

# Ataques contra Sistemas Computacionais

**Marcus Botacin & André Grégio**

UFPR

2018

# Tópicos

- 1 Introdução
  - Segurança
- 2 Ataques
  - Impacto
  - Como funcionam ?
- 3 Sistemas Modernos
  - Boas e Más idéias
- 4 Considerações Finais
  - Referências

# Motivação

- **Objetivo:** Compreender como adversários (e artefatos) maliciosos atuam durante o comprometimento de um sistema.

# Ataques

## Ataque ou ameaça computacional

**Definição:** Uma ação direcionada contra um ou mais sistemas com o intuito de violar sua segurança.

## Pilares da Segurança

- **Confidencialidade:** privacidade.
- **Integridade:** não corrupção.
- **Disponibilidade:** acesso.

## Relembre:

Outras propriedades, como **confiabilidade**, **anonimidade** e **responsabilidade** são combinações dos pilares.

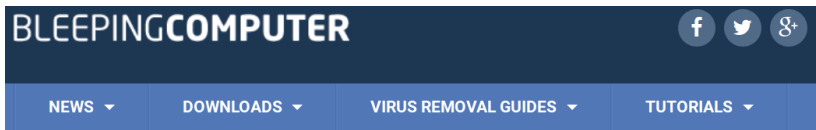
# Exemplos



Mobilidade > APPs, Criptografia

## WhatsApp implementa recursos de criptografia

**Figura: Confidencialidade:** Privacidade é uma propriedade derivada.



## CCleaner Compromised to Distribute Malware for Almost a Month

**Figura: Integridade:** Você checa o *checksum* ?

# Exemplos



## Volume de consultas ao IR provoca lentidão no site da Receita Federal

Figura: Disponibilidade: Um caso cotidiano



Figura: Disponibilidade: Um caso famoso.

# Princípios de Segurança

## Propriedades

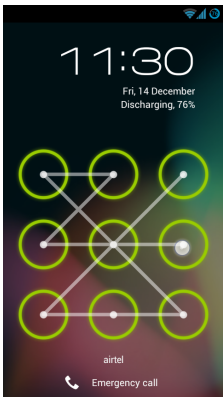
- Integridade
- Não-repúdio
- Confidencialidade
- Confiabilidade
- Disponibilidade
- Responsabilidade (*accountability*)
- Autenticidade
- Anonimidade

## Tecnologias

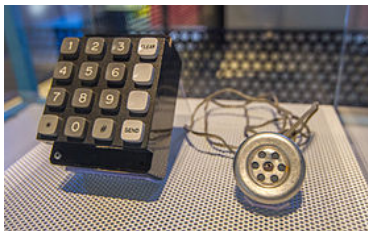
- Criptografia
- Controle de acesso (identificação, autorização, autenticação)
- Processos



# Exemplos



**Figura: Autenticação:** Exemplo Cotidiano.



**Figura: Autenticação:** Exemplo Histórico (*Blue Box*).

## Uma Falácia popular

# Site Seguro: a importância do cadeado verde para o seu negócio

Publicado / Atualizado 4 de Janeiro de 2018 por Gustavo Kennedy Renkel

Figura: Fonte: Secnet Blog

---

◀ VEJA TODOS OS POSTS

---

Quinta-feira, 05/11/2015, às 16:00, por Altieres Rohr

**Sites de Bradesco e HSBC perdem  
cadeado de site seguro; entenda**

Figura: Fonte: Altieres Rohr @ G1

# Uma Falácia popular



Alberto J Azevedo

[Follow](#)

Founder and CEO at SecOps — InfoSec Army, Dad, Information Security Specialist/Entrepreneur, International Speaker, Writer, Free Culture Enthusiast, DJ, ADHD...

Dec 12, 2017 · 5 min read

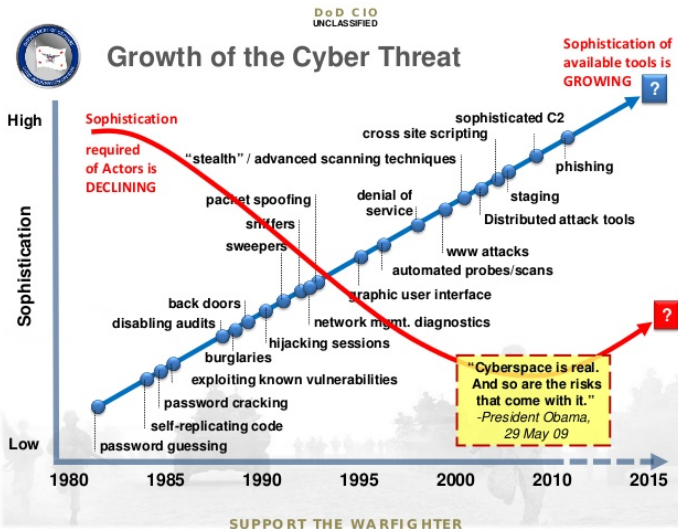
## Fantástico, como assim site falso não tem o cadeado?

Figura: Fonte: Alberto Azevedo @ Medium

# Tópicos

- 1 Introdução
  - Segurança
- 2 Ataques
  - Impacto
  - Como funcionam ?
- 3 Sistemas Modernos
  - Boas e Más idéias
- 4 Considerações Finais
  - Referências

# Evolução das Ameaças



Fonte: <http://www.slideshare.net/GTSCoalition/robert-carey-principal-cio>

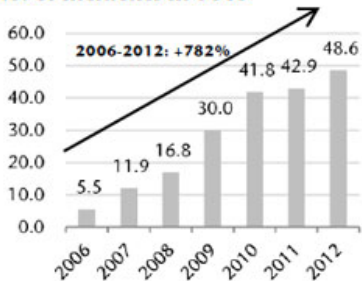
# Consequências das Ameaças

## \$\$\$ Perdas Financeiras!!!

- Danos à imagem
- Tomadas de decisão incorretas
- Implicações legais
- Injúrias físicas
- Violações em SLA
- Quebra de confidencialidade
- Impedimento na operação
- Perda/corrupção de dados

# Incidentes

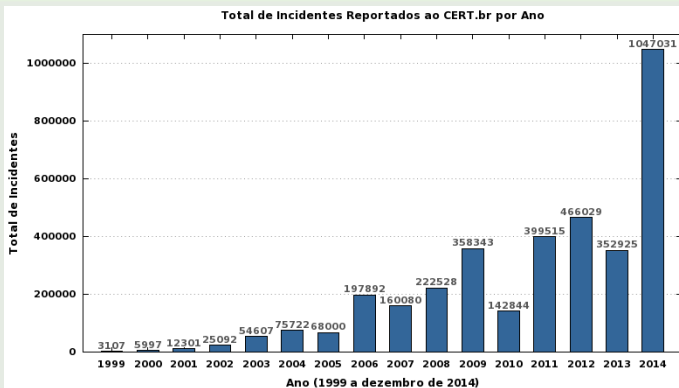
**Chart 1: Cyberattack Incidents  
Reported by Federal Agencies  
No. of Incidents in 000s**



Source: GAO, US-CERT data

# Incidentes @ BR (2014)

## Número de incidentes reportados

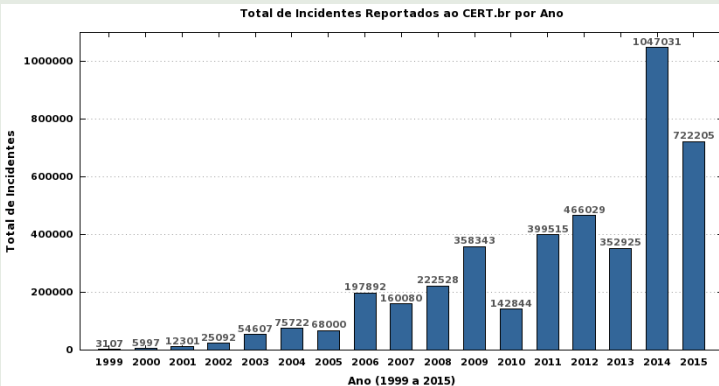


Fonte: <http://www.cert.br/stats/incidentes/>



# Incidentes @ BR (2015)

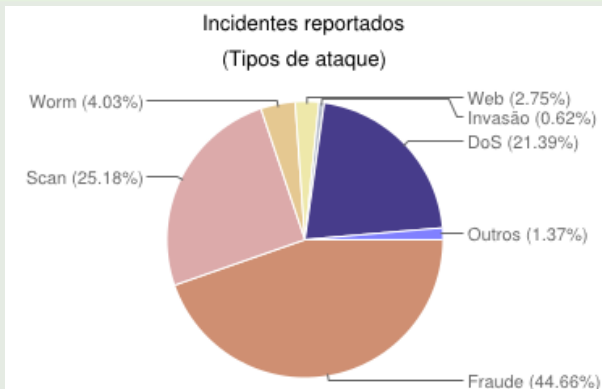
## Número de incidentes reportados



Fonte: <http://www.cert.br/stats/incidentes/>

# Ataques no Brasil (2014)

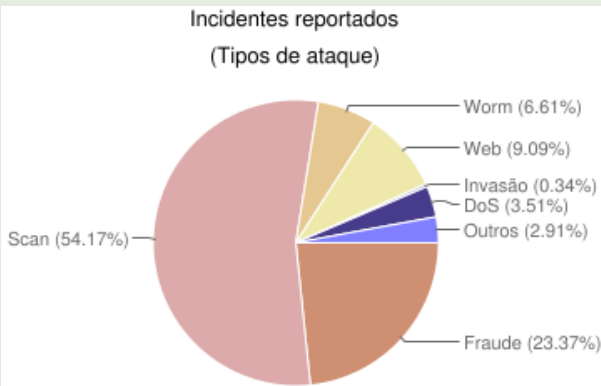
## Tipos de ataques



Fonte: <http://www.cert.br/stats/incidentes/>

# Ataques no Brasil (2015)

## Tipos de ataques



Fonte: <http://www.cert.br/stats/incidentes/>

# Tópicos

- 1 Introdução
  - Segurança
- 2 Ataques
  - Impacto
  - Como funcionam ?
- 3 Sistemas Modernos
  - Boas e Más idéias
- 4 Considerações Finais
  - Referências

# Passos de um Ataque

Um ataque consiste de um conjunto de etapas para ter sucesso:

- 1 Reconhecimento e enumeração;
- 2 Ganho de acesso (intrusão);
- 3 Manutenção do controle (persistência);
- 4 Ocultação de traços (limpeza);
- 5 [Fazer o alvo trabalhar para o atacante.]

# Reconhecimento



Figura: **Reconhecimento:** E você, reconhece isto ?

# Exemplos



**Figura: Reconhecimento:**  
*Wardriving.*



**Figura: Reconhecimento:**  
*Warflying.*

# Atividade Maliciosa



Figura: Trabalhando para o atacante.



# Atacantes

## Tipos de alvo

### 1 Alvos de oportunidade:

- Ataques não-direcionados;
- Buscam por sistemas vulneráveis aleatoriamente (varreduras por *ranges* inteiros);
- Exemplo: propagação de *worms*.

### 2 Alvos escolhidos:

- Ataques direcionados contra pessoas/instituições específicas;
- Envolvem melhor preparo para obtenção de sucesso;
- Dependem de **Engenharia Social**;
- Podem usar forja de identidade.

## Exemplo



TECNOLOGIA E GAMES

18/01/2011 09h32 - Atualizado em 18/01/2011 09h53

# Vírus que atrasou programa nuclear do Irã foi criado pelos EUA e por Israel

Figura: Ataque Direcionado: Stuxnet

# Ataques

## Meios de ataque

- **Físico:** envolve a destruição ou danos ao dispositivo.  
Ex.: incêndio, destruição do data center.
- **Eletrônico:** pulsos eletromagnéticos.  
Ex.: Tempest.
- **via Rede:** exploração por meio de sistemas remotamente conectados. Serão explorados nesta aula.

# Ataques

## Classes de ameaças

- **Disseminação/Exposição (*Disclosure*).**  
Acesso não autorizado a informação.
- **Enganação (*Deception*).**  
Aceitação de dados falsos/forjados.
- **Disrupção (*Disruption*).**  
Interrupção da operação “normal”.
- **Usurpação (*Usurpation*).**  
Controle não autorizado de um sistema (ou parte dele).

# Tópicos

- 1 Introdução
  - Segurança
- 2 Ataques
  - Impacto
  - Como funcionam ?
- 3 **Sistemas Modernos**
  - Boas e Más idéias
- 4 Considerações Finais
  - Referências

# Avalie

- Carros Inteligentes (Conectados)
- Casas Inteligentes/Internet das Coisas (Conectados)
- Cidades Inteligentes (Conectados)
- Marcapassos Inteligentes (Conectados)

## Carros Conectados



Figura: Falhas: Autenticação e Isolamento.

# Casas Conectadas

**SECURELIST**

THREATS ▾

CATEGORIES ▾

TAGS ▾

ENCYCLOPEDIA

RESEARCH

## IoT hack: how to break a smart home... again


By [Andrey Muravitsky](#), [Vladimir Dashchenko](#), [Roland Sako](#) on February 27, 2018. 10:00 am

Figura: **Falhas:** Todas.



# Cidades Conectadas



 Mundo

## Entediado em congestionamento, analista de TI invade outdoor e exibe pornô

Figura: **Falhas:** Autenticação.

# Dispositivos de saúde conectados



Figura: **Falhas:** Isolamento.

# Tópicos

- 1 Introdução
  - Segurança
- 2 Ataques
  - Impacto
  - Como funcionam ?
- 3 Sistemas Modernos
  - Boas e Más idéias
- 4 Considerações Finais
  - Referências

# Referências

## Livros

- A arte de enganar, Kevin Mitnick.
- The Cuckoo's Egg, Clifford Stoll.

## Filmes

- Jogos de Guerra (*Wargames*), 1983

# That's All Folks!

Contato

[mfbotacin@inf.ufpr.br](mailto:mfbotacin@inf.ufpr.br)