Ataques contra Sistemas Computacionais

CI1007

André Grégio
gregio@inf.ufpr.br

DInf/UFPR

4 de abril de 2024

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 (*integridade*, *confidencialidade* e/ou *disponibilidade*).

Relembre:

Pilares da Segurança

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

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

Exemplos

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

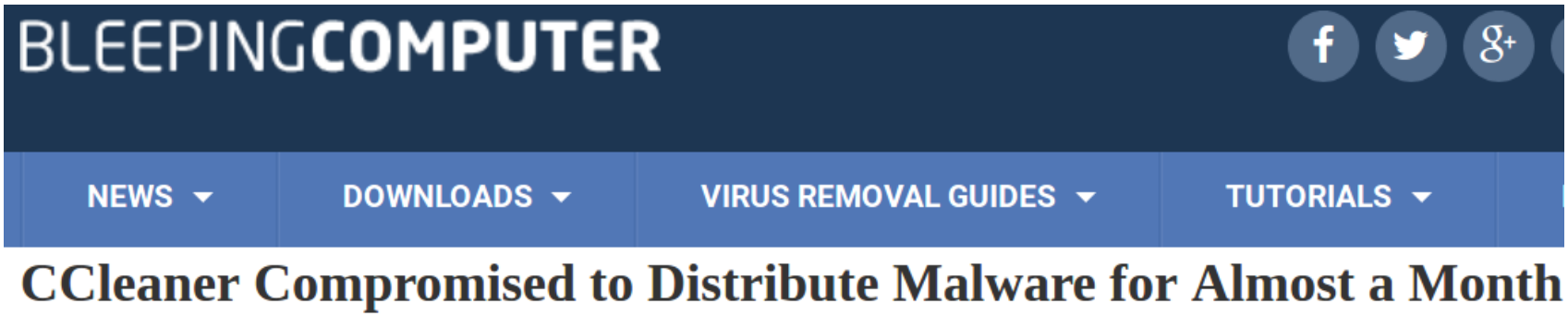


Figura: **Integridade**: Você checa o *checksum* ?

Exemplos

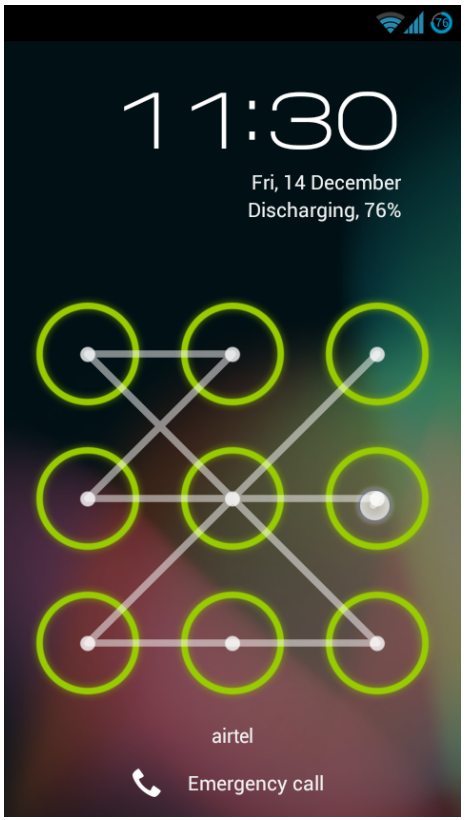


Figura: **Autenticação**: Exemplo Cotidiano.

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 Entusiast, DJ, ADHD...

Dec 12, 2017 · 5 min read

Fantástico, como assim site falso não tem o cadeado?

Figura: Fonte: Alberto Azevedo @ Medium

Revisão: Princípios de Segurança

Propriedades

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

Tecnologias

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

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).

Ataques

Espionagem (*snooping*)

- Interceptação da informação.
- Pode levar a **Exposição** não autorizada de dados sensíveis.
- Ataque Passivo → Escuta/Leitura/Acesso a comunicações/arquivos/informações.
- e.g. Escuta telemática/grampo (*wiretapping*), monitoração de redes (*sniffing*).
- Viola a **confidencialidade**.

Ataques

Modificação (ou Alteração)

- Mudança (não autorizada) da informação.
- Objetivo é **Enganação**:
  confiança em dados incorretos induz as ações posteriores!
- Leva a **Disrupção** e **Usurpação**:
  Dados modificados podem controlar operações no sistema atacado.
- Ataque Ativo → Resulta em mudanças na informação.
- e.g. Escuta ativa (*man-in-the-middle*).
- Viola a **Integridade**.

Ataques

Mascaramento (or Forja)

- Personificação da "identidade".
- **Enganação** e **Usurpação**:
  Faz com que uma ponta da comunicação acredita que a outra ponta é uma entidade diferente.
- Ataque Passivo[1] ou Ativo[2]:
  1. A vítima meramente acessa a entidade forjada (ex.: leitura de uma notícia falsa em uma página Web comprometida).
  2. O "falsificador" engana o usuário quanto a sua identidade (ex.: *site* clonado requer que a vítima dê suas credenciais).
- Viola a **Integridade (Autenticação)**.
- Delegação de autoridade é uma forma "legítima" de mascaramento. Todas as partes estão cientes de que uma parte irá atuar em nome de outra.

Ataques

Repúdio da origem

- É uma falsa negativa de que uma entidade **enviou/criou** algum objeto ou dado.
- **Enganação** $\rightarrow$ Pode resultar em prejuízos ($).
- Ex.: um acordo duvidoso que resulta em um vendedor (vítima) enviando o produto e não recebendo o pagamento porque o comprador (atacante) repudia a transação.
- Viola a **Integridade**.

Ataques

Negativa de recebimento

- É uma falsa negativa de que uma entidade **recebeu** algum objeto/dado.
- **Enganação** $\rightarrow$ Pode resultar em prejuízos (\$).
- Ex.: um vendedor envia um produto após o pagamento do cliente. O cliente recebe o produto, mas abre uma disputa dizendo que não o recebeu. O vendedor envia um novo produto sem custo para o cliente.
- Viola a **Integridade** e a **Disponibilidade**.

Ataques

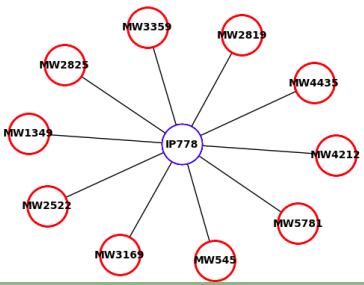
Atraso

- Inibição temporária de um serviço.
- **Usurpação**[1], mas pode auxiliar na **Enganação**[2]:
  1. Se um atacante manipula estruturas de controle de um sistema ou rede, pode forçar a demora na entrega de um dado.
  2. Quando uma entidade espera por uma autorização atrasada, o atacante pode "mascarar" um servidor secundário que provê informações incorretas.
- Viola a **Disponibilidade**.

Ataques

Negação de serviço (DoS)

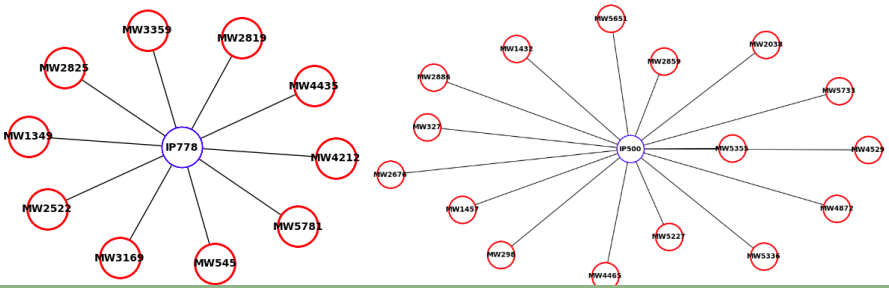
- Inibição de um serviço a longo prazo (*atraso infinito*).
- **Usurpação**[1], em geral usada c/ outro mec. p/ **Enganação**[2]:
  1. Impede um servidor de obter recursos (*DoS na origem*) ou atender requisições de clientes (*DoS no destino*), ou descarta mensagem de um ou ambos os lados da comunicação (*DoS no caminho intermediário*).
  2. Origem do ataque $\rightarrow$ geralmente forjada; o atacante pode bloquear o servidor legítimo e desviar o tráfego dos clientes para servidores comprometidos.
- Viola a **Disponibilidade**.



Ataques

Negação de serviço (DoS)

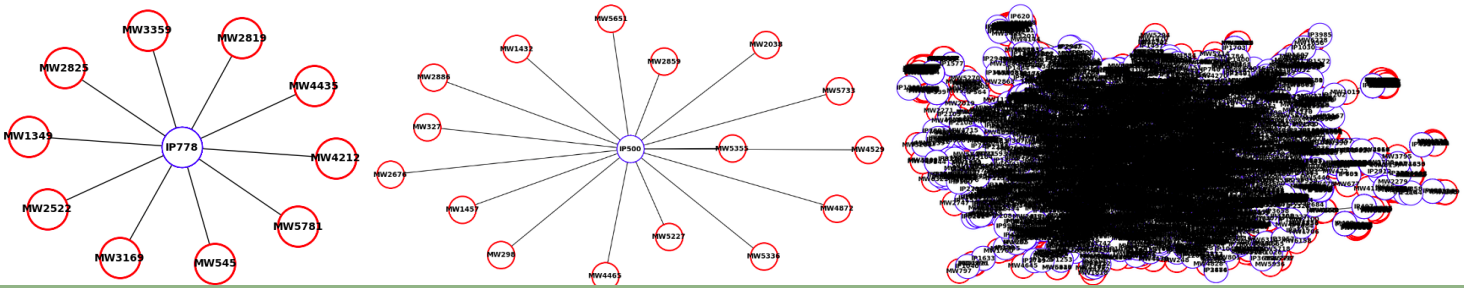
- Inibição de um serviço a longo prazo (*atraso infinito*).
- **Usurpação**[1], em geral usada c/ outro mec. p/ **Enganação**[2]:
  1. Impede um servidor de obter recursos (*DoS na origem*) ou atender requisições de clientes (*DoS no destino*), ou descarta mensagem de um ou ambos os lados da comunicação (*DoS no caminho intermediário*).
  2. Origem do ataque → geralmente forjada; o atacante pode bloquear o servidor legítimo e desviar o tráfego dos clientes para servidores comprometidos.
- Viola a **Disponibilidade**.



Ataques

Negação de serviço (DoS)

- Inibição de um serviço a longo prazo (*atraso infinito*).
- **Usurpação**[1], em geral usada c/ outro mec. p/ **Enganação**[2]:
  1. Impede um servidor de obter recursos (*DoS na origem*) ou atender requisições de clientes (*DoS no destino*), ou descarta mensagem de um ou ambos os lados da comunicação (*DoS no caminho intermediário*).
  2. Origem do ataque → geralmente forjada; o atacante pode bloquear o servidor legítimo e desviar o tráfego dos clientes para servidores comprometidos.
- Viola a **Disponibilidade**.

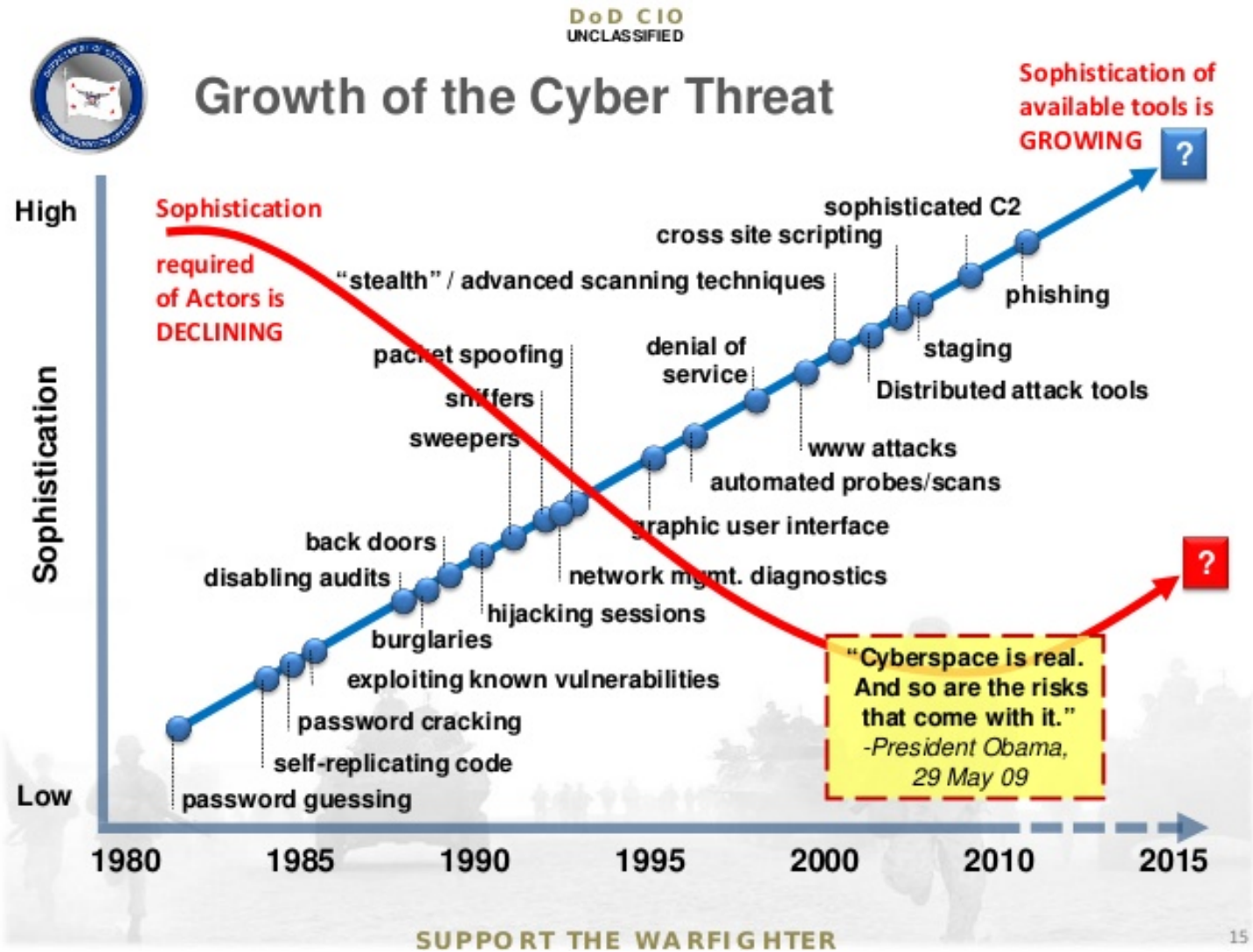


Ataques

Outros exemplos

- **Ataques contra senhas:**
  - força-bruta por esgotamento de variações;
  - ataques de dicionário;
  - *keyloggers* que capturam a senha enquanto o usuário a digita.
- **Ataques na camada de aplicação:**
  - Protocolos de aplicação podem ter vulnerabilidades;
  - Serviços podem estar mal configurados;
  - Podem ocorrer do lado cliente ou do lado servidor.

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

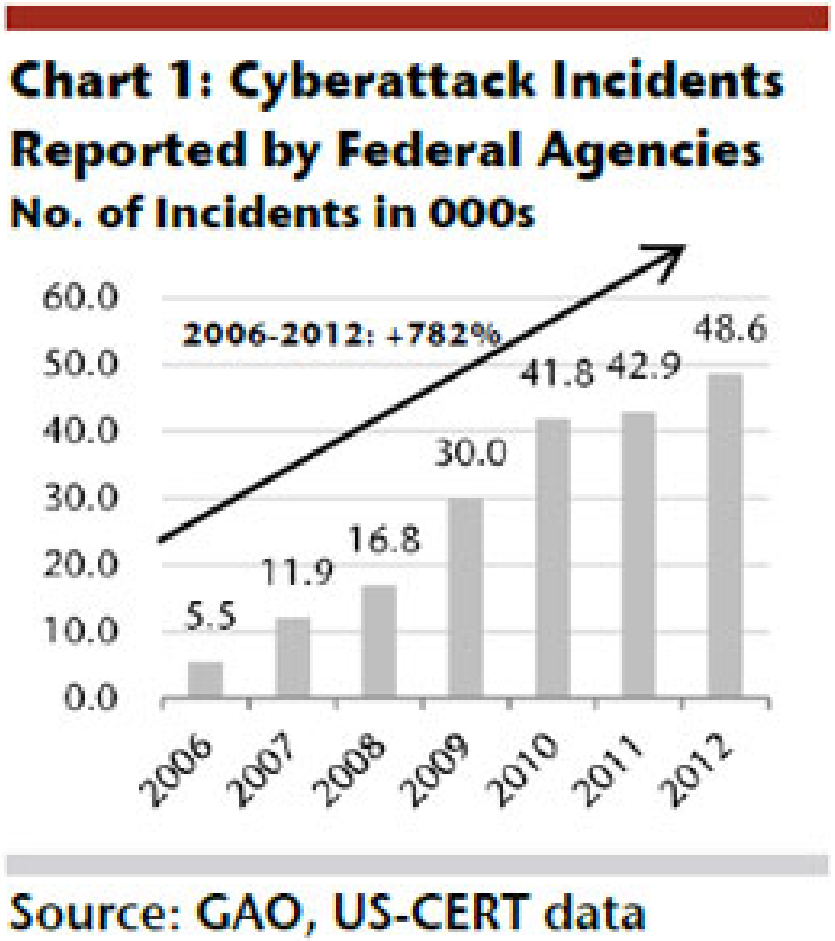
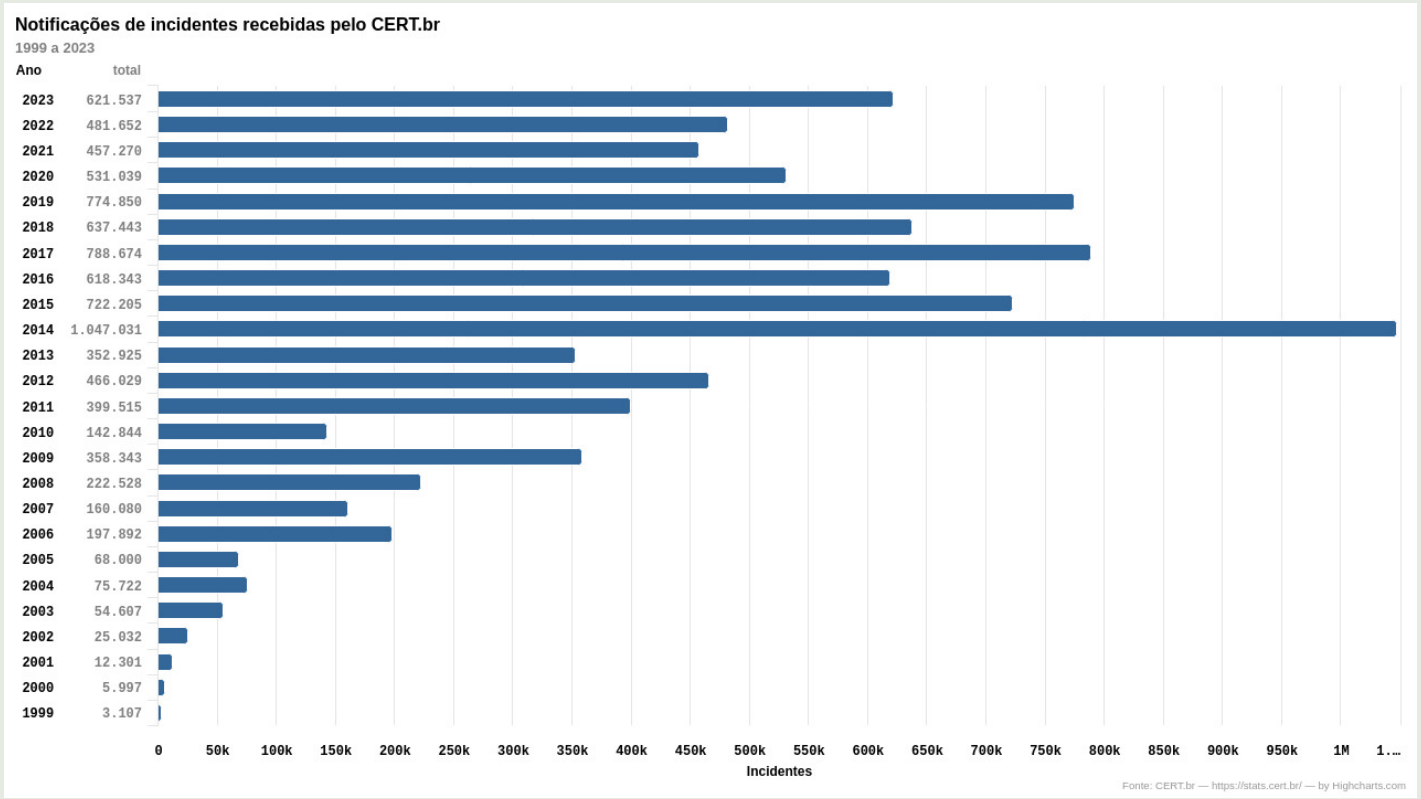


Chart 1: Cyberattack Incidents
Reported by Federal Agencies
No. of Incidents in 000s
60.0
50.0
40.0
30.0
20.0
10.0
0.0
2006-2012: +782%
5.5
11.9
16.8
30.0
41.8
42.9
48.6
2006
2007
2008
2009
2010
2011
2012
Source: GAO, US-CERT data

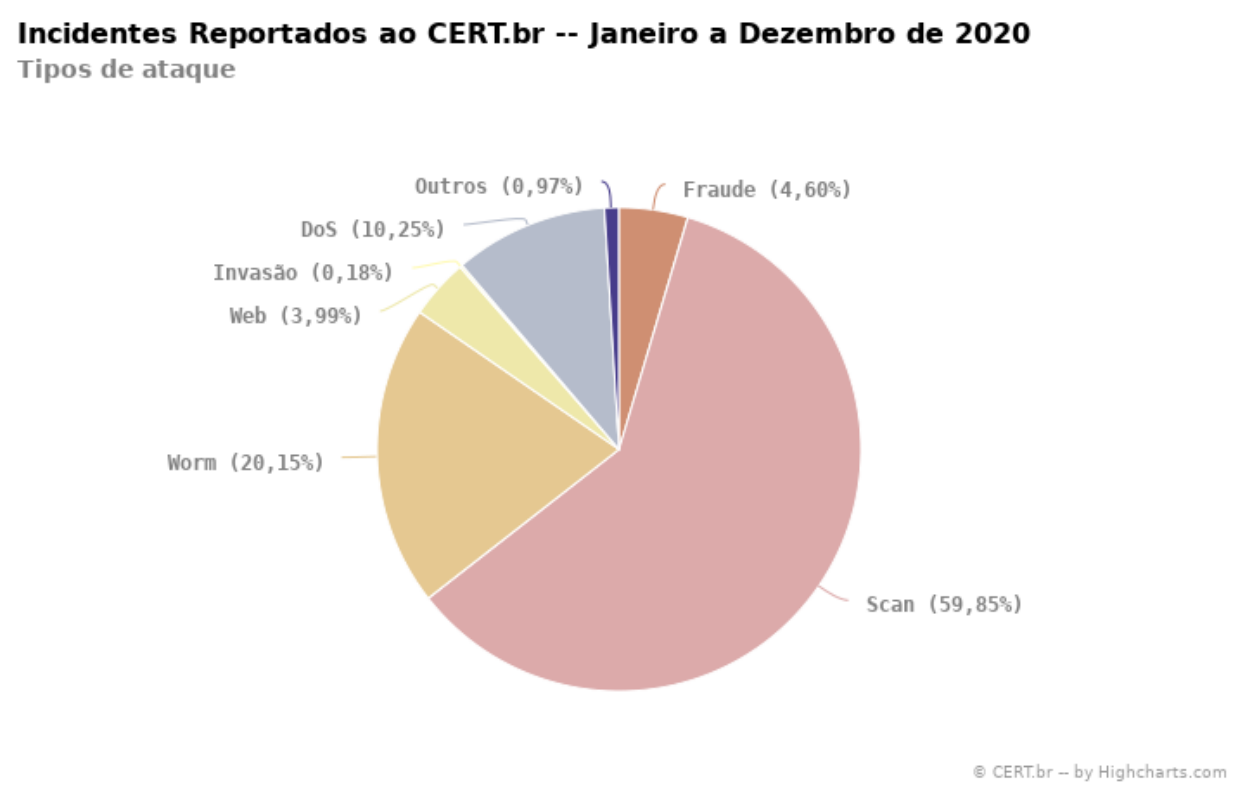
Número de incidentes reportados



Fonte: `https://stats.cert.br/incidentes/`

Ataques no Brasil (2020)

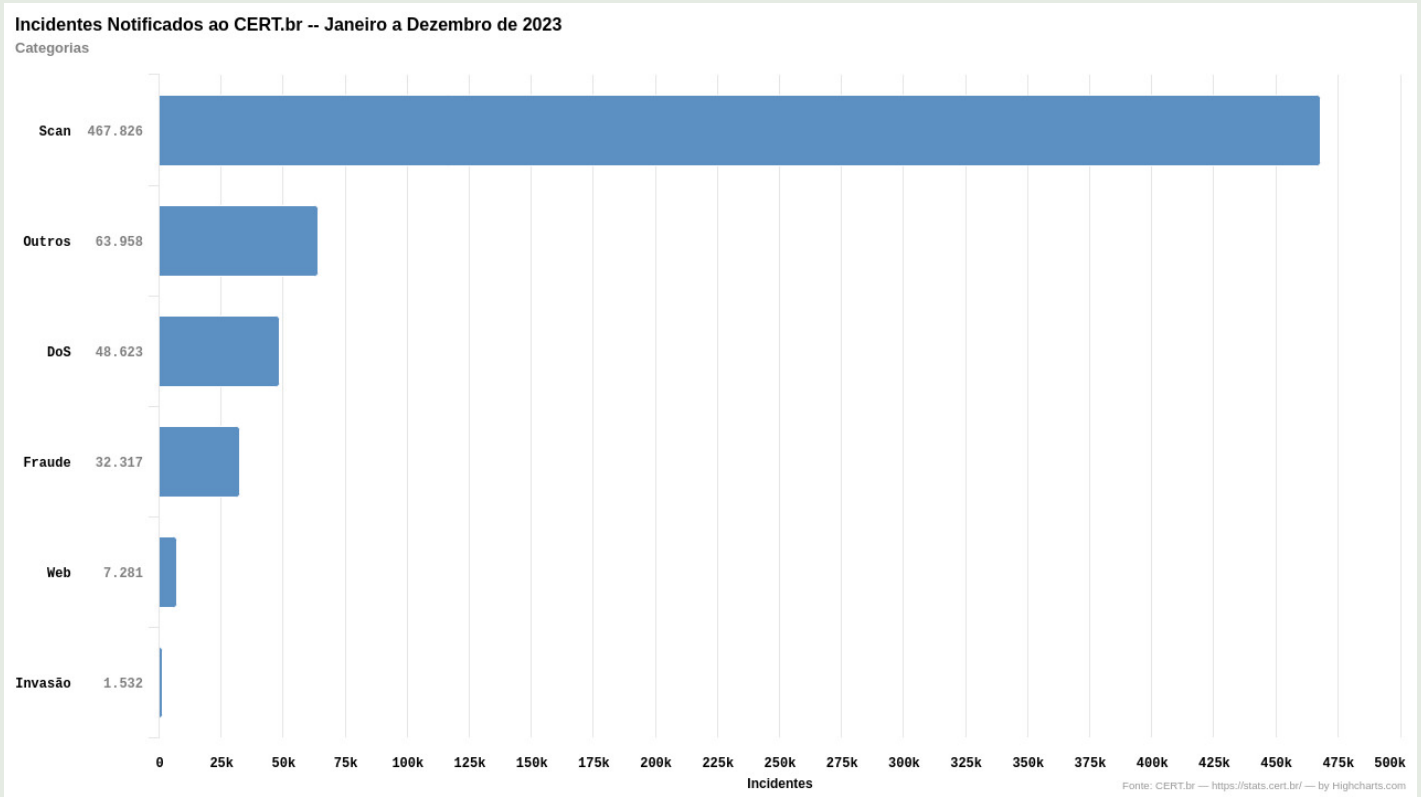
Tipos de ataques



Fonte: `http://www.cert.br/stats/incidentes/`

Incidentes @ BR (2023)

Tipos de Ataques



Fonte: `https://stats.cert.br/incidentes/`

Categorias de ataques

- **DoS (DoS – Denial of Service):** notificações de ataques de negação de serviço, onde o atacante utiliza um computador ou um conjunto de computadores para tirar de operação um serviço, dispositivo ou rede.
- **Invasão:** um ataque bem sucedido que resulte no acesso não autorizado a um computador ou rede.
- **Outros:** notificações de incidentes que não se enquadram nas demais categorias.

Categorias de ataques

- **Scan:** engloba além de notificações de varreduras em redes de computadores (scans), notificações envolvendo força bruta de senhas, tentativas mal sucedidas de explorar vulnerabilidades e outros ataques sem sucesso contra serviços de rede disponibilizados publicamente na Internet.
- **Web:** um caso particular de ataque visando especificamente o comprometimento de servidores web ou desfigurações de páginas na Internet.

Categorias de ataques

- **Fraude:** engloba as notificações de tentativas de fraude, ou seja, de incidentes em que ocorre uma tentativa de obter vantagem, que pode ou não ser financeira. O uso da palavra fraude é feito segundo Houaiss, que a define como "qualquer ato ardiloso, enganoso, de má-fé, com intuito de lesar ou ludibriar outrem, ou de não cumprir determinado dever; logro". Esta categoria, por sua vez, é dividida nas seguintes sub-categorias:
  - *Phishing:* notificações de casos de páginas falsas, tanto com intuito de obter vantagem financeira direta (envolvendo bancos, cartões de crédito, meios de pagamento e sites de comércio eletrônico), quanto aquelas em geral envolvendo serviços de webmail, acessos remotos corporativos, credenciais de serviços de nuvem, entre outros.
  - *Malware:* notificações sobre códigos maliciosos utilizados para furtar informações e credenciais.

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.

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.]

Atividade Maliciosa

ADRENALINE

MENU | TENDÊNCIAS | ANÁLISES | PROGRAMAS | VÍDEOS | PRODUTOS | ARQUIVO | FÓRUM

SEÇÕES: AMD | Intel | Nvidia | Apple | Google | Carro | Hardware | PC Games | Microsoft | Tech | Mobile

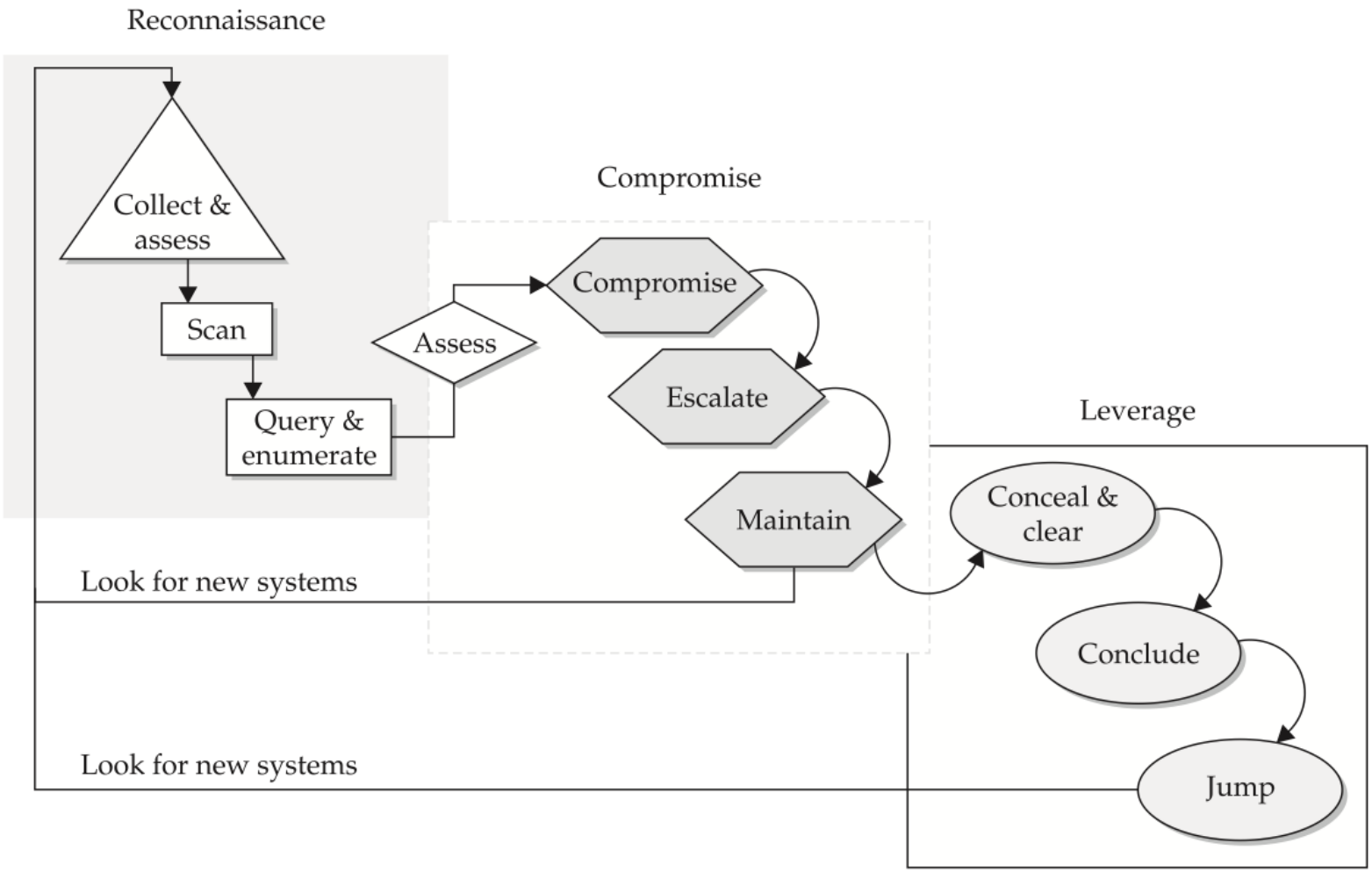
INTERNET | SEGURANÇA

Sites brasileiros começam a minerar bitcoin usando PCs dos usuários sem avisar

10/11/2017 11:21 | João Gabriel | @joao_gan | Reportar erro

Figura: Trabalhando para o atacante.

Modelagem de Ataques



Fonte: Hack Notes - Network Security Portable Reference. Mike Horton, Clinton Mugge. McGraw-Hill, 2003.

Reconhecimento

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

Exemplos

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

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

Reconhecimento

- **Levantamento de dados do alvo:**
  Obtenção de informações publicamente disponíveis (estrutura do alvo, informações de funcionários, domínios/endereços IP; determinação de quais dadosusar na varredura).
  - **Varredura:**
    Processo para identificar recursos "acessíveis" na rede ou sistema alvo.
  - **Enumeração:**
    Obtenção de detalhes sobre os recursos *online* identificados (versão do SO, serviços em execução, vulnerabilidades).

Reconhecimento

Coleta de informações

- Identificação de domínios
  - `whois <DOMÍNIO>`
- Identificação de endereços IP (*hostnames comuns*, como *ns1*, *ns2*, *www*, *smpt*...
  - `dig, nslookup`
- Enumeração de serviços "disponíveis"
  - `nmap -T5 -iL <LISTA DE ALVOS>`

NMap - Exemplo

Adversário

```
nmap -T4 -sV <TARGET_IP>
```

Vítima

Nmap scan report for TARGET_IP (xxx.y.y.zz)
Not shown: 993 closed ports
PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 3.0.2
22/tcp open ssh (protocol 2.0)
53/tcp open domain
80/tcp open http Apache httpd 2.4.7 ((Ubuntu))
389/tcp open ldap OpenLDAP 2.2.X - 2.3.X
3000/tcp open ntop-http Ntop web interface 5.0.1
12345/tcp open netbus?
...
Service Info: OS: Unix

Nmap done: 1 IP address (1 host up) scanned in 13.93 seconds

NMap - Tipos de Varredura

- `TCP connect() Scan [-sT]`: Tenta conectar em cada porta e, se obtiver sucesso, reporta como *open*. Facilmente detectável por *firewalls* e IDS. Servidores registram a origem da conexão.
- `SYN Stealth [-sS]`: "Meia" conexão. Detecta portas abertas (S, S/A, R); fechadas (S, R); filtradas (S, `drop` silencioso).
- `Ping [-sP]`: Verifica computadores online. 1^o método: ICMP Echo Request (se Reply, sistema está de pé com ICMP desbloqueado). 2^o método: TCP Ping (S ou A para 80, aguarda A ou R).

NMap - Tipos de Varredura

- TCP *flags*:
  - `FIN [-sF]` (F); `Null [-sN]` (nenhuma *flag*); `Xmas Tree [-sX]`: (F, U, P).
  - Funcionam em implementações de TCP/IP aderentes à RFC 793.
  - MS-Win não segue a RFC → combinação de varredura SYN com uma dessas pode servir para identificar máquinas Windows.
- `Version detection [-sV]`: obtém nome e número de versão dos serviços em execução nas portas varridas.

Intrusão

- **Comprometimento inicial:**
  Algum nível de acesso é alcançado. O atacante está dentro!
- **Escalada:**
  Ganho de privilégios adicionais (na vítima ou na rede).
- **Manutenção de acesso:**
  Eliminação da vulnerabilidade explorada na intrusão. Preparo do "retorno" (ex.: abrindo uma porta ou serviço remoto).

Alavancagem

- **Ocultando rastros:**
  Listagem das atividades realizadas e artefatos gerados para remoção de evidências;
- **Conclusão das atividades pretendidas:**
  Ex.: Atacante corrige vulnerabilidade explorada para evitar perder a máquina.
- **Trampolim:**
  Migração para outro *host* (volta à fase de reconhecimento ou abusa alguma credencial já obtida).

Atividades Subversivas

Programas maliciosos podem fazer as seguintes atividades subversivas/suspeitas:

1. Coleta de dados (sensíveis)
2. Ocultação de presença
3. Comunicação dissimulada
4. Comando e controle

Fonte: Exploiting Software - How to Break Code. Greg Hoglund, Gary McGraw. Addison Wesley, 2004.

Atividades Subversivas

Coleta de dados

- Captura de pacotes (*sniffing*):
  - Monitoração de tráfego de redes.
- Captura de pressionamento de teclas:
  - Pode haver captura de *screenshots* ou área abaixo/ao redor do clique do *mouse*.
  - Feita em geral por *spyware* (*keyloggers*) para roubo de senhas.
- Escoamento de bancos de dados:
  - Má-configuração pode levar ao vazamento de informações.

Atividades Subversivas

Ocultação

- Ocultação de arquivos (inclusive logs):
  - Ex.: desabilitar e apagar o histórico; remover os registros do EventViewer (no Windows); deletar arquivos temporários ou artefatos gerados na intrusão; modificação de atributos de arquivos/diretórios para que fiquem "invisíveis" ao usuário.
- Ocultação de processos:
  - Técnica usada por *rootkits* para esconder o processo malicioso da lista de processos do sistema (*TaskList* no Windows).
- Ocultação de usuários:
  - Remoção de usuários criados durante o ataque da tela de *login* do sistema.

Atividades Subversivas

Comunicação dissimulada

- Permite acesso remoto sem detecção por parte da vítima:
  - Ex.: instalação de uma *backdoor* com processo oculto e tráfego cifrado ou de protocolos "legítimos" (HTTP).
- Transferência de dados sensíveis para fora do sistema vítima:
  - Ex.: instalação de um *keylogger* que capture e envie dados via Internet (pode usar método HTTP POST).
- Canais dissimulados (*covert channels*) e esteganografia:
  - Ex.: uso de campos vazios em protocolos de aplicação legítimos; informações embutidas em figuras.

Atividades Subversivas

Comando e controle

- Permite controle remoto de um sistema:
  - Ex.: um atacante forma uma *botnet* e envia comandos para as máquinas invadidas.
- Sabotagem:
  - Ex.: instalação de um *Trojan* que modifique a execução de um programa legítimo.
- Negação do controle de um sistema (DoS):
  - Ex.: um atacante assume o sistema da vítima e nega o acesso aos usuários autorizados.

Motivação para os ataques

Características da Internet

- Anonimato:
  - Fraudes (por meio de "laranjas")
  - Roubo de identidade
  - Legislação varia de país para país
- Abertura:
  - Protocolos de comunicação documentados e públicos
  - Dados transmitidos entre os nós $\Rightarrow$ interceptação
  - Dados na nuvem, buscas, mecanismos de *analytics* $\Rightarrow$ privacidade nula!

Segurança por obscuridade

- Obscuridade é muitas vezes usada para esconder problemas:
  - "Se o adversário não sabe que existe um problema, o alvo não será atacado."
- Esconder um problema nunca garantiu a segurança:
  - Vulnerabilidades em sistemas operacionais proprietários são descobertas e exploradas a todo momento.

Obscuridade vs. Segurança

Exemplos

- Utilização de algoritmo de criptografia desenvolvido pela própria empresa ou programador:
  - Como o adversário não conhece o algoritmo, não conseguirá quebrá-lo.
- Criptanálise: problemas no algoritmo ou na implementação permitem a quebra.

Obscuridade vs. Segurança

Exemplos

- Banco de dados conectado à Internet não possui um nome atribuído, mas possui IP:
  - O adversário não conhece o endereço do servidor então não irá atacá-lo.
- Varredura: ferramentas de mapeamento de rede podem encontrar facilmente servidores com endereços IP ativos, bem como as versões do sistema operacional e aplicações em execução.

Obscuridade vs. Segurança

Vantagens

- Obscuridade não garante segurança, mas...
  pode ser utilizada como elemento para dificultar eventuais ataques.
- Exemplo:
  - Troca de *strings/banners* de aplicações.
  - Adversários buscando padrões antes do lançamento de um ataque podem ser despistados.

Obscuridade vs. Segurança

Troca de *banners*

- **Ubuntu:** `/etc/update-motd.d/`
- **SSH:** Não dá, precisa recompilar o fonte.
  `/etc/ssh/sshd_config`
  (Descomentar `Banner /etc/issue.net`)
- **Apache:** `/etc/apache2/conf-enable/security.conf` $\Rightarrow$
  $\Rightarrow$ (`ServerSignature Off`)

Obscuridade vs. Segurança

Troca de porta padrão

- **OpenSSH:** `/etc/ssh/sshd_config`

  ```
  Port 22
  service ssh restart
  ```

- **Apache:** `/etc/apache2/ports.conf`

  ```
  service apache2 restart
  ```

- Testar "obscuridade" com NMap...

Leitura Recomendada

- `https://nmap.org/nmap_doc.html` (*The Art of Port Scanning - by Fyodor*)