



# OS RISCOS CIBERNÉTICOS NA AGENDA DAS CORPORAÇÕES BRASIL E GLOBAL

Cyber Insurance

10 DE MARÇO DE 2018

# AGENDA



1. SEGURANÇA CIBERNÉTICA
2. DADOS DA PESQUISA
3. CENÁRIO REAL
4. CYBER INSURANCE
5. ABORDAGENS CONSULTIVAS
6. PERGUNTAS?



# SEGURANÇA CIBERNÉTICA

# O QUE MUDOU?

## VISÃO TRADICIONAL DE SEGURANÇA DA INFORMAÇÃO

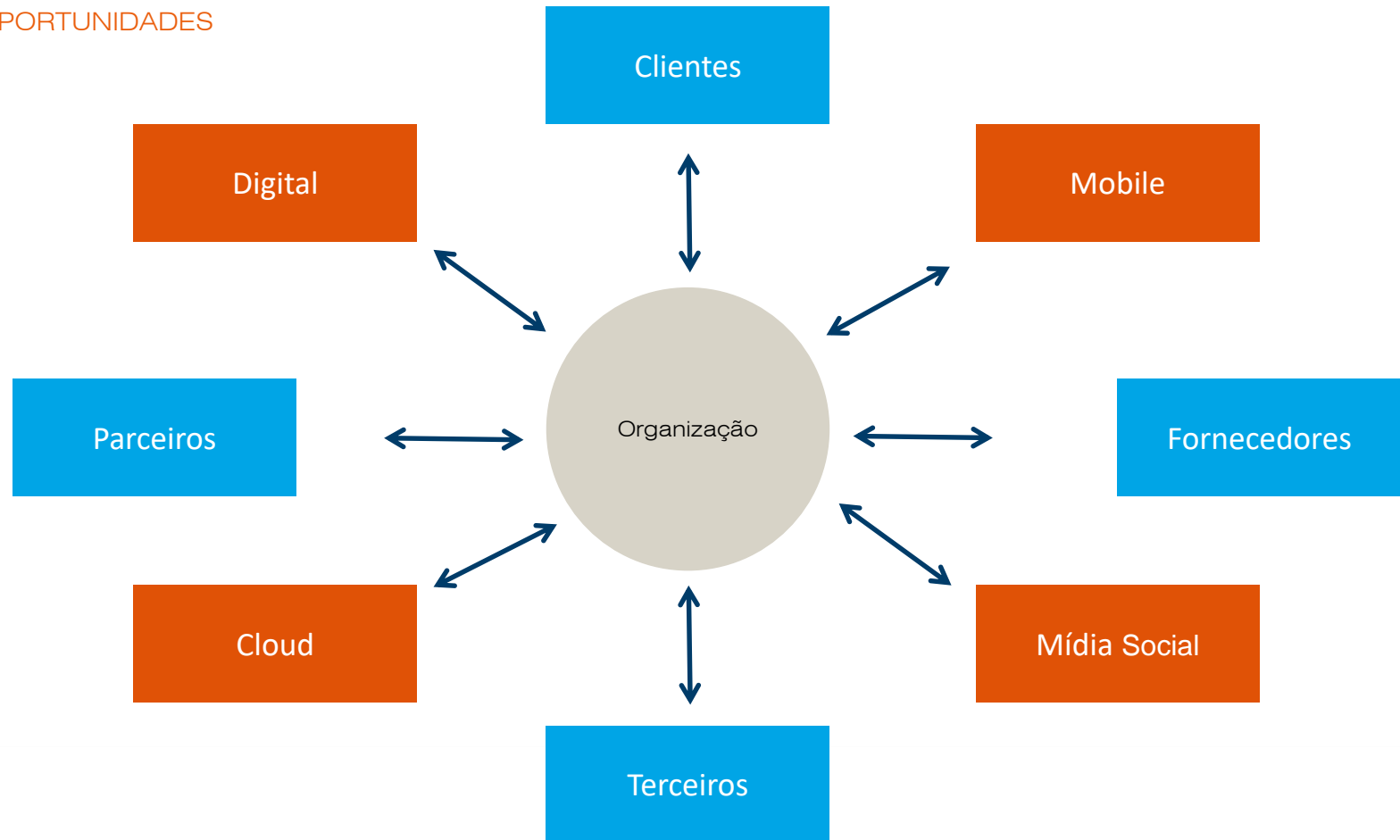


# O QUE MUDOU?

## CYBER SECURITY – ECOSSISTEMA TECNOLÓGICO

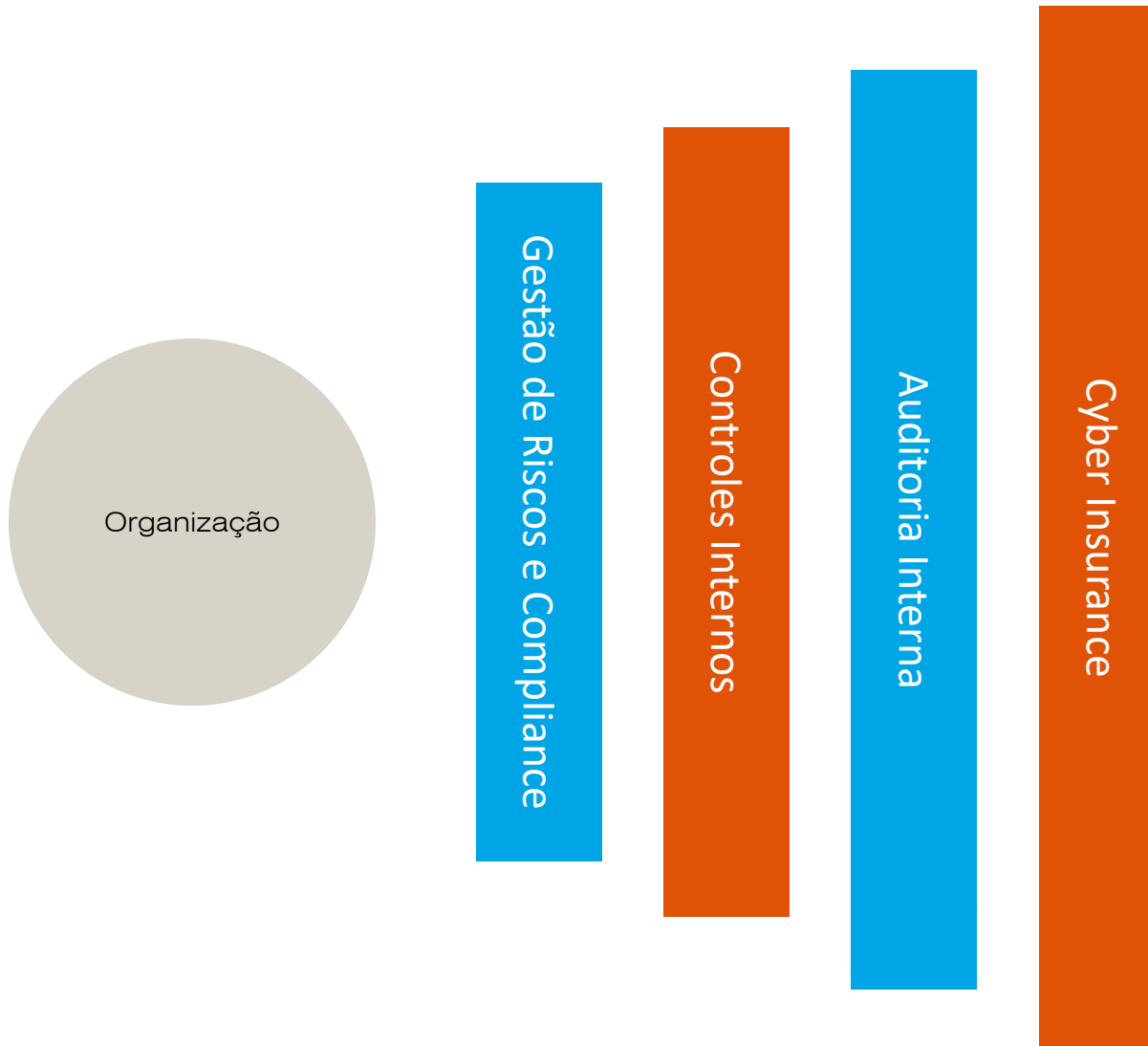
■ NEGÓCIOS

■ OPORTUNIDADES



# AS LINHAS DE DEFESA

CYBER INSURANCE – NOVA LINHA DE DEFESA





2

# DADOS DA PESQUISA



# RESULTADOS DO BRASIL

## REPORT CARD – ATAQUES CIBERNÉTICOS



PERCENTAGE OF RESPONDENTS AFFECTED BY CYBER INCIDENTS IN THE PAST 12 MONTHS.

- ▲ 13% points above 2016
- ▲ 3% points above global average

### CYBER SECURITY

#### MOST COMMON TYPES OF CYBER INCIDENT

Global Avg.

Virus/worm attack	45%	36%
Email-based phishing attack	37%	33%

#### MOST COMMON PERPETRATORS

Global Avg.

Ex-employees	32%	28%
--------------	-----	-----

#### MOST COMMON TARGET

Global Avg.

Customer records	47%	48%
Trade secrets/R&D/IP	44%	40%

#### MOST COMMON PARTY TO CONTACT WHEN A CYBER INCIDENT OCCURRED

Global Avg.

IT service vendor	47%	35%
-------------------	-----	-----

- No Brasil, **89%** dos respondentes afirmaram ter sido alvo de ataques cibernéticos, em relação à **76%** apontado no ano anterior.
- Este percentual é praticamente **o mesmo do resultado Global**.
- Estudos internos demonstram que a **detecção ainda é um problema**, mas o aumento da percepção está diretamente relacionado com o **surgimentos dos impactos**.
- Demanda de negócios relacionados com **Resposta a Incidentes**, **cresceu 63%** em relação ao ano passado.
- As ações maliciosas buscam a **monetização** dos ataques.



# RESULTADOS DO BRASIL

## PRINCIPAIS TIPOS DE CIBERATAQUES

MOST COMMON TYPES OF CYBER INCIDENT		Global Avg.
Virus/worm attack	63%	62%
Email-based phishing attack	61%	57%
Alteration or change of data	55%	56%
Data breach (e.g., resulting in loss of customer or employee data, IP/trade secrets/R&D)	55%	55%
Ransomware attack	55%	55%
Denial of service attack	55%	52%

- Tanto no Brasil quanto globalmente, ataque por vírus/ worm foi mencionado como o principal preocupação das empresas. **Tratam-se de ataques em massa.**

# HAAS – HACKER AS A SERVICE

## Terceirizando os ataques - Ransomwares

The screenshot displays the BlackHatStore.ru interface. At the top, a navigation bar includes links for Home, Profile, Top Up, CCs, Banks, Ebay, Paypal, Accounts, BIN Search, Checker, Rules, Articles, and FAQ. Below this, the user's profile for 'Tox - Viruses' is shown, with a bio 'toxicola7qvw37qj.onion' and a 'LIVE SUPPORT offline' status. A summary table shows 1 virus, 6 infected, and 0 paid. A 'Create a virus' form is visible at the bottom, with fields for Ransom (\$), Notes, and Captcha. A sidebar on the left contains a 'News' section and a 'MESSAGING' section with an 'Inbox (1)'.

Home

News

20.06.2013  
bitcoin au  
working n

10.06.2013  
Big updat  
Little upd

06.06.2013  
ukash pay  
tomorrow

05.06.2013  
Paymer to  
send us N  
again !

04.06.2013  
WU fixed.  
pls do all  
ask top up  
Send MTC  
home pag  
after fill al  
when u as  
after u got  
send mtr  
page or fr

03.06.2013  
sorry for d  
some bon

My account Forum

Help | Replacements

Dashboard  
Order history  
Buy credits  
Transfer credits  
Replacement pi  
Sign Out

MESSAGING  
Inbox (1)  
Compose  
Sent mail  
Trash

BlackHatStore.ru

blackhat®

chat LIVE SUPPORT offline

Hello, crack3d! You have 0 credits.

Tox - Viruses  
toxicola7qvw37qj.onion

Summary

Viruses	1
Infected	6
Of which paid	0

Total profit 0.00 \$

To withdraw (net) Currently unavailable

Your BTC address Withdraw

Create a virus

Ransom - \$ Ransom in dollars (min. 50)

Notes Optional, ex: For Mr. Smith

Captcha Captcha

# RESULTADOS DO BRASIL

## PRINCIPAIS TIPOS DE CIBERATAQUES

<b>MOST COMMON TYPES OF CYBER INCIDENT</b>		<i>Global Avg.</i>
Virus/worm attack	63%	62%
Email-based phishing attack	61%	57%
Alteration or change of data	55%	56%
Data breach <i>(e.g., resulting in loss of customer or employee data, IP/trade secrets/R&amp;D)</i>	55%	55%
Ransomware attack	55%	55%
Denial of service attack	55%	52%

- Ataques de Phishing passaram da 6ª para a 2ª posição, em relação ao último ano.

# BEC - Attack

## Business E-mail Compromise

Criminosos se passam por funcionários do alto escalão da empresa e utilizam suas contas de e-mail, ou sutilmente parecidas, para enganar funcionários responsáveis por movimentações financeiras.



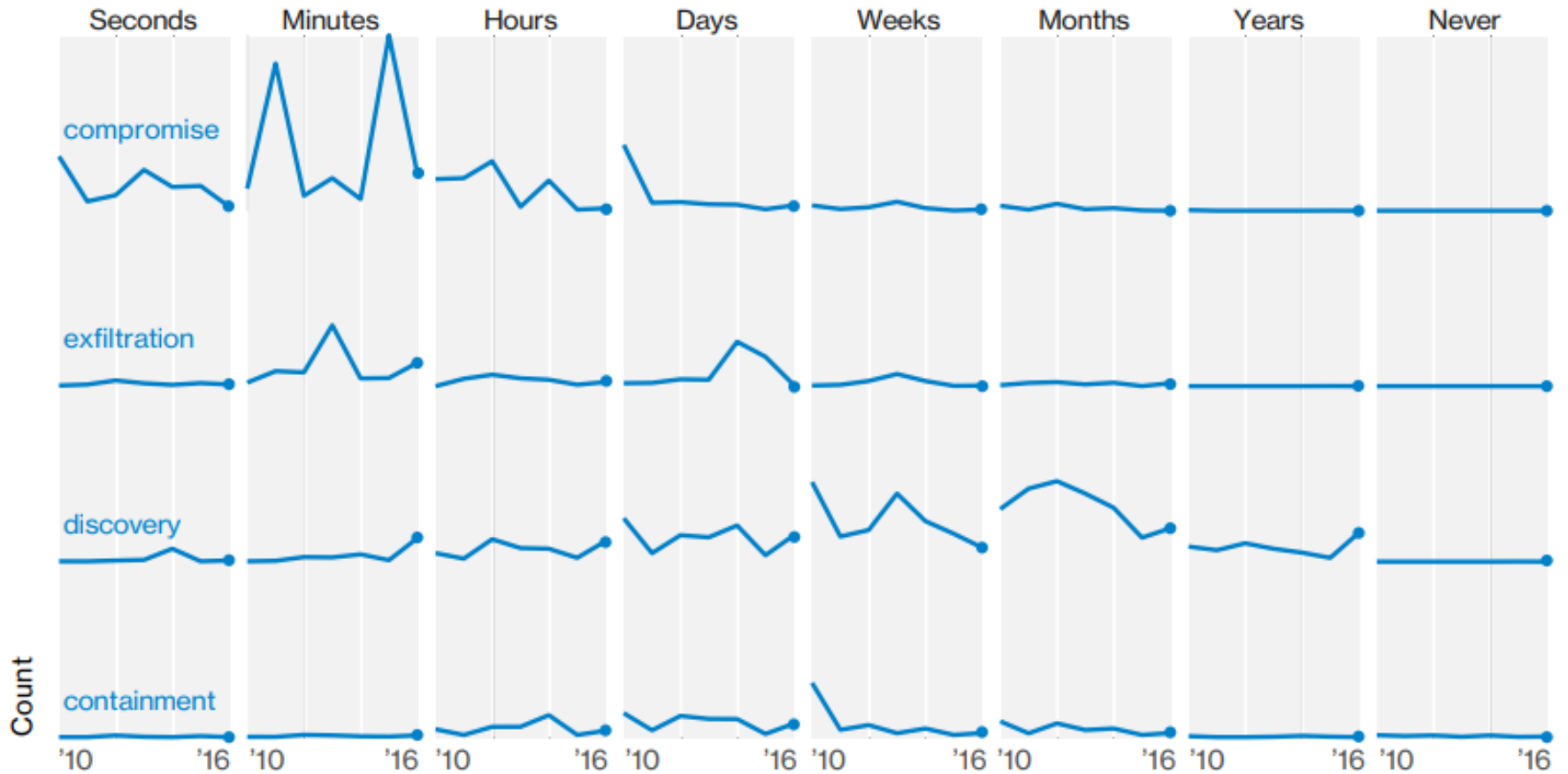
Cibercriminoso se passa por executivo da empresa e envia e-mail para o departamento financeiro

Financeiro realiza transação, conforme solicitação, para a conta do cibercriminoso.

Cibercriminoso recebe o pagamento e limpa rastros do ataque.

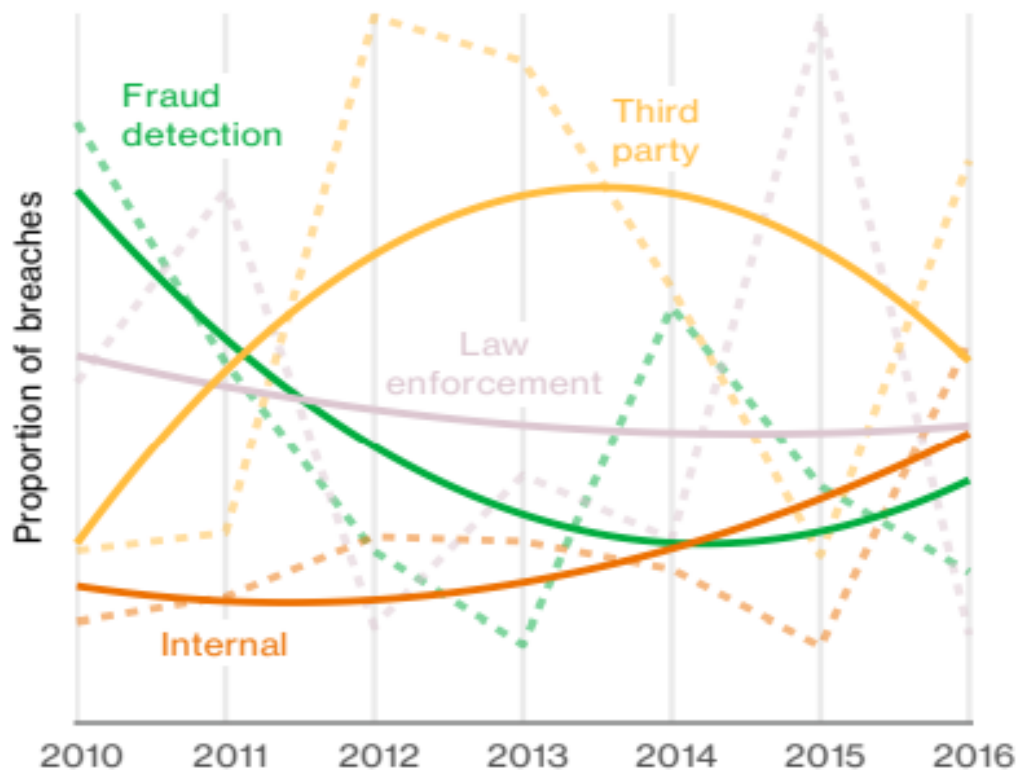
# RESULTADOS DO BRASIL

## INDICADORES DE OUTRAS PESQUISAS



# DETECÇÃO DOS ATAQUES

Mudança de panorama



- Detecções ainda ocorrem através de terceiros;
- Controles internos e mecanismos de detecção de fraude aumentando a eficiência.

# RESULTADOS DO BRASIL

## PRINCIPAIS OBJETIVOS DOS ATAQUES

MOST COMMON TARGET		Global Avg.
Customer records	47%	48%
Trade secrets/R&D/IP	44%	40%

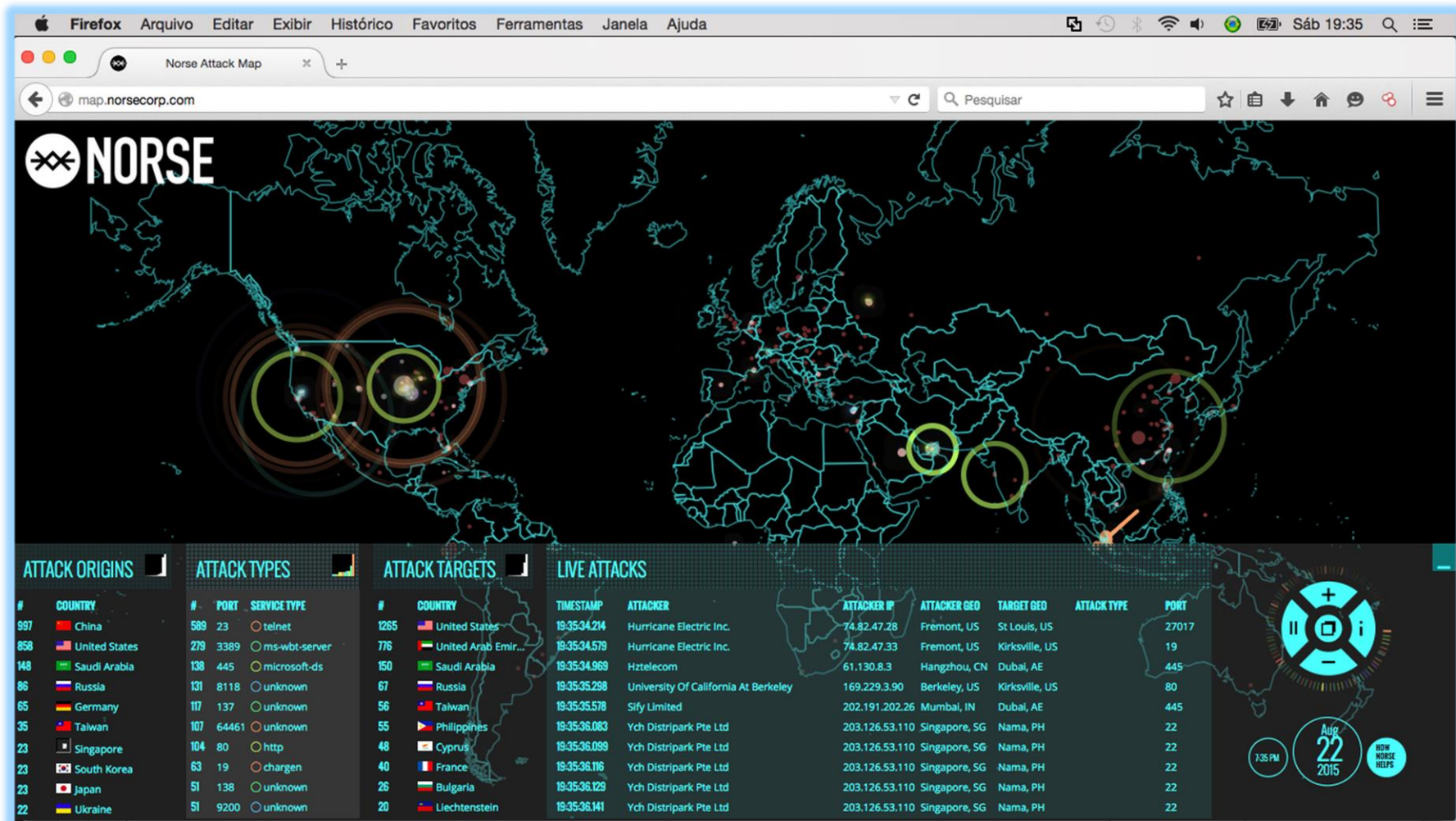
- Objetivo principal é obter acesso à informações sensíveis das empresas (informações sobre clientes, funcionários, identidade, segredos comerciais) e monetizar.





# CENÁRIO DOS ATAQUES – GLOBAL

Fluxo de ataques em tempo real



# RESULTADOS DO BRASIL

## PERPETRADORES DAS FRAUDES CIBERNÉTICAS

MOST COMMON PERPETRATORS		Global Avg.
Ex-employees	32%	28%

- Os principais responsáveis incidentes cibernéticos são funcionários e ex-funcionários das empresas, seguidos dos concorrentes.

3

CENÁRIO REAL



# DEMONSTRAÇÃO

COMO ISSO FUNCIONA NA VIDA REAL?



WikiLeaks

!;--have i been pwned?



PASTEBIN



SHODAN

**EXPLOIT  
DATABASE** 

Google **H4CKING**

# DEMONSTRAÇÃO

COMO ISSO FUNCIONA NA VIDA REAL?

The image shows a browser window with two overlapping pages. The background page is Pastebin.com, displaying several pasted links and snippets of text, including email addresses and dates. The foreground page is Shodan, a search engine for open-source intelligence. It shows search results for the keyword 'heartbleed'. The search results include a total of 97 results, a world map highlighting the United States, and a detailed view of a specific result from Amazon. The detailed view shows the IP address 54.162.21.29, the domain ec2-54-162-21-29.compute-1.amazonaws.com, and the location United States, Ashburn. It also displays technologies like nginx and SSL certificate information for \*.hockeyapp.net.

**PASTEBIN** + new paste trends API tools faq search...

1k Emails|senha - Pastebin.com  
<https://pastebin.com/ikEB0cg2>  
Oct 30, 2016 ... rodrigo  
MARKUP.PESSOAL@

LOGINS EMAIL|SENHA - Pastebin.com  
<https://pastebin.com/ikEB0cg2>  
May 13, 2017 ... elisabete  
gleiciane- black@hotmail.com

DB EMAIL E SENHA - Pastebin.com  
<https://pastebin.com/ikEB0cg2>  
Jun 28, 2016 ... karina  
moniknack@bol.com.br

erin\_moran@att.net - Pastebin.com  
<https://pastebin.com/ikEB0cg2>  
Jan 12, 2017 ... erin\_moran  
gmail.com senha: nicol

**SHODAN** heartbleed

Exploits Maps Share Search Download Results Create Report

TOTAL RESULTS  
**97**

TOP COUNTRIES

Country	Count
United States	71
Germany	17
China	3
Italy	1
Ireland	1

TOP SERVICES

Service	Count
HTTPS	74

**Sign In – Warmup**  
54.162.21.29  
ec2-54-162-21-29.compute-1.amazonaws.com  
**Amazon**  
Added on 2018-02-17 16:33:37 GMT  
United States, Ashburn  
Technologies: nginx  
**Details**  
cloud

**SSL Certificate**  
Issued By:  
|- Common Name: Microsoft IT SSL  
**SHA2**  
|- Organization: Microsoft Corporation  
Issued To:  
|- Common Name: \*.hockeyapp.net  
|- Organization: Microsoft Corporation

**Supported SSL Versions**  
TLSv1, TLSv1.1, TLSv1.2

HTTP/1.1 200 OK  
Server: nginx  
Date: Sat, 17 Feb 2018 16:33:37 GMT  
Content-Type: text/html; charset=utf-8  
Content-Length: 7848  
Connection: keep-alive  
Status: 200 OK  
Content-Security-Policy: frame-ancestors https://rink.hockeyapp.net http:

# CYBER INSURANCE?

Seguro cibernético aparece em **13o** lugar das principais ações e controle de mitigação.





# CYBER INSURANCE

# CYBER INSURANCE

## NOVA LINHA DE DEFESA CIBERNÉTICA

Proteção dos negócios, contando com cobertura como:

- **Violação de dados / privacidade e gestão de crises:** Despesas relacionadas com a gestão do incidente, investigação, remediação, notificação, custos legais e procedimentos em tribunais.
- **Danos reputacionais:** Custos relacionados a **violação de propriedade intelectual**, direitos autorais, calúnia e difamação.
- **Extorsões cibernéticas:** Despesas relacionadas a casos de extorsões, mediando a **sequestro de dados** e servidores e criptografia de arquivos realizadas pelo crime organizado.
- **Riscos Operacionais:** Custos relacionadas a inoperância e/ou **indisponibilidade da rede** de computadores, além do roubo de dados.

# ABORDAGENS CONSULTIVAS

# ABORDAGEM CONSULTIVA

## AVALIAÇÃO REAL DOS RISCOS CIBERNÉTICO

A grande maioria das empresas que operam no Brasil não sabem dimensionar os custos relacionados aos impactos dos **riscos cibernéticos**, devido a falta de consciência situacional e o baixo nível de maturidade em Cyber.

Um bom começo é a identificação dos riscos e quantificação dos impactos, através de um **Cyber Risk Assessment**.

Como resultado deste levantamento, a organização estará apta a determinar seu nível atual de maturidade em Cyber e saber qual o nível mínimo aceitável para o seu negócio, trabalhando nos **Gap's** identificados.

# ABORDAGEM CONSULTIVA

## AValiação REAL DOS RISCOS CIBERNÉTICO

### AVALIAÇÃO DE RISCOS DE TI

- Nível de consciência da organização
- Levantamento das políticas, procedimentos e controle
- Avaliação dos ativos e topologia de rede
- Avaliação dos processos de resposta e remediação

### ANÁLISE DE VULNERABILIDADES

- Implanta variedade de ferramentas de código aberto e proprietárias para identificar vulnerabilidades
- Examina componentes da infraestrutura de rede nos perímetros interno e externo
- Prove análise de aplicações Web

### TESTE DE INTRUSÃO

- Implantar ferramentas open source e proprietárias para explorar vulnerabilidades identificadas
- Intrusão "controlada" aos sistemas e ativos
- Criação dos cenários para Engenharia Social
- Relatórios detalhados sobre as ações e remediações

### AVALIAÇÕES ESPECIALIZADAS

- Conformidade com órgãos reguladores
- Avaliação de Segurança em ambientes Wireless e VoIP
- Avaliação de Segurança em Terceiros
- Investigação e Computação Forense
- Avaliações customizadas

# ABORDAGEM CONSULTIVA

## RESPOSTA A INCIDENTES

Capacidade de investigar aos incidentes, com o objetivo de:

- Erradicação do ataque
- Identificação da causa raiz
- Retroalimentação dos controles
- Atribuição de culpabilidade
- Retorno a normalidade



PERGUNTAS?



OBRIGADO

