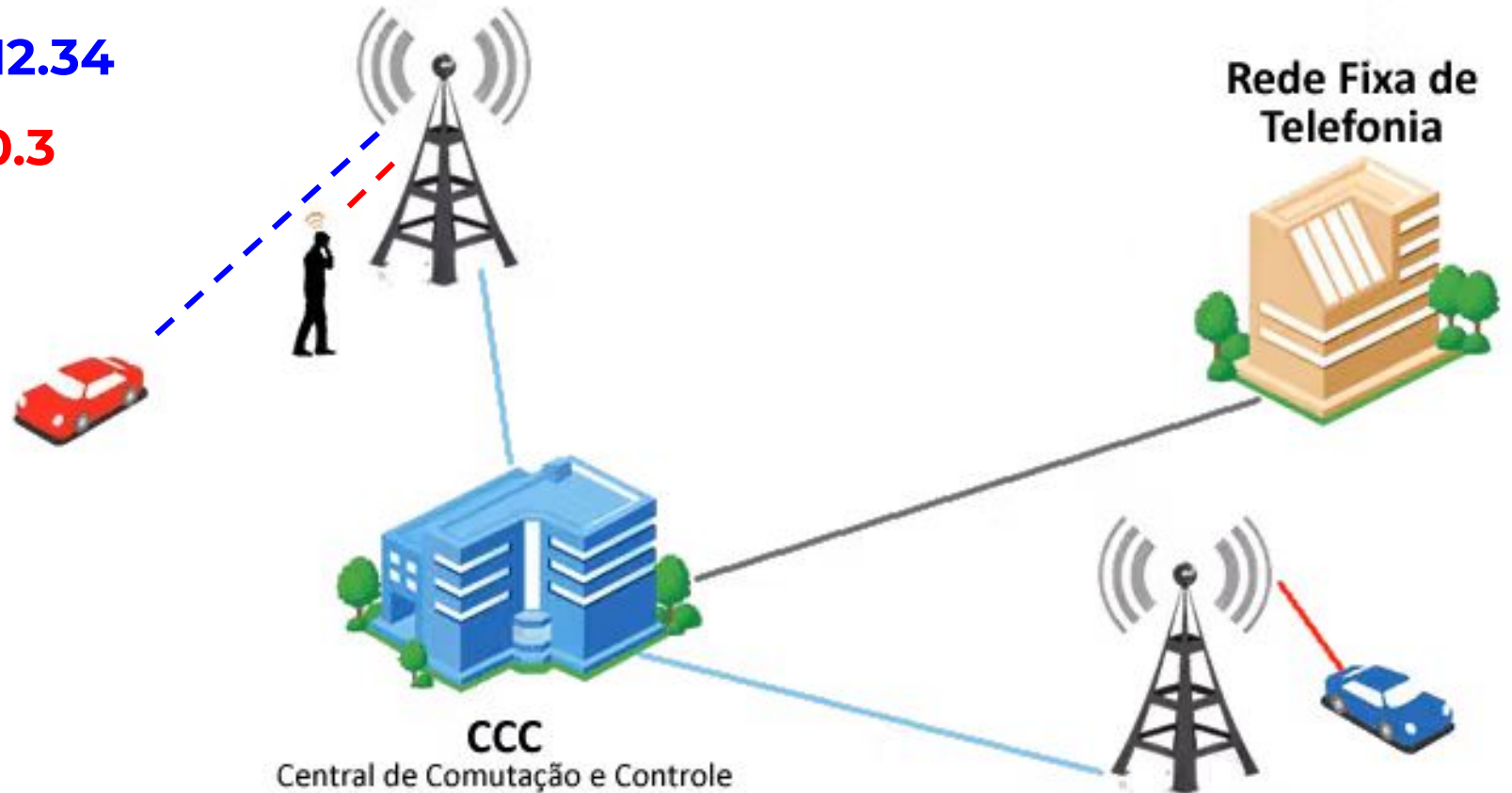
- 196.254.12.34
- 207.25.10.3



Internet Protocol (IP)

Por que IPs mobile são “melhores”?

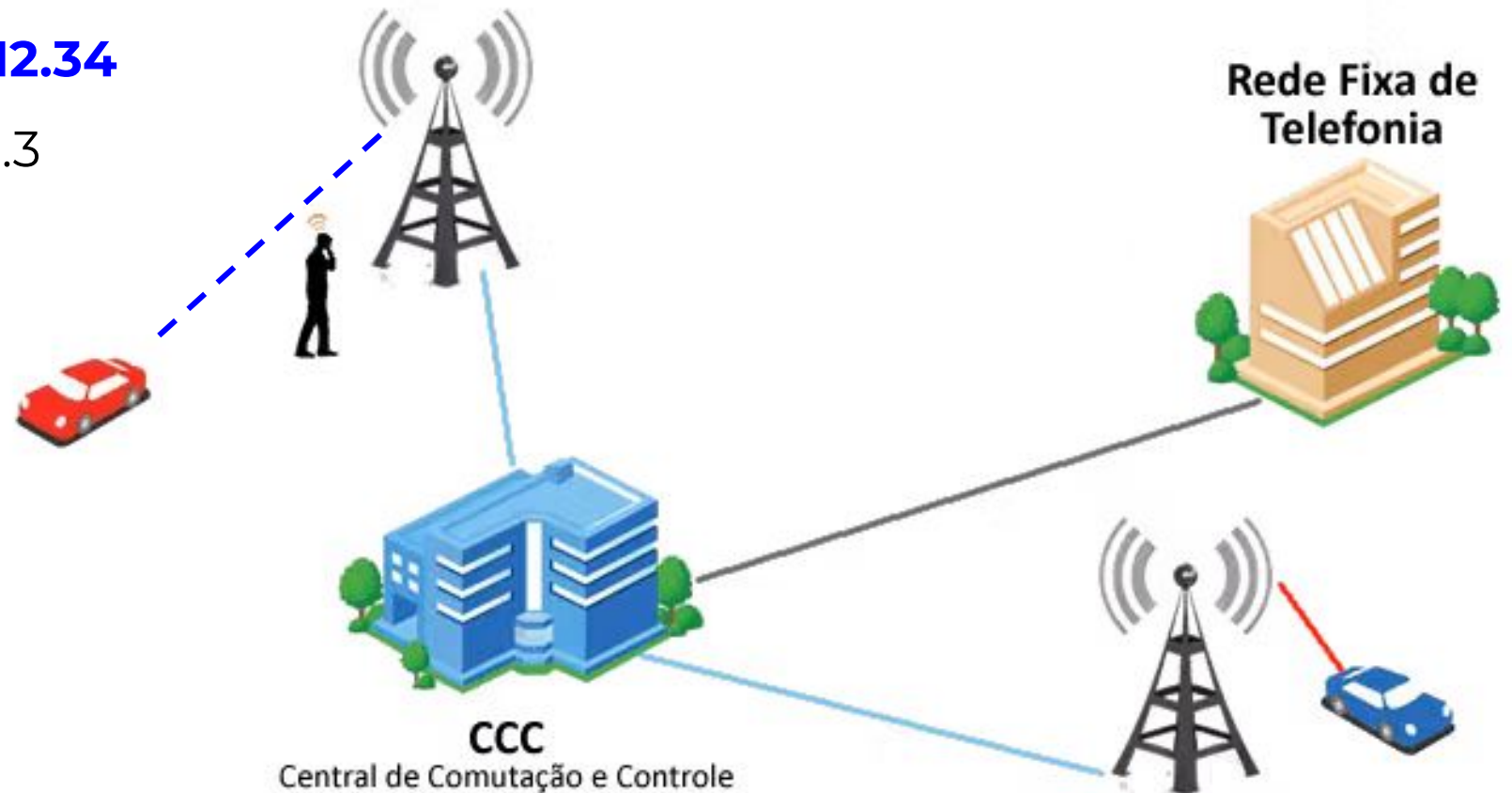
- 196.254.12.34
- 207.25.10.3



Internet Protocol (IP)

Por que IPs mobile são “melhores”?

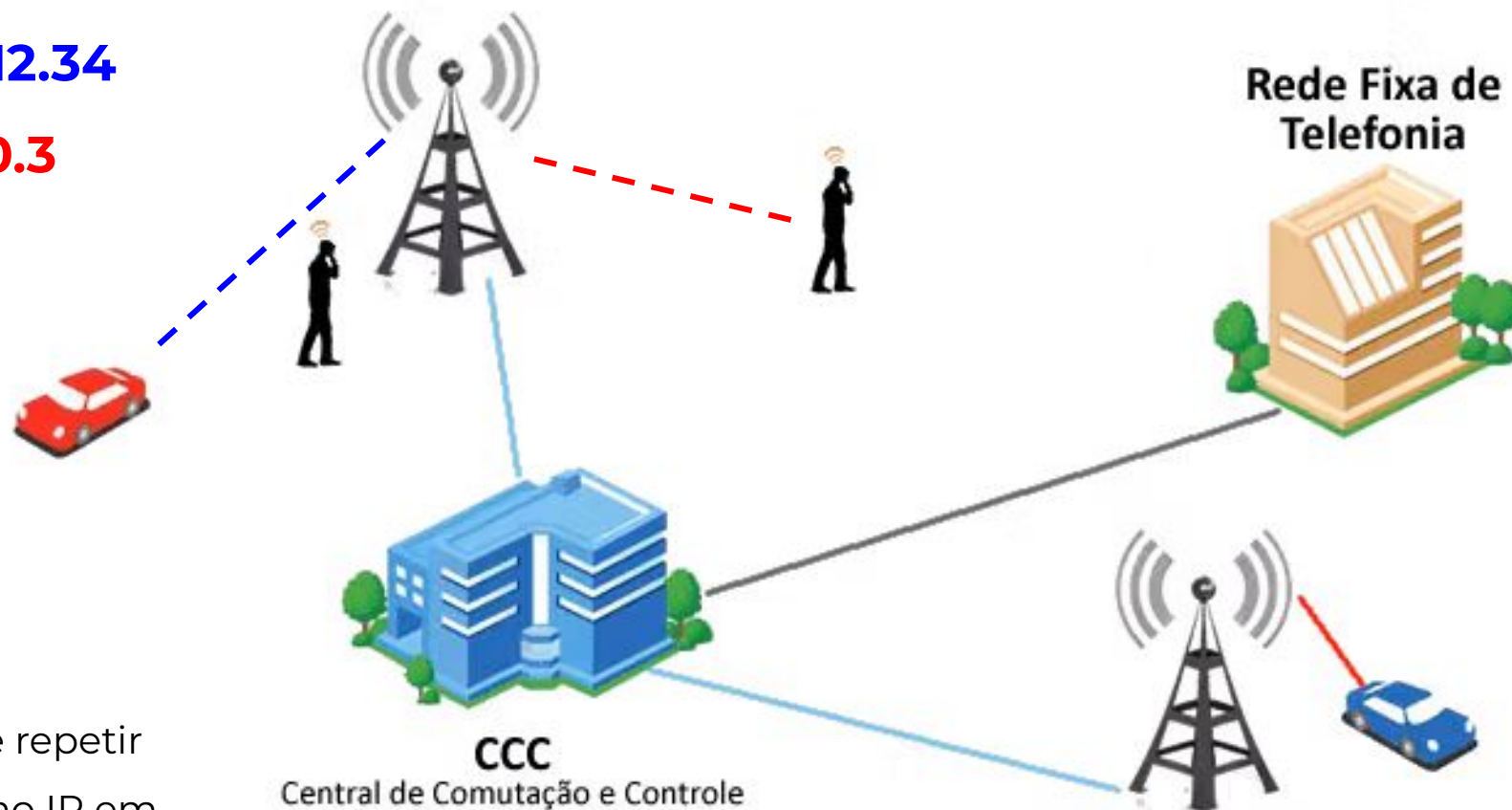
- 196.254.12.34
- 207.25.10.3



Internet Protocol (IP)

Por que IPs mobile são “melhores”?

- 196.254.12.34
- 207.25.10.3



Pulo do Rato: pode repetir
de 3 até 5x o mesmo IP em
contas diferentes

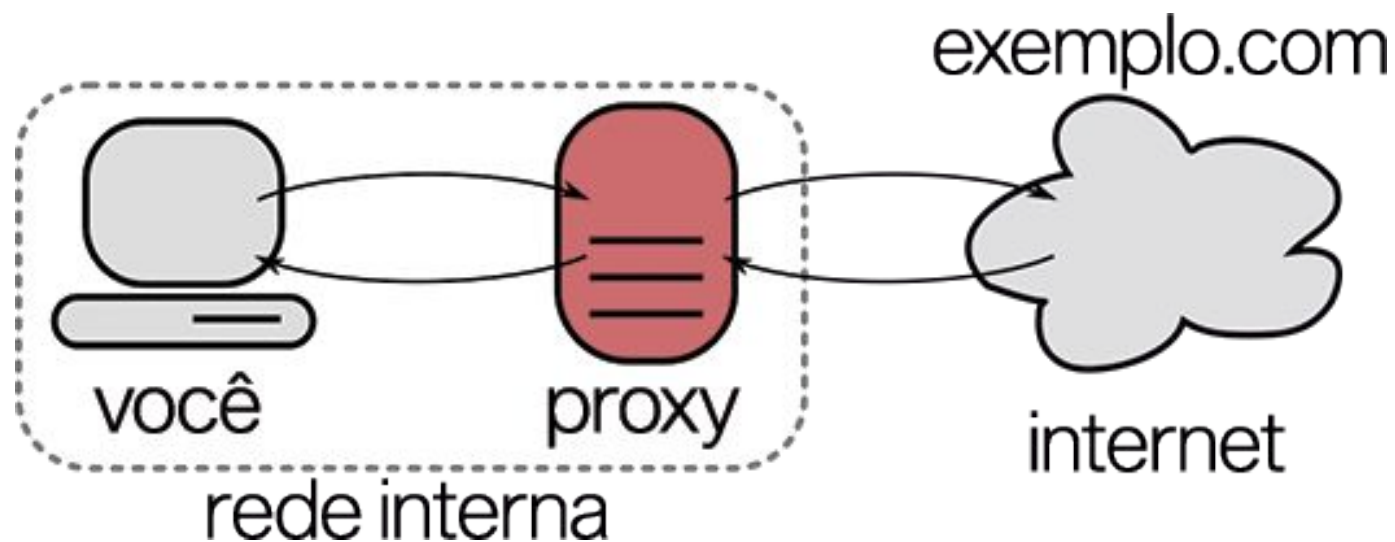
PASSO 3

Proxy

Proxy

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

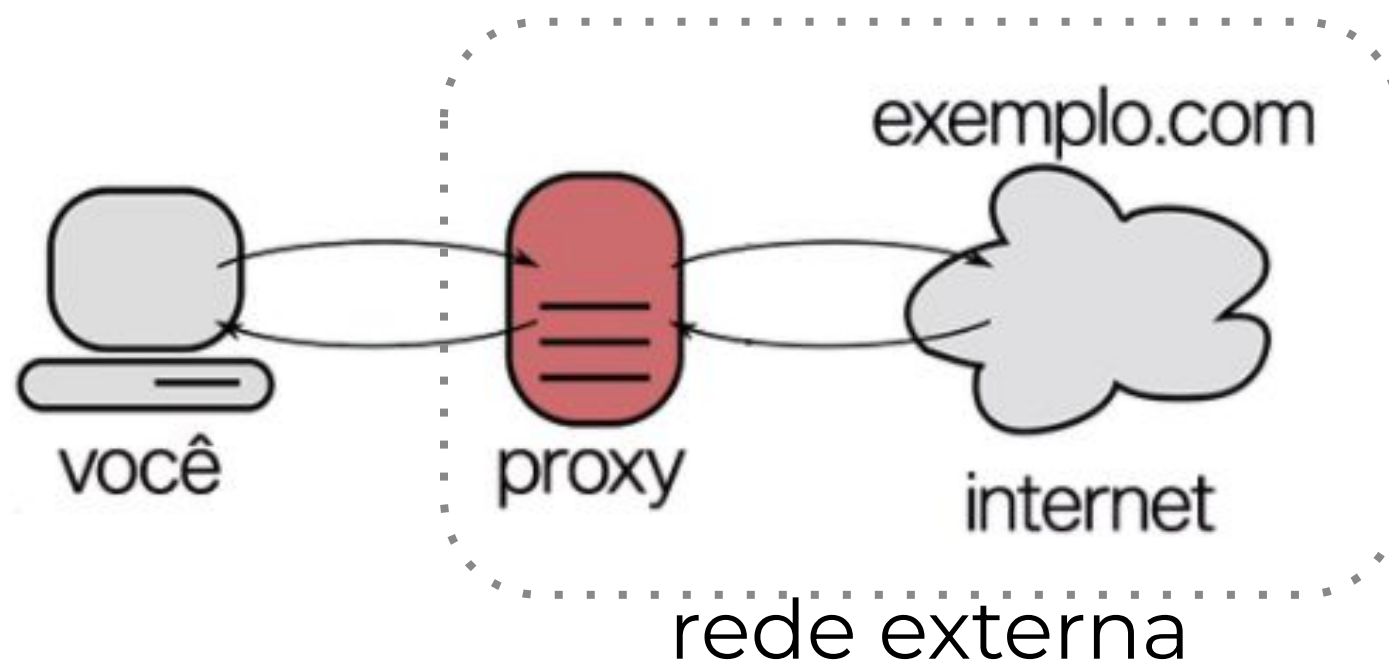
Ele direciona o tráfego por uma rota específica. Desse modo, é possível bloquear sites, gerar mais privacidade para a navegação e evitar situações de risco, por exemplo.



Proxy

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

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



	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

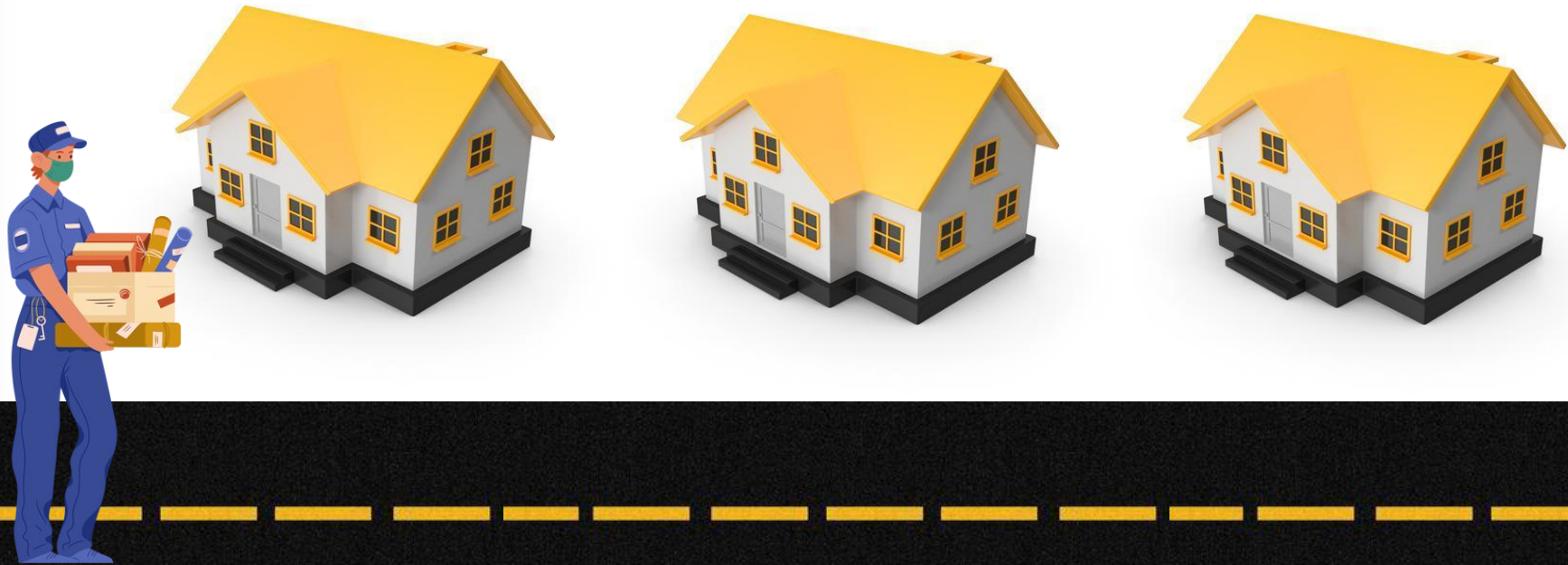
Imagine que um carteiro precisa fazer uma entrega em uma casa e tem a rua e o número da residência...

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



Portas TCP/UDP

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



Rua Maria Figueiredo, 560
197.25.34.108/24

Portas TCP/UDP

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



Rua Maria Figueiredo, 560 - Apto 87
197.25.34.108/24 PORTA 5938

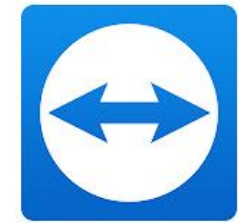
Portas TCP/UDP

Um “prédio” enviando informações para outro
“prédio”



197.25.34.108/24

PORTA 5938



TeamViewer

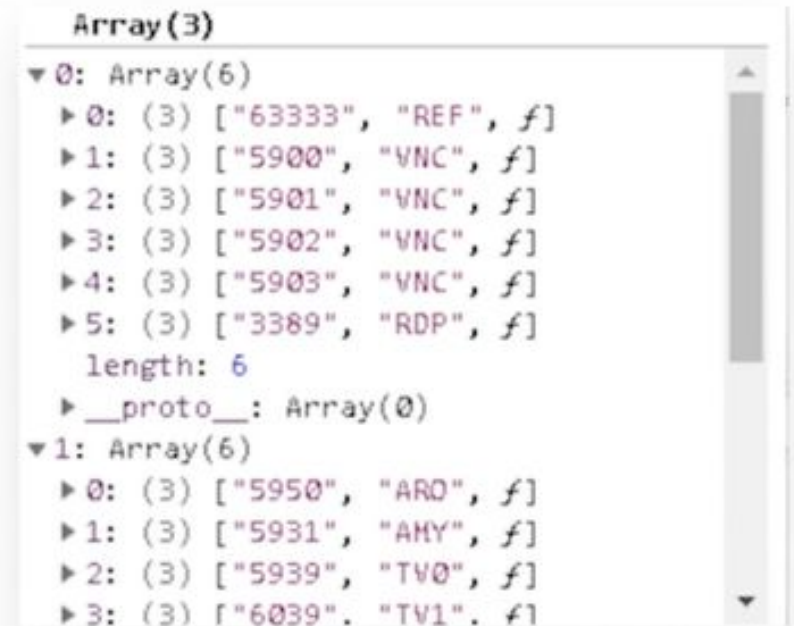
203.110.1.32/11

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.

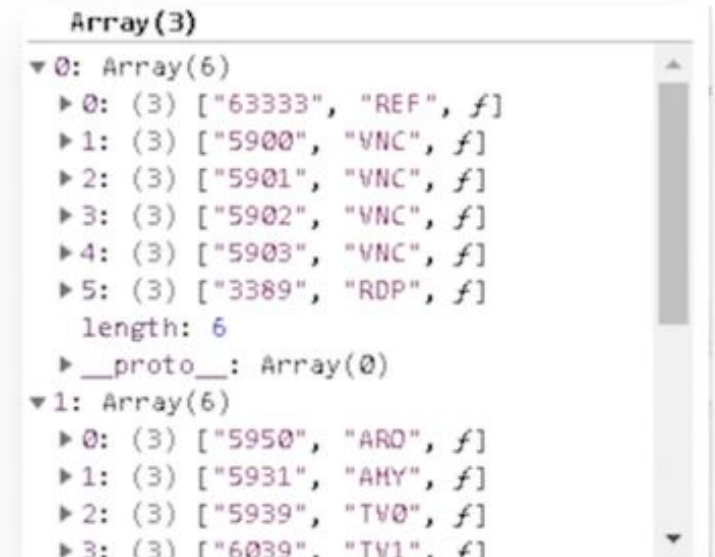


Portas TCP/UDP

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 com o Multilogin ou Dolphin Anty

Portas 3389,5900,5800,7070,6568 e 5938



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 website interface. At the top, there are navigation links for NEWS, LIVE TV, and APP. Below these is a red navigation bar with links for HOME, MY FEED, ELECTIONS, CORONA, INDIA, BUSINESS, WORLD, TECH, MOVIES, and HAPPINESS QUE. A blue banner below the navigation bar features a hand cursor icon, the text 'Assembly Election 2022', and an 'ASSOCIATE SPONSOR' logo for 'Simpliify'. The main headline reads 'Facebook confirms that it tracks how you move mouse on the computer screen'. Below the headline is a sub-headline: '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, and dated June 12, 2018, with an update on June 13, 2018. Social media sharing icons for YouTube, Facebook, Twitter, WhatsApp, and others are visible at the bottom right of the article content area.

NEWS • LIVE TV INDIA TODAY APP

HOME MY FEED ELECTIONS CORONA INDIA BUSINESS WORLD TECH MOVIES HAPPINESS QUE

Assembly Election 2022 ASSOCIATE SPONSOR Simpliify

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.

Shweta Ganjoo
New Delhi
June 12, 2018 UPDATED: June 13, 2018 19:43 IST

YouTube Facebook Twitter WhatsApp

PASSO 6

User Behavior

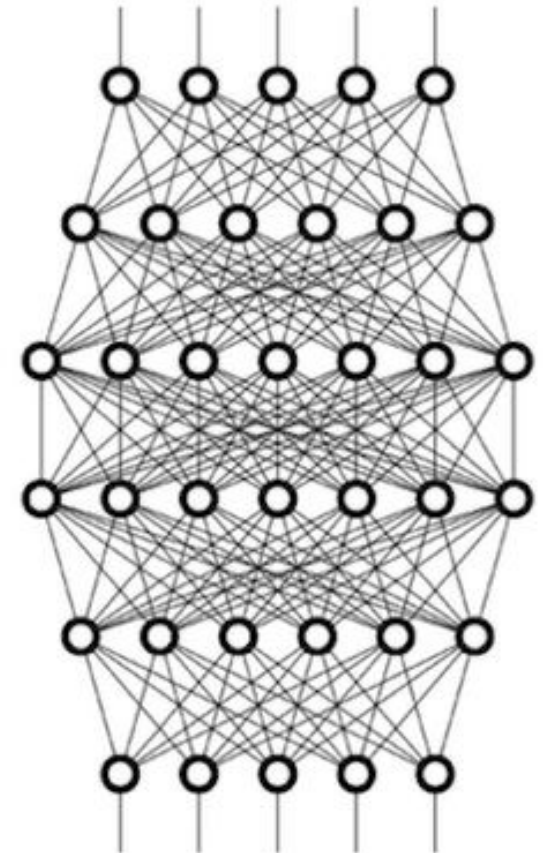
User Behavior

Como as redes usam isso a seu favor

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...

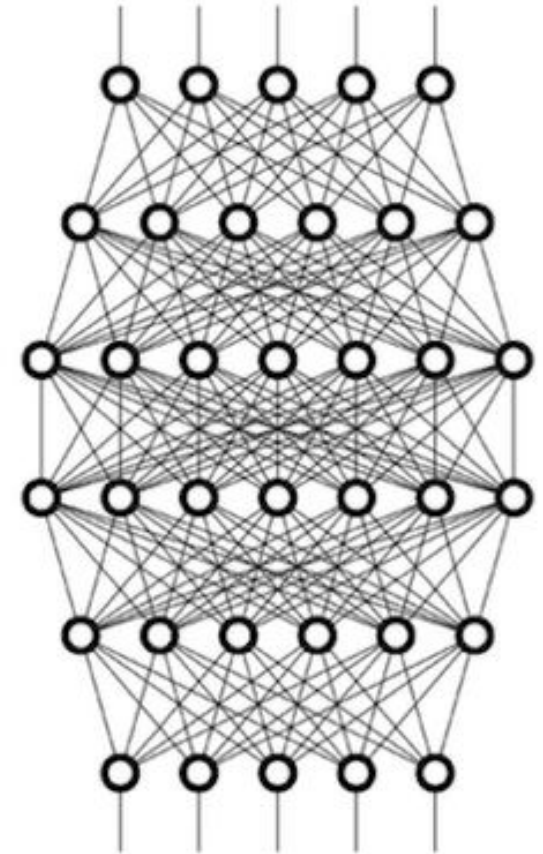
- Facebook e Google já possuem muitos desses tipos de dados **(é muito fácil para eles usarem isso para criar modelos preditivos muito eficazes)**



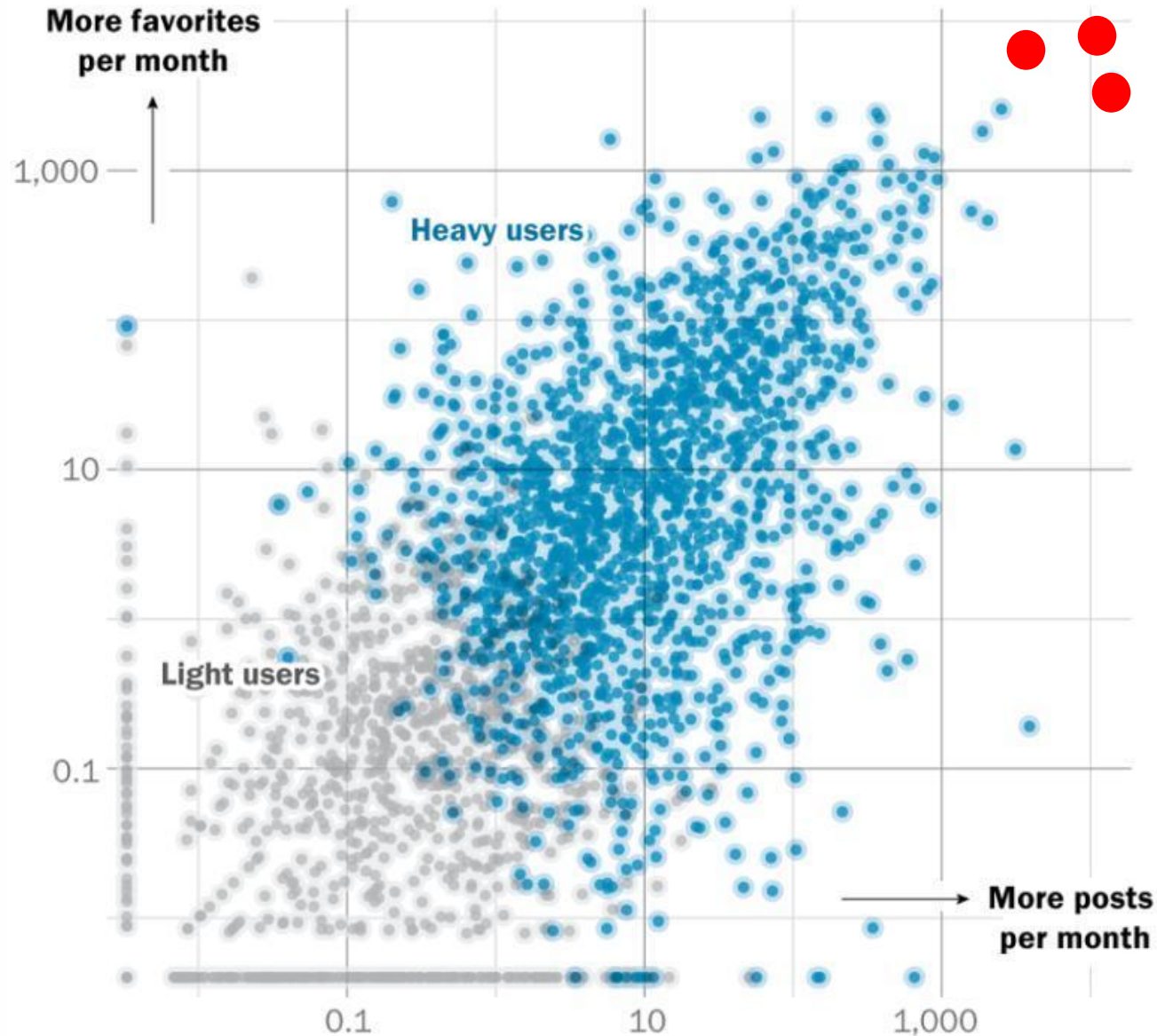
User Behavior

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 e comportamentos sejam muito mais importantes**, pois ele detecta com facilidade um usuário comum de um anunciante que sobe anúncios proibidos.



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



**Se misture na
multidão, mas na
multidão certa!
Não seja o cara com
uma melancia no
pescoço.**



User Behavior

O que não fazer

- Repetir criativos
- Ativos criados recentemente e que seguem um padrão de aquecimento: foto de mulher na página, post de engajamento pra aquecer conta...
- Domínios convencionais no meio digital: .fun, .online, .site
- Use perfis reais
- Use ativos antigos (+1 ano)
- Landing Pages com estrutura HTML únicas
- Domínios mais “normais” com mais de 1 ano (Hack: MOZ)

User Behavior

A máxima do dia é...

Eu poderia listar muito mais coisas a se fazer, mas entrariamos em um paradoxo no qual as coisas que falar irão parar de funcionar. Portanto, pense por si e crie o seu método único!

BÔNUS

Conteúdos movidos para a área gratuita do fórum até 14h de amanhã!

- Aprenda como forçar ZRD e recuperar o perfil
- Como recuperar BMs, CAs, Páginas e Perfis que não foram reativados após cair
- Contingência de contas: o verdadeiro INFERNO no Google Ads
- CTR 50% – Bug do Facebook – Substituição criativa

Acesse <https://www.blackrat.pro/forum/144-conte%C3%BAdo-free>

Obrigado!