TOMORROW\\

TOMORRO\\\

O PODER DA TECNOLOGIA PARA SOLUCIONAR OS DESAFIOS DA COMUNICAÇÃO DIGITAL.

Com sede em Nova York, escritórios em São Paulo, Cingapura e Dubai, e em expansão global, a TOMORRO\\\ é uma integradora e distribuidora de soluções de tecnologia para Publicidade e Marketing Digital.

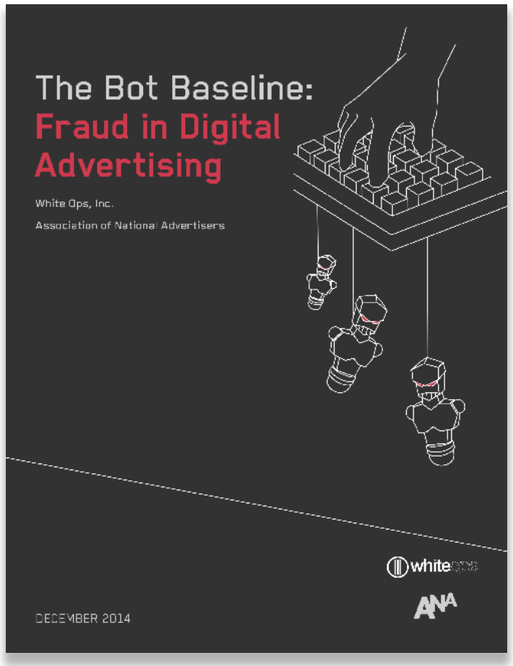
Selecionamos de forma independente, empresas e desenvolvedores de tecnologia, que podem potencialmente solucionar os problemas e desafios da indústria de comunicação.

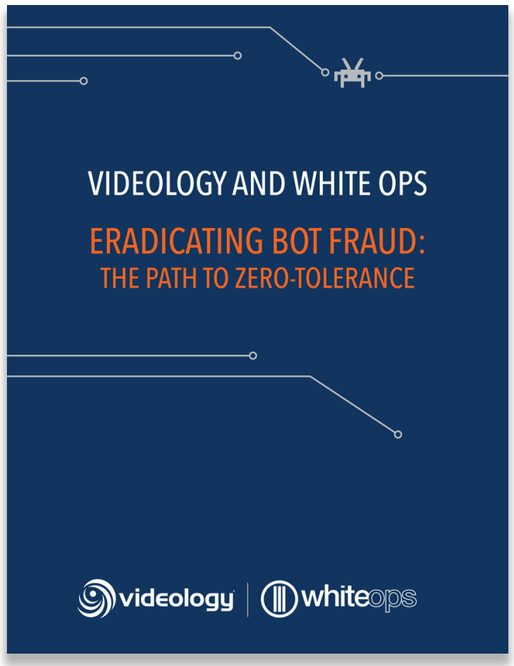
Agregamos as tecnologias e estruturamos soluções abrangentes, eficazes e de fácil implementação, que são distribuídas pela rede TOMORRO\\\, acrescentando diferenciais competitivos e de valor à oferta local das Marcas, Agências e Empresas de Mídia.

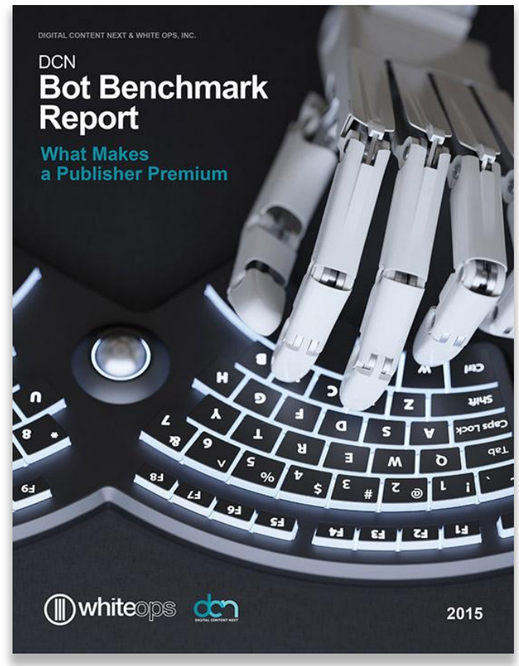
Estamos criando canais de acesso global às mais avançadas soluções de publicidade digital, viabilizando o conhecimento e competitividade internacional para as empresas locais.

WHITE OPS

O PADRÃO EM PREVENÇÃO E DETECÇÃO DE FRAUDE ROBÓTICA DIGITAL NA PUBLICIDADE







A FRAUDE ROBÓTICA NA PROPAGANDA DIGITAL

- COMO VOCÊ DECIDE SUAS COMPRAS DE MÍDIA DIGITAL?
- ALGUMA SUSPEITA DE QUE SUAS CAMPANHAS TENHAM SIDO FRAUDADAS?
- E COMO VOCÊ LIDA COM A FRAUDE?

HOJE, A FRAUDE ROBÓTICA É O MAIS LUCRATIVO CRIME CIBERNÉTICO:

A FRAUDE EM PROPAGANDA DIGITAL CUSTARÁ

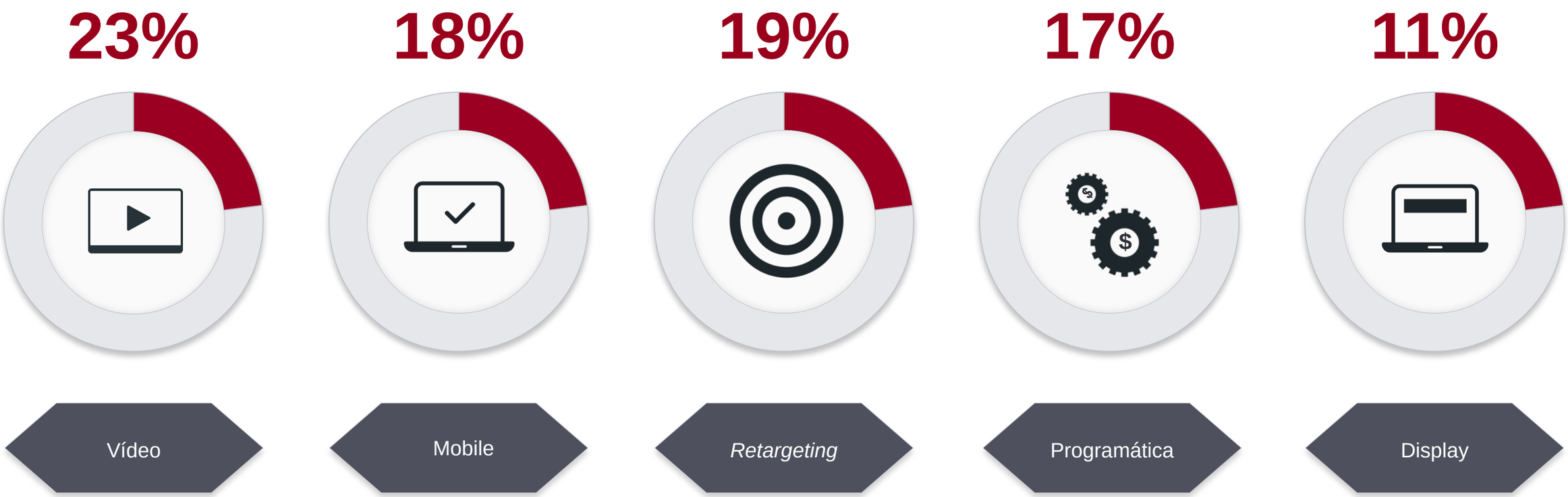
US$ 7.2 BILHÕES

2016

FONTE: 2015 Bot Baseline Report

A FRAUDE ROBÓTICA PROSPERA EM TODO TIPO DE MÍDIA DIGITAL

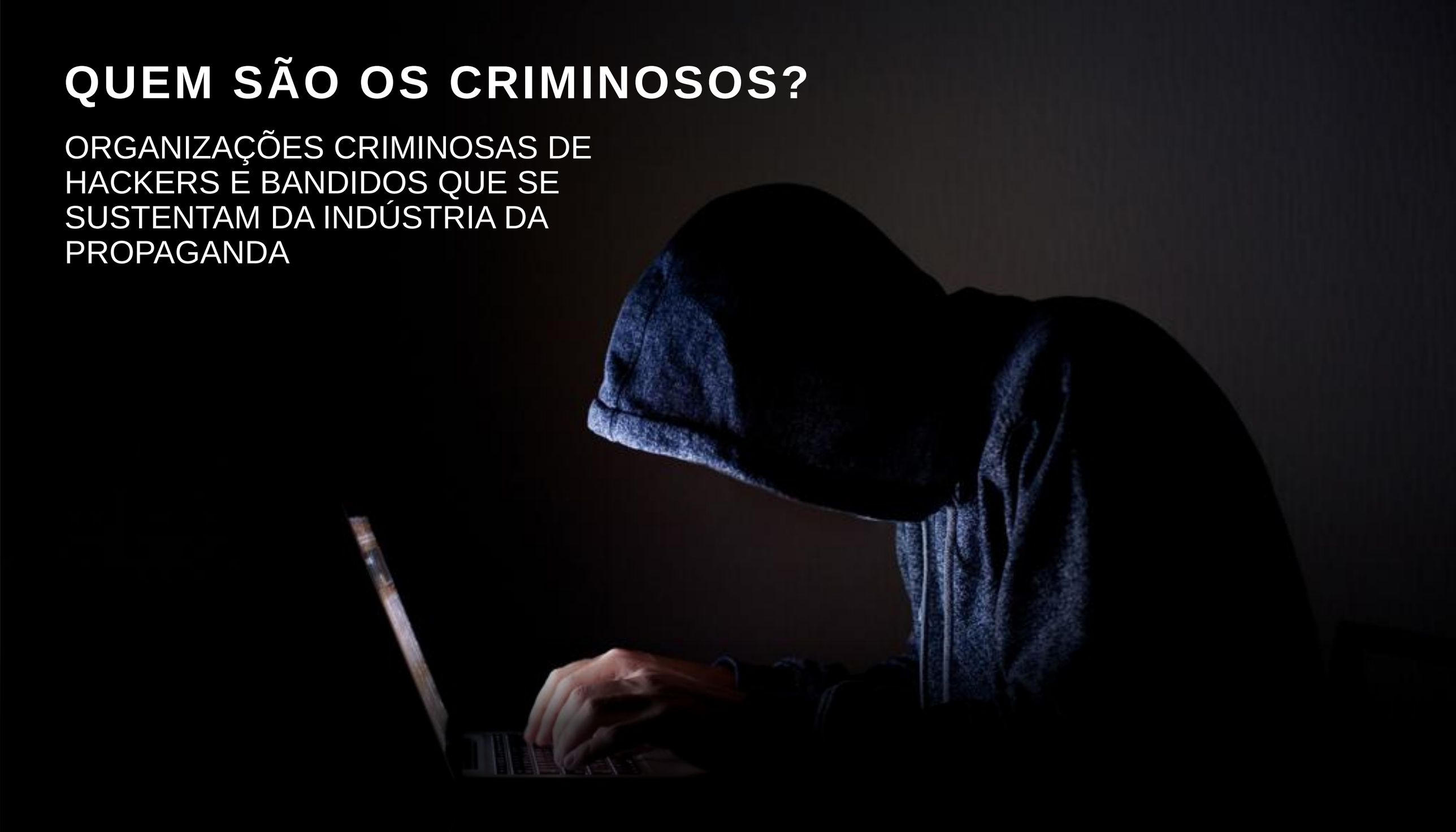
É MAIOR, QUANTO MAIOR O CPM



FONTE: 2014 & 2015 Bot Baseline Reports. As percentagens refletem a média detectada nos estudos dos dois anos.

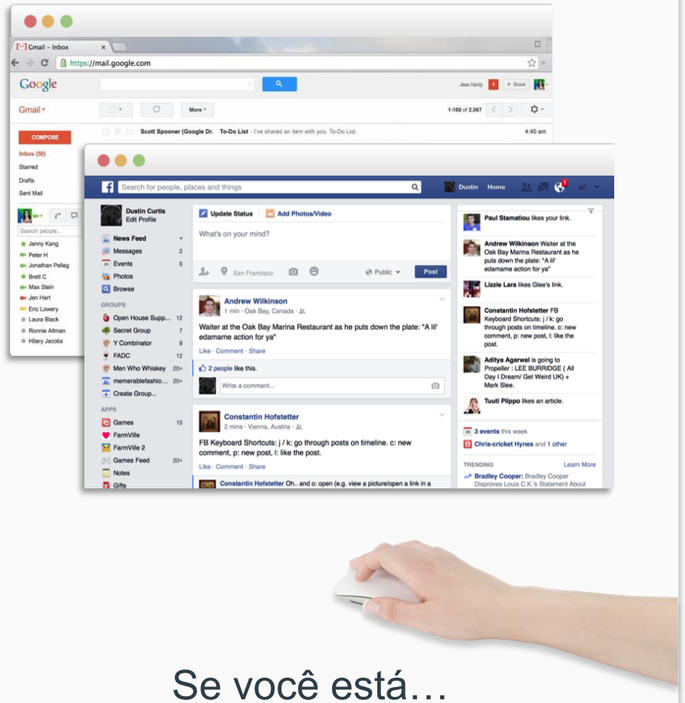
QUEM SÃO OS CRIMINOSOS?

ORGANIZAÇÕES CRIMINOSAS DE HACKERS E BANDIDOS QUE SE SUSTENTAM DA INDÚSTRIA DA PROPAGANDA

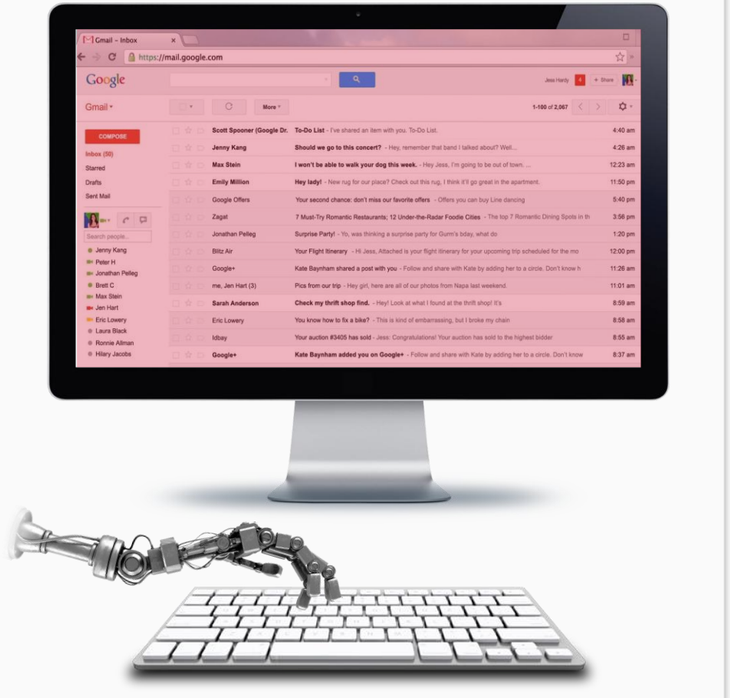


PRIMEIRO, OS *HACKERS* INFECTAM COMPUTADORES COM *MALWARE*

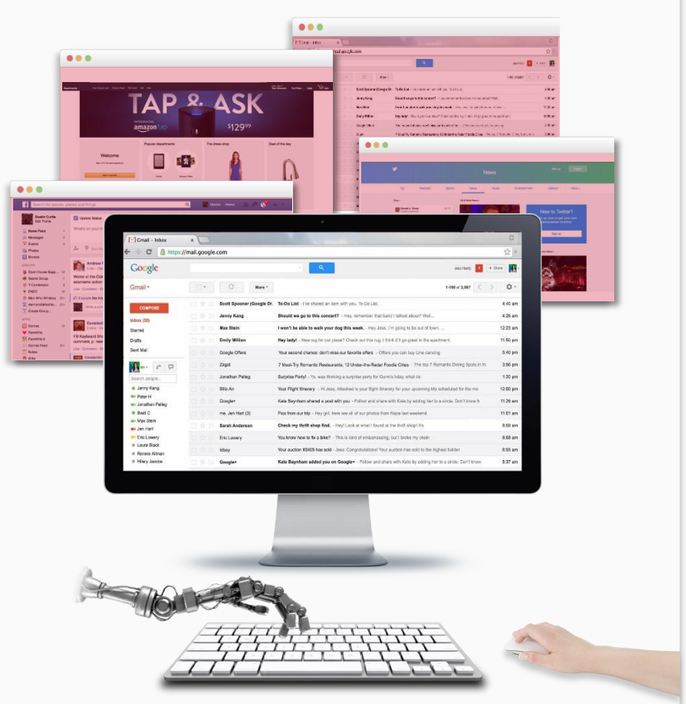
OS COMPUTADORES INFECTADOS IMITAM OS MOVIMENTOS HUMANOS NOS *BROWSERS*



Se você está…
logado no Facebook,
checando seu Gmail,
comprando no e-commerce…



E tem um malware
no seu computador…



o malware está fazendo as
mesmas coisas... imitando
seus hábitos.

OS *BOTS* ESTÃO ATIVOS EM TODO MUNDO, NESTE MOMENTO

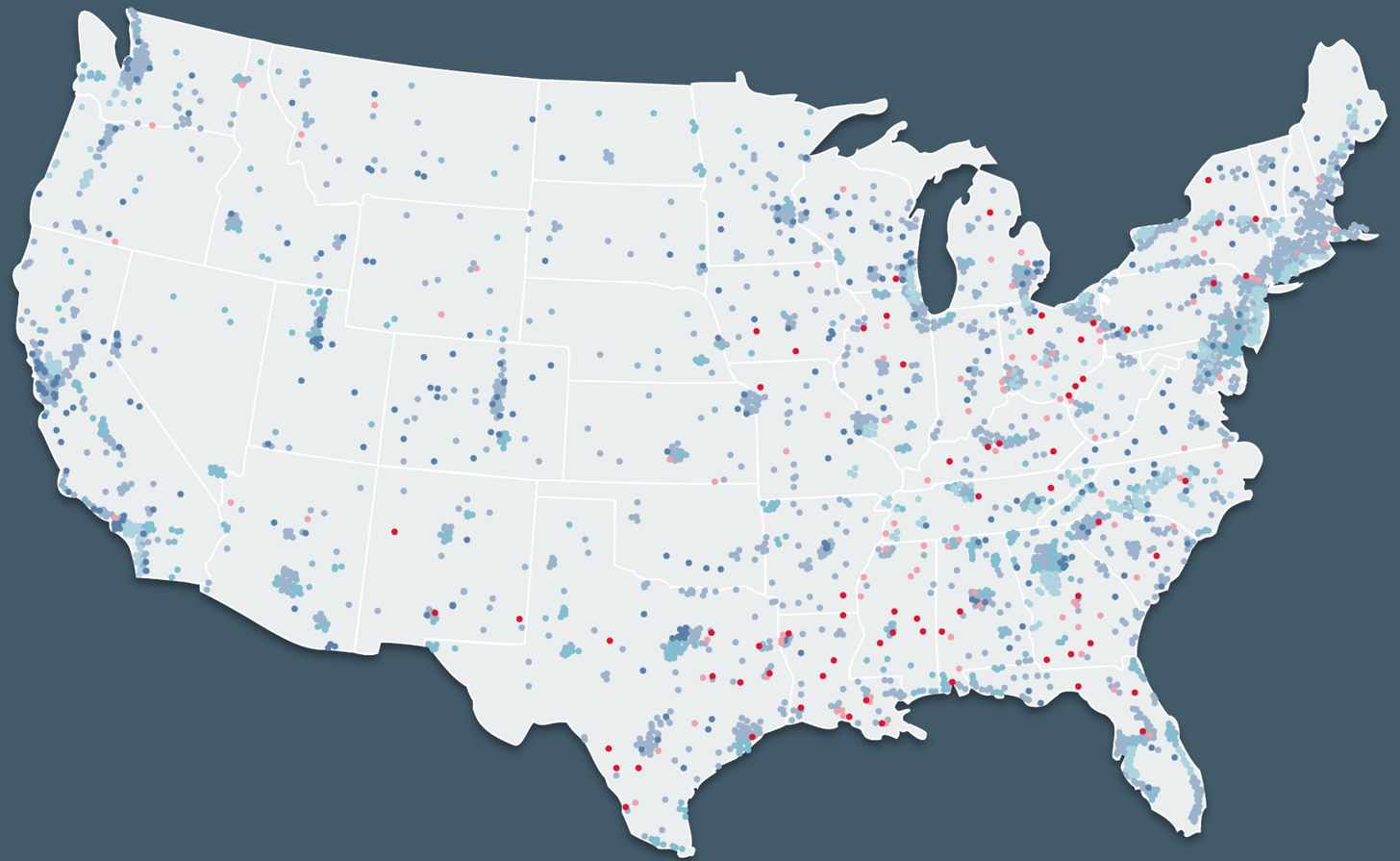
NOS EUA, A CONCENTRAÇÃO DE *BOTS* ACOMPANHA A DENSIDADE DEMOGRÁFICA

30%

dos computadores domésticos nos EUA estão infectados com malware

2/3

do tráfego de bots vem de computadores em residências



BOT RATES

- > 10.0%
- 8.0 – 10.0%
- 6.0 – 8.0%
- 4.0 – 6.0%
- 2.5 – 4.0%
- 0.0 – 2.5%

FONTE: 2016 Bot Baseline Report

E COMO A FRAUDE SE PERPETUA?

OS HACKERS OPERAM FACILMENTE EM UM AMBIENTE COMPLEXO COMO O DA MÍDIA DIGITAL

CLIENTE

PUBLISHER

CONSUMIDOR

UMA NOVA PRÁTICA FACILITOU A FRAUDE

O ‘TRÁFEGO COMPRADO’ DE 3os IMPREGNA O INVENTÁRIO COM IMPRESSÕES FALSAS

‘SOURCED TRAFFIC’

3x **MAIS PROVÁVEL**

de conter *bots* do que tráfego controlado.

1

PUBLISHER

Faz acordo com um terceiro para preencher inventário

2

INTERMEDIÁRIO
3RD PARTY TRAFFIC BROKER

Terceiro faz acordo com outro terceiro para originar mais tráfego

3

ANUNCIANTE
& *PUBLISHER*

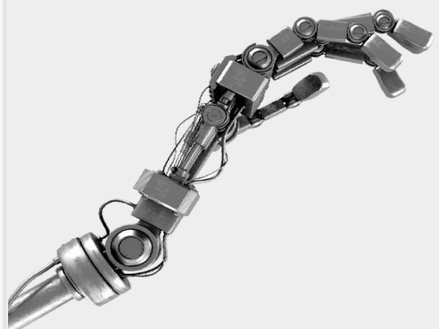
Tráfego terceirizado contendo *bots* cria falsas visualizações

FONTE: 2015 Bot Baseline Report

whiteops

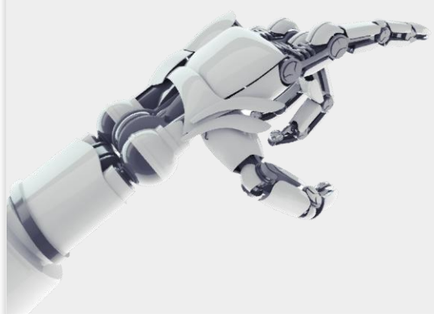
A FRAUDE REALIZADA POR BOTS SOFISTICADOS É CRESCENTE

CLASSIFICAÇÃO DO **MEDIA RATING COUNCIL DOS EUA** PARA TRÁFICO INVÁLIDO



General Invalid Traffic (GIVT):

*"Automated **bot** entities capable of consuming any digital content, including text, video, images, audio, and other data. These agents may intentionally or unintentionally view ads, watch videos, listen to radio spots, fake viewability, and click on ads".*



Sophisticated Invalid Traffic (SIVT):

"Includes bot traffic only identified through advanced analytics, multipoint corroboration, human intervention—such as hijacked devices, ad tags, or creative; adware; malware; misappropriated content.

FONTES: 2015 Bot Baseline Report; Media Rating Council - Invalid Traffic (IVT) & Filtration Guidelines (October 2015)

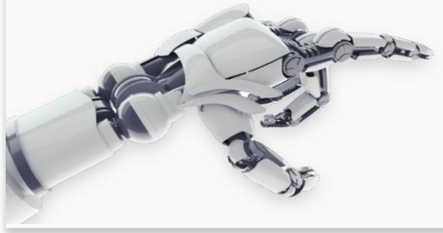
ESTES *BOTS* SÃO DESENVOLVIDOS PARA ENGANAR MÉTRICAS

Bots...

Exploram os *cookies* dos usuários para parecerem humanos

Trabalham imitando hábitos do usuário.

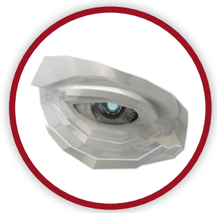
São mais ativos em períodos importantes, como datas comemorativas.



MÉTRICAS DE *VIEWABILITY* SÃO **FALSIFICADAS** por *Bots* Sofisticados

3 A CADA 4X

47%



43%

Human

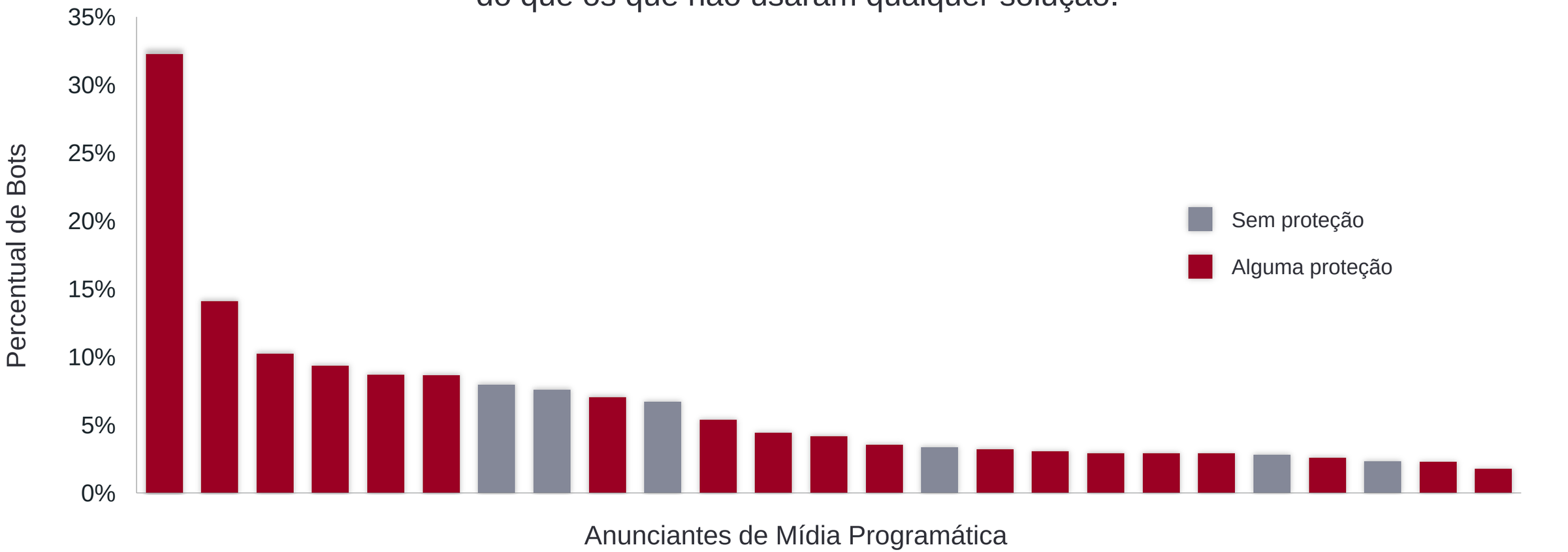
Sophisticated Robot

Source: 2015 Bot Baseline Report

UM FALSO SENSO DE SEGURANÇA

SOLUÇÕES DE SEGURANÇA DIGITAL GENÉRICAS, NÃO TÊM SIDO EFICAZES.

Membros da Associação Nacional dos Anunciantes (EUA) **usando soluções genéricas**, tiveram piores resultados do que os que não usaram qualquer solução.



FONTE: 2015 Bot Baseline Report

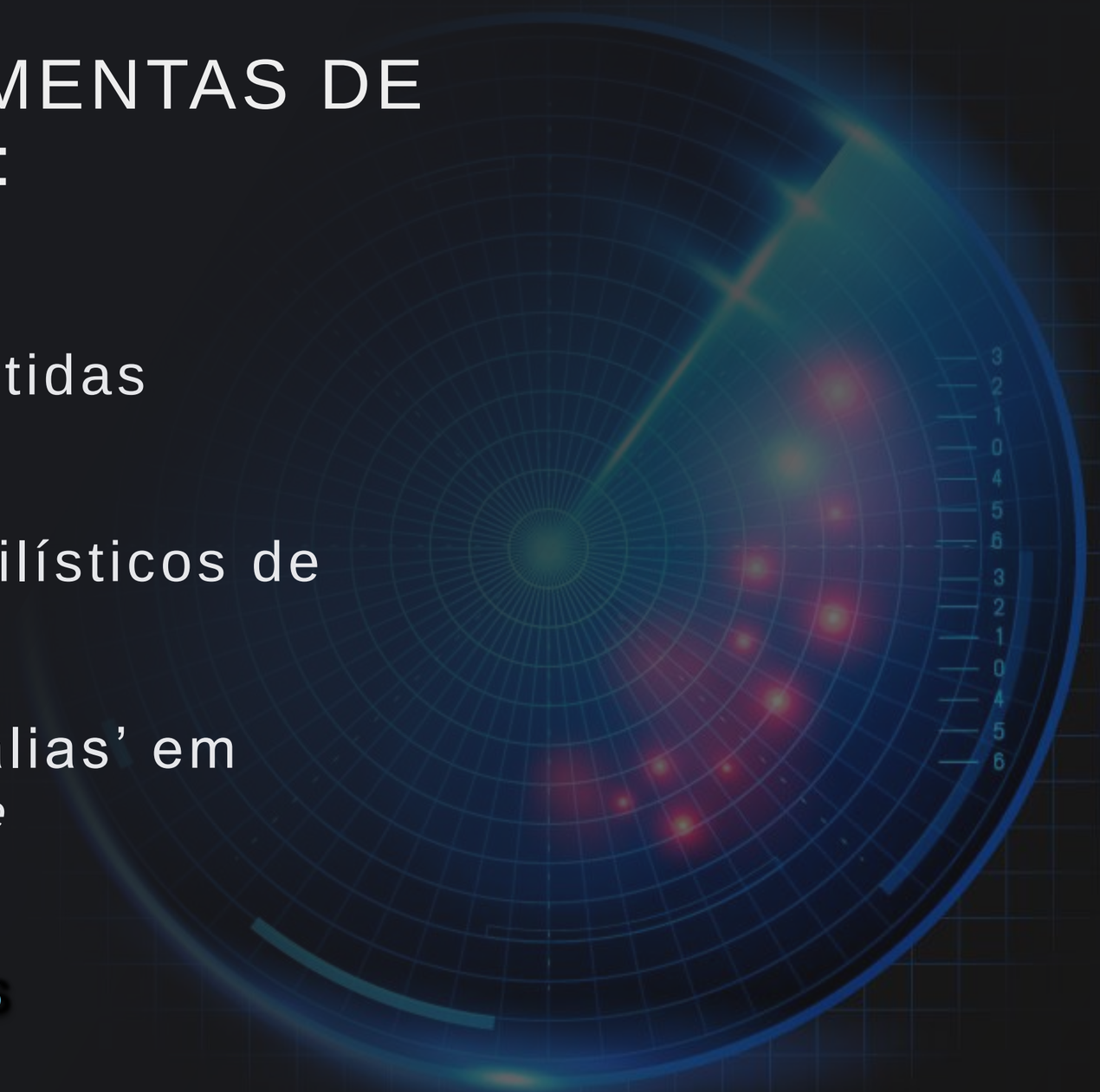
A MAIORIA DAS FERRAMENTAS DE FRAUDE NÃO É EFICAZ:

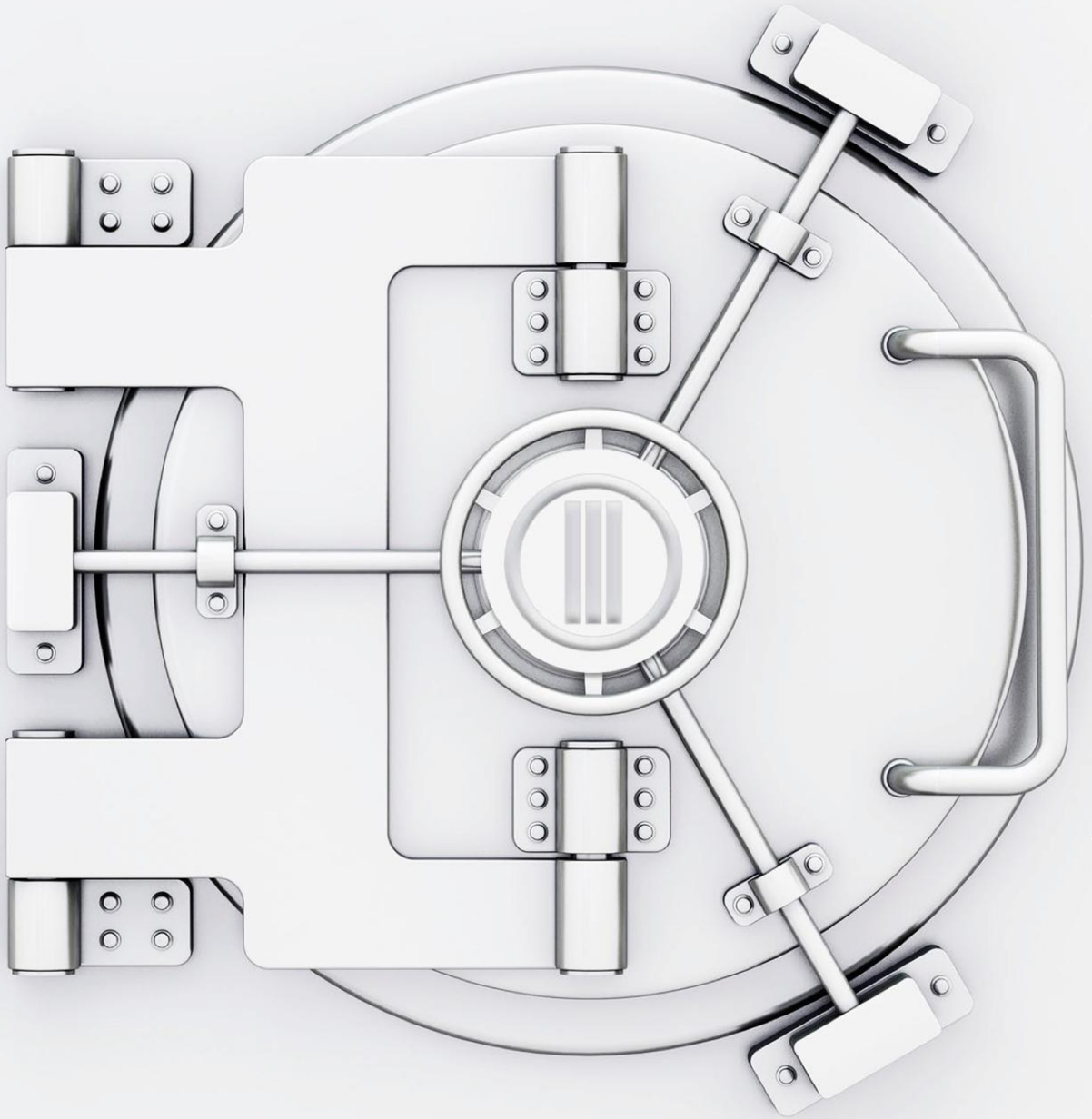
Facilmente detectadas e revertidas pelos fraudadores.

Baseadas em métodos probabilísticos de detecção

Baseadas na busca de ‘anomalias’ em dados passados *(Post Exposure Analysis).*

E NÃO COMBATEM OS BOTS MAIS SOFISTICADOS E LUCRATIVOS.





A melhor proteção se inicia com a detecção mais imediata.

A IMPORTÂNCIA DE INTERCEPTAR A “JANELA DE OPORTUNIDADE”

80% DAS OCORRÊNCIAS DE FRAUDE OCORREM COM USUÁRIOS RECÉM INFECTADOS

Máquina Afetada #1

PONTO DE INFECÇÃO | X | PONTO DE DETECÇÃO

TEMPO MAIOR

Máquina Afetada #2

PONTO DE INFECÇÃO | X | PONTO DE DETECÇÃO

TEMPO MAIOR

Máquina Afetada #3

PONTO DE INFECÇÃO | PONTO DE DETECÇÃO COM **WHITE OPS**

MENOS TEMPO

O QUE FAZ A *WHITE OPS* ?

ACREDITAMOS QUE DETECTAR E COMBATER O CRIME CIBERNÉTICO REQUEIRA *EXPERTISE* E FOCO EM SEGURANÇA VIRTUAL

Apuração determinística, fundamentada em ‘evidências’

Abordagem em tempo real e em todas etapas do ecossistema

Diferenciação entre tráfego humano e *bot*, do mesmo computador, ao mesmo tempo

Relatórios contínuos e detalhados de impressões

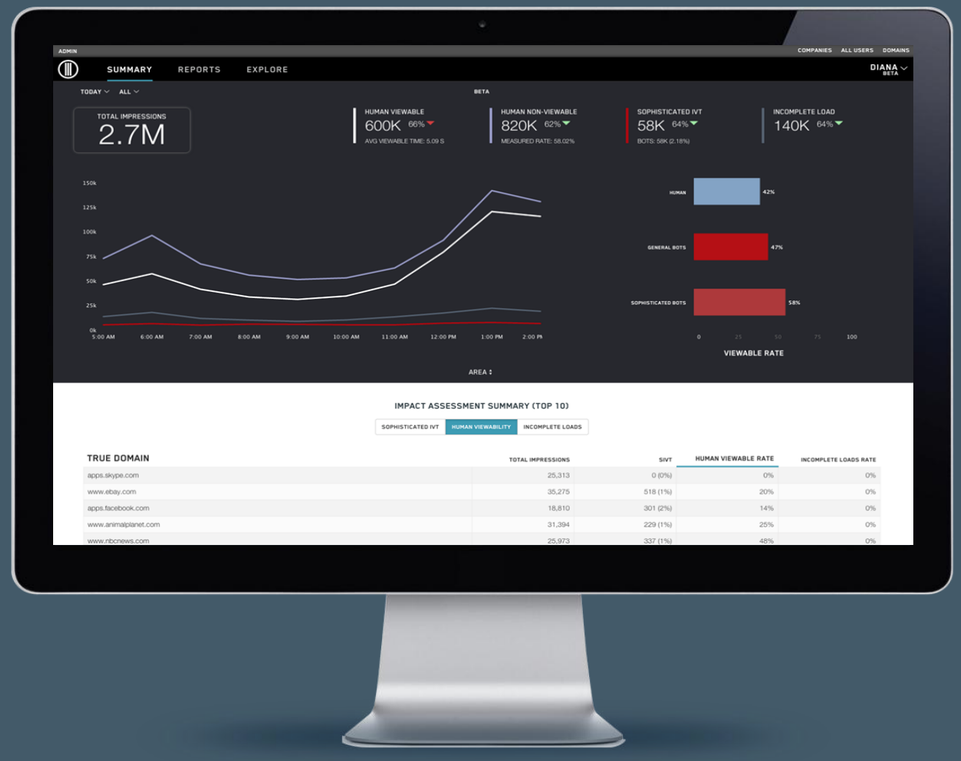
FRAUDSENSOR: O SISTEMA DE DETECÇÃO *WHITE OPS*

A PRIMEIRA PLATAFORMA CERTIFICADA PELO MRC PARA COMBATER O PADRÃO SIVT DE FRAUDES

“White Ops *SIVT Detection* inclui procedimentos mais complexos de detecção, compreendendo analítica avançada, coordenação multiponto e significativa intervenção.”

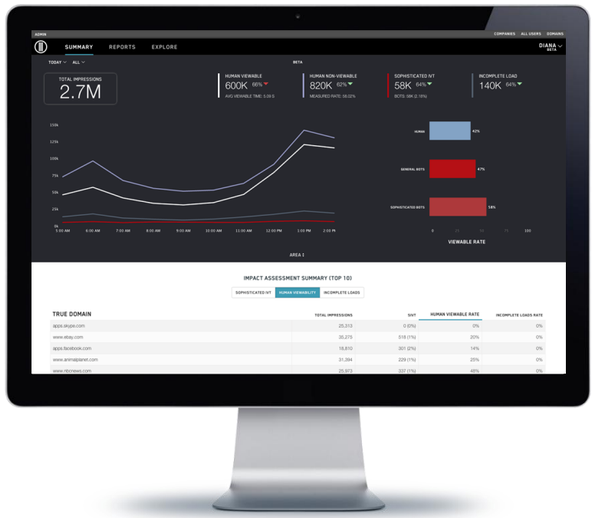
MRC

SIVT = detecção ao nível de impressão, em *desktop*, vídeo e *mobile*.



FRAUDSENSOR

BLOQUEIA A FRAUDE COM UMA SOLUÇÃO DE ALTÍSSIMA ASSERTIVIDADE: ~99%



BLACKLIST

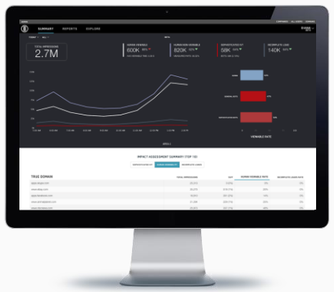
PLATAFORMA
DSP

- Bloqueio por Lista Negra Dinâmica
- Bloqueio Dinâmico de *Streaming*
- MediaGuard: varredura de ~95% das impressões, com *bot precision* de ~99%

DETECÇÃO REALIZADA DE PONTA A PONTA

ANALISA POTENCIAL FRAUDES EM COMPRAS DE MÍDIA, EM TRÁFEGO DE SITES E EM COOKIES.

Compras de Mídia



Toma Ação

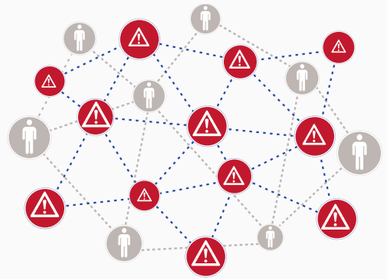
Analisa as impressões em tempo real e reage quando a fraude ocorre.

Tráfego do Site

Verifica

Analisa a validade do tráfego e certifica que os dados (*site analytics*) estão corretos

Cookie Pools

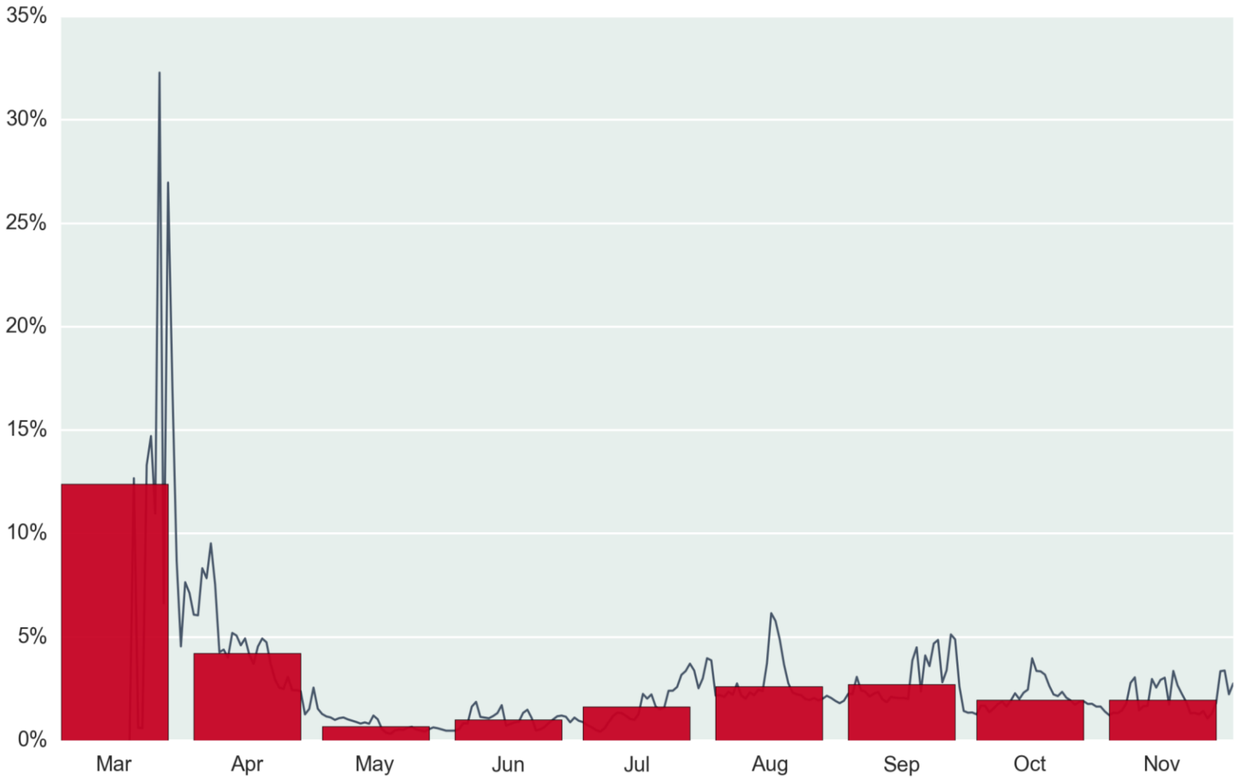


Limpa

Garante a validade de cookies de *retargeting*, removendo potenciais cookies inseridos por *bots*

UM EXEMPLO: A REDUÇÃO DE FRAUDES ROBÓTICAS PARA UM GRANDE ANUNCIANTE.

White Ops diminuiu com sucesso, os níveis de fraude deste grande anunciante com uma média de 2 bilhões de Impressões mensais.



DE 1º TRI (Média) **12%** **para** **2%** **4º TRI**

Ações tomadas:

- **Listas Negras semanais de *Publishers***.
- **Envolvimento dos *Ad Servers*** na implementação dos *tags* da *White Ops*
- TOMORRO\\\ orientando os responsáveis por operação, nas diversas agências de propaganda.

COMBATER A FRAUDE ROBÓTICA PODE AUMENTAR DRASTICAMENTE A EFICIÊNCIA DO SEU INVESTIMENTO EM MARKETING DIGITAL

+2~10x ROI

E VOCÊ, COMO VAI COMBATER ?

TOMORRO\\\

TOMORRO\\\ International
32 Union Square East, 4th floor,
New York NY 10003 USA

TOMORRO\\\ Brasil
Av. Eng. Luis Carlos Berrini, 1700
São Paulo – SP 04571-935 Brazil

Luiz J. Kroeff
Business Development – Americas
+55 11 97644.4604
lk@tomorrollc.com

Michel Namora
Country Manager – Brasil
+55 11 94470.0550
michel@tomorrollc.com

www.tomorrollc.com