



Principais Aspectos da Segurança Cibernética relativos aos Órgãos da Administração Pública Federal nos Jogos Olímpicos e Paralímpicos RIO 2016



CTIRGov



ATIVOS DE INFORMAÇÃO

Pessoas

Processos

Ambiente

Tecnologias



ASSUNTOS

Ameaças

**Protocolos de
Notificação**

CTIR Gov



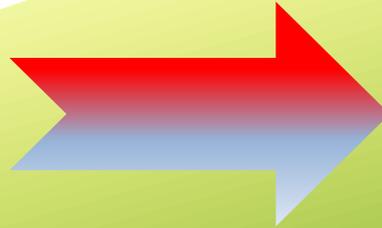
ETIR/APF

Vídeo 1: <https://www.youtube.com/watch?v=MK0SrxBC1xs>



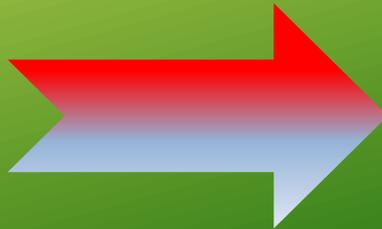
COMO AS AMEAÇAS SÃO VISTAS

Para os países desenvolvidos



- Espionagem
- Sabotagem
- Terrorismo
- Roubo

Para os países em desenvolvimento



- Fraudes bancárias
- Vazamento de dados



CENÁRIO ATUAL



Relatório da McAfee Labs revela novas ameaças de conluio entre aplicativos de dispositivos móveis

Quinta, 23 Junho 2016 14:29 Fonte/Autor por: Medialink Comunicação Publicado em Info & TI Imprimir E-mail Compartilhar:



23/06/2016 20h49 - Atualizado em 24/06/2016 11h58

Hackers de Mogi movimentaram cerca de R\$ 10 milhões, diz polícia

Air India: Police launch probe after hackers steal frequent-flyer miles worth Rs 1.6m

Brasil registra mais de 4 milhões de ciberataques

Risk Report 20/06/2016

International Business Times

20/06/2016 07:00 - Geral

Câmera de celular e até aparelhos de babá eletrônica são alvos de hacker

Para especialista, qualquer câmera num dispositivo com acesso à Internet é vulnerável



TECNOLOGIA

20/06/2016 20:44

Coreia do Sul treina hackers em batalha contra o Norte





TENDÊNCIAS

- Aumento do número de oponentes.





TENDÊNCIAS

- Crescimento do CaS – *Cybercrime-as-a-Service*.

A captura de tela mostra a interface de um site de contratação de hackers. O cabeçalho é verde escuro com ícones de lupa, mais, e perguntas. O menu principal contém: Find Hackers, Bid Projects, How It Works, FAQ, Register, Login e uma lupa. O conteúdo principal é uma grade de fotos de pessoas de diversas etnias e idades. Sobreposto ao centro da grade, há um texto em branco que diz: "Find professional hackers for hire". Abaixo disso, um texto menor afirma: "People need professional hackers for hire. So, we connect people who need professional hackers to professional hackers for hire around the world. Safe, fast and secure Learn how it works." Na base da grade, há dois botões: "Browse OR" e "Start a Project for Free".



Cybercrime-as-a-Service





Cybercrime-as-a-Service

THE ORIGINAL HACKER FOR HIRE SERVICE - **THE #1 HACKER FOR HIRE SERVICE IN THE WORLD**



ENTERTAINERS - ATHLETES - POLITICIANS - CORPORATIONS - PARENTS - HUSBANDS/WIVES - CONSUMERS

[HOME](#) [ABOUT US](#) [SPY SHOP](#) [BLOG](#)

Hacking

- Have you been hacked?
- Do you want to find out if your website, computer or network can be or has been hacked?
- Would you like to hack into a computer, website or network?

Social Media Threats

- Has your Facebook, Twitter or Google+ account been hacked? We can help get it restored and track the person who did it in many cases.

Computer Spying and Surveillance

- Do you want to install spyware on a cellphone or computer?
- Do you want to know if you have spyware on your computer?



This Resource is Not Available (Inactive)



TENDÊNCIAS

- Aumento da sofisticação tecnológica dos oponentes, dificultando ainda mais a detecção e a reação.

A captura de tela do site SHODAN, uma plataforma de busca de dispositivos online. No topo, há o logo SHODAN e uma barra de busca com o botão "Search". Abaixo, um mapa do mundo em tons de vermelho indica a localização de dispositivos descobertos. O texto principal diz "EXPOSE ONLINE DEVICES." e lista exemplos: "WEBCAMS. ROUTERS. POWER PLANTS. IPHONES. WIND TURBINES. REFRIGERATORS. VOIP PHONES." Há dois botões: "TAKE A TOUR" em vermelho e "FREE SIGN UP" em verde. Na base, uma seção de "Popular Search Queries" menciona "default password" e afirma que encontra resultados com essa palavra no banner.



TENDÊNCIAS

- Crescimento dos *Spear Phishing* em detrimento das mensagens de *phishing*.





TENDÊNCIAS

- Crescimento dos sítios de *Phishing*.

live.equi-score.de/home/login.do2562.html?quyeygczp11xdgzjwismpn81jhwflijqs2u7jhprc4vipj3c4j1252omze8zmmw2xfk241nmiqk1dzl2v3t3ozp5avohk1vhdqjdd5upro7y3

Auto Atendimento Área Logada Atendimento SAC BB Ouvidoria Ajuda

RECADASTRAMENTO DE SEGURANÇA

Aviso do Banco do Brasil para seus respectivos clientes

Informamos que a reativação preventivo de segurança online do Banco do Brasil é uma operação obrigatória, que soluciona e corrige problemas na segurança de dados de nossos clientes, possibilitando assim mais conforto, rapidez e segurança nas transações através do sistema online

Caso não for constatado a reativação preventivo de segurança, o acesso a operações bancárias será suspensão por medidas de segurança.

- * A operação é rápida e fácil, não deve demorar mais de 5 minutos, após a realização desta operação o nosso sistema enviará um e-mail de confirmação de seus dados cadastrais.
- * Clique no botão Acessar para iniciar a reativação.

Material de Construção

Parcele a aquisição do material de construção e realize o sonho de reformar a sua casa. Simule.

Crédito Consignado INSS

Você, aposentado, tem crédito com preço mais barato e taxa de juros a partir de 0,79% ao mês. Simule.

BB Crédito Veículo

Quem faz as contas financia o carro no Banco do Brasil e tem até 180 dias para começar a pagar.

Eletroeletrônico

Use o cartão Ourocard para parcelar suas compras. Taxas de juros máxima de 1,98% ao mês. Simule.



Sítios de *Phishing*



TENDÊNCIAS

- **Crescimento do Ransomware.**

“Tipo de malware que restringe o acesso ao sistema infectado e cobra um valor de "resgate" para que o acesso possa ser reestabelecido.”

Relatório de Pesquisa da Kaspersky Security Network:
718.536 pessoas foram afetadas por ataques de ransomware entre abril de 2015 e março de 2016.



RANSOMWARE

RANSOMWARE ATTACKERS REFUSE TO DECRYPT HOSPITAL'S FILES AFTER BEING PAID OFF

By Justin Pot — May 24, 2016

Brian A Jackson/Shutterstock



“Negotiating with criminals doesn’t always work out, as Kansas Heart Hospital in Wichita learned last week. The hospital paid to get files back after falling victim to ransomware, but only got “partial access” and a demand for more money.”



TENDÊNCIAS

- Incremento na capacidade dos oponentes de aliar ataques cibernéticos a consequências cinéticas.



Vídeo 2: <https://www.youtube.com/watch?v=Oz3-NethUNY>



TENDÊNCIAS

- Aumento das ameaças APT (*Advanced Persistent Threat*).
 - Pacientes e persistentes
 - Organizados
 - Custo elevado
 - Sofisticação: autoproteção, camuflagem, mutação
 - “O que for preciso!”
 - Organizações criminosas ou países





APT

Rússia vs Geórgia (2008)



- Geórgia vs Ossetas (apoiado pela Rússia).
- Negação de Serviço e Abuso de Sítios, conjugado com ataques por terra e ar.
- Sites governamentais, de empresas públicas e privadas foram tirados do ar.



APT

Stuxnet (2010)



- *Worm* de computador projetado especificamente para atacar o sistema operacional SCADA , desenvolvido pela Siemens para controlar as centrífugas de enriquecimento de urânio do Irã.
- Dupla função: fazer as centrífugas girarem 40% mais rápido por 15 min e inibir os sistemas de alarme.



APT Sony (2014)

Hacked By #GOP

Warning :

We've already warned you, and this is just a beginning.
We continue till our request be met.
We've obtained all your internal data including your secrets and top secrets.
If you don't obey us, we'll release data shown below to the world.
Determine what will you do till November the **24th, 11:00 PM(GMT).**
Data Link :

<https://www.sonypicturesstockfootage.com/SPEData.zip>
<http://dm1plaewh36.spe.sony.com/SPEData.zip>
<http://www.ntcnt.ru/SPEData.zip>
<http://www.thammasatpress.com/SPEData.zip>
<http://moodle.universidadebematech.com.br/SPEData.zip>

Guardians of Peace (GOP)

- Travou os PCs;
- Sobrescreveu os HD;
- Alterou os registros de boot;
- Bloqueou acesso a e-mails;
- Bloqueou acesso a rede interna.
- Prejuízo estimado: USD 100 milhões.



TENDÊNCIAS

- Aumento do recurso de *defacement*.

Fatal Error Crew



sup3rm4n ownz you - Pwned !!!

Apenas por diversão e conhecimento!!!!

Uma vez que você tenha experimentado voar, você andar^á pela terra com seus olhos voltados para céu, pois lá você esteve e para lá você desejar^á voltar."

Somos: Elemento_pcx - s4r4d0 - sup3rm4n

2015 - Fatal Error - All Copyright



Defacement

الجزائر مع فلسطين ظالمة او مظلومه

Algeria with Palestine unjust or oppressed





Defacement





|| HACKED ||

Su sistema tiene algunos fallos, fallos humanos por encima de los tecnicos.

El administrador no aprende de sus errores ni los corrige...

Una de mis intenciones es advertir los agujeros de seguridad presentes

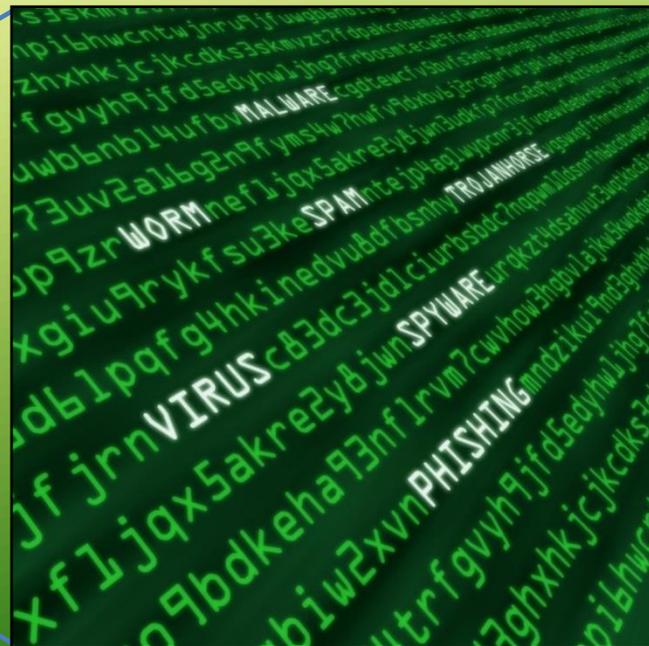
Por estigmatizar la (in)seguridad es que estamos como estamos... Con nuestras instituciones vulnerables ante el mundo. ¿Es posible vivir en un mundo donde aprendamos de nuestros errores?

Anonymous_CCG - Colombian_Hackers



AMEAÇAS

Quais são nossas ameaças?



Vídeo 3: <https://www.youtube.com/watch?v=-UjKf8SBDSO>



Quais são nossas ameaças?



Funcionário não-confiável?



Extremistas?



Lobo solitário?



Grupos especializados?



Qual a origem das ameaças?

Internas

Infiltrado

Erro humano

Insider

Infraestrutura

Externas

Alvo de Oportunidade

Crime organizado

Lobo solitário

Extremistas

Terroristas

Estados-Nação



Ameaças Internas

Infiltrado

Agente

Sabotador





Ameaças Internas

Erro humano



Procedimentos

Conhecimentos

Violações

Projetos de Segurança



Ameaças Internas

A large, dark, high-contrast photograph of a man's face. He has a serious, intense expression and is holding his right index finger to his lips in a universal gesture for silence or secrecy. The lighting is dramatic, highlighting his features against a dark background.

O Insider



Ameaças Internas

**Funcionário
desapontado**

Acesso às redes

**Cooptado por
organização terrorista**

Insider

**Roubo, espionagem,
sabotagem, dano**

**Desentendimentos no
processo de demissão**

**Nível de privilégio de
acesso**

**Cooptado por
organização criminosa**

Vídeo 4: <https://www.youtube.com/watch?v=HtTUsOKJWyQ>

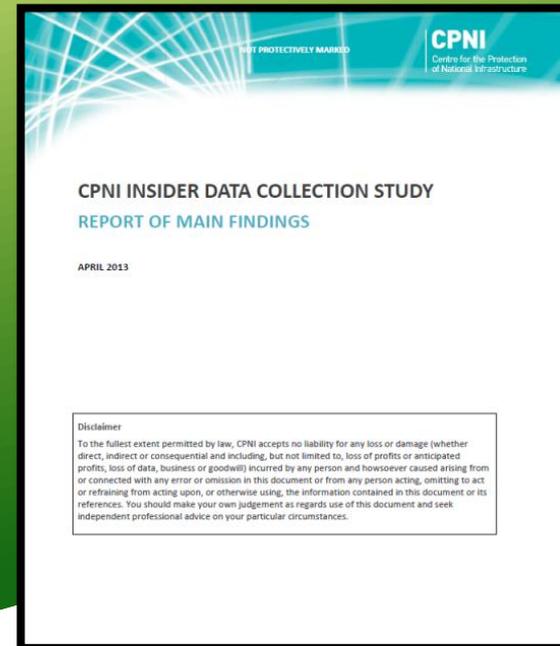
Vídeo 5: <https://www.youtube.com/watch?v=-blxOo41VSg>



Ameaças Internas

Quem é o Insider?

- Frequentemente objeto de *bullying*.
- Versado em computação – conhecimento de grupos hacker; acesso remoto; planeja os ataques.
- Graves problemas de relacionamento familiar.
- Problemas financeiros.
- Notoriamente insatisfeito.
- Desejo de reconhecimento.
- Lealdade a amigos, parentes, etc.
- Vingança





Ameaças Internas

Vazamento não intencional

- Enviar documento por email
- Copiar e colar
- Publicar sem autorização
- Renomear documento
- Alterar o tipo de documento
- Copiar dados parcialmente
- Apagar senhas

Vazamento malicioso

- “Printar” a tela
- Codificar caracteres
- Ocultar os dados
- Fotografar os dados



Ameaças Internas

Segundo o “Insider Threat Study – 2013”, os *insiders* descobertos haviam incorrido nas seguintes ações:

- Divulgação não autorizada de informações sensíveis.
- Processos de corrupção.
- Facilitação de acesso a terceiros aos ativos de informação da organização.
- Sabotagem física.
- Sabotagem de TI.



Ciclo de Vida do Empregado

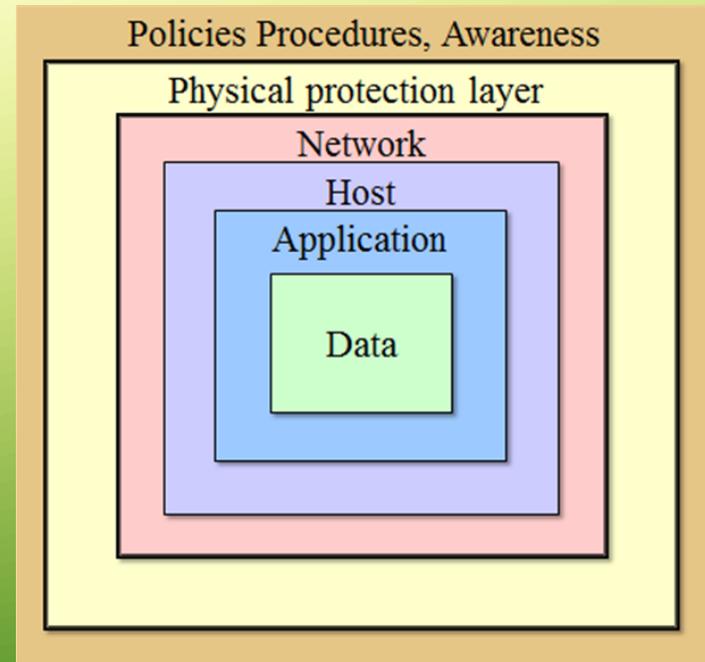


Vídeo 6: <https://www.youtube.com/watch?v=PMZ24C9DCZA>



Controles de Acesso

- Defesa em profundidade
- Algo que você sabe
- Algo que você possui
- Algo que você é



Password:





Instalações de tratamento de esgoto do Condado de Maroochy, Queensland, Australia (2000)



- Vitek Boden trabalhava na Hunter Watertech (instalou o sistema de tratamento de Maroochy)
- Em 1999 foi demitido (mas permaneceu por um tempo).
- Tentou emprego no Conselho do Condado mas foi recusado.
- Plano: vingar-se de ambos, lançando ataques contra o sistema SCADA para que a empresa fosse culpada.



Instalações de tratamento de esgoto do Condado de Maroochy, Queensland, Australia (2000)



- Possuía um programa de configuração do SCADA que instalou em seu notebook.
- Possuía um rádio e um computador da empresa que podia simular um computador de controle de uma estação de bombeamento.
- Mudou as configurações dos controles das estações de bombeamento.

Mais de **1 milhão de litros de esgoto não tratados** foram lançados em vias fluviais e parques públicos.

Vídeo 7: <https://www.youtube.com/watch?v=fJyWngDco3g>



Ameaças Internas

Infraestrutura

- Atenção à integração das redes de segurança.
- Mecanismos de segurança física.



Hackers usam milhares de câmeras de segurança "zumbis" para atacar site





Ameaças Externas

Alvo de Oportunidade

Identificado em varredura

Alvo compensador





Ameaças Externas

Crime Organizado

Negócios ilícitos

Suporte financeiro

Extratratificação de funções

MAIS DE UM MILHÃO DE IPS FORAM UTILIZADOS EM TENTATIVA DE INVASÃO A EMPRESAS



Hackers hit central banks in Indonesia and South Korea





Ameaças Externas

Lobo solitário

Causar danos

Motivação religiosa

Motivação ideológica

Apoio pessoal a uma causa





Ameaças Externas

Extremistas

Propagar mensagem

Motivação ideológica

Apoio a uma causa





Ameaças Externas

Terroristas

Mensagem de ódio

Maior dano possível

Motivação religiosa

Boa organização





Ameaças Externas

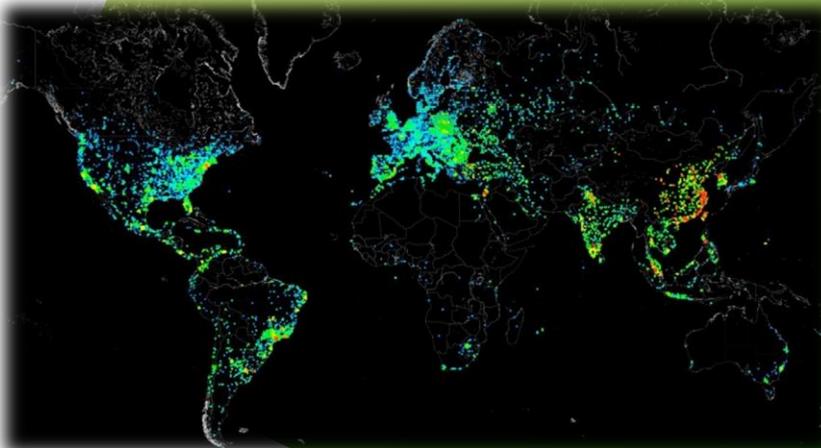
Estados-Nação

Muitos recursos

Muito boa organização

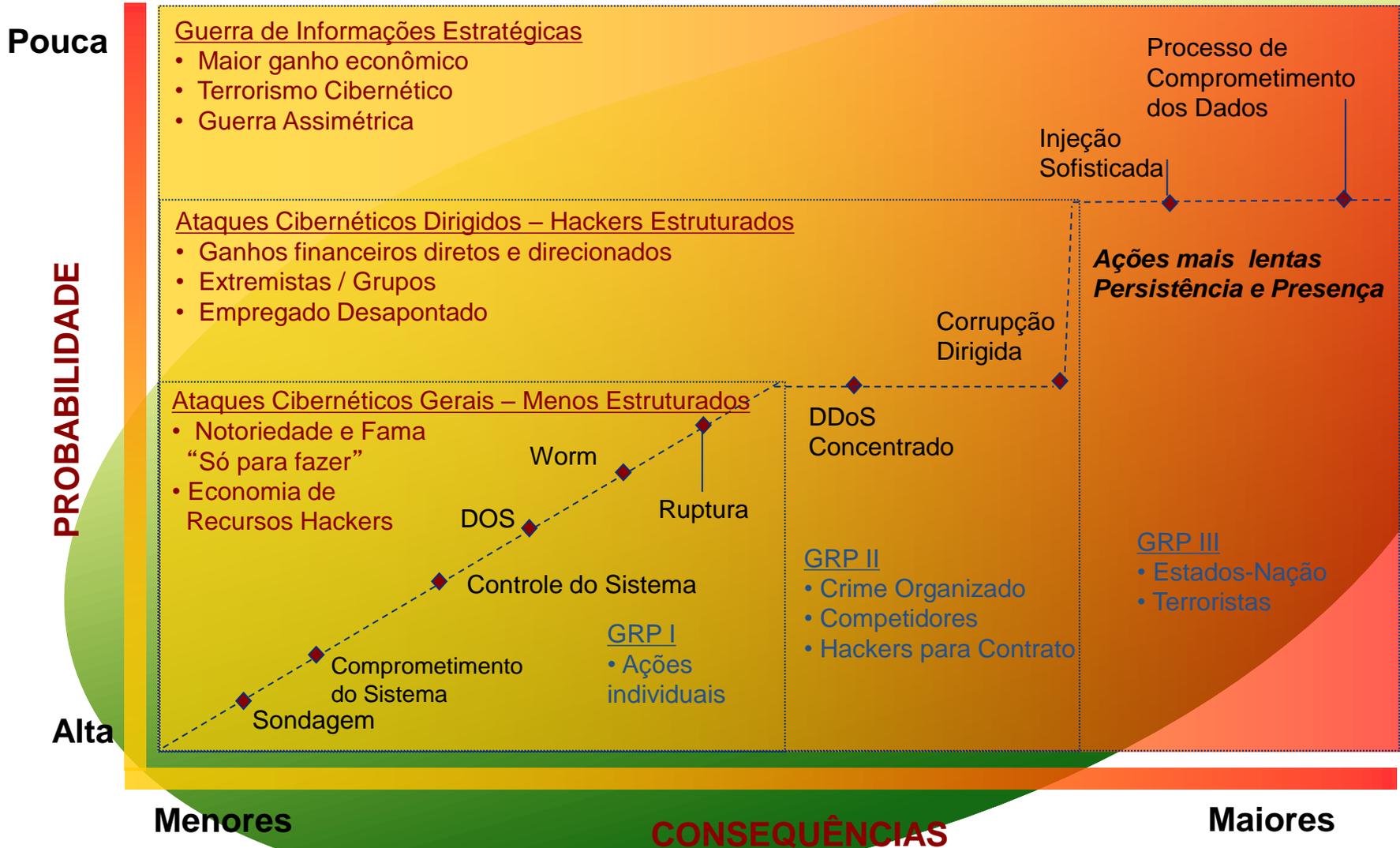
Segredos industriais

Infraestruturas Críticas





Características das Ameaças





Aspectos que favorecem o Atacante

Habilidade

Capacidade

Oportunidade

Motivação

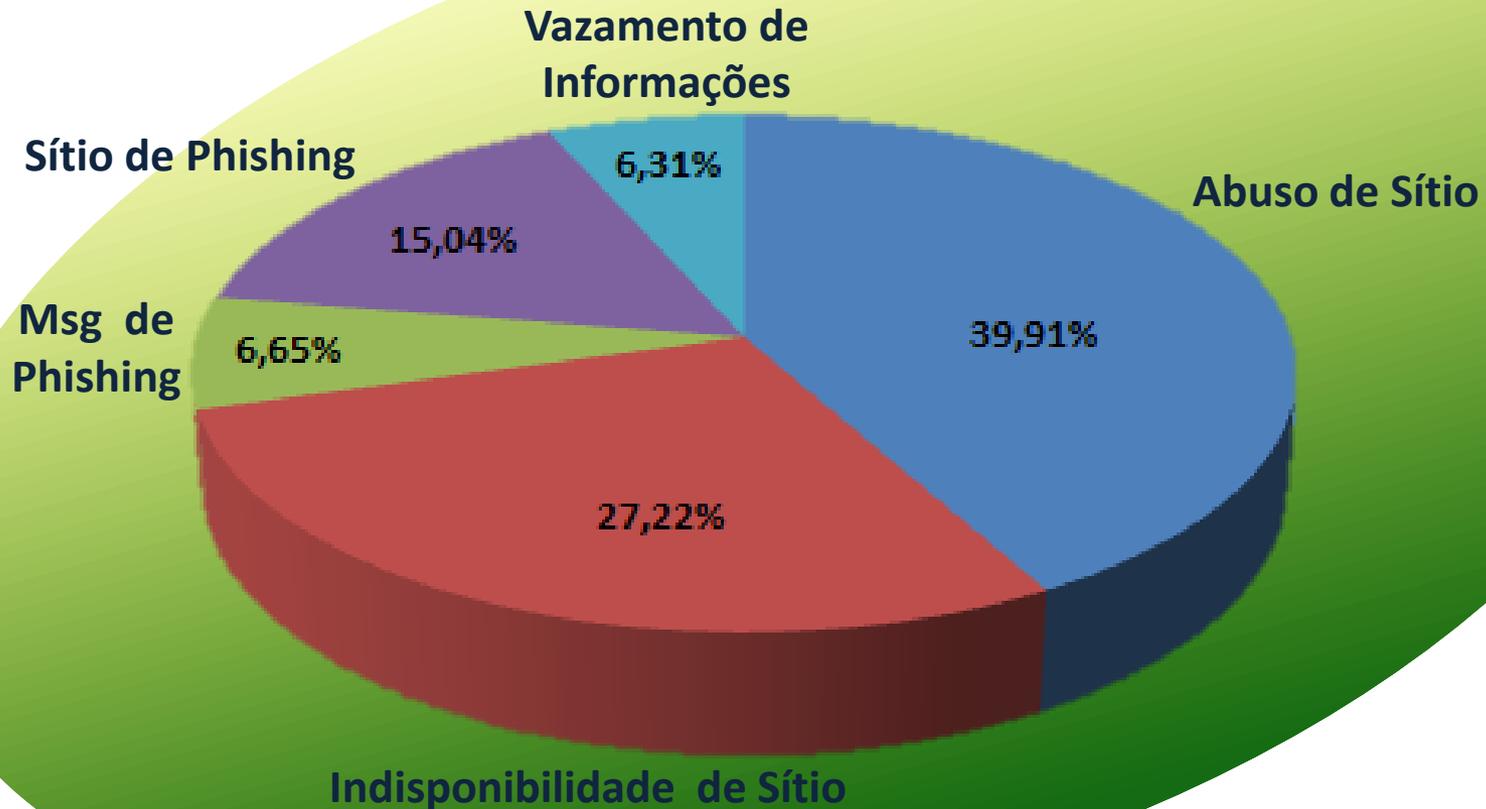


Vídeo 8: <https://www.youtube.com/watch?v=32JgSIYpL8o>

Vídeo 9: <https://www.youtube.com/watch?v=zcmmlFQGxMNU>



Principais Incidentes – APF (Jan a Jul/16)





Principais Tipos de Ataques em Grandes Eventos

Negação de Serviço (DDoS)



Abuso de Sítio



Engenharia Social

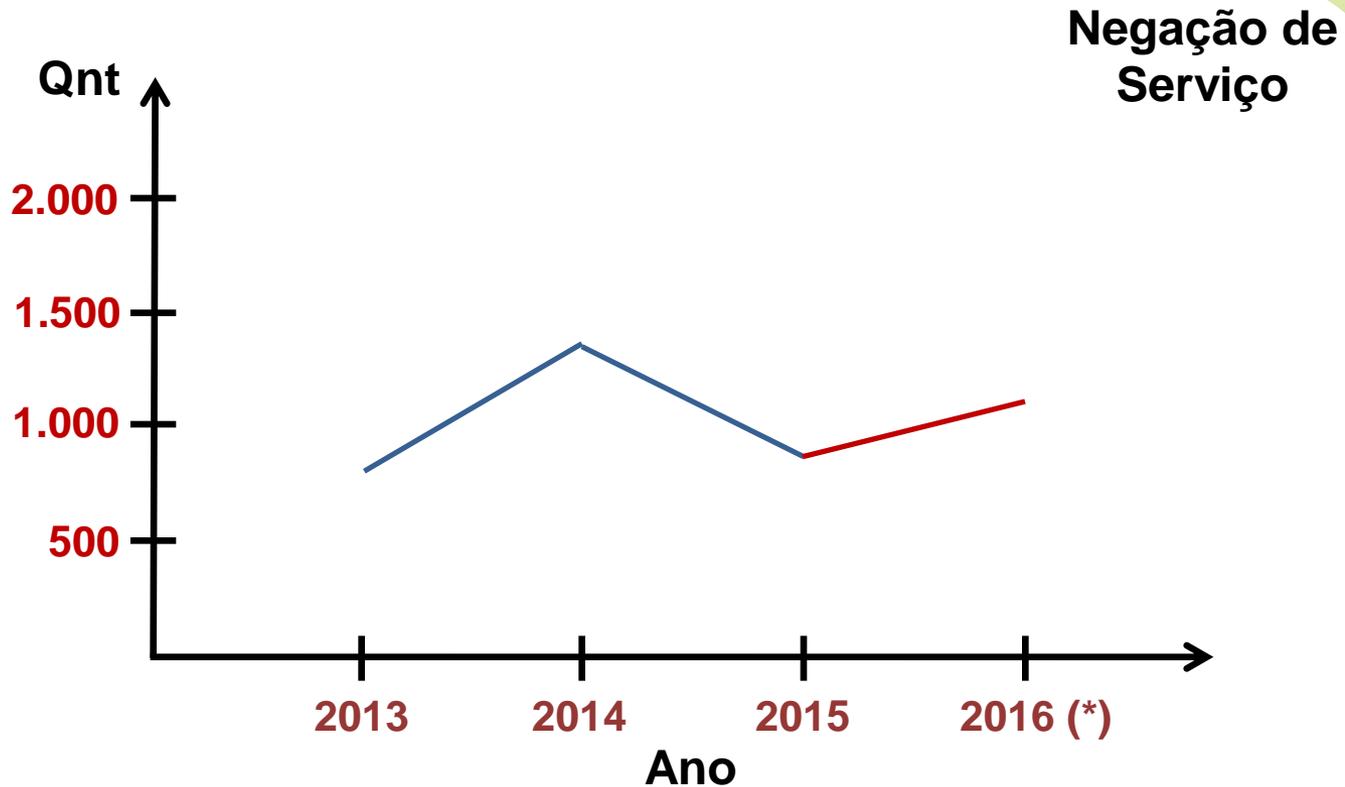


Exposição de Info Sensíveis





Negação de Serviço (*Distributed Denial of Service - DDoS*)





Negação de Serviço (*Distributed Denial of Service - DDoS*)

cert.br

Centro de Estudos, Resposta e Tratamento
de Incidentes de Segurança no Brasil

“Recomendações para Melhorar o
Cenário de Ataques Distribuídos de
Negação de Serviço (DDoS)”

<http://www.cert.br/docs/>



Engenharia Social

Pessoas

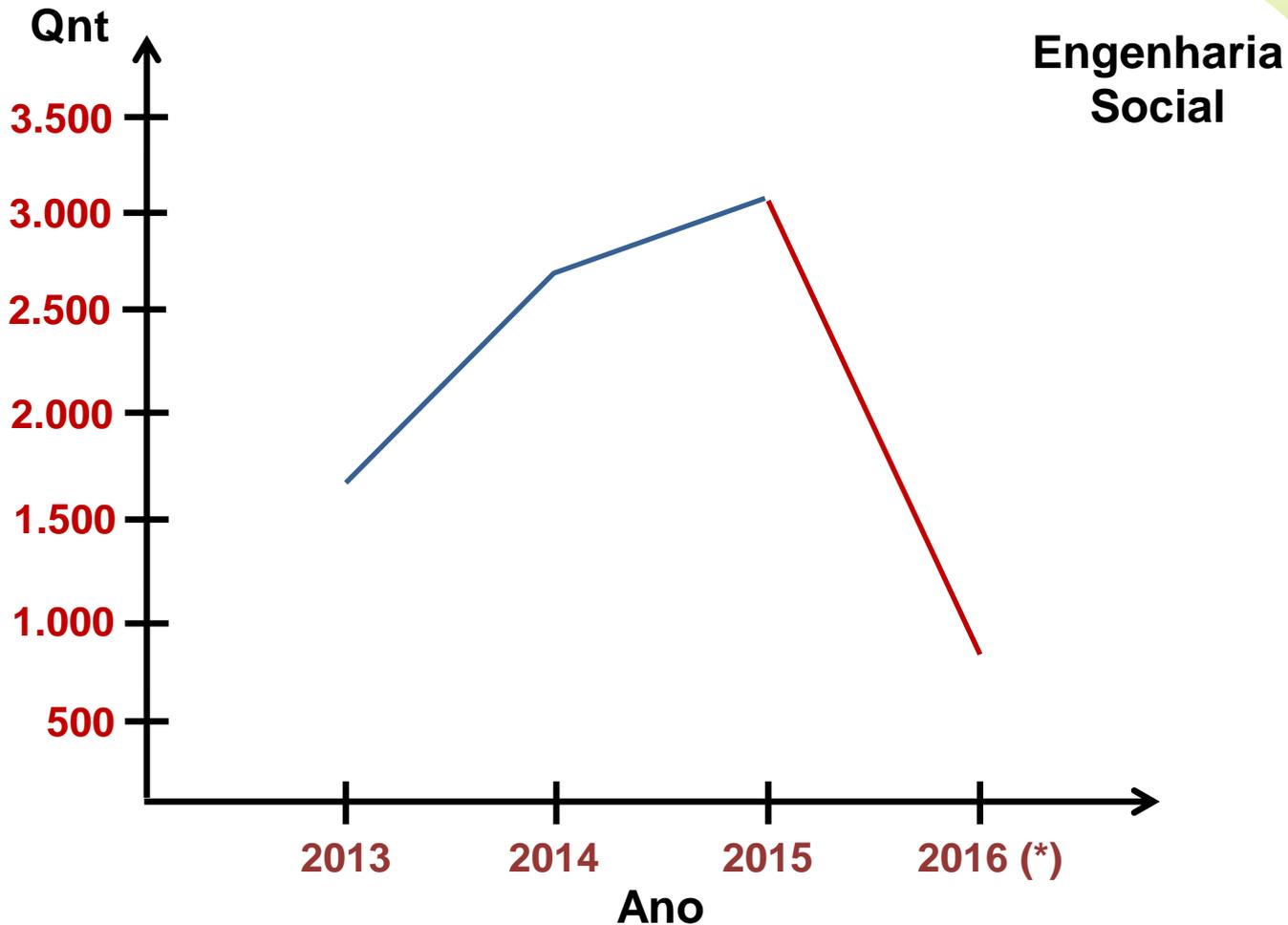
Ativo mais crítico das organizações



Capacitação, Treinamento, Sensibilização

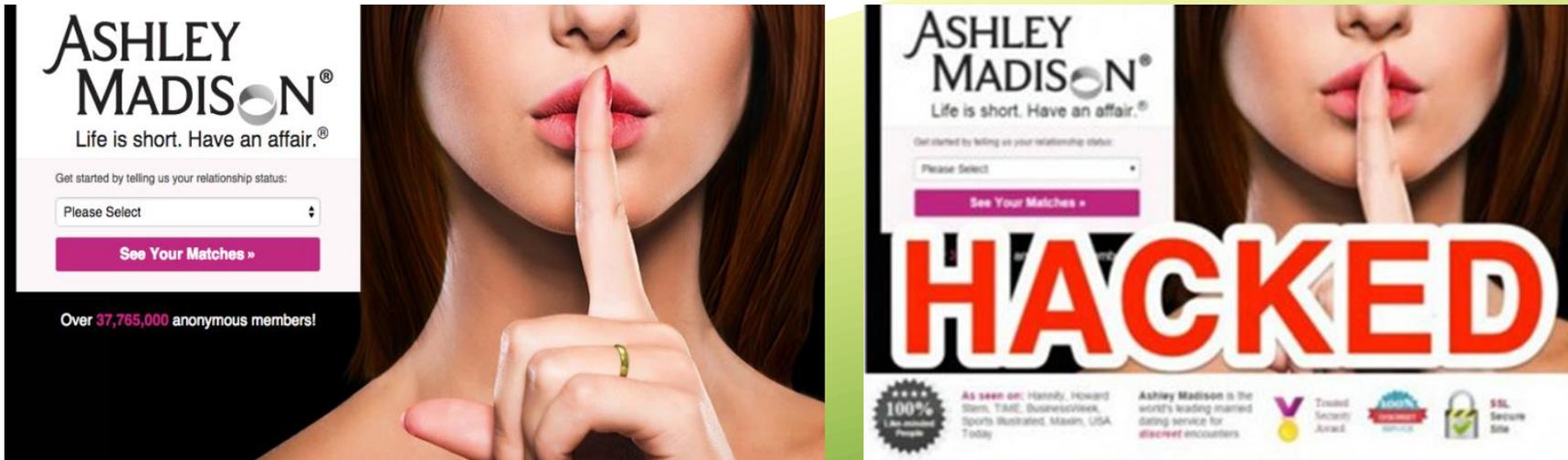


Engenharia Social





Exposição de Informações Sensíveis



- Grupo de hackers: *Impact Team*.
- Protesto à não exclusão total dos dados dos usuários que solicitavam a remoção dos seus dados.
- Exposição dos dados de mais de 37 milhões de usuários.
- Alvo de investigação na Comissão Federal de Comércio (FTC).



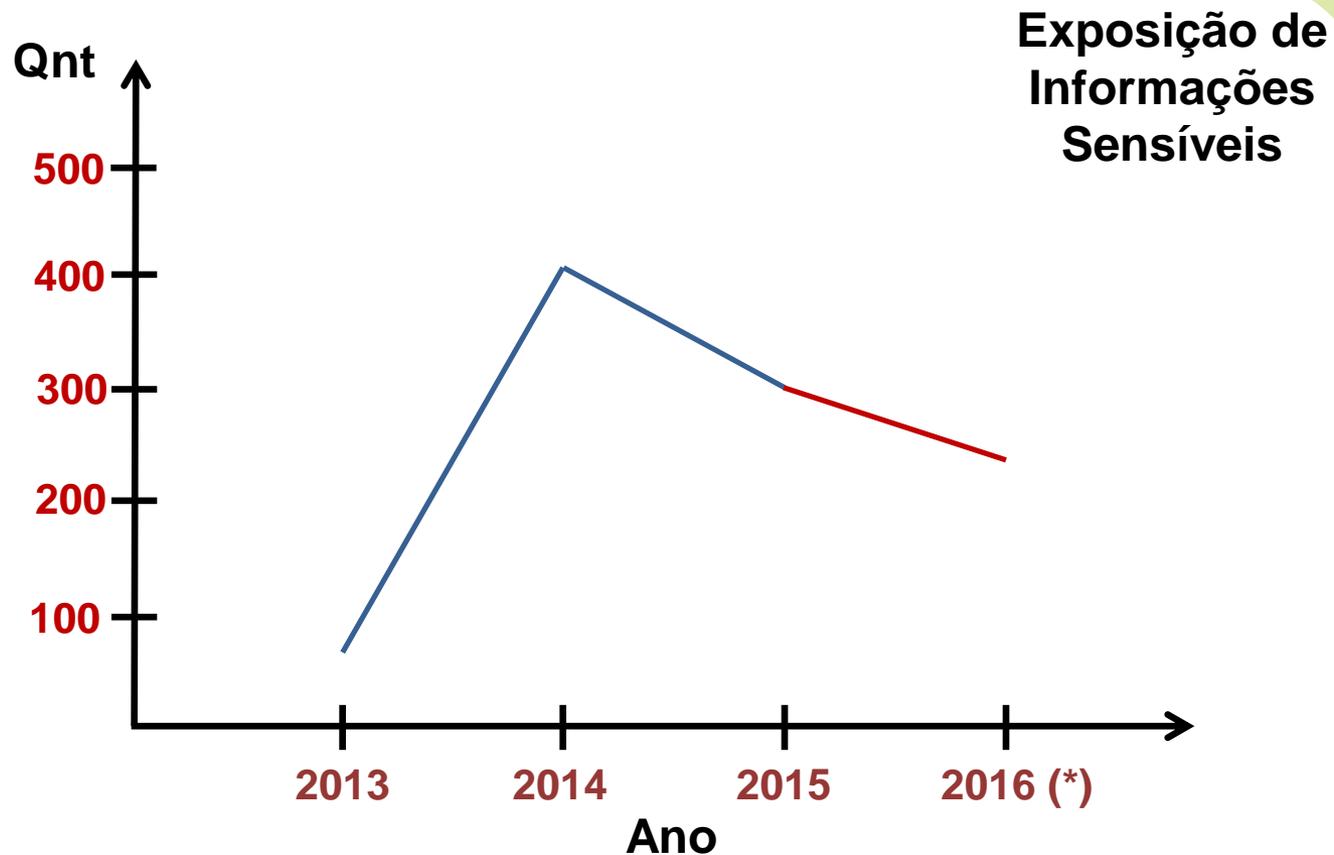
Exposição de Informações Sensíveis

- Aquisição / teste de software: preocupação com exfiltração de dados, atualizações e repositórios.





Exposição de Informações Sensíveis





Abuso de Sítio

Hacked By Anarchy Ghost

Hackeado por Sm0ld3r



Hoje é dia de cobrança e quem deve vai morrer !!



Abuso de Sítio



Hacked by **AlfabetoVirtual**

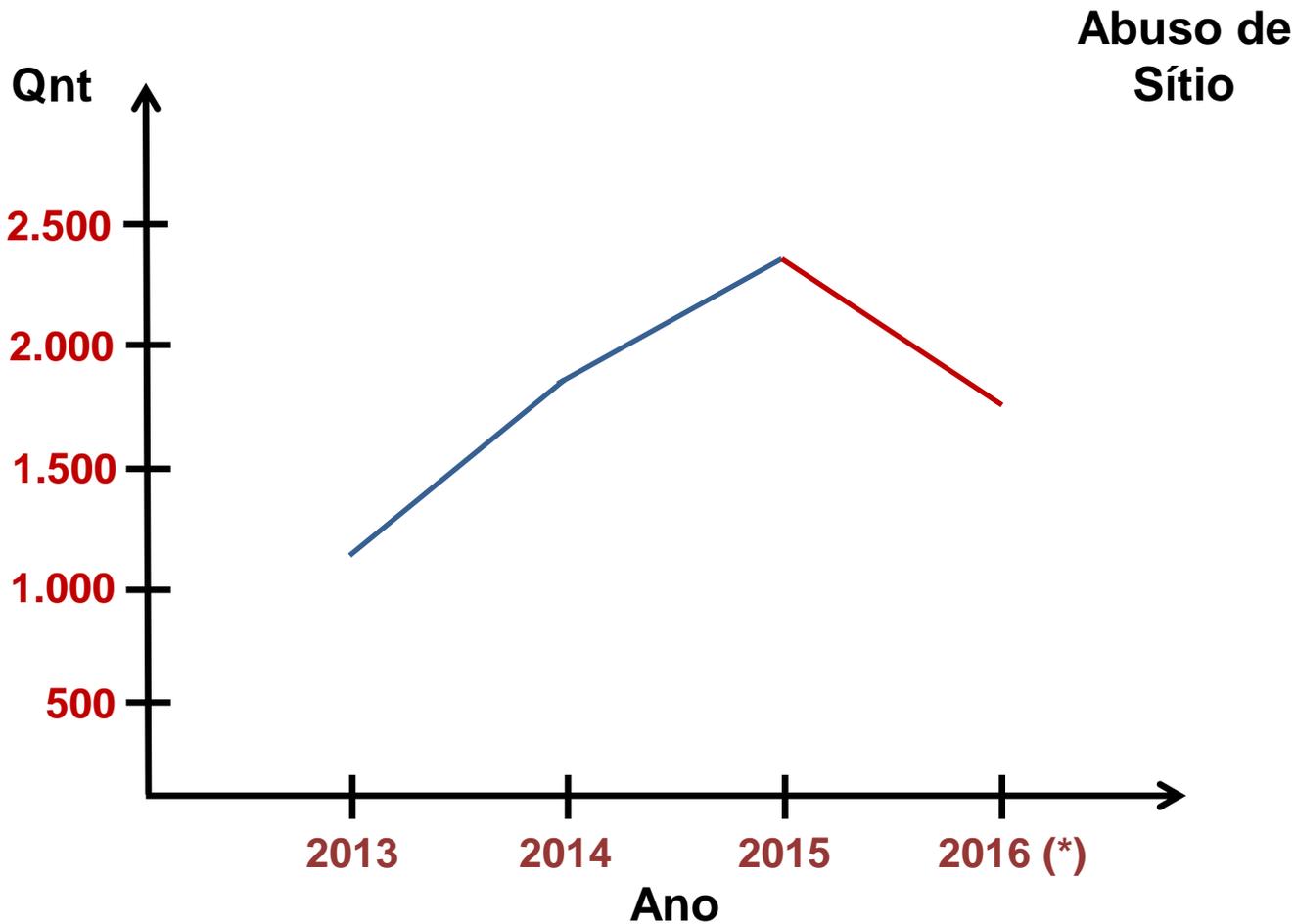
I'M NOT **GONNA CHANGE** FOR ANYONE.
I DON'T CARE WHAT PEOPLE THINK ABOUT ME, **THAT'S I AM**, AND PROUD OF IT.

Brazil: Dilma um beijo querida!





Principais Tipos de Ataque em Grandes Eventos





Sequência de um Ataque

1. Reconhecimento

2. Identificação do alvo

3. Comprometimento do sistema

4. Execução do ataque

5. Negação ou Divulgação

Ataque bem-sucedido



Protocolo de Notificações

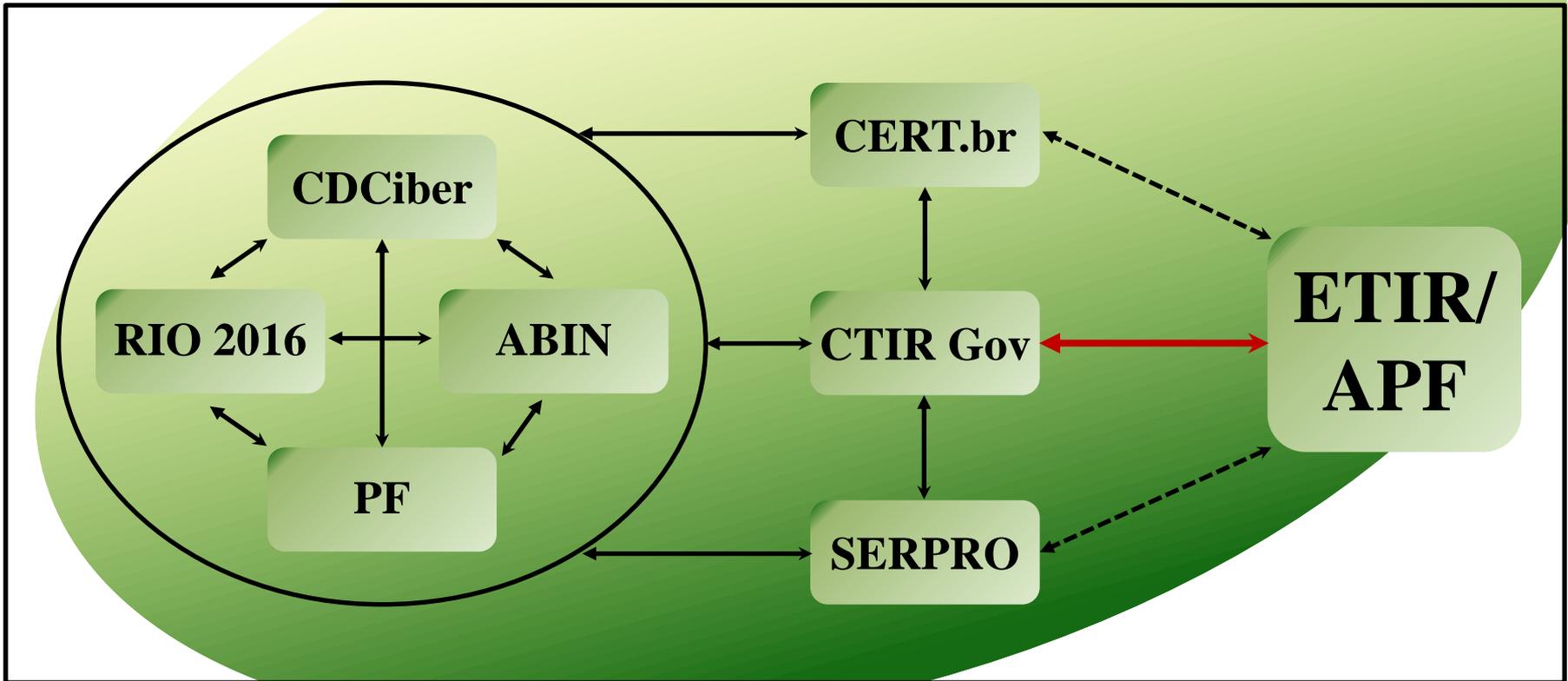
Princípios

Simplicidade
Objetividade
Clareza
Celeridade
Economia de meios



Protocolo de Notificações

Ligações





Protocolo de Notificações

Procedimentos

**Dias Úteis
(08:00 às 19:00 hs)**

**Dias não úteis e
dias úteis
(após às 19:00 hs)**



Dias Úteis (08:00 às 19:00 hs)

- A notificação deverá ocorrer pelo e-mail ctir@ctir.gov.br
- Diferença entre “Para” e “CC”.
- Inserir a Tag **[RIO2016]** no campo “Assuntos” nas mensagens que tenham relação com a segurança do evento.

- Caso o órgão deseje realizar maiores esclarecimentos:
 - Telefone INOC (**10954*810**); ou
 - Telefone de sobreaviso (**61-99995-7859**).

- Contato do CTIR Gov com os órgãos: **e-mail e Telefone.**



Dias não Úteis/dias Úteis (após às 19:00 hs)

- A notificação deverá ocorrer pelo e-mail ctir@ctir.gov.br
- O CTIR Gov também deverá ser contatado pelo telefone de sobreaviso ([61-99995-7859](tel:61-99995-7859)).
- Contato do CTIR Gov com os órgãos: **e-mail e telefone.**



Contatos

E-mail: ctir@ctir.gov.br

INOC-DBA BR: 10954*810

Sobreaviso (24 hs): 61-99995-7859

Chave PGP (pública):

<http://www.ctir.gov.br/arquivos/certificados/ctir2009.asc>



CONSIDERAÇÕES FINAIS

- **Crença no trabalho realizado.**
- **Respeito às características de todos os órgãos.**
- **Intensa disseminação de informações.**
- **Respeito aos ativos de informação dos órgãos.**
- **Reforço à mentalidade preventiva.**
- **Incentivo ao multi-preparo.**
- **Relevância ao uso de indicadores.**
- **Busca da resiliência.**
- **Cooperação, integração e confiança.**

**Fizemos Ontem,
Fazemos Hoje,
Faremos Sempre!**





Muito Obrigado!

arthur.sabbat@presidencia.gov.br

(61) 3411-4383