Vigilância e ameaças no mundo digital

Rodolfo Avelino

9ª SeTEC **ADS – Fatec Presidente Prudente – nov/2017**

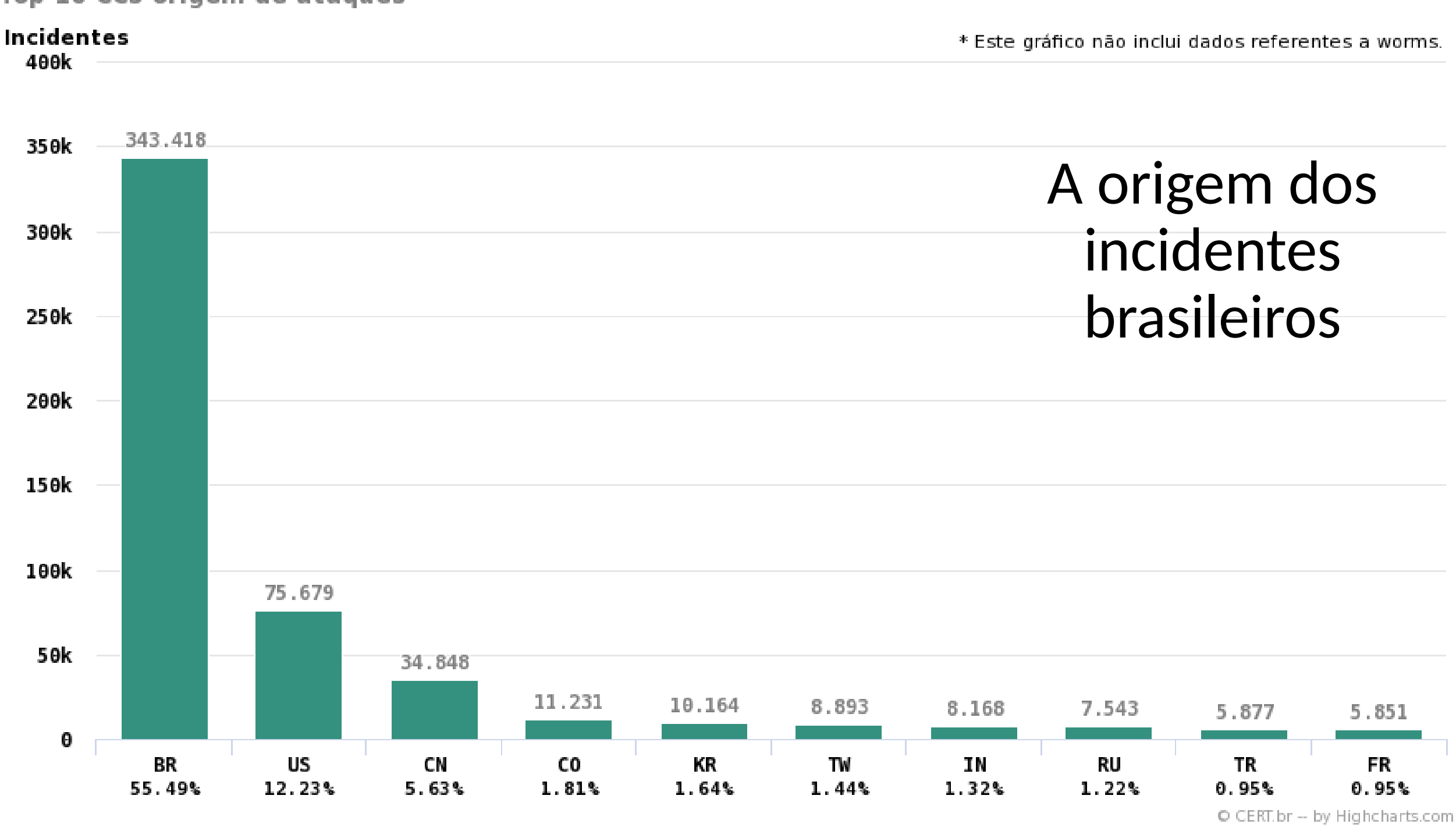
About me

- Especialista em Segurança da Informação.
- Coordenador de curso de graduação e pós graduação.
- Diretor das ONGs Actantes e Coletivo Digital.
- Ativista e entusiasta em sistemas Open Source.
- Diretor empresa MakroTrust

Formação

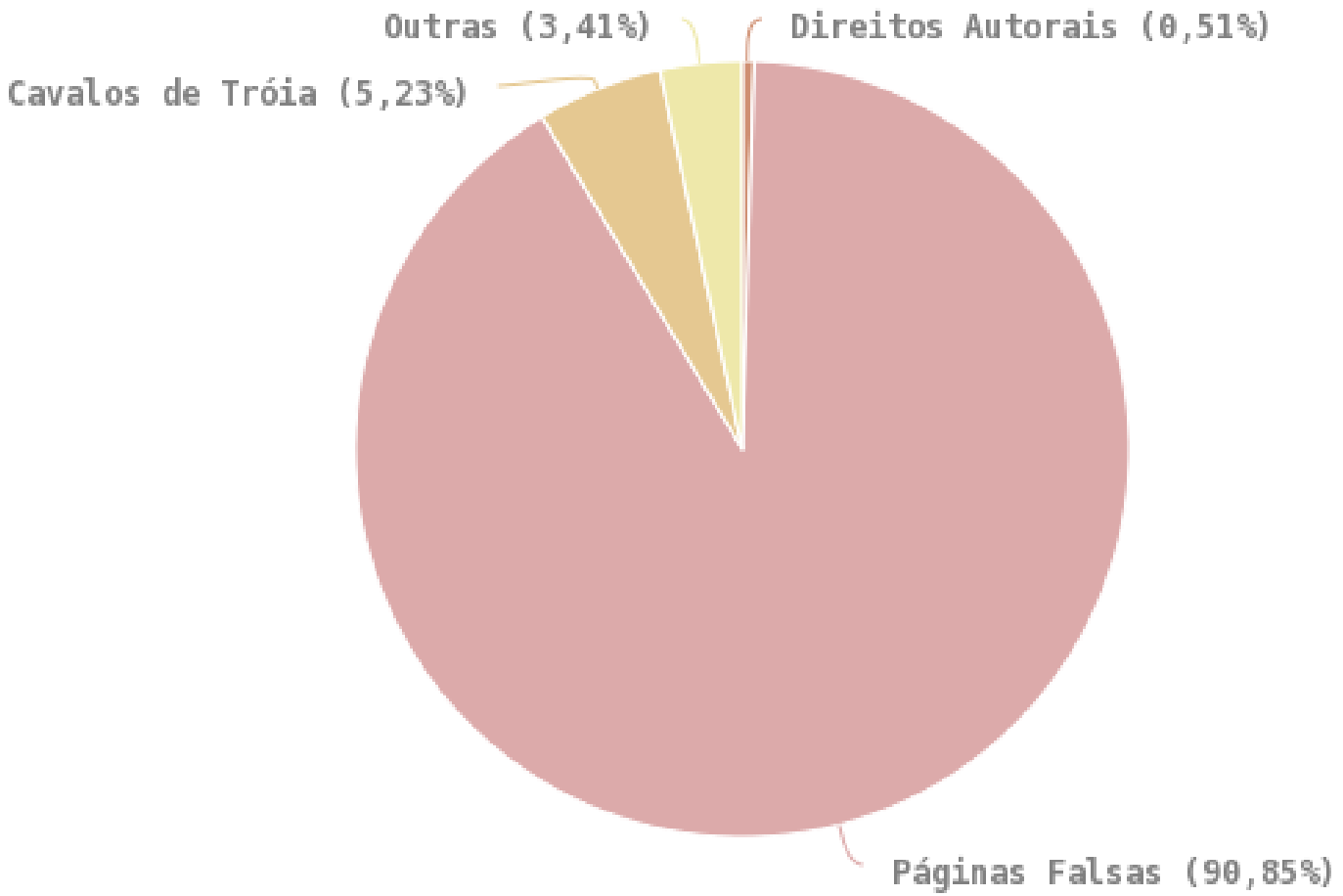
- Doutorando Programa PCHS da UFABC
- Mestre em TV Digital UNESP
- Design Instrucional para EAD Virtual – Federal de Itajubá
- MBA Gestão e Tecnologia em Seg da Informação – FIT
- Bacharelado em Sistemas de Informação – CUFSA.

Tendências e desafios atuais na Segurança da Informação


Top 10 dos origem de ataques
Incidentes
* Este gráfico não inclui dados referentes a worms.
400k
350k
300k
250k
200k
150k
100k
50k
0
343.418
75.679
34.848
11.231
10.164
8.893
8.168
7.543
5.877
5.851
BR
55.49%
US
12.23%
CN
5.63%
CO
1.81%
KR
1.64%
TW
1.44%
IN
1.32%
RU
1.22%
TR
0.95%
FR
0.95%
A origem dos incidentes brasileiros
© CERT.br – by Highcharts.com

Incidentes Reportados ao CERT.br -- Janeiro a Dezembro de 2016

Tentativas de fraudes



YOUR COMPUTER HAS BEEN LOCKED!

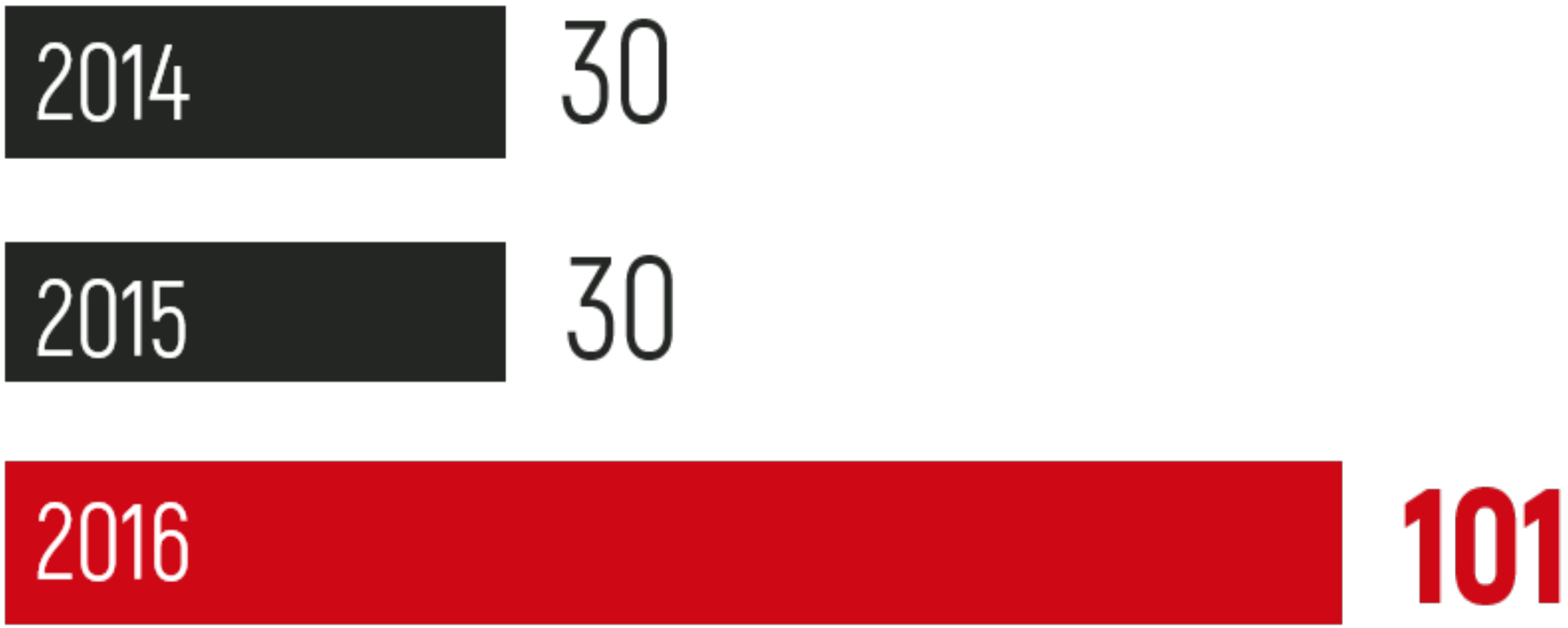
This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)
Following violations were detected:
Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.
This computer lock is aimed to stop your illegal activity.

To unlock the computer you are obliged to pay a fine of $200.

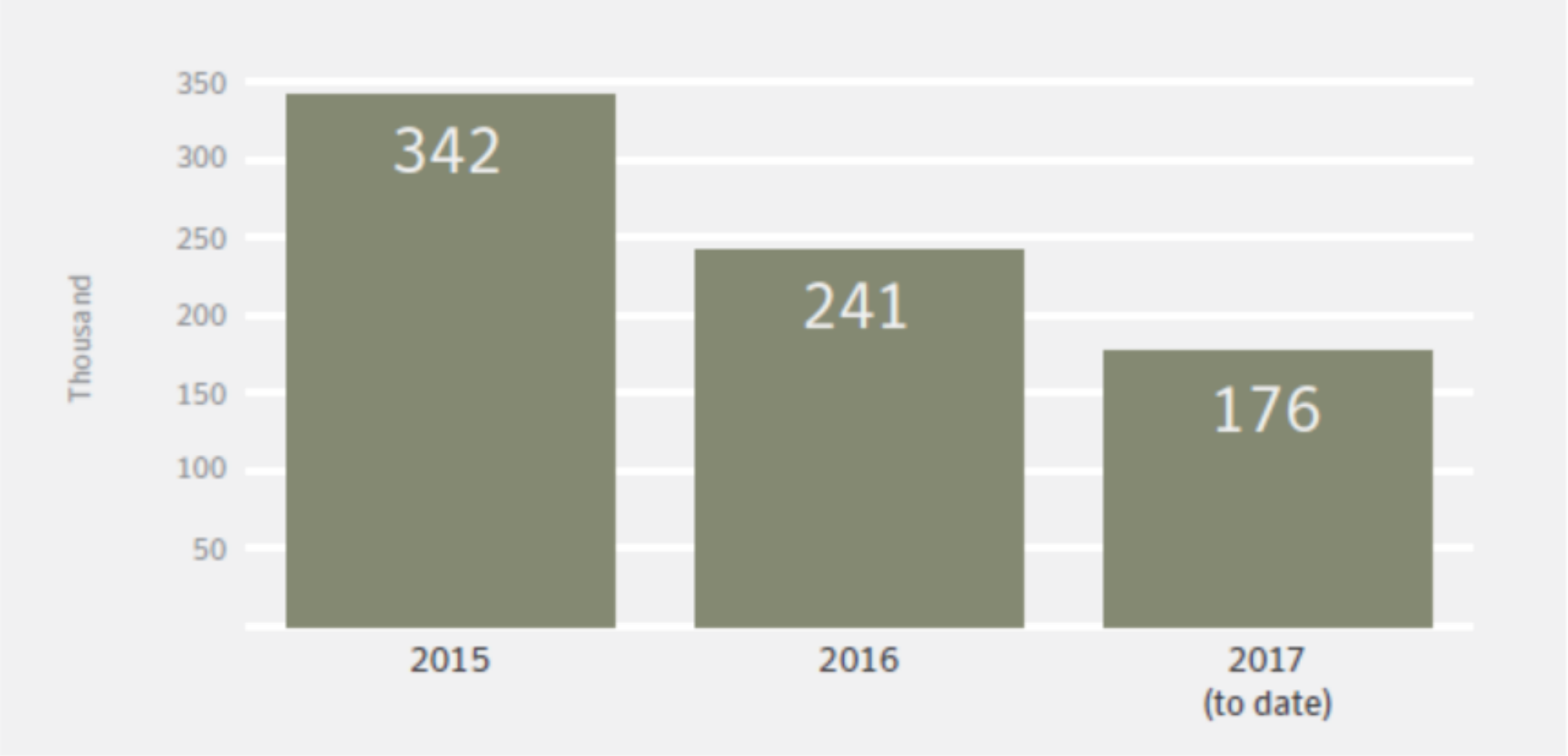
No caso do Brasil, um estudo da Kaspersky Lab (2017) revelou que o país é o mais afetado por ataques de ransomware na América Latina.

Apenas 34% das empresas brasileiras reconhecem a seriedade da ameaça, o que afeta gravemente a capacidade de prevenir e responder a esse tipo de malware.

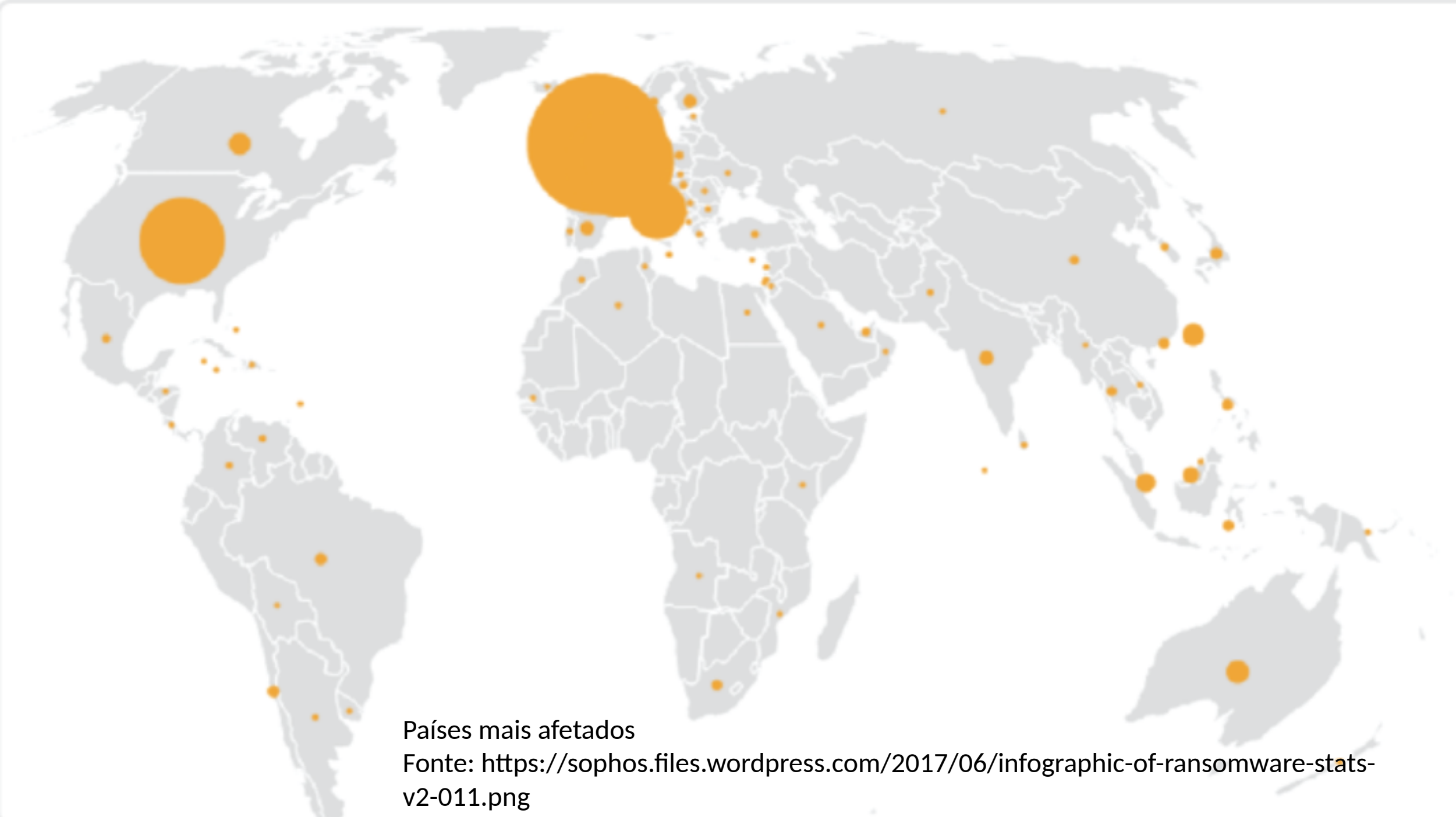
NOVAS FAMÍLIAS DE RANSOMWARE



Novas variantes



Fonte: Symantec jun 2017



Países mais afetados
Fonte: https://sophos.files.wordpress.com/2017/06/infographic-of-ransomware-stats-v2-011.png

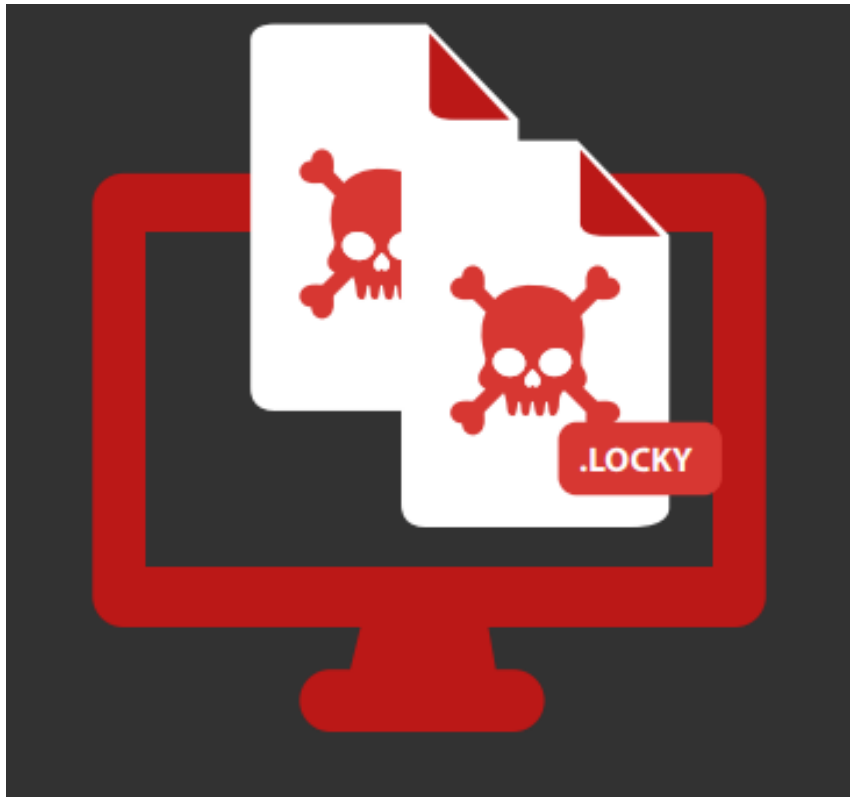
ATAQUES DE CRYPTO-RANSOMWARE

Cryptolocker

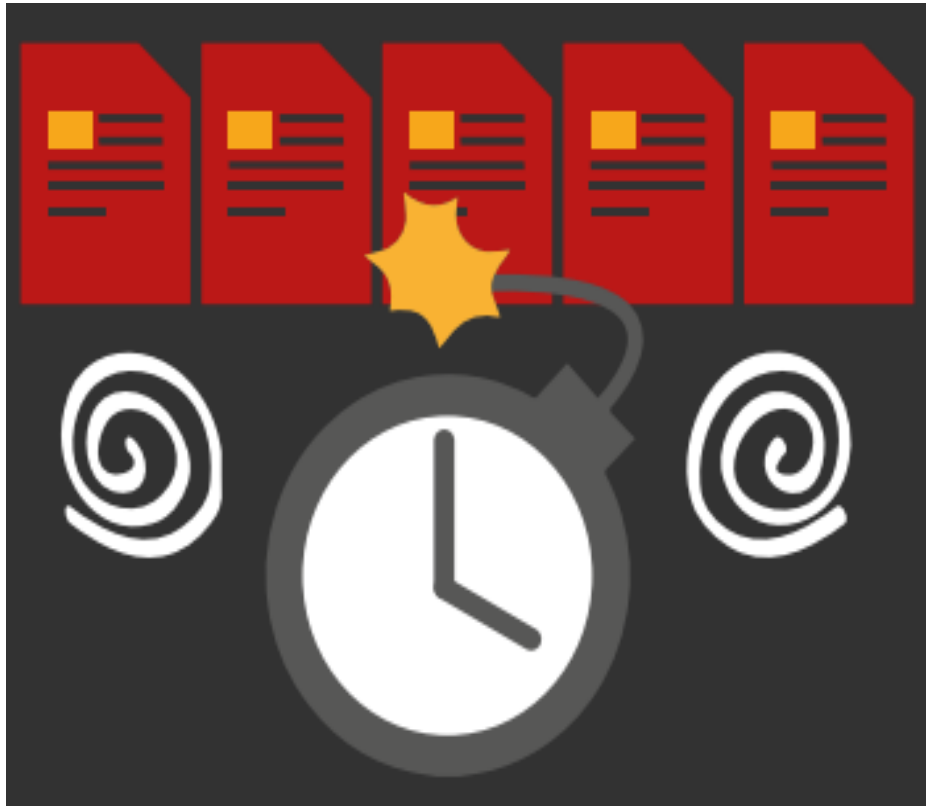
O ataque se inicia quando o usuário abre o arquivo ZIP, digitando a senha inclusa na mensagem, e tenta abrir o PDF (que na verdade é um arquivo executável).

Locky

Se espalha por meio de campanhas agressivas de spam e sites comprometidos.
Ao criptografar a máquina da vítima, o malware criptografa arquivos, adiciona a eles a extensão .locky



Jigsaw

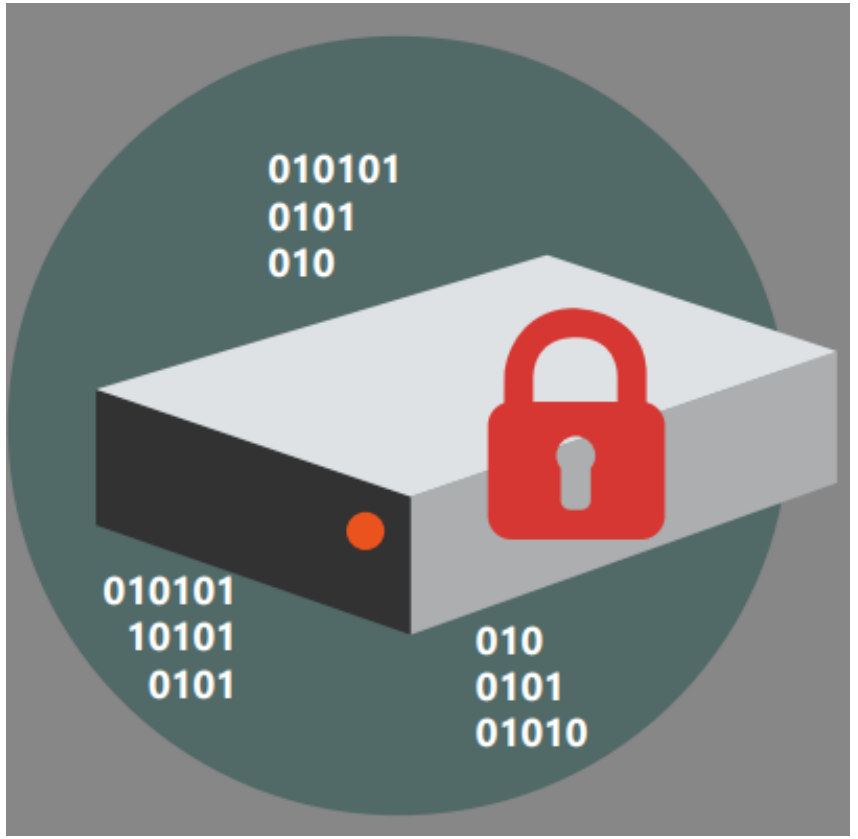


Vai deletando os arquivos da vítima de hora em hora para que ela pague o resgate o mais rápido possível.
A cada hora o ransomware reinicia a contagem e deleta milhares de arquivos de uma só vez, tornando-o um dos malwares de criptografia mais destrutivos do cenário atual.

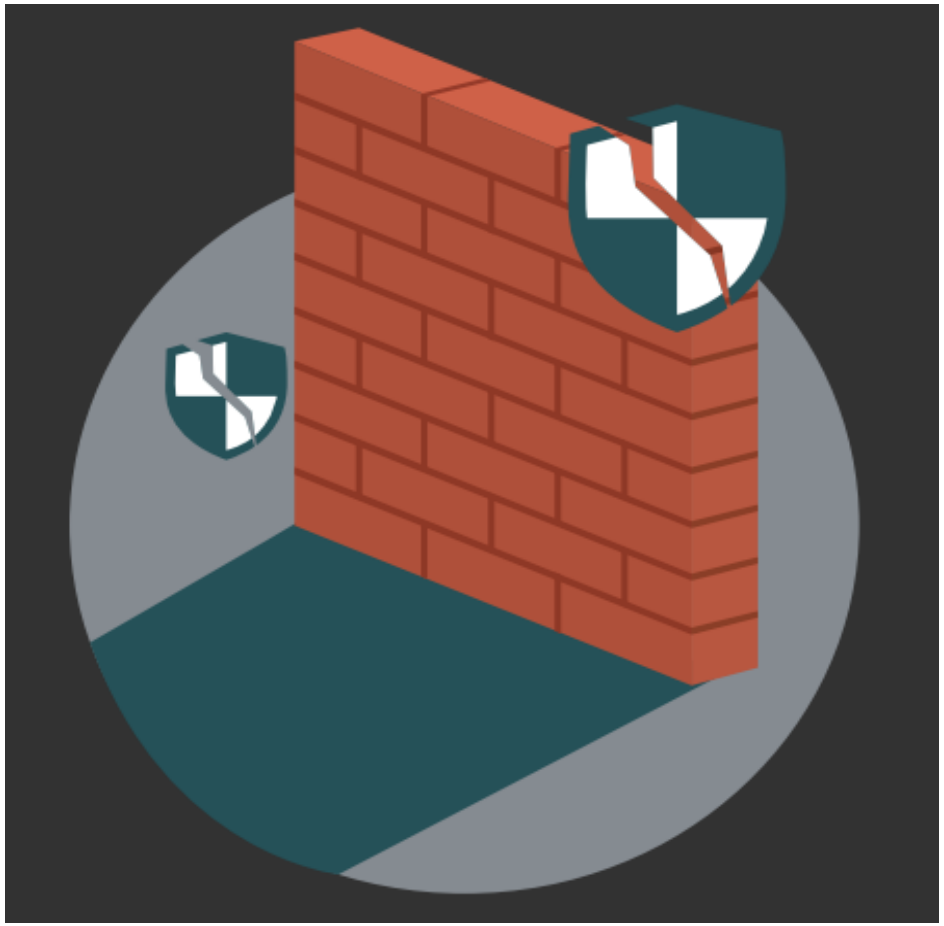
Petya

Capaz de criptografar o HD inteiro, o Petya se espalha via e-mails direcionados a profissionais de RH.

Os e-mails vêm com um link Dropbox que contém um arquivo ZIP malicioso que é, supostamente, um portfólio de um candidato a emprego.



CryptoWall



Um dos mais antigos em atuação, é distribuído por meio de kits de exploração, campanhas de spam e técnicas de malvertising.

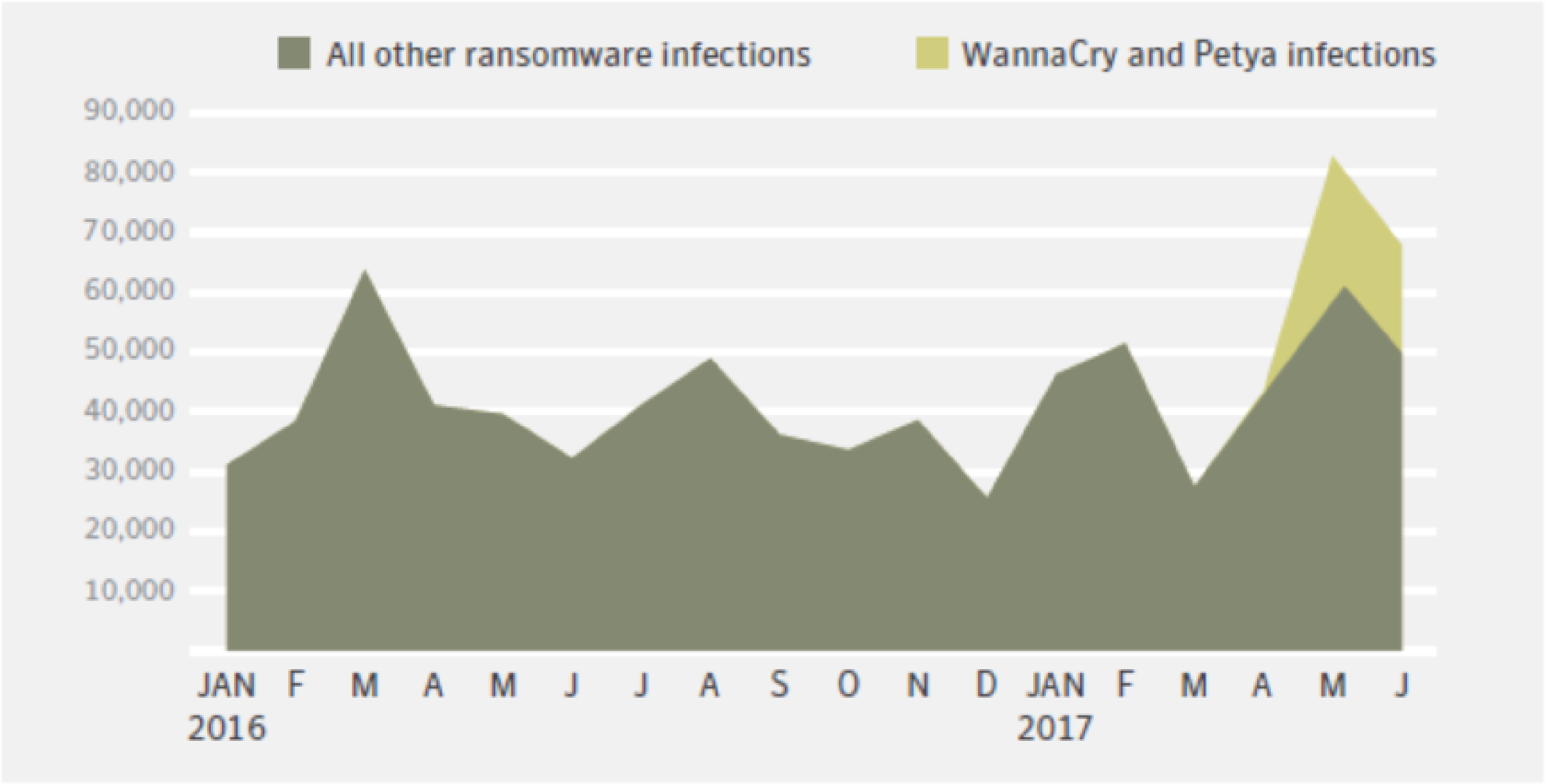
Quando está na máquina, um código binário é comprimido ou codificado com uma série de instruções que dão a ele a capacidade de burlar o antivírus.

Wannacry

Utiliza exploits do Windows Server 2003, se infiltrando pelo código remoto em execução SMBv2 do sistema operacional.

NotPetya

Muito similar ao WannaCry, contudo ele bloqueia o acesso ao computador e não apenas aos arquivos como os anteriores.



Fonte: Symantec

Tendências e desafios

- *Os ataques DDoS IOT*
- *Mudança de ataques exploit para ataques sociais direcionados*

- ***Infraestrutura financeira com maior risco de ataque -*** phishing direcionado ou whaling (caça à baleia) continua a crescer. Esses ataques usam informação detalhada de executivos das empresas com o objetivo de enganar funcionários para comprometer contas e viabilizar o pagamento aos fraudadores.

Notícias

Ataques de DDoS chegaram a 800 Gbps impulsionados por dispositivos de IoT

segundo o 12o Relatório Anual sobre Segurança da Infraestrutura Global de Redes da Arbor Networks

Da Redação
Publicada em 15 de fevereiro de 2017 às 08h45

// Overview / Mercado

DDoS e ataques direcionados serão tendência em 2017

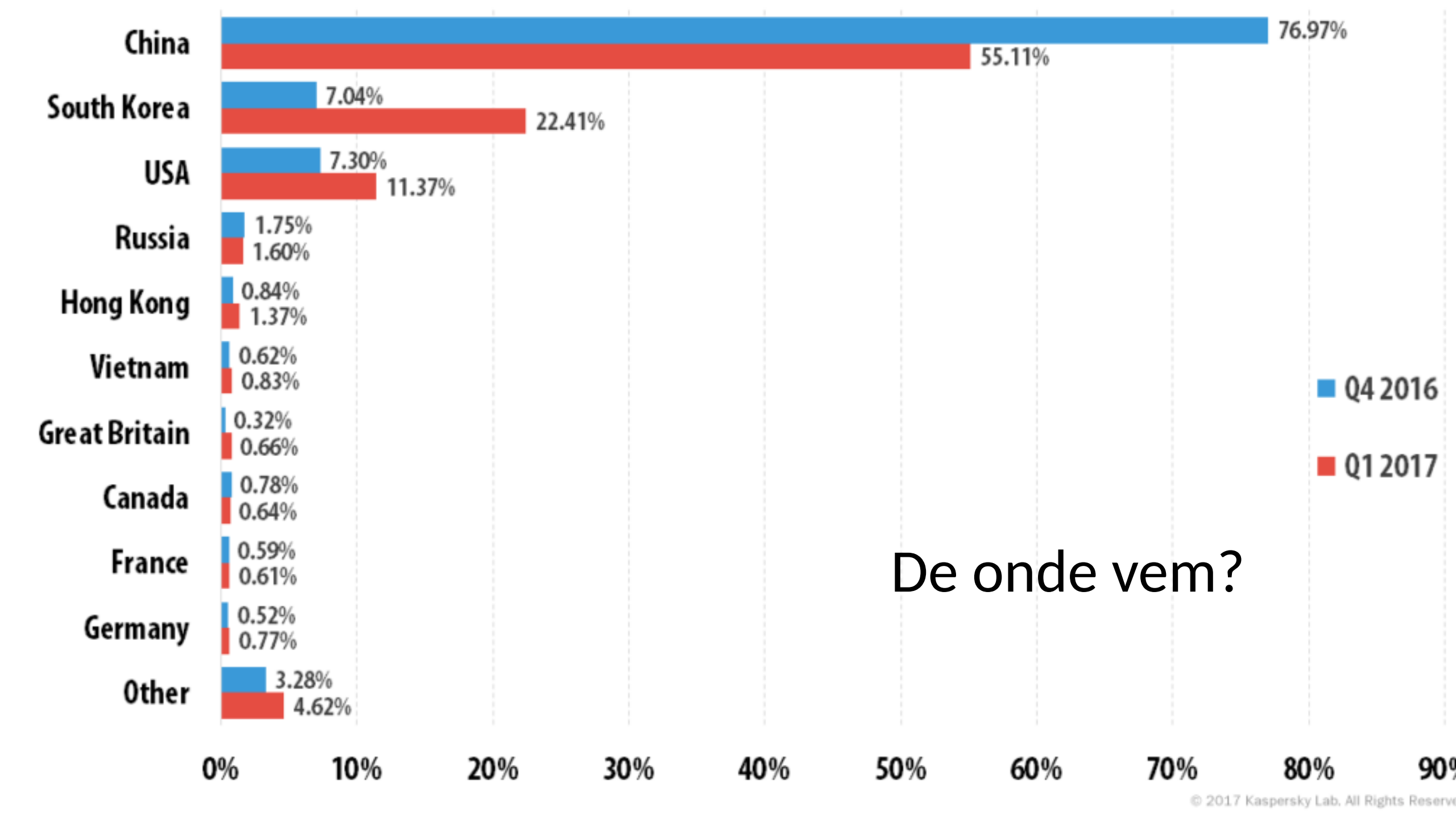
Segundo levantamento da Sophos, uso de IoT e ataques contra órgãos do Estado e serviços estarão na mira dos cibercriminosos

tele.síntese
Portal de Telecomunicações, Internet e TICs

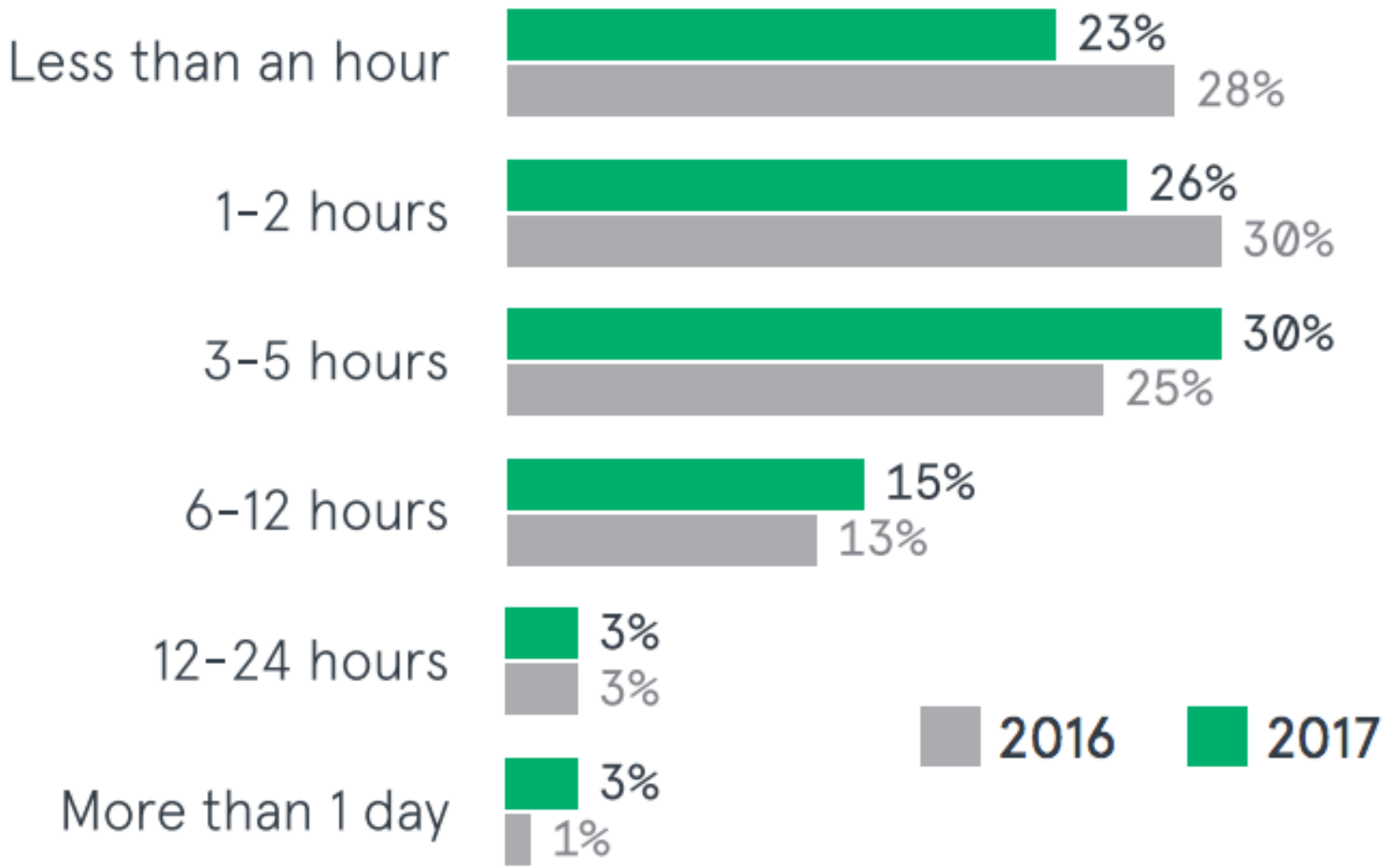
INTERNET

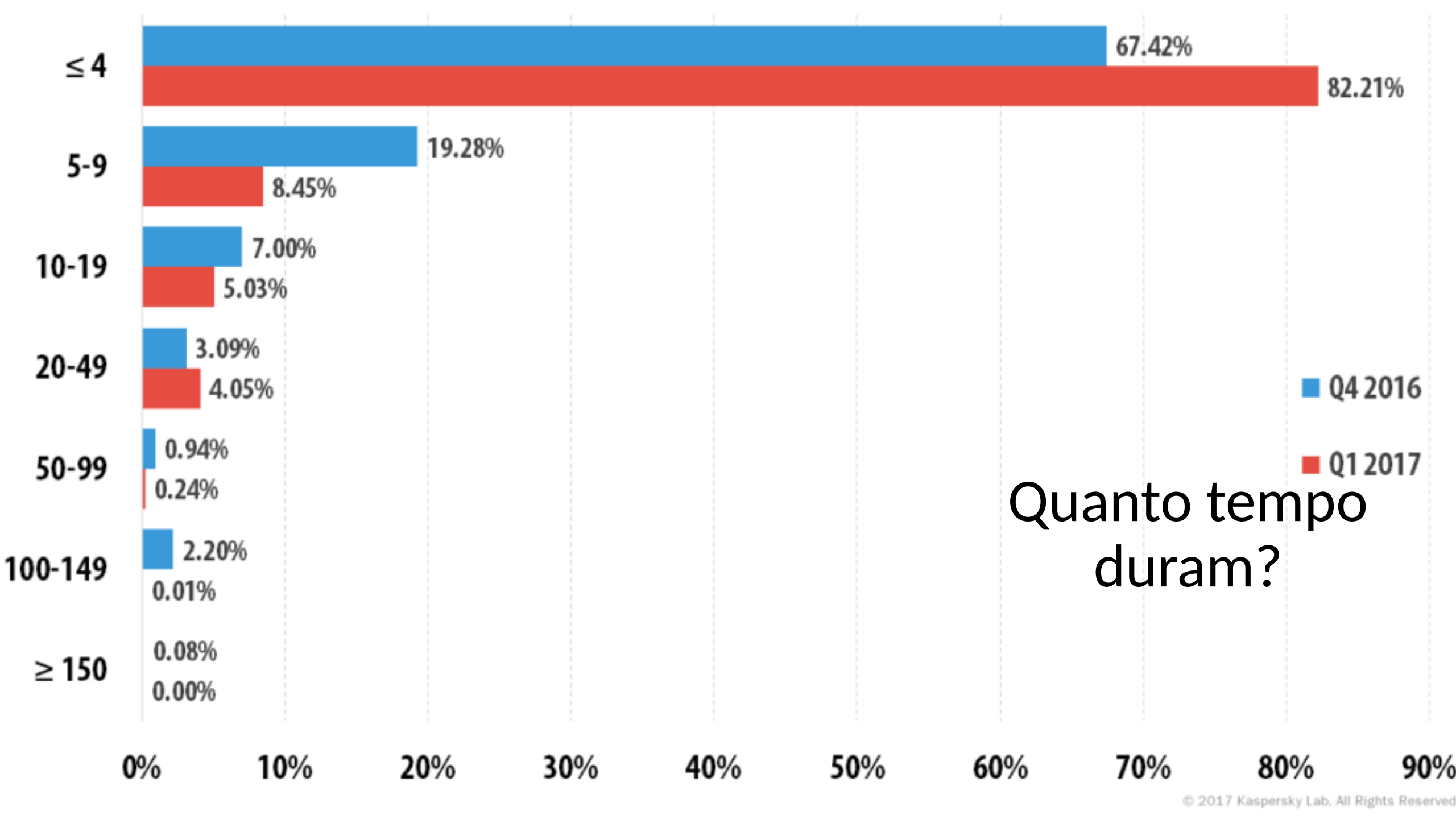
NÚMERO DE ATAQUES DDOS DISPARA NO BRASIL

Houve alta de 138% nas notificações de DDoS registradas pelo CERT.br. A raiz do aumento é a vulnerabilidade de equipamentos de internet das coisas.



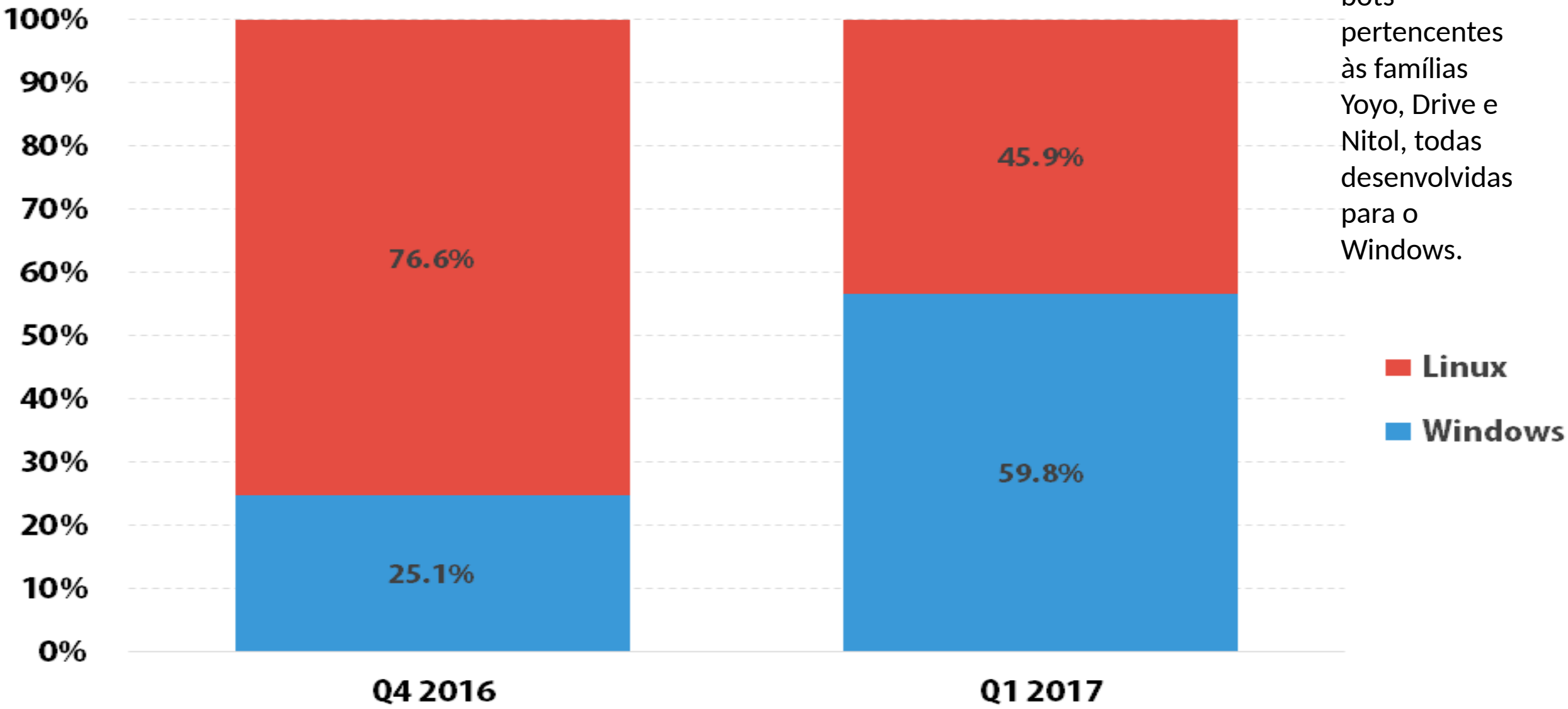
HOW LONG IT TOOK TO DETECT DDOS ATTACK · GLOBAL





Bot por sistema operacional

2017 atividade crescente por bots pertencentes às famílias Yoyo, Drive e Nitol, todas desenvolvidas para o Windows.



Tipos de Malwares e ameaças no Brasil

E o problema dos navegadores web

Droppers

é um programa que foi concebido para "instalar" algum tipo de malwares (vírus, backdoor,...) em um sistema (destino).
Existem dois tipos principais de Droppers:
- aqueles que não requerem interação do usuário e são executados por meio da exploração de um sistema através de vulnerabilidades;
- e aqueles que exigem interação do usuário convencendo-o de que é algum programa idôneo.

Droppers

Os Droppers que instalam um malware em memória são chamados de um injector.

Alguns tipos de Malwares
extensão navegador

- Não necessariamente ele será um processo;
- É altamente intrusivo e, por vezes, difícil de remover, é um dos tipo mais utilizados por fraudadores brasileiros;
- Alguns estão interessados no comportamento de navegação online da vitima. Outros, podem levá-lo a sites maliciosos;
- Só é executado quando o navegador está em execução.

How Dyre Works

Infection

The victim's machine is infected with the Trojan via SPAM

The malware uses browser hooks to forward all login attempts to a dropzone before they are encrypted with SSL.

Interception

Login requests are intercepted. Malicious content is returned to the victim.

Injection

The victim shares additional sensitive information by interacting with malicious content.

The attacker uses or sells the stolen information and/or can take control of the victim's machine

VNC Module

Fraud

Data Theft

DDoS

Extensão navegador
Sinais de infecção

- **Possíveis sintomas de um navegador infectado:**
- Página inicial alterada (e difícil de ser alterada);
- Ter que preencher formulários on-line pelo menos duas vezes;
- Navegação extraordinariamente lenta;
- *Popups* Comerciais aparecendo o tempo todo, mesmo quando você está visitando sites que não servem *popups*.

Ameaças para Mobile
Trojan-Ransom.AndroidOS.Egat

bloqueio de dispositivo, sobrepõe todas as janelas abertas com sua própria janela e, em seguida, exige dinheiro para desbloquear o dispositivo.

Tendências para os próximos anos..

- Até 2020, 60% das empresas digitas sofrerão falhas em seus principais serviços, devido à incapacidade das equipes de segurança de gerenciar o risco digital.
- Até 2020, 60% dos orçamentos das empresas para segurança da informação serão alocados para a detecção rápida e abordagens de resposta a ameaças, o que representa um aumento de menos de 30% em relação a 2016.
- Até 2018, 25% do tráfego de dados corporativos fluirão diretamente a partir de dispositivos móveis para a nuvem, ignorando os controles de segurança da empresa.
- Em 2018, mais 50% dos fabricantes de dispositivos móveis não serão capazes de conter as ameaças devido a autenticação fraca.

Tendências para os próximos anos..

- Uma "corrida armamentista" na esfera do aprendizado de máquina se travará entre defensores e atacantes.
- O ransomware passará por uma transição da extorsão convencional para novos alvos, tecnologias e objetivos.
- Prestadores de serviços e fabricantes de dispositivos domésticos conectados tentarão solucionar as baixas margens de lucro através da coleta de mais dados pessoais dos usuários — com ou sem o seu consentimento — transformando a casa das pessoas em uma vitrine corporativa.

Fonte: 5 tendências de cibersegurança para 2018, segundo a McAfee

Vigilância x Privacidade

A Tecnologia está presente...no cotidiano


...quando estamos reunidos com amigos


... Quando nos alimentamos

...nos registros de acidentes.

...


.... nos namoros

Todos os dias mais e mais pessoas utilizam a Internet...

JUN 2017

GLOBAL DIGITAL SNAPSHOT

THE LATEST NUMBERS FOR INTERNET, SOCIAL MEDIA, AND MOBILE USAGE AROUND THE WORLD

TOTAL POPULATION	INTERNET USERS	ACTIVE SOCIAL MEDIA USERS	UNIQUE MOBILE USERS	ACTIVE MOBILE SOCIAL USERS
				
7.511 BILLION	**3.811 BILLION**	**2.895 BILLION**	**5.007 BILLION**	**2.692 BILLION**
URBANISATION: **54%**	PENETRATION: **51%**	PENETRATION: **39%**	PENETRATION: **67%**	PENETRATION: **36%**

SOURCES: POPULATION: UNITED NATIONS; U.S. CENSUS BUREAU; WORLDOMETERS.INFO; INTERNET: INTERNETWORLDSTATS; ITU; INTERNETLIVESTATS; CIA WORLD FACTBOOK; FACEBOOK; NATIONAL REGULATORY AUTHORITIES; SOCIAL MEDIA AND MOBILE SOCIAL MEDIA: FACEBOOK; TENCENT; VKONTAKTE; LIVEINTERNET.RU; KAKAO; NAVER; NIKI AGHAEI; CAFEBAZAAR.IR; SIMILARWEB; DING; EXTRAPOLATION OF TNS DATA; MOBILE: GSMA INTELLIGENCE; EXTRAPOLATION OF EMARKETER AND ERICSSON DATA.

O que as pessoas acessam na Internet?

1. GOOGLE.COM
2. YOUTUBE.COM
3. FACEBOOK.COM
4. BAIDU.COM
5. WIKIPEDIA
6. YAHOO.COM
7. GOOGLE.CO.IN
8. REDDIT.COM
9. Qq.COM
10. TABAO.COM

Contextualização

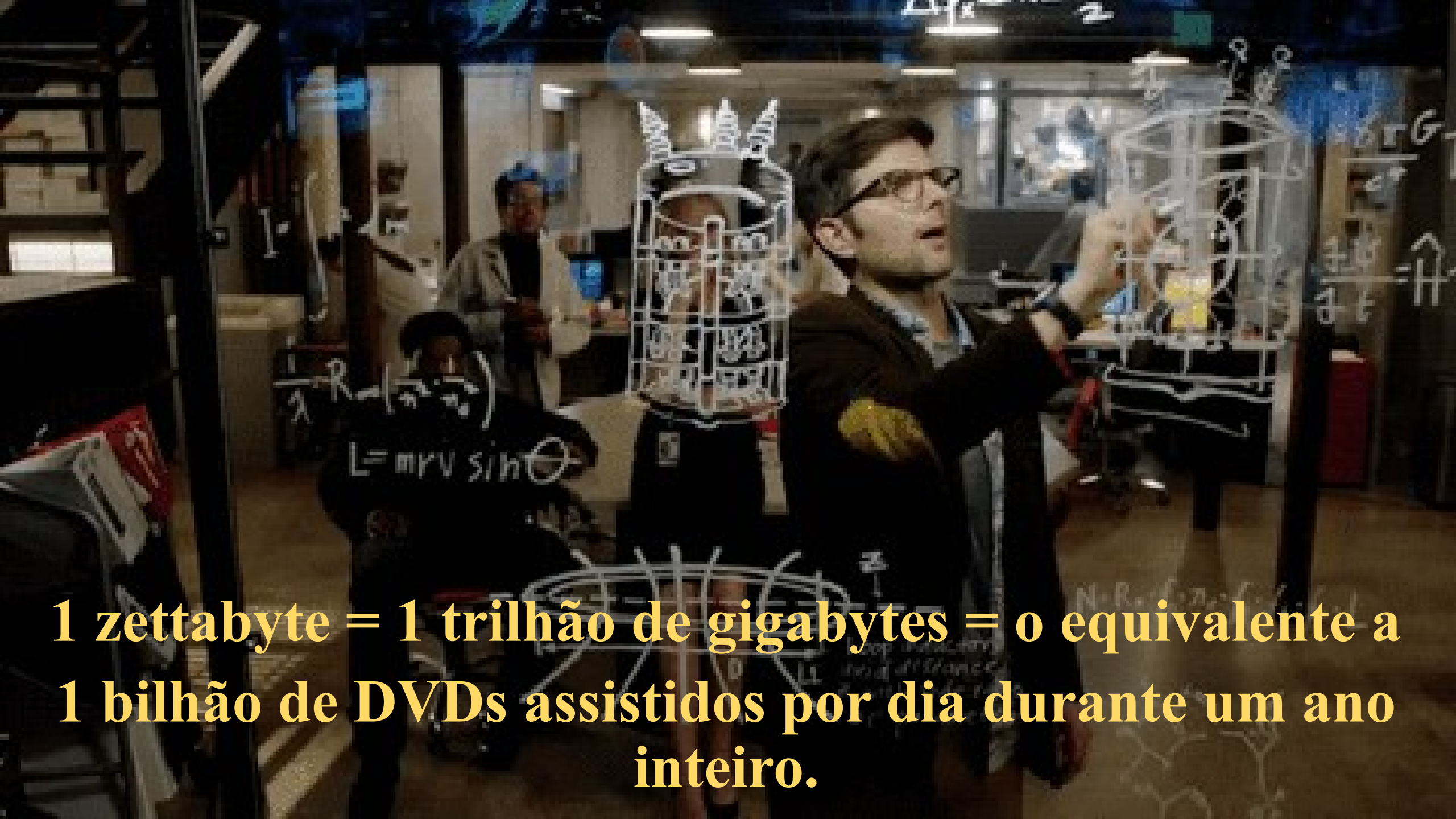
A partir da convergência da informática com as telecomunicações, a Internet se tornou um grande instrumento de possibilidades de monitoramento, coleta e classificação de dados pessoais por meio de algoritmos.

Contextualização

A crescente quantidade de dados pessoais cotidianamente produzido, possibilitou a criação de uma infraestrutura invisível formada por empresas de análise de audiência, agência de marketing especializada em mídia eletrônica, publicidade online direcionada, entre outras atividades de análise de dados.

Ultrapassamos
1 zettabyte/ano
pelas redes digitais

Quanto criamos de dados?



1 zettabyte = 1 trilhão de gigabytes = o equivalente a 1 bilhão de DVDs assistidos por dia durante um ano inteiro.

O cenário

a **falta de transparência técnica** em uma simples navegação em um site, permite ao usuário ter **a sensação de segurança** do acesso e assim **disponibilizar e fornecer informações pessoais** como endereço, fotos familiares, número de documentos ou telefone em formulários e em redes sociais.

Naturalmente a evolução das ferramentas de rastreamento e vigilância aconteceram, e puderam criar mecanismos para personalizar suas bases, sobretudo, buscando entender a experiência de navegação e os interesses de acesso do usuário, possibilitando assim o aprimoramento das técnicas de controle de navegação.

O que acontece com o grande volume dados que alimentamos diariamente na Internet?

Permitiu a criação de empresas de Tecnologia que buscam **formar nosso perfil**, ou seja, **reunir informações sobre nosso comportamento**, nossas **preferências** e nossas **escolhas** na rede.

São empresas que coletam, analisam e interpretam dados de acessos em várias fontes, sobretudo de sites “terceiros”, e representam hoje uma grande economia mundial a partir de dados pessoais.

Tecnologias de rastreamento de comportamento online

Web tracking

Evolução da experiência na Internet

A Internet sem as Redes Sociais online

- Sites estáticos e com pouca atualização;
- Usuário passivo no processo (broadcast);
- Modelo de negócio ainda não definido; (alguns sites cobravam para o acesso a notícias);
- Internet com baixas taxas de transmissão de dados;
- Computadores pessoais com baixo poder de armazenamento e processamento.

Site UOL em 30 de abril de 1998.
Fonte: Web Archive

terra

Search

Shopping | Chat | Assine | Disco Virtual | Agenda

zaz

Internet, mais sua do que nunca

terça, 22/11/2016

ASSINE TERRA

Serviços

» AGENDA
» DISCADOR TERRA
» DISCO VIRTUAL
» PERSONAL PAGES
» TERRA DIRETO
» TERRA MAIL
» TERRA PLUS

Canais

» ALMANAQUE
» ALMAS GÊMEAS
» AUTOMÓVEL
» AVENTURA
» BUSCA - METABUSCA
» CARTÕES
» CHAT
» CIDADE VIRTUAL

escolha uma

» CULINÁRIA
» DIVERSÃO & CULTURA
» ECONOMIA
» EDUCAÇÃO

EXCLUSIVO!

Veja as fotos do filho de Ronaldinho e Milene

Envie um e-mail para o bebê

NOTÍCIAS

Comissão livra Pitta de acusação

» Últimas notícias

· Acidente em rodovia de Sergipe mata nove pessoas
· Marinha dos EUA intercepta petroleiro russo
· Palmeiras perde para time boliviano por 4 a 2
· Trem descarrila e deixa mais de 20 feridos em SP
· Juventude perde no Equador pela Libertadores

À sua disposição

HOJE NA TERRA

500 ANOS
Teste seus conhecimentos no *jogo do descobrimento*

SEU TIME
Teste sua sorte apostando no resultado das rodadas do futebol

SHOPPING

INFINITY HYPERSTORE
Promoção exclusiva Terra: celular Gradiente *Chroma* por R$ 739,00

AMERICANAS.COM

Enquete

Como você prefere declarar o Imposto de Renda?

- Pela Internet
- Pelo telefone
- Por disquete
- No bom e velho formulário
- Não tenho nada a declarar

Votar

Todo o dia na Terra

Horóscopo	Cartões
Cotações	Cruzadas
Culinária	Curiosidades

Revistas

IstoÉ
Documento acusa sete vereadores de São Paulo de recebimento de propina

Dinheiro na Web
Os sete erros mais cometidos por quem

Site Terra em 7 de abril de 2000. Fonte: Web archive

Internet com as Redes Sociais online

- Avanço das linguagens de programação;
- Aumento na capacidade de processamento e armazenamento dos computadores pessoais;
- Aumento das taxas de transmissão de dados nas conexões de dados;
- Digitalização de bens culturais (e a forma de distribuição e compartilhamento).

Internet com as Redes Sociais online

- Usuário deixa de ser apenas consumidor e passa também a criar conteúdo;
- Evolução das tecnologias de armazenamento e serviços em “Nuvem”;
- Modelo de negócio baseado em dados pessoais.

- Cookies
- Web tags
- Flash cookies
- Armazenamento local
- Canvas Fingerprint
- .....

Há uma grande variedade de tecnologias para o rastreamento do comportamento online dos usuários. Contudo, este trabalho investigou a tecnologia de rastreamento baseada em web cookies inseridos na navegação dos dez sites de notícias mais acessados por usuários de Internet brasileiros em abril de 2015 e maio de 2016.

BANCO DE DADOS COMPORTAMENTAIS

- Segundo a Microsoft, dados pessoais estão se tornando rapidamente uma moeda fundamental para o relacionamento entre a marca e o consumidor.
- 80% dos consumidores estão dispostos a compartilhar informações básicas como nome, e-mail e nacionalidade com as empresas. (AIMA)
- Mais de 70% compartilham informações como data de nascimento, ocupação, hobbies e interesses. (AIMA)

Agentes de rastreamento

- **Trackers:** Empresas de análise de audiência na Internet, agência de marketing especializada em mídia eletrônica, publicidade online direcionada, entre outras atividades de análise de dados.
- **Governos / Agência de Inteligência:** Agências de Inteligência, defesa e vigilância mantidas por governos.
- **Plataformas de controle:** São grandes empresas que criam ambientes controlados e personalizados para o usuário, geralmente atuando em diversas plataformas e serviços.

Canvas Fingerprinting

instrui os navegadores a desenhar uma imagem secreta e cada computador é capaz de produzir uma imagem diferente, única, como uma impressão digital. Uma impressão digital que irá te seguir enquanto você estiver online.

Flash Cookies

Semelhantes aos cookies de navegador, são pequenos arquivos flash e podem coletar dados sobre você e sua atividade na web.

Browser Fingerprinting

Coleta informações sobre seu navegador que permitem a sites e terceiros identificá-lo. Informações como as configurações do navegador, plugins instalados, fontes instaladas e configuração IP são muitas vezes combinados para criar uma "impressão digital única".

A Electronic Frontier Foundation criou uma ferramenta para você testar e aprender sobre a singularidade do seu navegador. Confira: https://panopticlick.eff.org/

Web TAGS

```
<?xml version="1.0" encoding="UTF-8"?>
<web-app id="WebApp_ID" version="2.4" xmlns="http://java.sun.com/xml/ns/j2ee"
         xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
         xsi:schemaLocation="http://java.sun.com/xml/ns/j2ee
         http://java.sun.com/xml/ns/j2ee/web-app_2_4.xsd">

   <jsp-config>
      <taglib>
         <taglib-uri>http://mySite/myTags</taglib-uri>
         <taglib-location>/WEB-INF/mytags.tld</taglib-location>
      </taglib>
   </jsp-config>

</web-app>
```

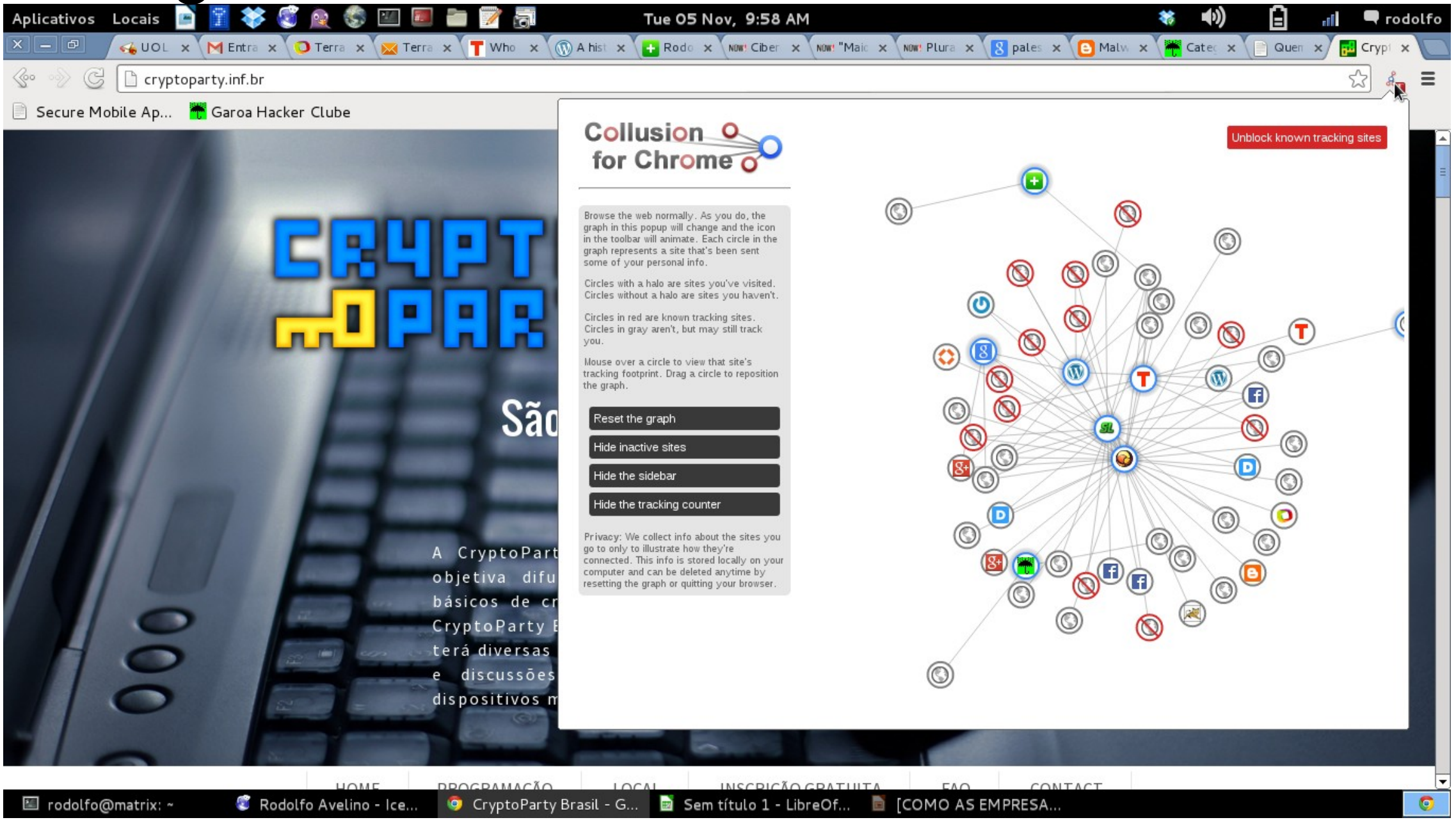
Uma web tag é um código colocado pelos parceiros em seus websites para coletar informações sobre padrões gerais de visita. As web tags são geralmente utilizadas por empresas por toda Internet para entender as visitas em seus websites.

Fonte: Score Card Research
http://www.scorecardresearch.com/About.aspx

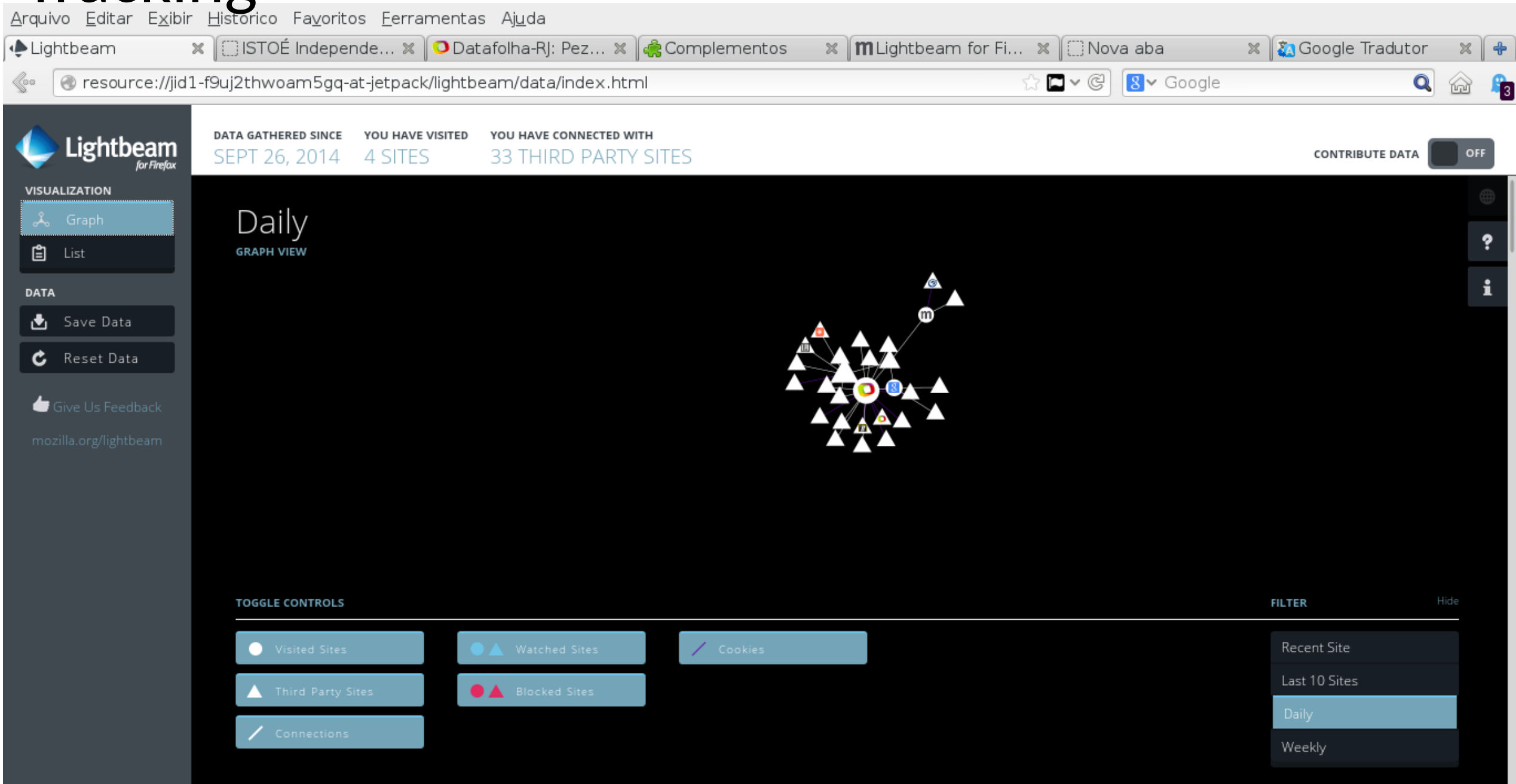
Web Beacons

É uma técnicas utilizadas para monitorar quem está lendo uma página na web ou email. Também pode ser usado para verificar se um determinado e-mail foi lido ou se uma determinada matéria foi copiada indevidamente para outro site.

Tracking


Aplicativos Locais
Tue 05 Nov, 9:58 AM
rodolfo
cryptoparty.inf.br
Secure Mobile Ap...
Garoa Hacker Clube
Collusion for Chrome
Unblock known tracking sites
Browse the web normally. As you do, the graph in this popup will change and the icon in the toolbar will animate. Each circle in the graph represents a site that's been sent some of your personal info.
Circles with a halo are sites you've visited. Circles without a halo are sites you haven't.
Circles in red are known tracking sites. Circles in gray aren't, but may still track you.
Mouse over a circle to view that site's tracking footprint. Drag a circle to reposition the graph.
Reset the graph
Hide inactive sites
Hide the sidebar
Hide the tracking counter
Privacy: We collect info about the sites you go to only to illustrate how they're connected. This info is stored locally on your computer and can be deleted anytime by resetting the graph or quitting your browser.
HOME
PROGRAMAÇÃO
LOCAL
INSCRIÇÃO GRATUITA
FAQ
CONTACT
rodolfo@matrix: ~
Rodolfo Avelino - Ice...
CryptoParty Brasil - G...
Sem título 1 - LibreOf...
[COMO AS EMPRESA...

Tracking

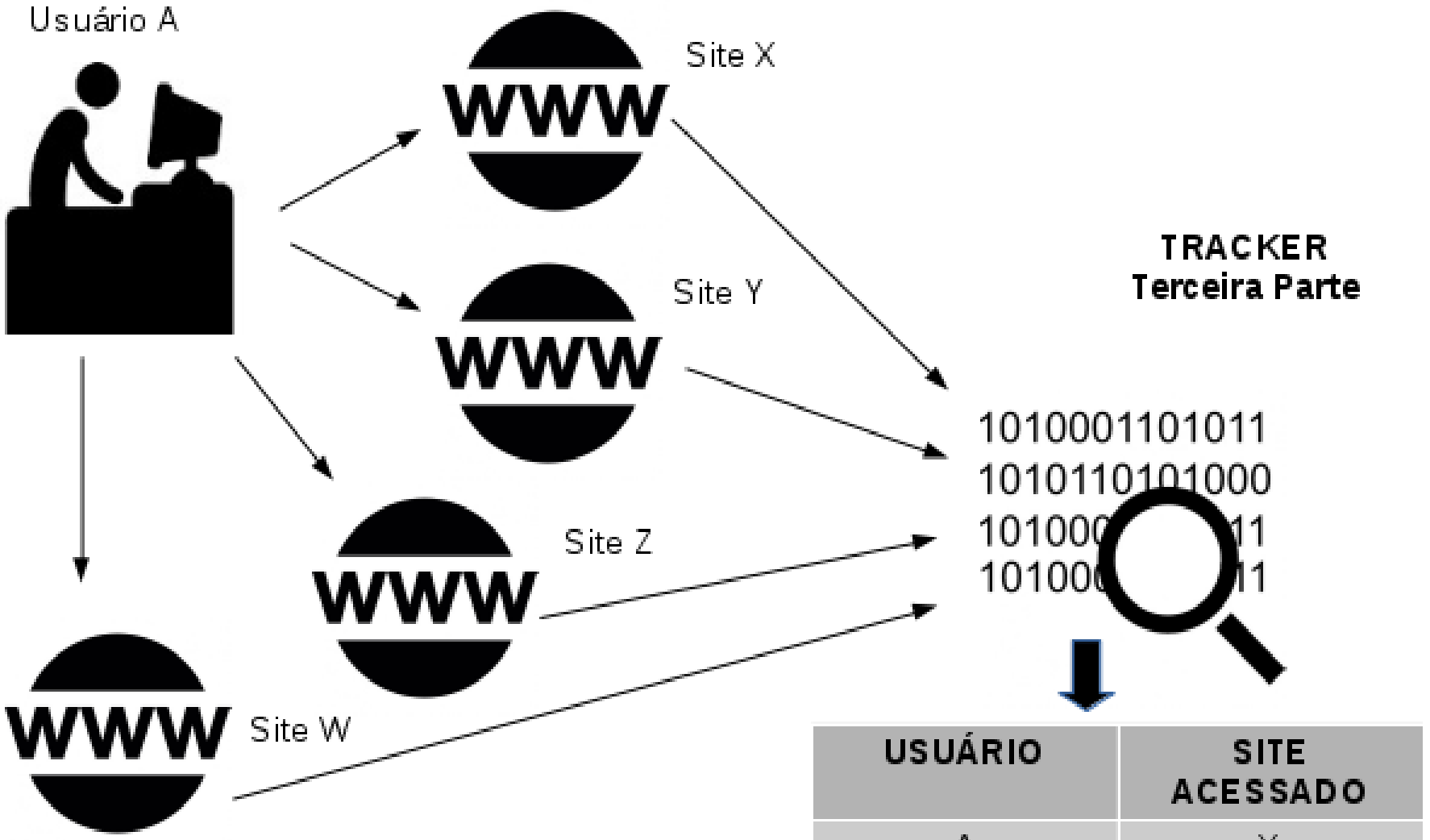

Arquivo Editar Exibir Histórico Favoritos Ferramentas Ajuda
Lightbeam
ISTOÉ Independe...
Datafolha-RJ: Pez...
Complementos
Lightbeam for Fi...
Nova aba
Google Tradutor
resource://jid1-f9uj2thwoam5gq-at-jetpack/lightbeam/data/index.html
Google
Lightbeam for Firefox
DATA GATHERED SINCE
SEPT 26, 2014
YOU HAVE VISITED
4 SITES
YOU HAVE CONNECTED WITH
33 THIRD PARTY SITES
CONTRIBUTE DATA
OFF
VISUALIZATION
Graph
List
DATA
Save Data
Reset Data
Give Us Feedback
mozilla.org/lightbeam
Daily
GRAPH VIEW
TOGGLE CONTROLS
Visited Sites
Watched Sites
Cookies
Third Party Sites
Blocked Sites
Connections
FILTER
Hide
Recent Site
Last 10 Sites
Daily
Weekly

Cookies

O principal propósito do web cookies é identificar usuários e possivelmente preparar páginas personalizadas ou para salvar as informações de sessão de um site.

Classificação Cookies

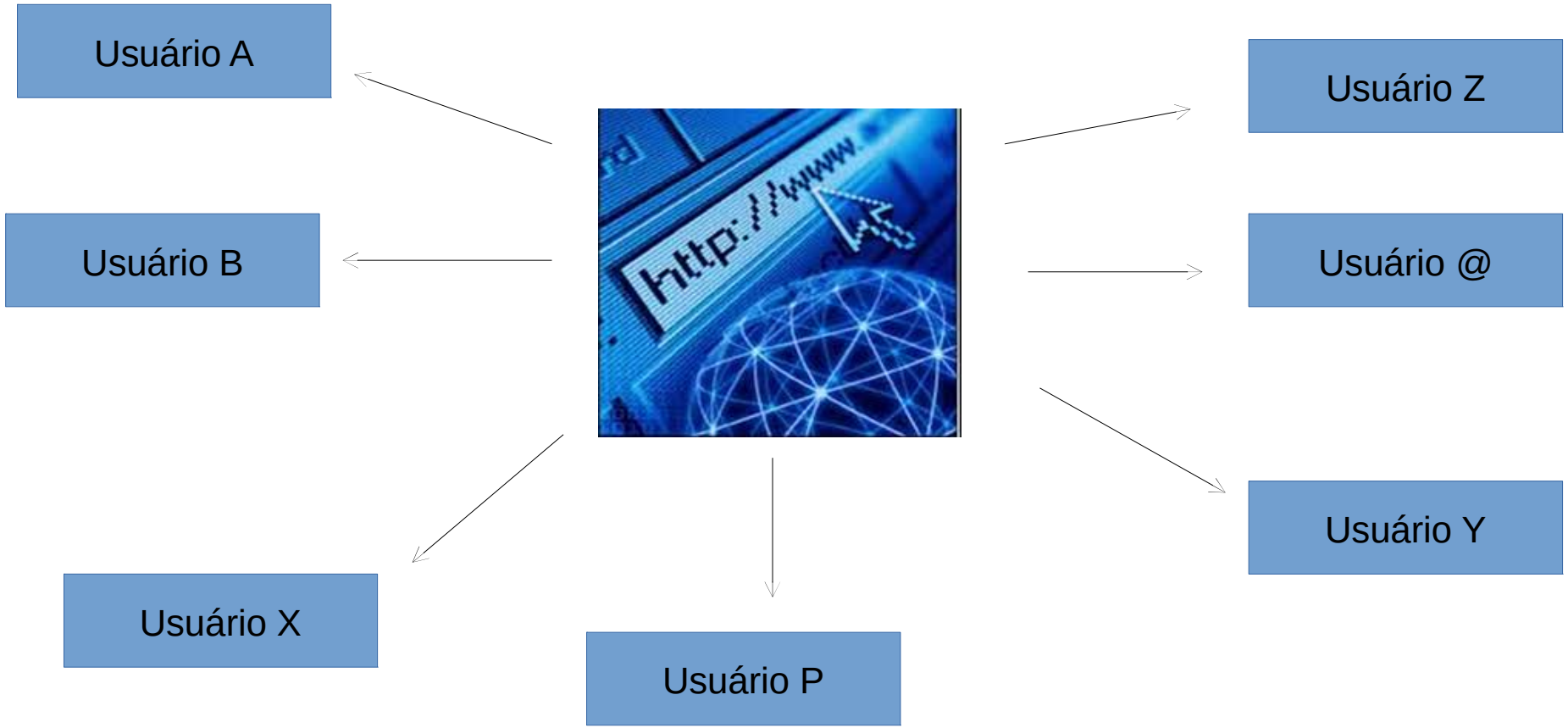
- **Sessão** : São criados e armazenados temporariamente durante uma sessão de navegação em um site e são excluídos do dispositivo do usuário quando o navegador é fechado.
- **Persistente:** não é excluído após o navegador ser fechado, e sim depois de um período de tempo específico definido pelo seu servidor.
- **Terceira parte:** criados a partir de um site que não seja o que o usuário acessou. A maior parte destes web cookies são gerenciados por trackers



USUÁRIO	SITE ACESSADO
A	X
A	Y
A	Z
A	W

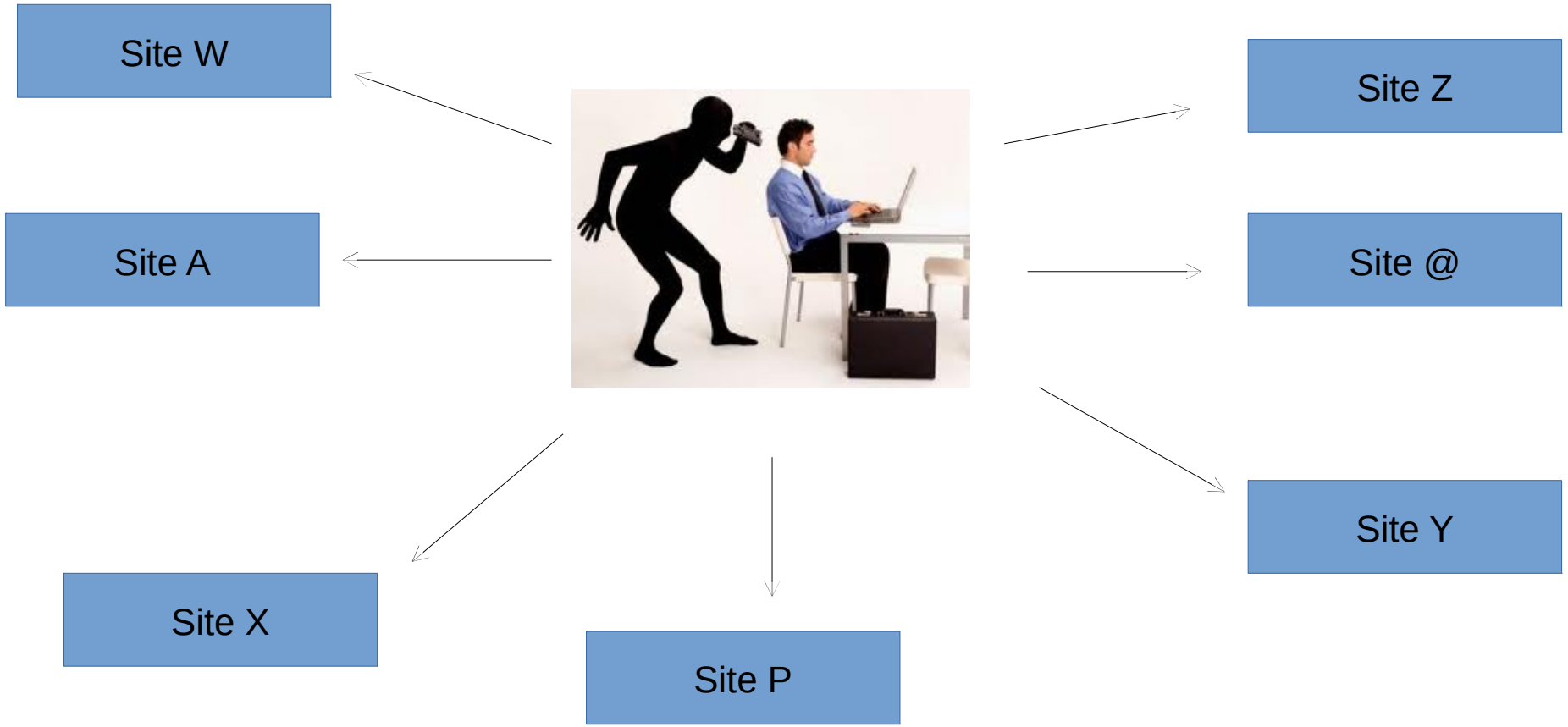
Controle 1

Controlar quais Usuários acessam um determinado site.



Controle 2

Controlar os sites que um determinado Usuário acessa.



Além das empresas de Marketing Digital, no ecossistema da Internet existem outros agentes que diante de seus interesses firmam acordos de cooperação ou desenvolvem tecnologias de rastreamento de comportamento e vigilância na Internet.

Os 10 sites de noticias mais acessados no Brasil

Nome do Site	Endereço (url)
UOL	uol.com.br
Terra	terra.com.br
Globo.com	globo.com
R7	r7.com
Folha de São Paulo	folha.uol.com.br
IG	ig.com.br
Estadão	estadao.com.br
MSN	msn.com
Tecmundo	tecmundo.com.br
BOL	bol.com.br

Tabela 1: Os dez sites de notícias mais acessados no Brasil (2015 e 2016)

Quantidades de cookies por site

Nome do Site	Abril de 2015	Maio de 2016
Uol	60	161
Terra	120	44
Globo.com	46	1
R7	25	25
Folha de São Paulo	70	35
IG	70	38
Estadão	34	34
MSN	15	27
Tecmundo	23	33
BOL	10	10

Tabela 2: Quantidade de web cookies inseridos por site.

Comparação entre os períodos

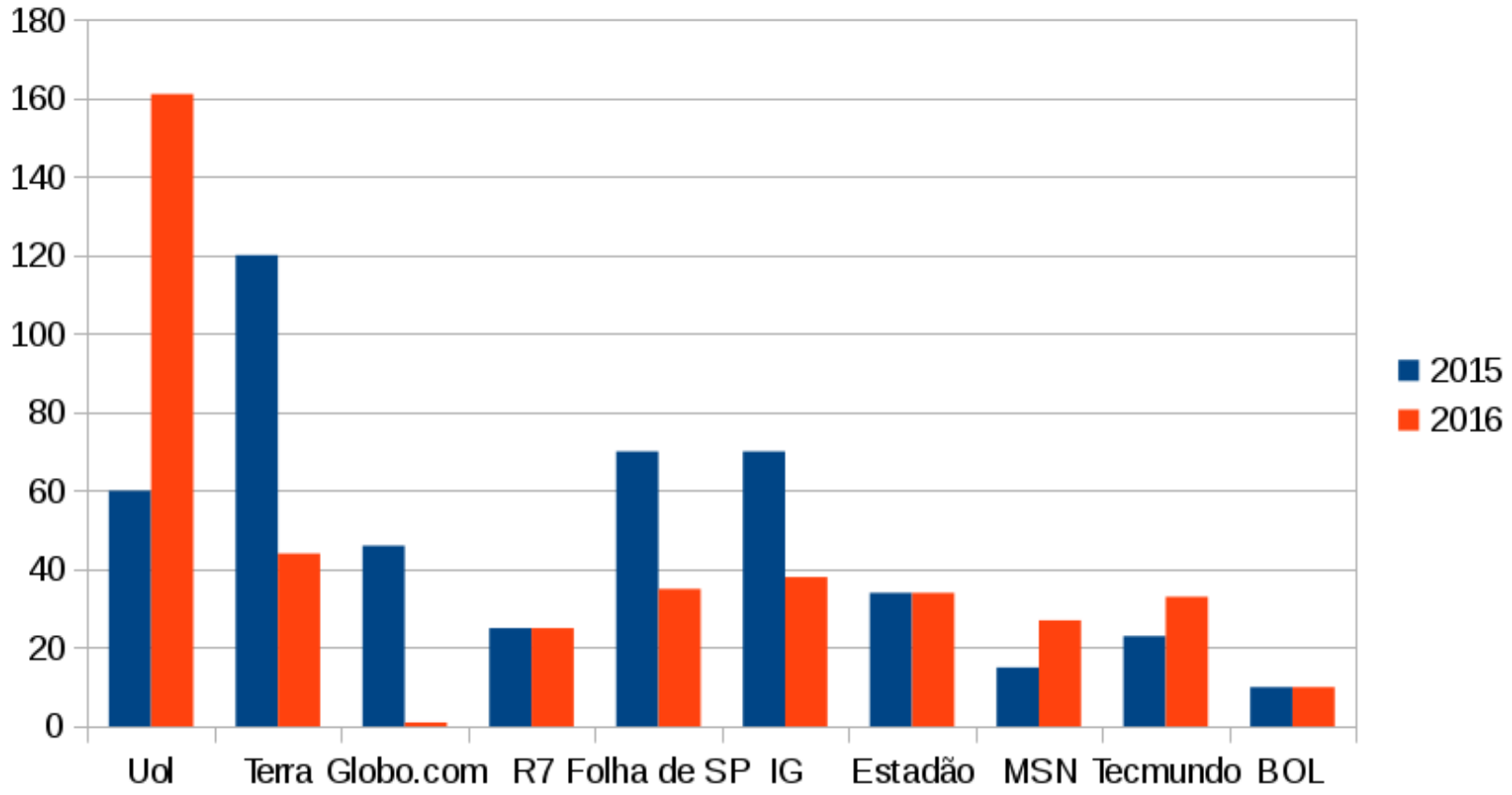
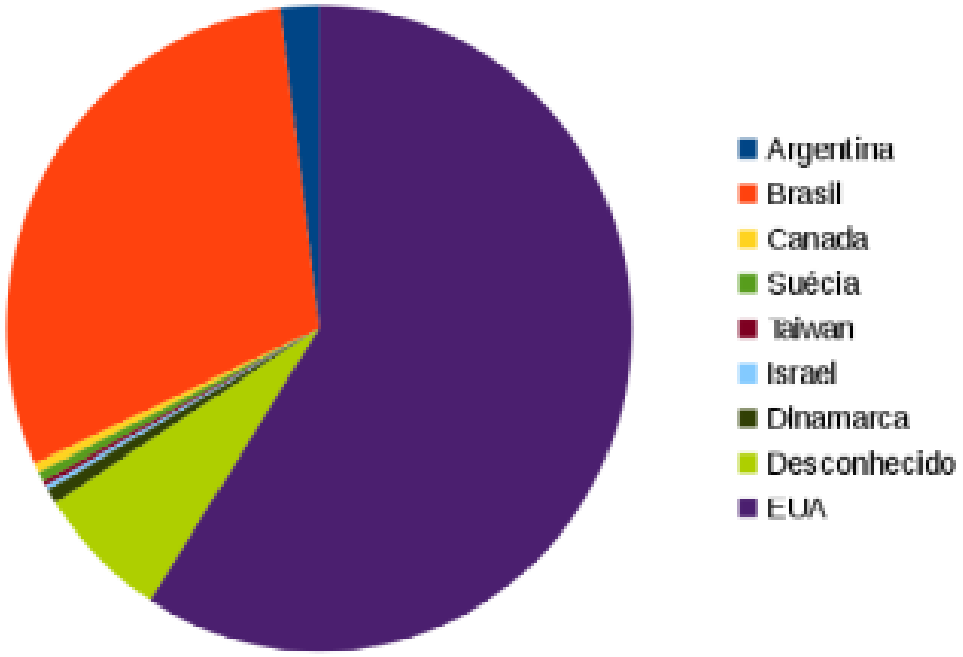


Figura 1: Comparação entre o período de análise.

Cookies por tipo

Site de notícias	Nº de web cookies de terceira parte	Nº de web cookies persistentes	Nº de web cookies de sessão e de terceira parte
Uol	36	141	10
Terra	16	38	1
Globo.com	1	1	0
R7	12	20	1
Folha de São Paulo	21	27	3
IG	15	24	2
Estadão	15	23	3
MSN	10	22	0
Tecmundo	13	28	3
BOL	6	7	3

Origem dos servidores que injetaram os cookies



Argentina	8
Brasil	122
Canada	2
Suécia	2
Taiwan	1
Israel	1
Dinamarca	3
Desconhecido	28
EUA	241

Conclusões:
Será o Fim dos cookies???

Dúvidas?

Facebook: rodolfoavelino