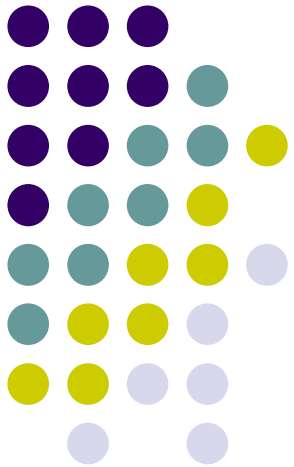
Universidade Federal de São Paulo – UNIFESP

Segurança Computacional

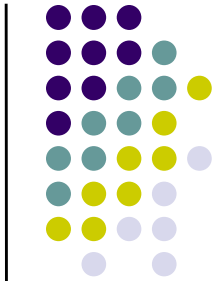
Clique para adicionar texto
Aula 01 - Introdução



Prof.
Valério Rosset
2016-1

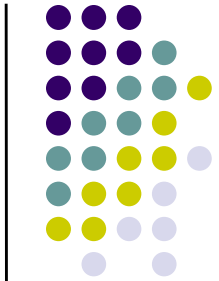
Figures and Charts from:Computer Networks: A Systems Approach, 5e
Larry L. Peterson and Bruce S. Davie; Computer Networks: Top Down, Kurose and Ross. Computer Networks: Andrew Tanenbaum and Davis Wetherall. IBM X-Force Annual Reports 2012, 2013 and 2014.

Segurança



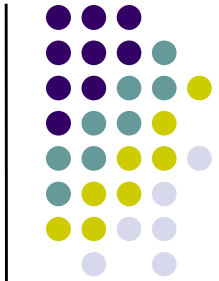
- O que significa.
- Quem gosta.
- Quem não gosta.
- Segurança a qualquer preço.
- Relação Tempo – Segurança.

Perguntas que devemos fazer



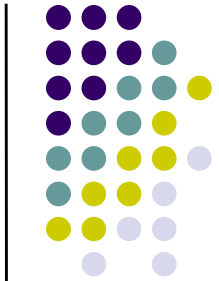
- Você se sente seguro?
- Será que alguém cuida de você ou você deve aprender a se cuidar?
- Quem deve promover segurança?
- O que tenho a perder se não investir em segurança?

Motivação



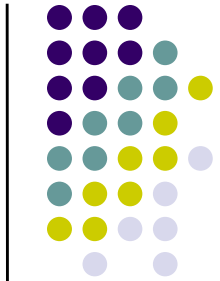
- Desafios da Segurança:
  - Proteger recursos de pessoas mal intencionadas
  - Assegurar o acesso aos recursos a quem tem direito.
- Uma referência global de como o sistema deve se comportar e gerenciar os acessos aos recursos se faz necessário.

Motivação



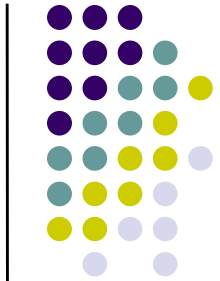
- Mercado de Trabalho:
  - Profissional com formação em segurança computacional é valorizado.
  - Empresas contratam mais pessoas a cada dia (equipes de segurança e resposta a incidentes).
  - O que é preciso: *Conhecimento de técnicas de programação segura, sistemas seguros, configuração de firewalls, detecção de intrusão, configuração de serviços de rede, principais vulnerabilidades de programas e SOs etc.*

Motivação



- *Necessário para ambos*
  - *Persistência*
  - *Paciência*
  - *Muito Trabalho*

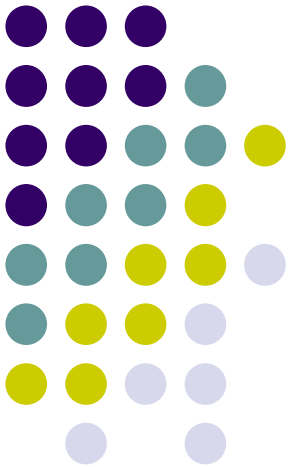
Motivação



- Pesquisa:
  - Desenvolvimento de novos algoritmos e métodos criptográficos.
  - Sistemas e Arquiteturas seguras.
  - O que é preciso: *Conhecimentos de teoria para computação, matemática, métodos criptográficos, algoritmos criptográficos, algoritmos de força bruta, sistemas computacionais seguros, serviços, protocolos de comunicação, mecanismos e políticas de controle e distribuição de direitos de acesso.*

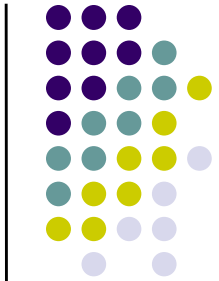
Conceitos Básicos

Clique para adicionar texto



Conceitos Básicos

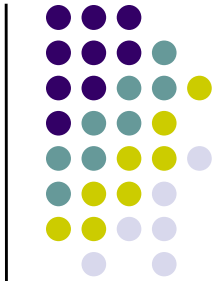
Definição



- A segurança computacional pode ser definida como a Proteção de Recursos através da prevenção e detecção de ações não autorizadas em um sistema computacional.
- Propriedades fundamentais para Proteção :
  - Confidencialidade : (privacidade e segredo)
  - Integridade : (originalidade de conteúdo)
  - Disponibilidade: (alocação de recursos)
  - Autenticidade : (informação autêntica)
  - Responsabilidade: (rastreio, logs)

Conceitos Básicos

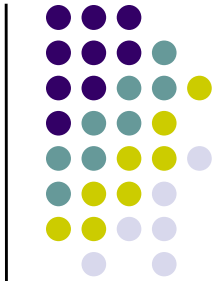
Propriedades Fundamentais



- Confidencialidade
  - Está intimamente ligada aos termos de segredo e privacidade.
    - Proteção entre dados pessoais (privacidade)
    - Proteção de dados pertencentes a uma organização (segredo).
  - Pode-se dizer que garantir a confidencialidade de uma informação é tornar possível que apenas pessoas autorizadas possam conhecê-la.
  - Algumas vezes, segurança e confidencialidade são utilizadas erroneamente como sinônimos.

Conceitos Básicos

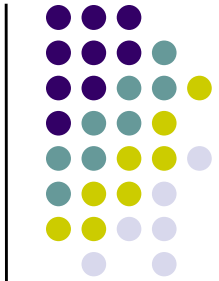
Propriedades Fundamentais



- Integridade
  - A Integridade está ligada a certeza de que uma informação realmente possui um conteúdo verdadeiro e original, mesmo que esta informação esteja transitando em um sistema computacional.
  - Por exemplo, em uma comunicação entre sistemas computacionais a informação que sai de uma origem deve ser igual a informação que chega ao destino.
  - Integridade é implementada através da criptografia, por exemplo por Algoritmos Hash.

Conceitos Básicos

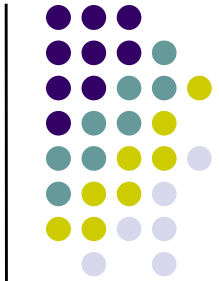
Propriedades Fundamentais



- Disponibilidade
  - A disponibilidade trata da alocação de recursos e informações sempre que sejam necessários.
  - É necessário um esforço para prevenir contra a indisponibilidade de acesso a um recurso pelos usuários legítimos.
  - Quando um recurso fica bloqueado é caracterizado uma negação de serviço (DoS).

Conceitos Básicos

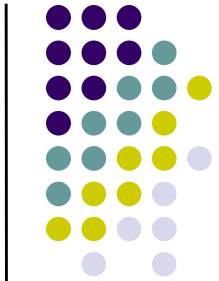
Propriedades Fundamentais



- Autenticidade
  - A autenticidade trata da certificação de que a origem de uma informação é identificada corretamente, e que a sua identidade não é falsa.
  - A autenticação assegura que uma informação é autêntica.

Conceitos Básicos

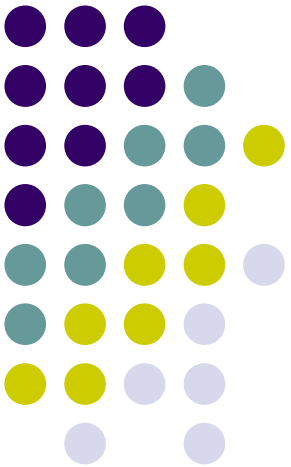
Propriedades Fundamentais



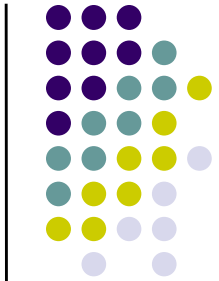
- Responsabilidade
  - O princípio da responsabilidade determina que informações de auditoria precisam ser mantidas e protegidas, para que essas sejam usadas para rastrear e determinar a parte responsável por ações (maliciosas ou não) que venham afetar negativamente um sistema.

Ameaças de Segurança, Ataques e Vulnerabilidades

Clique para adicionar texto

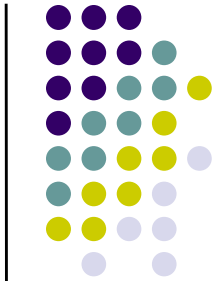


Ameaças de Segurança



- A menos que você entenda as ameaças que você deve enfrentar, você não pode preparar sua defesa!
- Uma ameaça pode ser caracterizada como uma ação em potencial e inesperada, que pode geralmente produzir danos em proporções indesejáveis a um sistema computacional
- Ameaças podem ser:
  - Intencionais
  - Não Intencionais

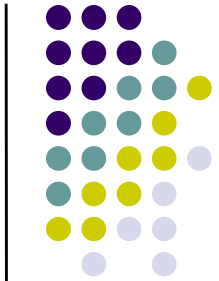
Ameaças de Segurança



- Ações não intencionais não são premeditadas e podem ser caracterizadas como falhas de software e hardware.

- Ações intencionais são premeditadas e geralmente são realizadas com base em algum conhecimento de ***vulnerabilidades*** de sistemas computacionais.

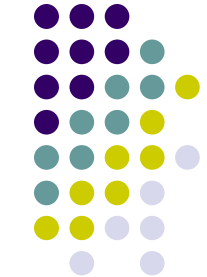
Tipos de Ameaças



- As ameaças de segurança podem ser divididas em três grupos: ameaças de revelação, ameaças de integridade e ameaças de negação de serviço.

- A ***ameaça de revelação*** envolve a disseminação da informação para um individuo para quem esta informação não poderia ser vista. No contexto de segurança computacional, esse tipo de ameaça ocorre sempre que algo secreto, que está armazenado em um sistema computacional ou trafegando entre sistemas computacionais, é revelada a alguém que não poderia conhecer o segredo.

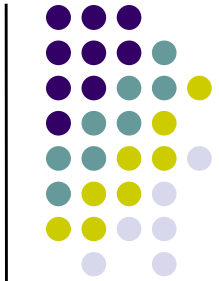
Tipos de Ameaças



- A ***ameaça de integridade*** envolve uma alteração não autorizada da informação que está armazenada em um sistema computacional ou quando está transitando entre os sistemas computacionais.

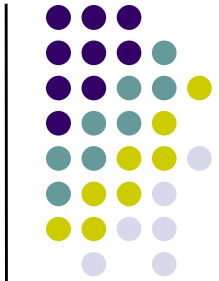
- Quando um intruso malicioso altera alguma informação, considera-se que a integridade da informação foi comprometida. A integridade também é comprometida quando a informação é alterada de maneira inocente, através de um erro, provocando uma alteração não autorizada.

Tipos de Ameaças



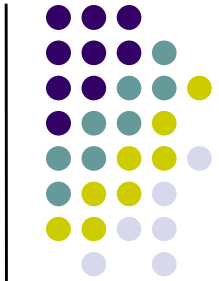
- A ***ameaça de negação de serviço***
  - diz respeito ao bloqueio de acesso a algum sistema computacional intencionalmente, como resultado de uma ação maliciosa executada por um outro usuário. Quando um usuário requer acesso a um serviço/recurso mas o mesmo encontra-se bloqueado, é caracterizada uma negação de serviço.

Vulnerabilidade



- A *vulnerabilidade* de um sistema consiste na existência de uma ameaça.
- Define-se vulnerabilidade: como alguma característica inoportuna que torne possível a ocorrência de uma ameaça em potencial.
- A exploração de uma vulnerabilidade, por parte de uma ação intencional, consiste em um ataque ao sistema.

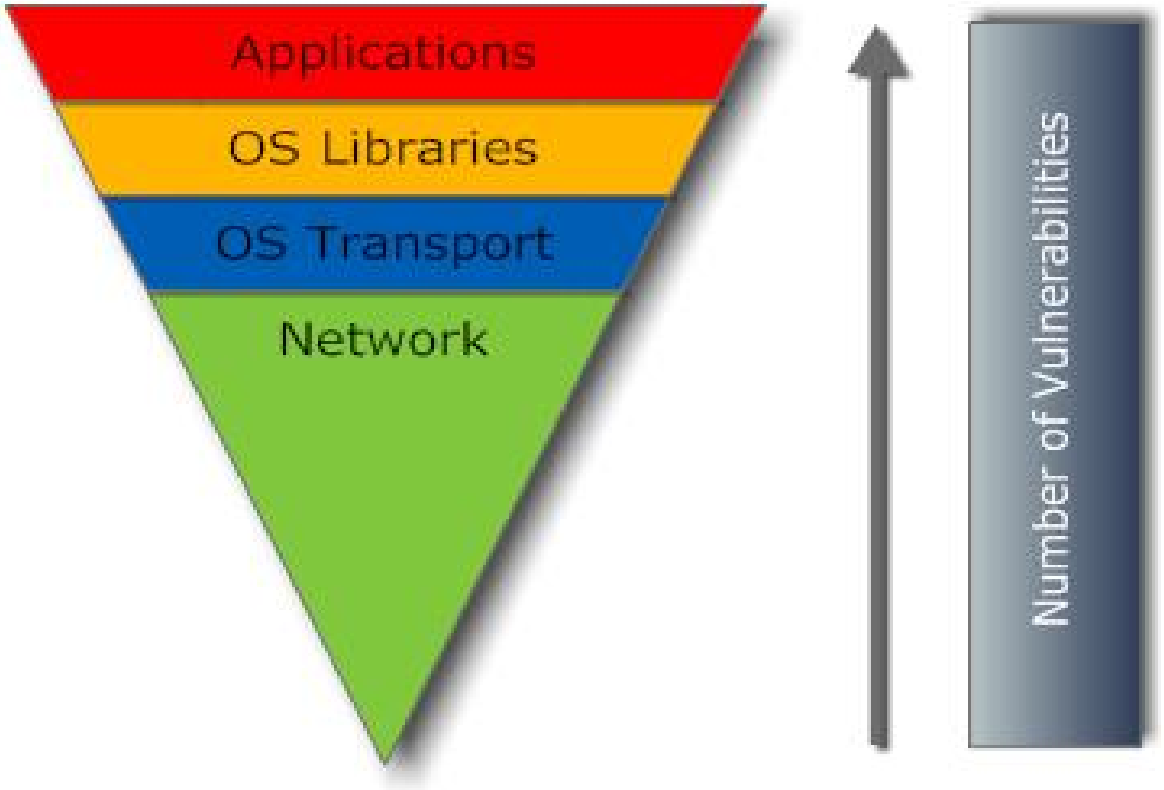
Ataques



- Ataques (ou seja, exploração das vulnerabilidades) podem ocorrer nos mais diversos níveis um sistema computacional. Sendo que o número de vulnerabilidades relatados é muito maior ao nível de aplicações, o número de ataques a aplicações é muito maior que ataques a sistemas operacionais.

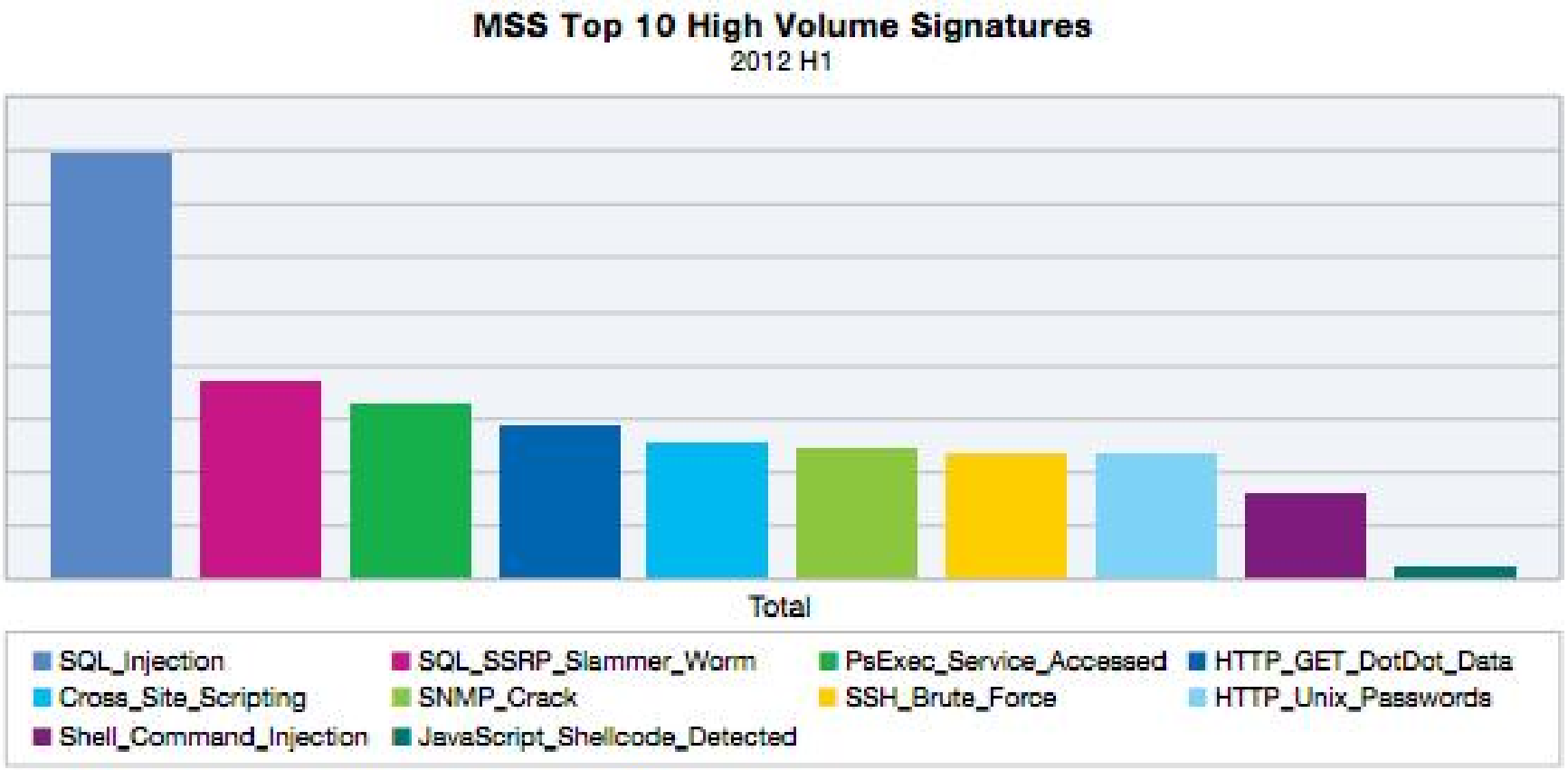
- A partir de agora utilizaremos os termos **Atacante** e **Alvo.**

Vulnerabilidades vs Ataques



Ataques

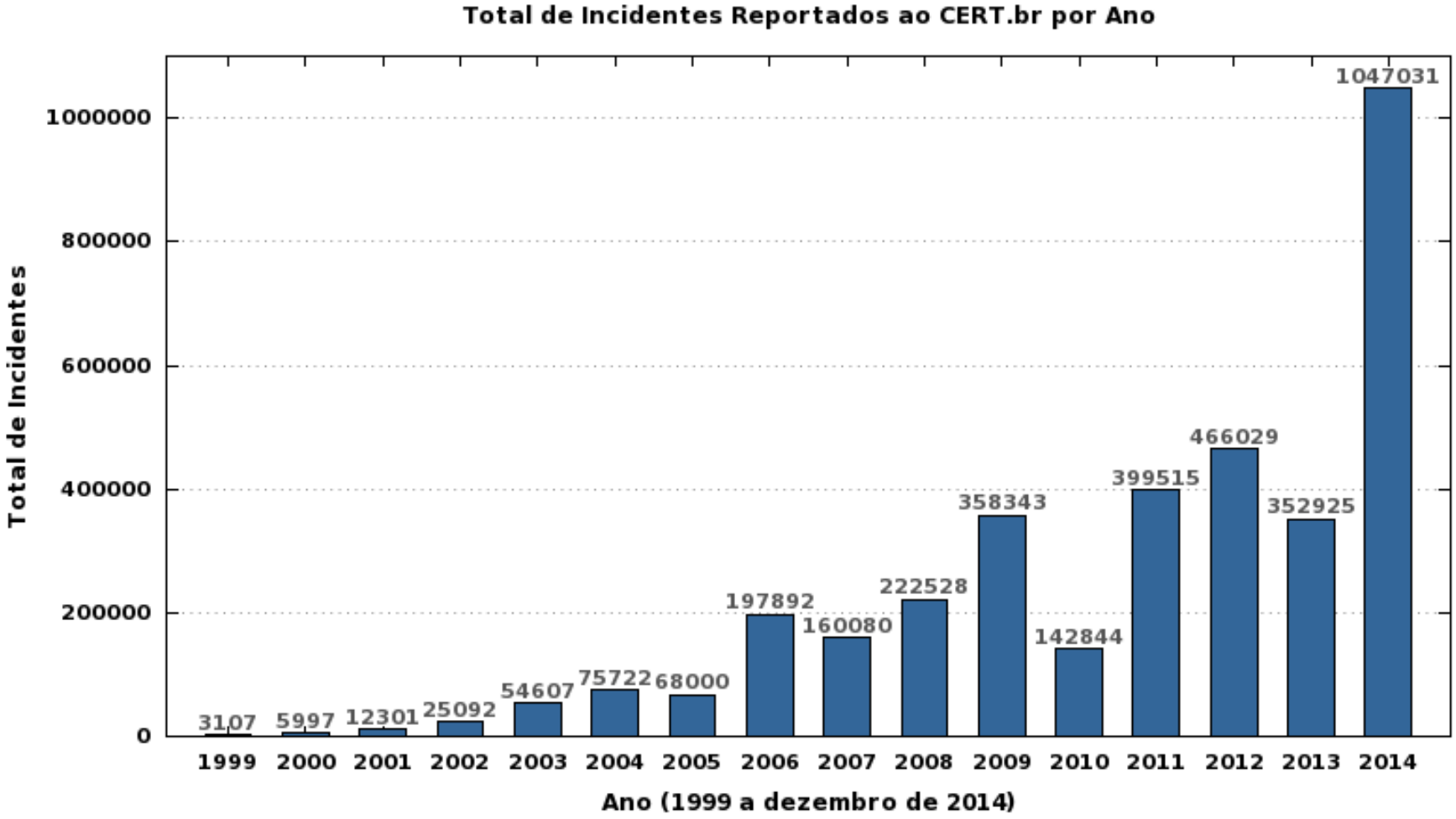
- **Top 10 primeiro semestre de 2012 (X-Force IBM)**



Fonte: http://www-935.ibm.com/services/us/iss/xforce/trendreports/

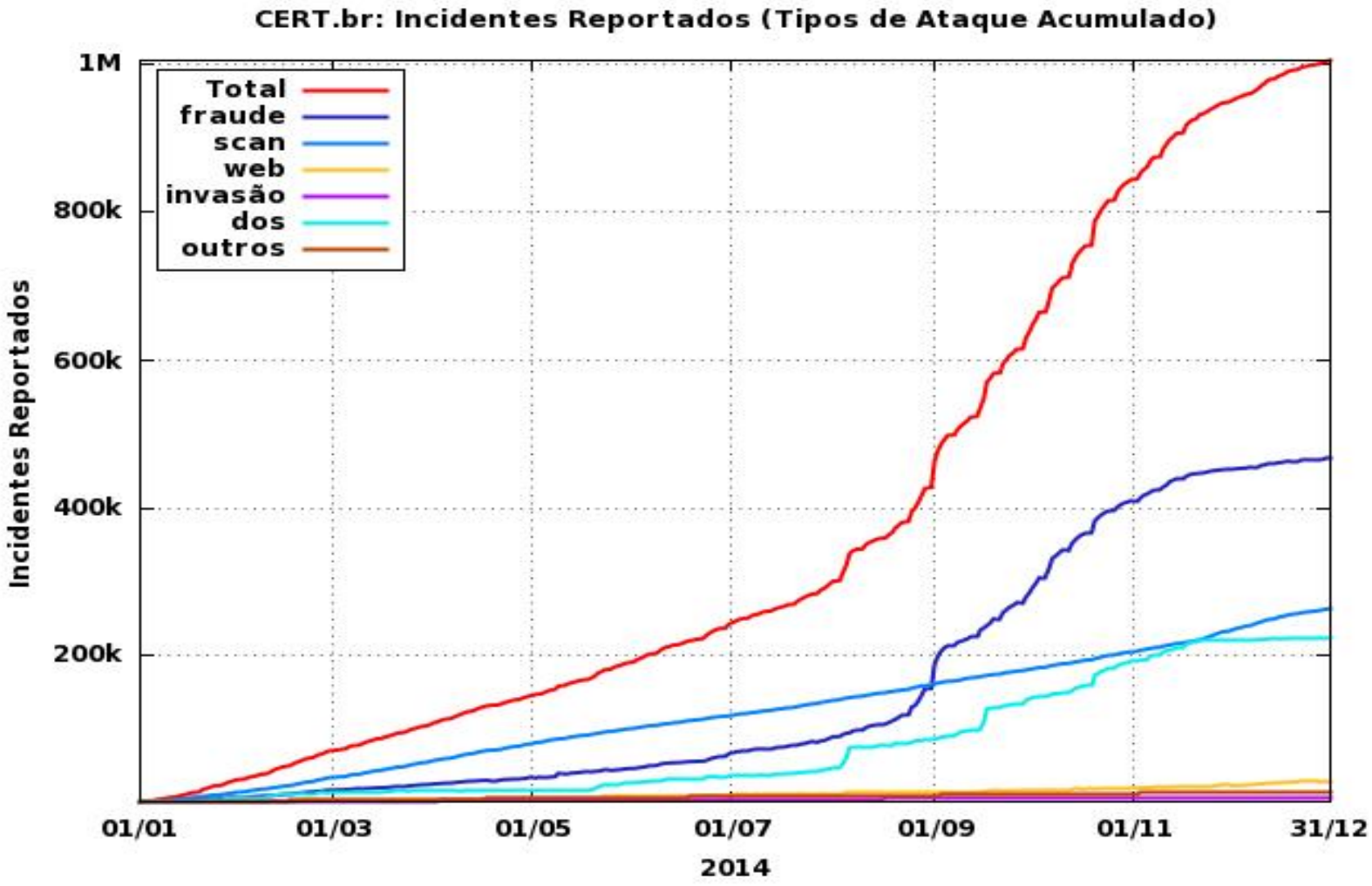
Ataques

- Estatísticas dos Incidentes Reportados ao CERT.br por ano.



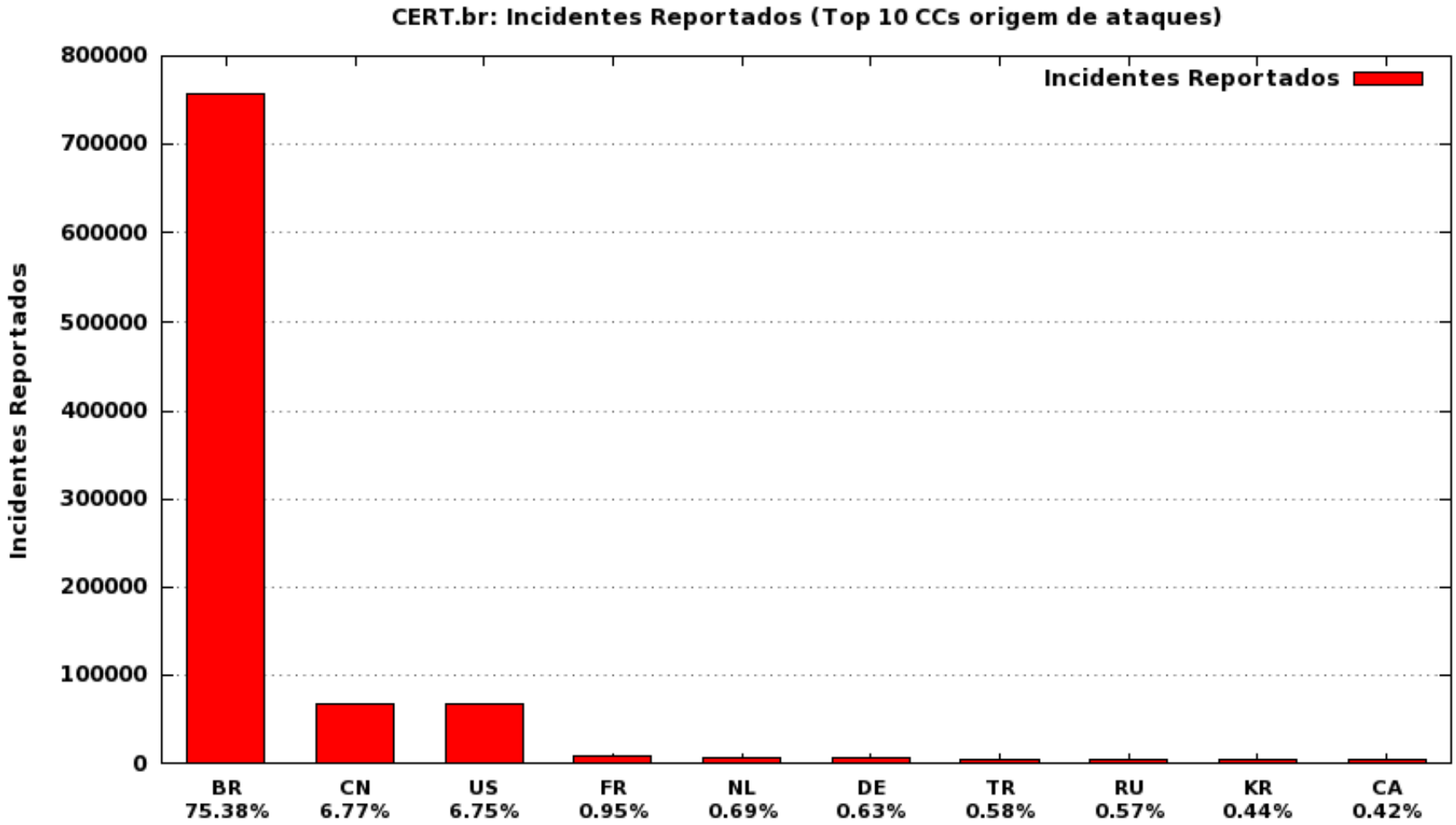
Ataques

- Estatísticas dos Incidentes Reportados ao CERT.br por ano.



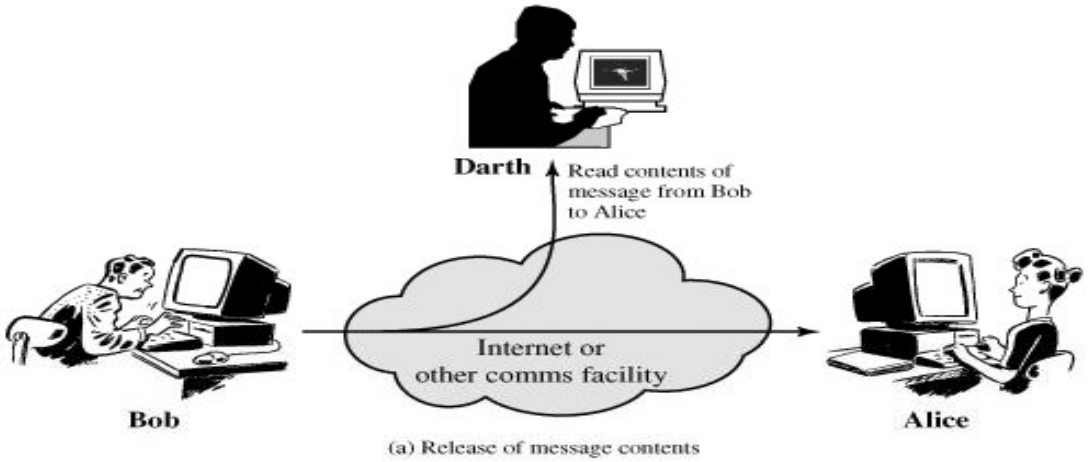
Ataques

- Estatísticas dos Incidentes Reportados ao CERT.br por ano.

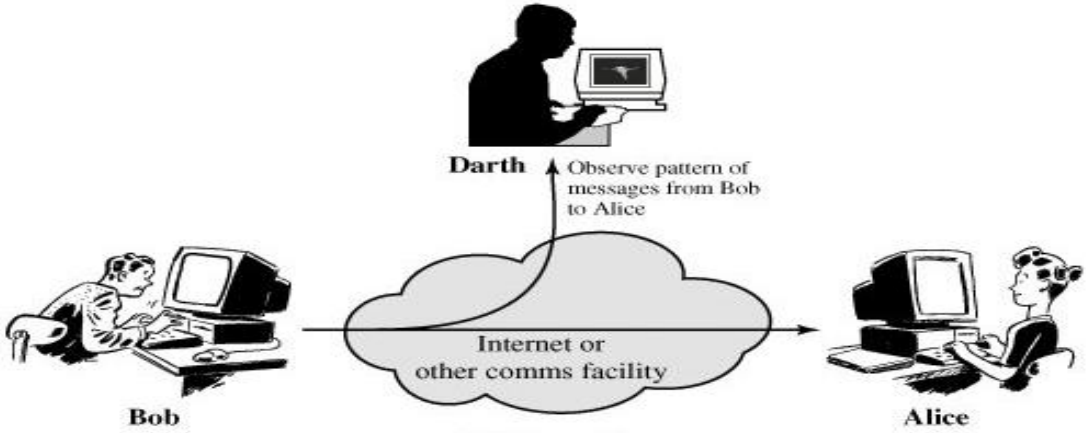


Ataques-Passivos

- Ocorrem sem interação direta com o alvo.
- Nesse tipo de ataque o principal objetivo é a coleta de dados para posterior análise e uso.



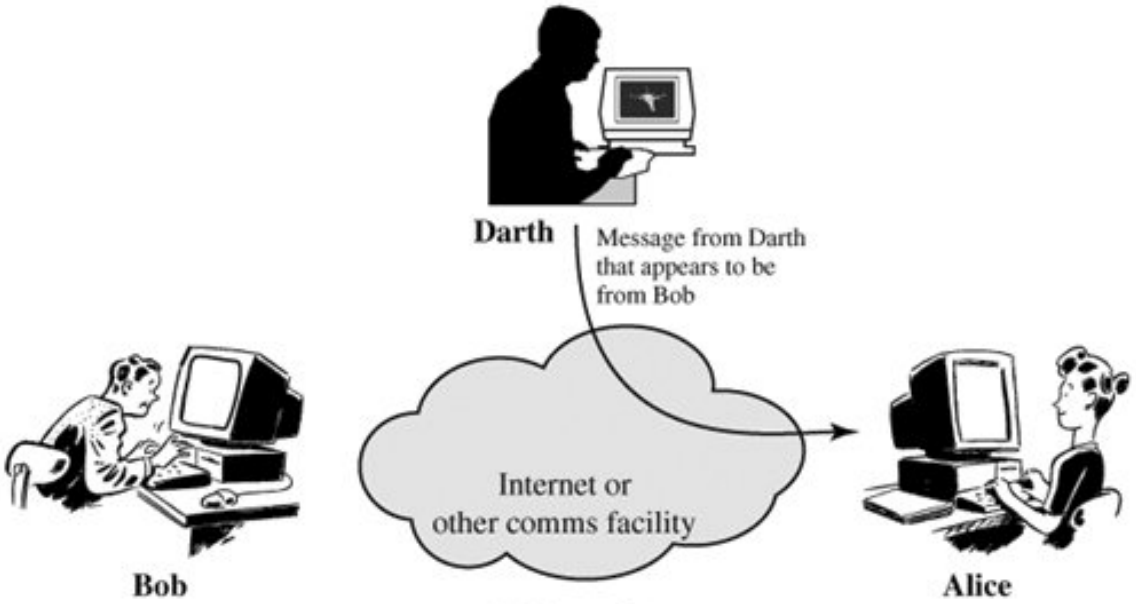
(a) Release of message contents



(b) Traffic analysis

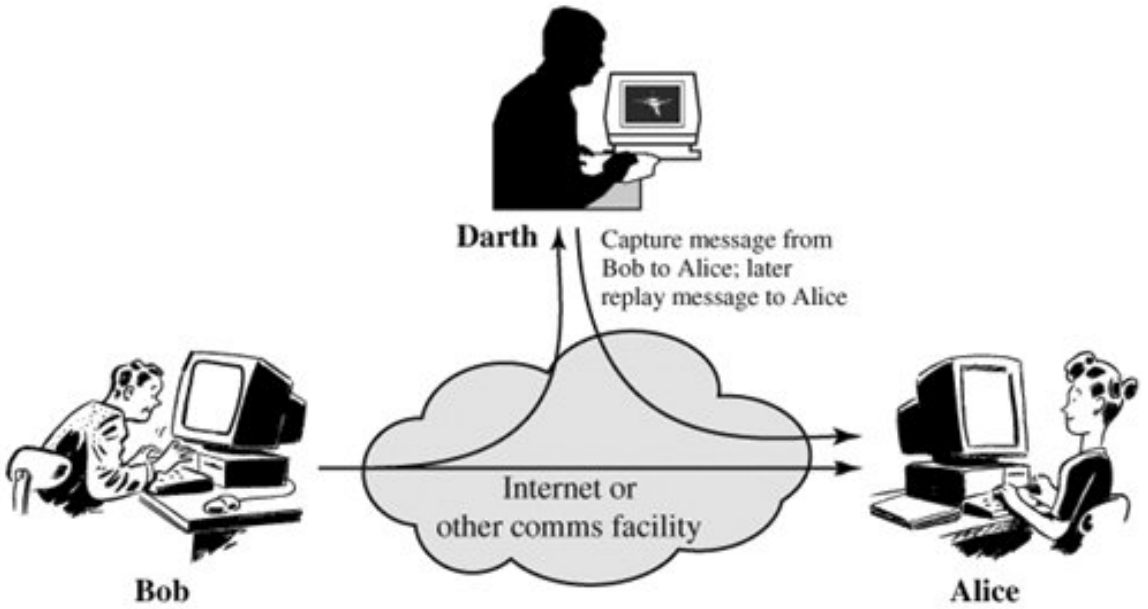
Ataques Ativos - Tipos

- Personificação
  - Em uma comunicação entre pelo menos duas entidades, o atacante faz-se passar por uma delas para casuar efeitos indesejáveis ao alvo;

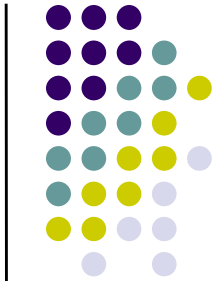


Ataques Ativos - Tipos

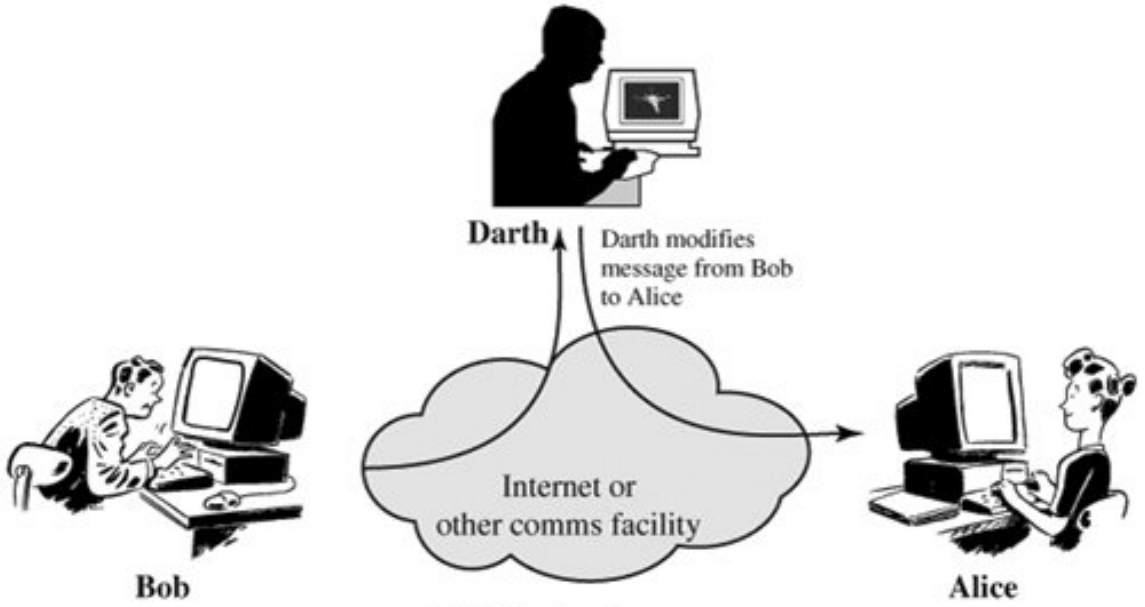
- Replay:
  - Ocorre quando uma mensagem, ou parte dela é interceptada pelo atacante, e posteriormente transmitida para produzir um efeito indesejável sobre o alvo:



Ataques Ativos - Tipos

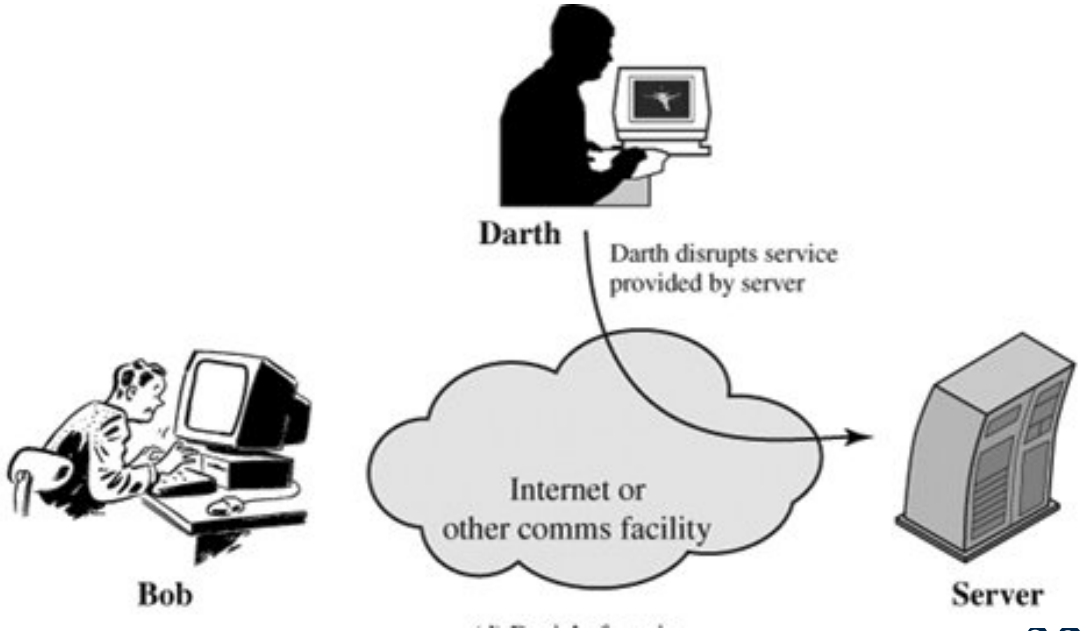


- Modificação:
  - o conteúdo de uma mensagem é alterado implicando em efeitos não autorizados sem que o sistema alvo consiga detectar a alteração;

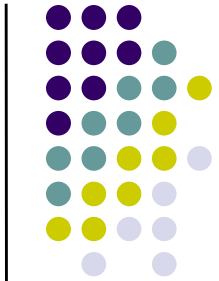


Ataques Ativos - Tipos

- *Negação de serviço*:
  - ocorre quando um atacante bloqueia um recurso não permite que usuários legítimos acessem os recursos ou executem suas funções;

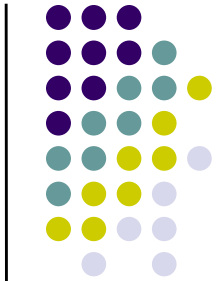


Ataques Ativos



- Algumas Definições:
  - *Malwere:* qualquer software com objetivos maliciosos.
  - *Ataques internos*: ocorrem quando usuários legítimos comportam-se de maneira não autorizada ou não esperada;
  - *Zero-day attack*: É uma denominação adotada para classificar qualquer ataque que ocorra no período de tempo entre a descoberta de uma vulnerabilidade e sua correção.

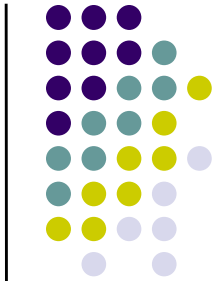
Ataques Ativos



- *Armadilhas (TrapDoor)*: ocorre quando uma entidade do sistema é modificada para produzir efeitos não autorizados em resposta a um comando ou evento premeditados;

- *Cavalos de Tróia (Trojan Horse)*: é uma entidade, que executa funções não autorizadas, em adição às que está autorizada a executar.

Ataques Ativos

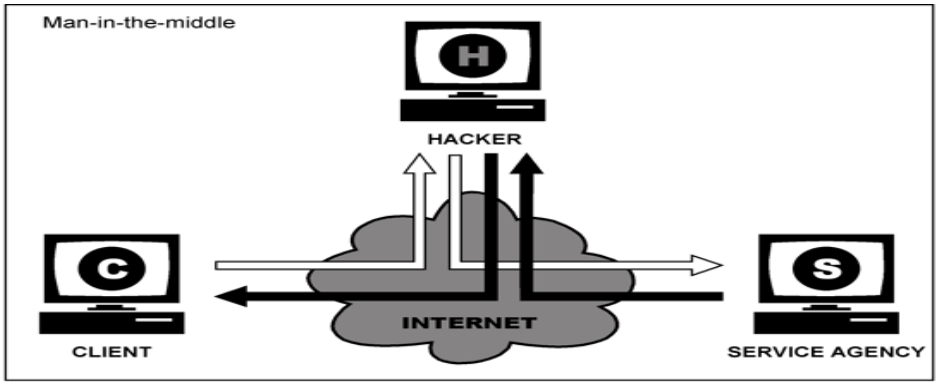


- *Spyware*: é parecido com o cavalo de tróia, porém esse software está geralmente embutido em uma outra entidade, e coleta informações e as distribuí sem o consentimento dos usuários.

- *Exploits*: softwares ou trechos de códigos utilizados para explorar vulnerabilidades específicas de um sistema.

Ataques Específicos

- ***Man-in-the-middle***: é um ataque onde um usuário malicioso intercepta mensagens de outros usuários e as utiliza a sua vontade. Nesse ataque o usuário malicioso pode reter, alterar e retransmitir mensagens. Assim ele caracteriza uma mescla entre ataques de personificação, replay e modificação.



Ataques Específicos

- ***Phishing***:
  - técnica que usa meios de engenharia social para iludir usuários e assim possibilitar o roubo de informações sensíveis (senhas de cartão).

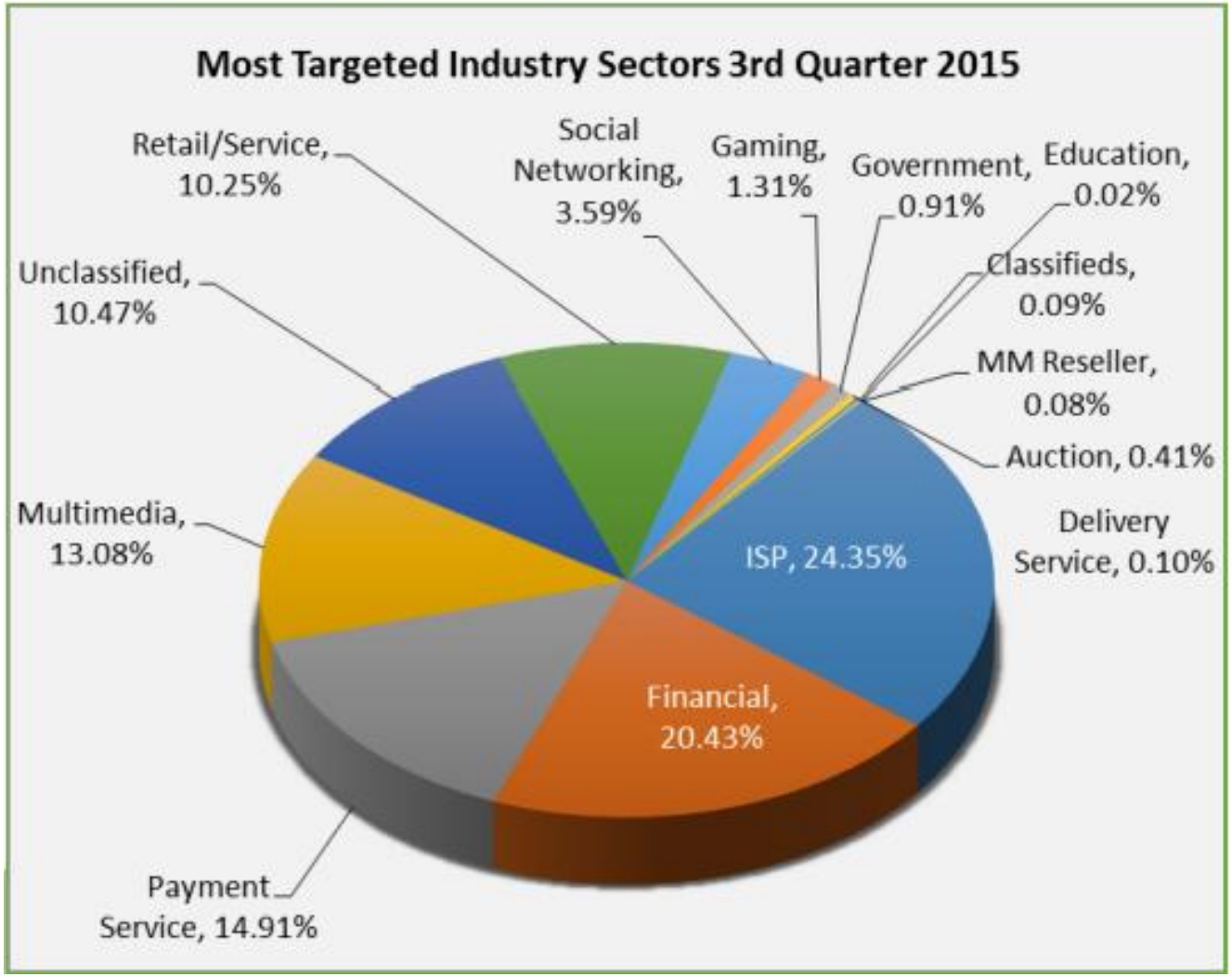
Ataques Específicos

- ***Phishing*** :

Fonte: APWG: Phishing Activity Trends Report

Ataques Específicos

- ***Phishing*** :

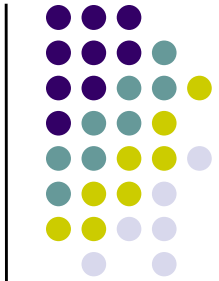


Fonte: AWG: Phishing Activity Trends Report.

Ataques Específicos

- ***Injeção de SQL (SQL-Injection)***:
  - Inclui pedaços de códigos SQL em páginas para burlar mecanismos de segurança e ter acesso a informações.

Ataques Específicos

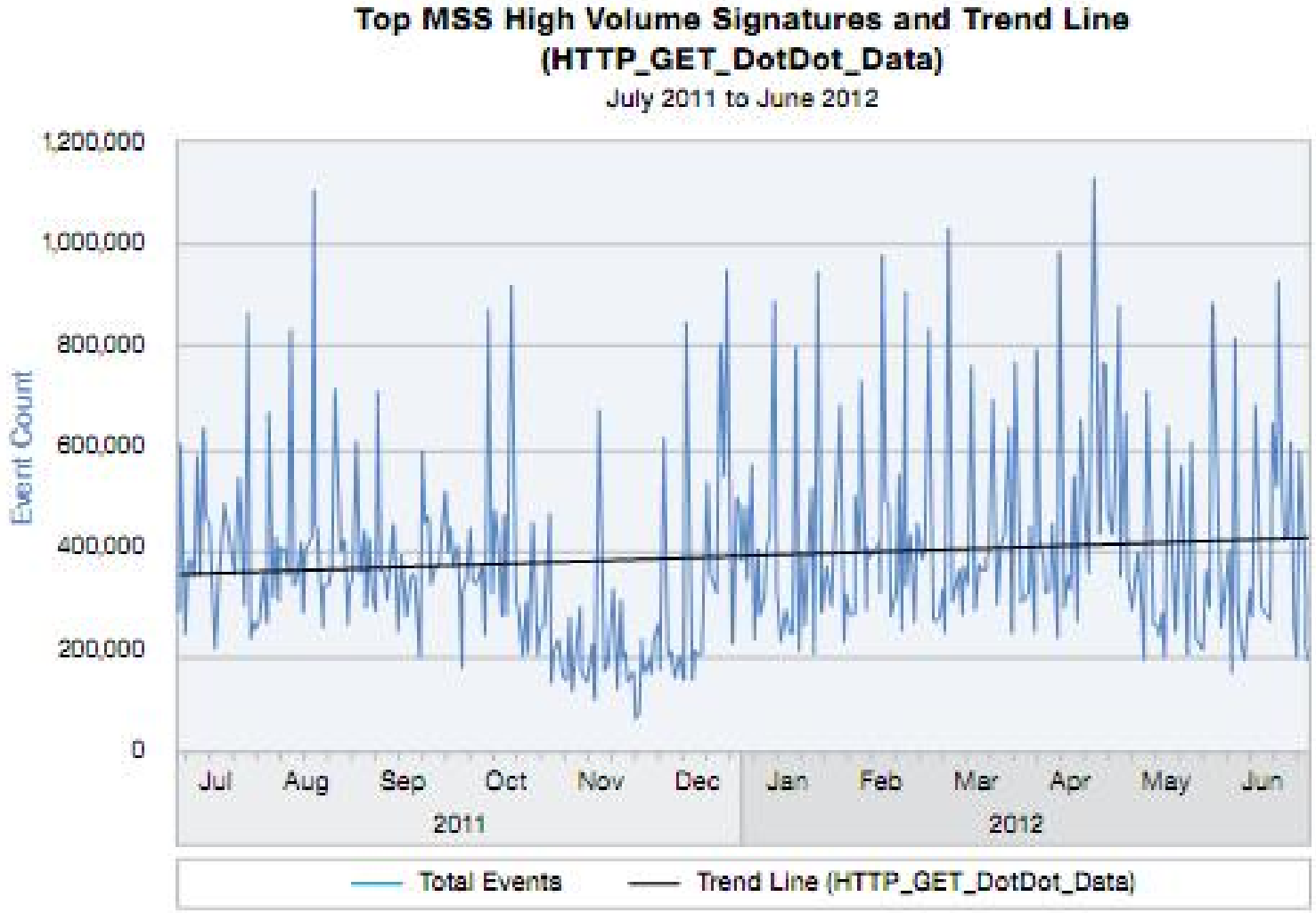


- ***Cross-Site Script (XSS)***:

  - Inclusão de scripts maliciosos em sites considerados confiáveis. A inclusão desses códigos em meio a outros elementos de uma página web, por exemplo, podem produzir uma ilusão e o visitante do site vai acreditar que esteja em um ambiente seguro.

Ataques Específicos

- ***Cross-Site Script (XSS)***:

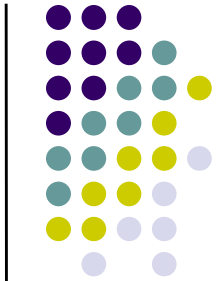


Ataques Específicos

- ***Watering Hole***: o atacante infecta sites de comum acesso para um grupo de usuários alvo. Assim o atacante espera que o site de confiança do grupo alvo não seja reconhecido como uma ameaça.

  - 3 etapas:
    - Infecta o site.
    - Quando acessado o site redireciona para outro site (exploit).
    - Infecta o dispositivo alvo com cavalo de tróia com acesso remoto.
  - Esse é uma técnica nova, descoberta em Julho de 2012.

Mais Ataques



Injeção de scripts (Script-Injection):

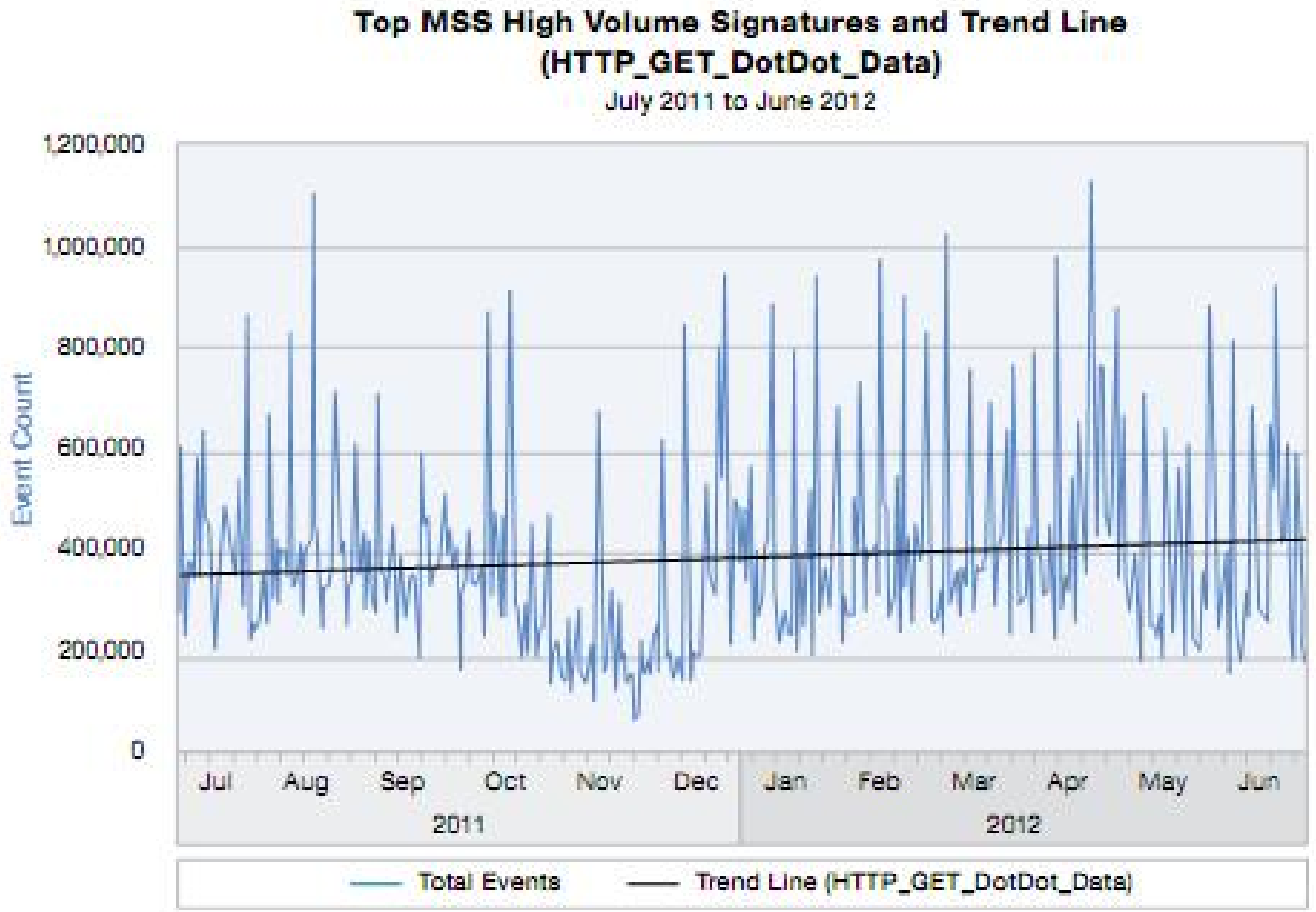
- Segue o mesmo princípio do SQL-Injection, porém se utiliza de códigos em JavaScript ou outros.

- **DNS spoofing (DNS cache poisoning):**
  - altera dados em servidores DNS, redirecionando acesso para sites maliciosos.

- Dot Dot Slash Attack ("../" ou Directory Traversal)
  - Antigo porém ainda eficiente em alguns sistemas.

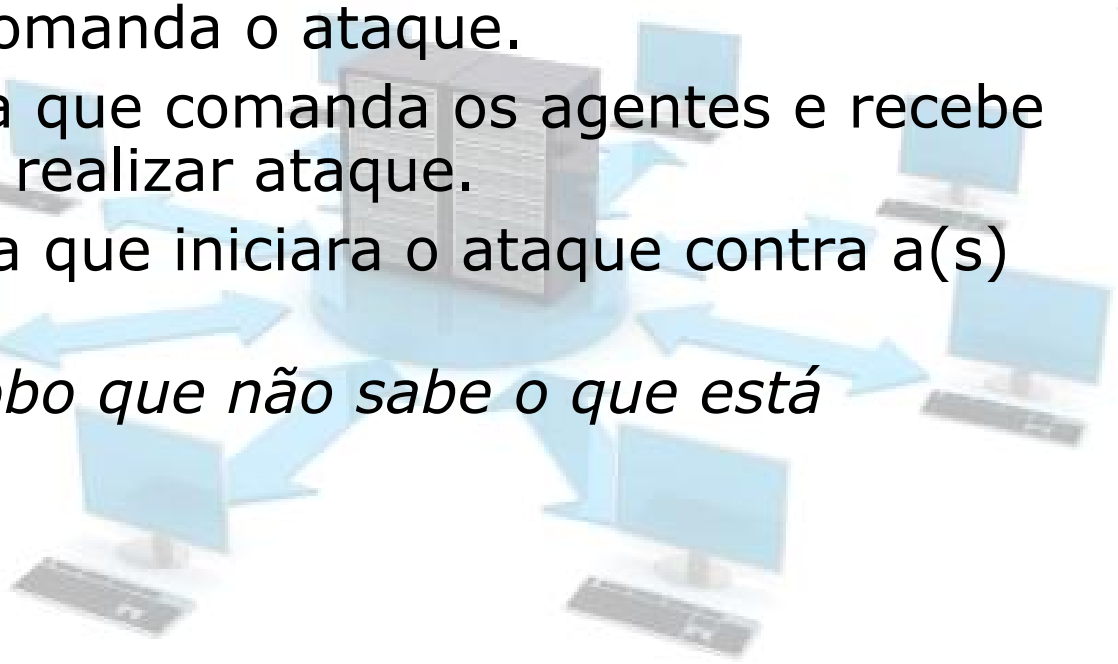
Mais Ataques

- Dot Dot Slash Attack ("../" ou Directory Traversal)
  - Antigo porém ainda eficiente em alguns sistemas.



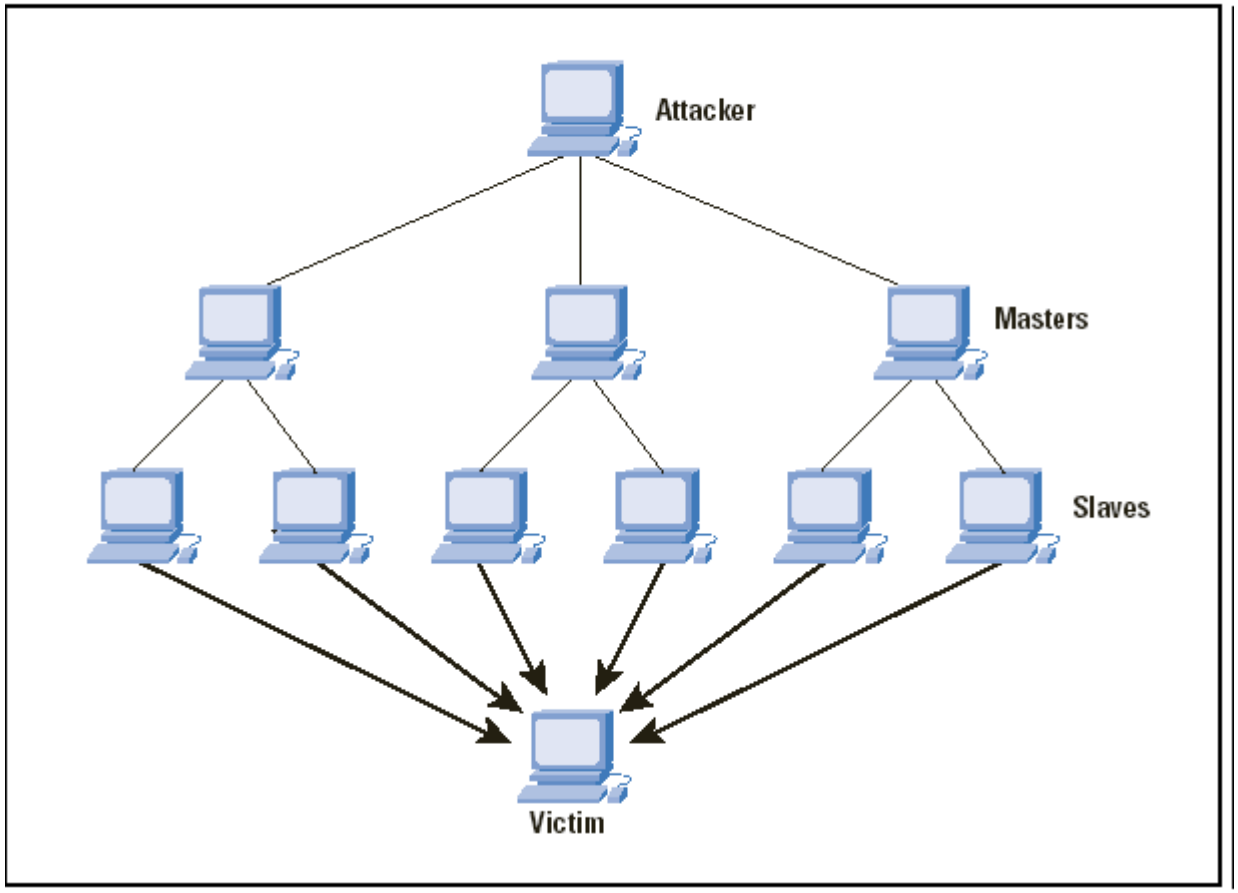
Ataque DoS e DDoS

- DoS (Denial of Service)
  - Torna indisponível um serviço
  - Analogia à “Virada de ano!”
  - Uma andorinha só não faz verão, então DDoS.
- Organização de um DoS
  - Atacante: Quem comanda o ataque.
  - Master: A máquina que comanda os agentes e recebe as instruções para realizar ataque.
  - Agente: A máquina que iniciara o ataque contra a(s) vitima(s).
  - Alvo (… a*quele bobo que não sabe o que está acontecendo …*)



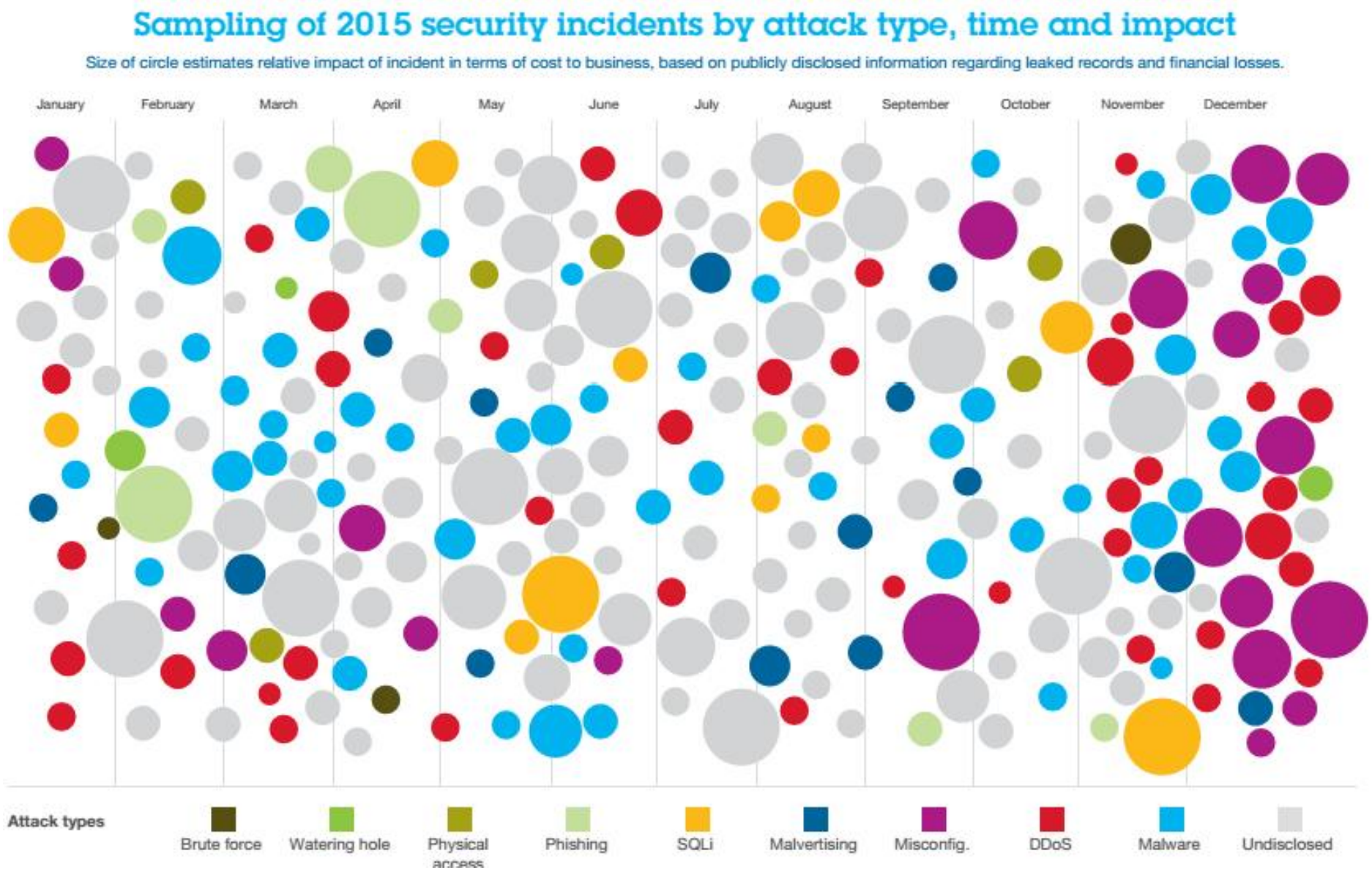
DDoS como Funciona

Figure 4: A DDoS Attack

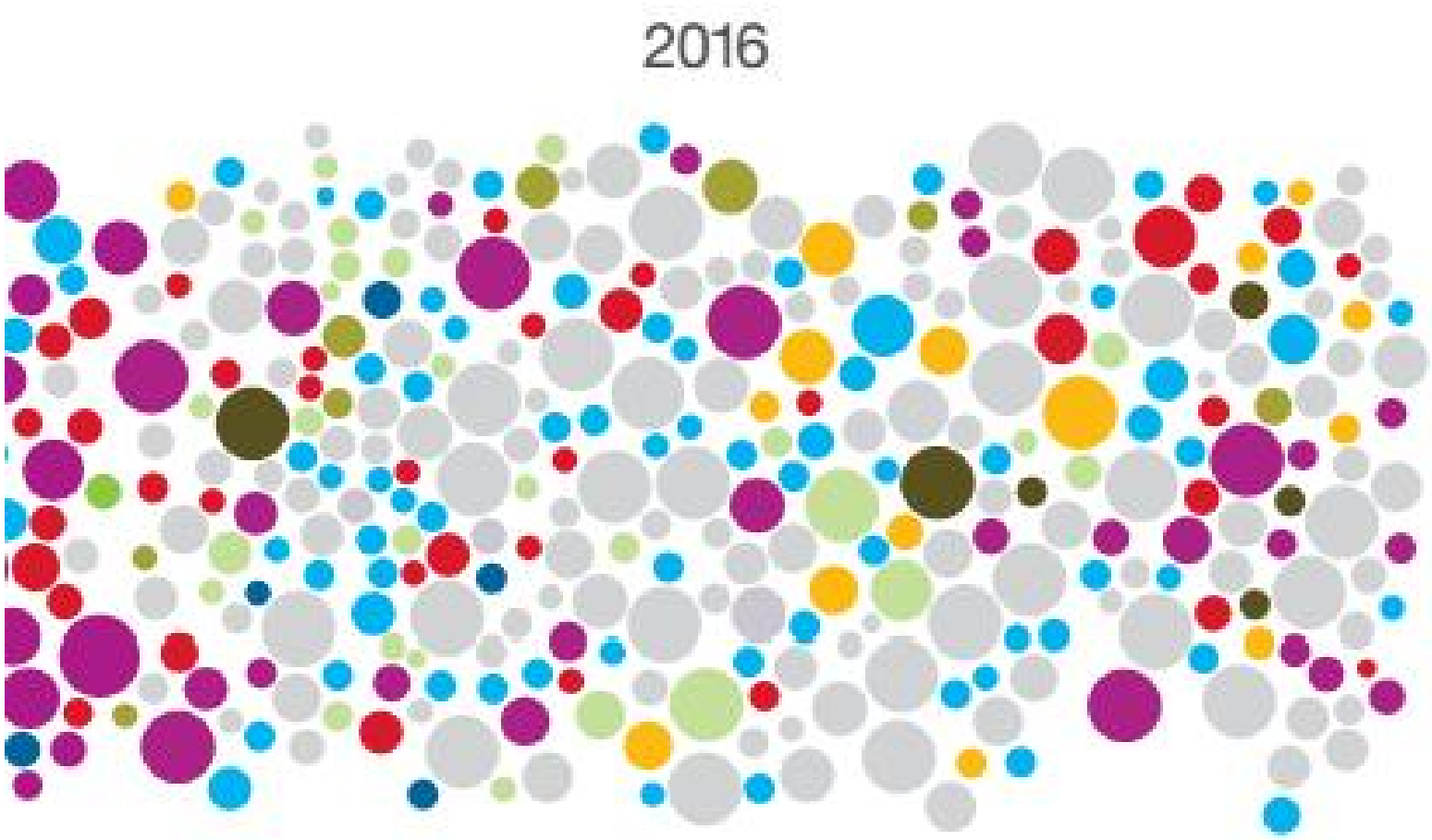


fonte: www.cisco.com

Alguns Números



Fonte: IBM X-Force Report - 2016.



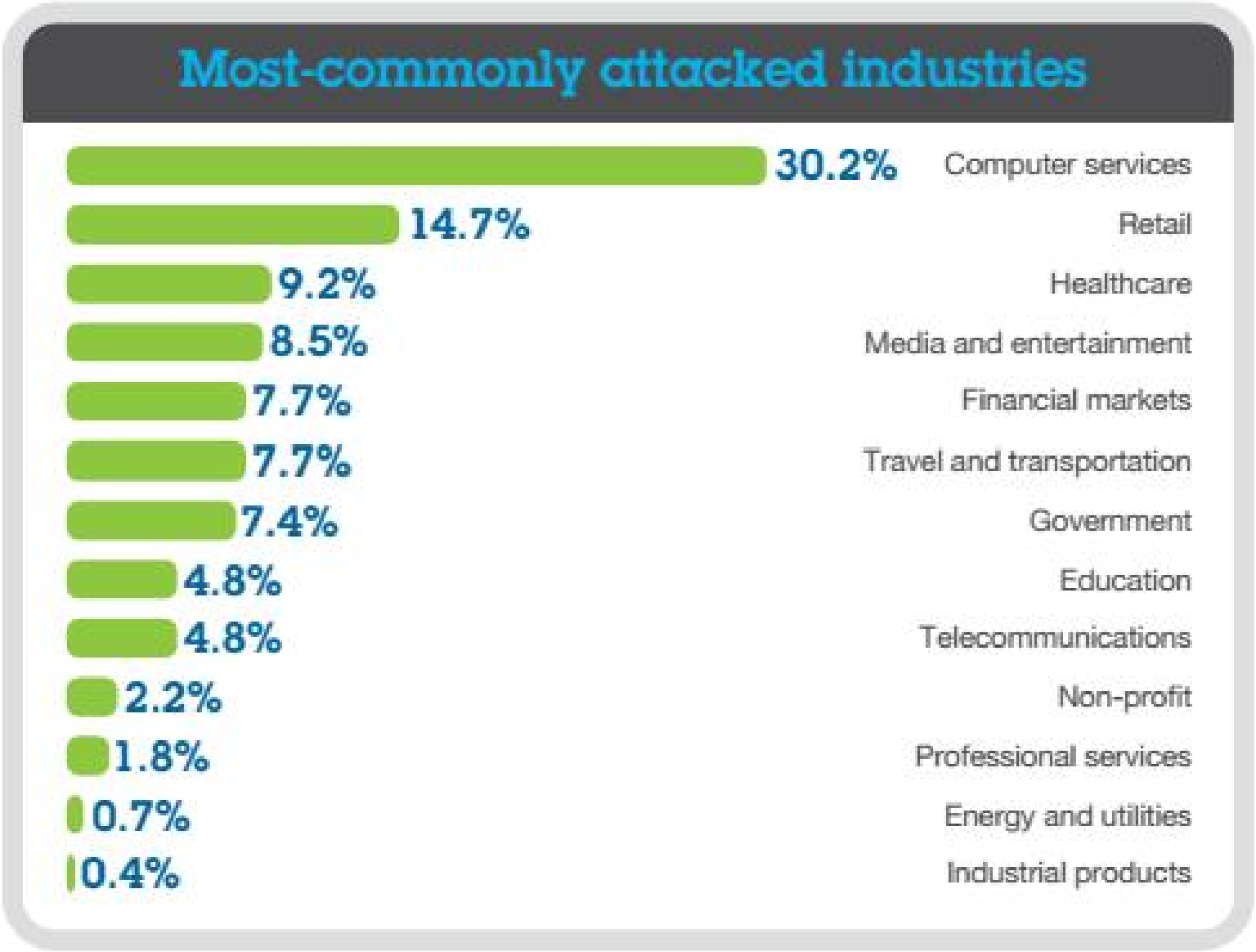
Sampling of security incidents by attack type, time and impact,

Attack types

XSS
Physical access
Brute force
Misconfig.
Malvertising
Watering hole
Phishing
SQLi
DDoS
Malware
Heartbleed
Undisclosed

Size of circle estimates relative impact of incident in terms of cost to business, based on publicly disclosed information regarding leaked records and financial losses.

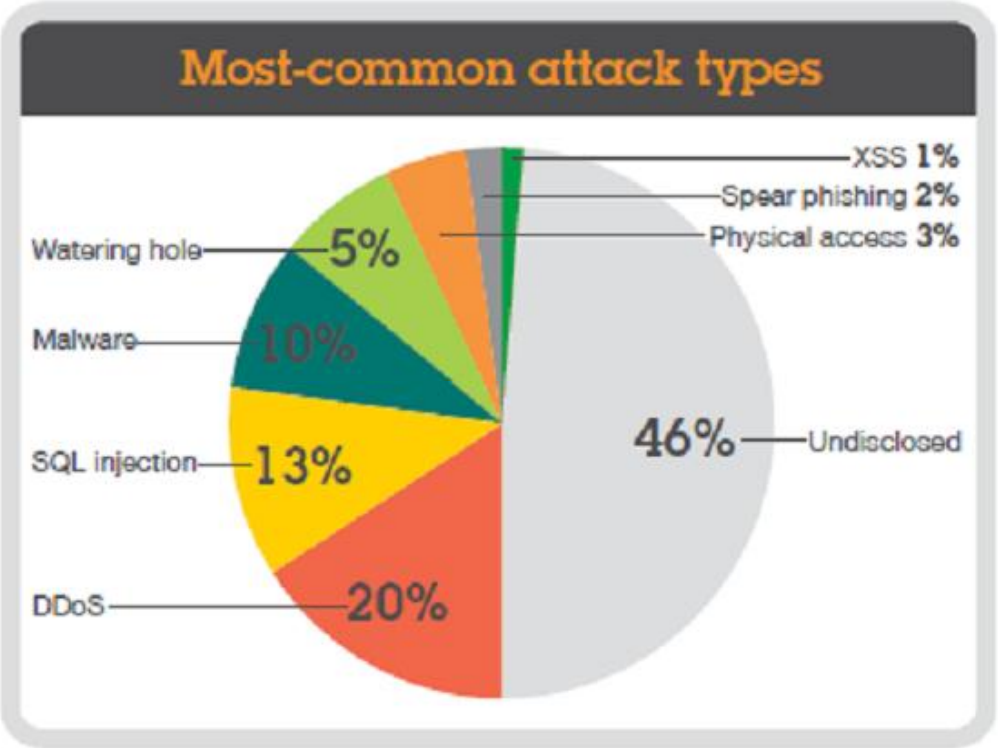
Alguns Números



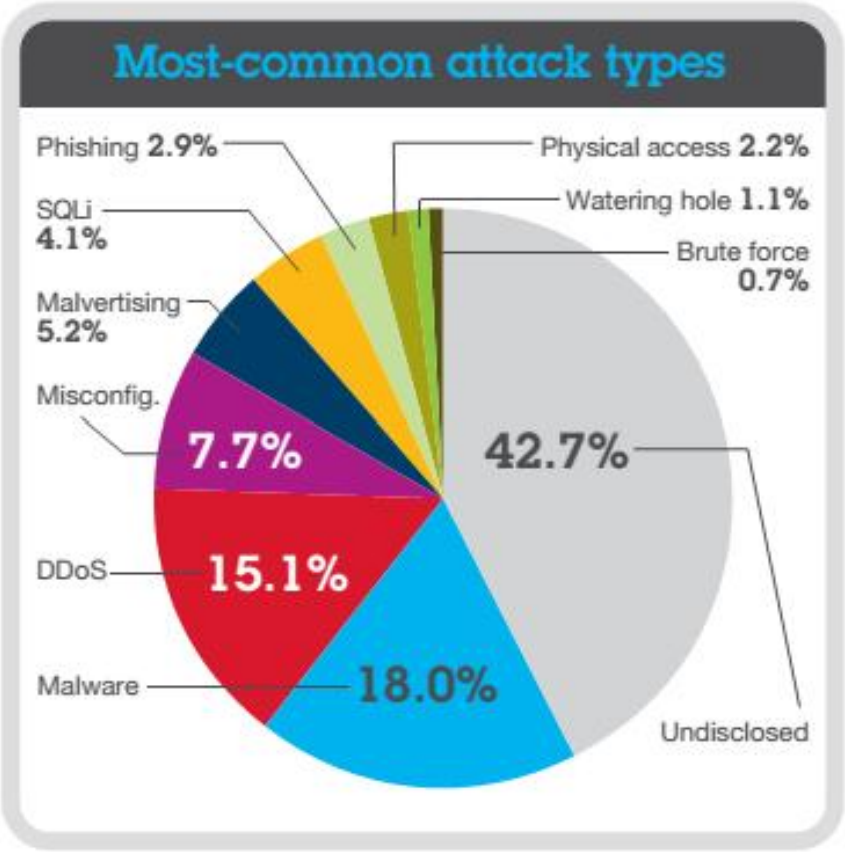
Fonte: IBM X-Force Report - 2016.

Alguns Números

2014



2015



Fonte: IBM X-Force Report - 2016.

Alguns Números

Fonte: IBM X-Force Report - 2016.

Notícias

Australia and the United Kingdom**,††

- Breaches at big-brand retail businesses, resulting in the theft of millions of customer account records and credit card data, were reminiscent of similar US-based incidents in years past.
- A SQL injection vulnerability at a UK ISP led to a data breach expected to cost an estimated GBP30+ million in damages.

France††

- Phishing emails sent to several French journalists provided attackers a foothold to wreak havoc at TV5Monde, an international broadcasting network.
- At the peak of the attack, 11 channels were off-air for 18+ hours, and official social media accounts were hijacked.

Turkey§§

- In December, banks, government agencies and private websites in Turkey were targeted by wide-scale DDoS attacks with peaks of over 220Gbps. By flooding the national domain registrar with traffic, attackers were able to centrally disrupt access to more than 400,000 websites that use the ".tr" top-level domain.
- Earlier in the year, 50+ million Turkish citizens were at risk for identity theft when their national identity information was leaked from a government database.

Notícias

Canada*,†

- Data was leaked from several widely-used dating and social community websites.
- Hacktivists threatened to release stolen top secret intelligence reportedly gathered from government sources.

Carbanak Global Heist†

- Since 2013, attackers have stolen more than USD1 billion from 100+ banks, in around 30 countries, including Russia, Japan, the United States and several in Europe.
- The attackers infected employee endpoints and gained access to ATM and cash transfer systems. By monitoring employee activity, they were able to mimic legitimate transactions to avoid triggering suspicion.

Japan§

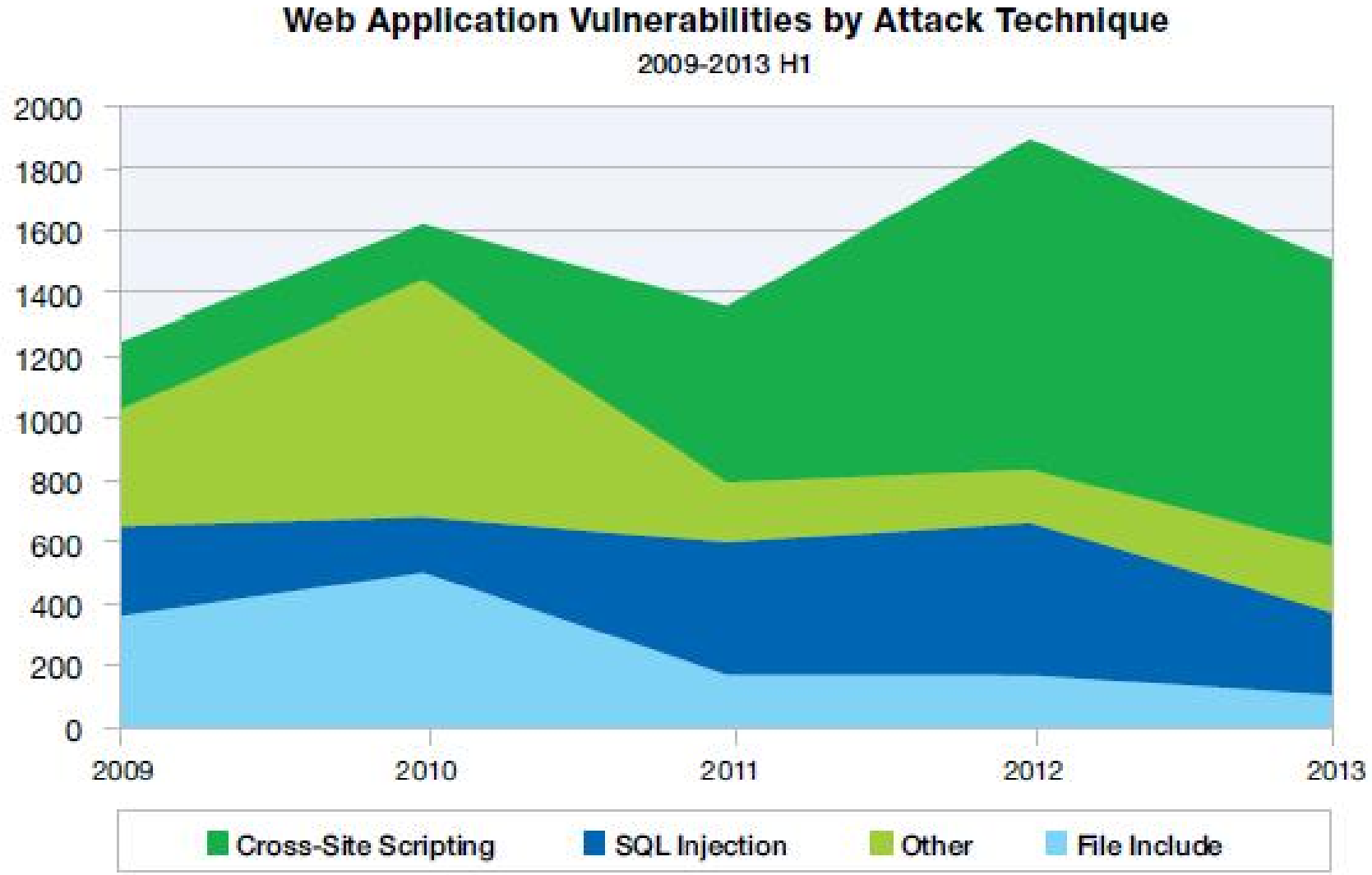
- More than one million Japanese citizens were exposed when employees at the pension service were tricked into opening a malicious email attachment, which resulted in a data breach of sensitive private information.

Quem faz uso de ataques?

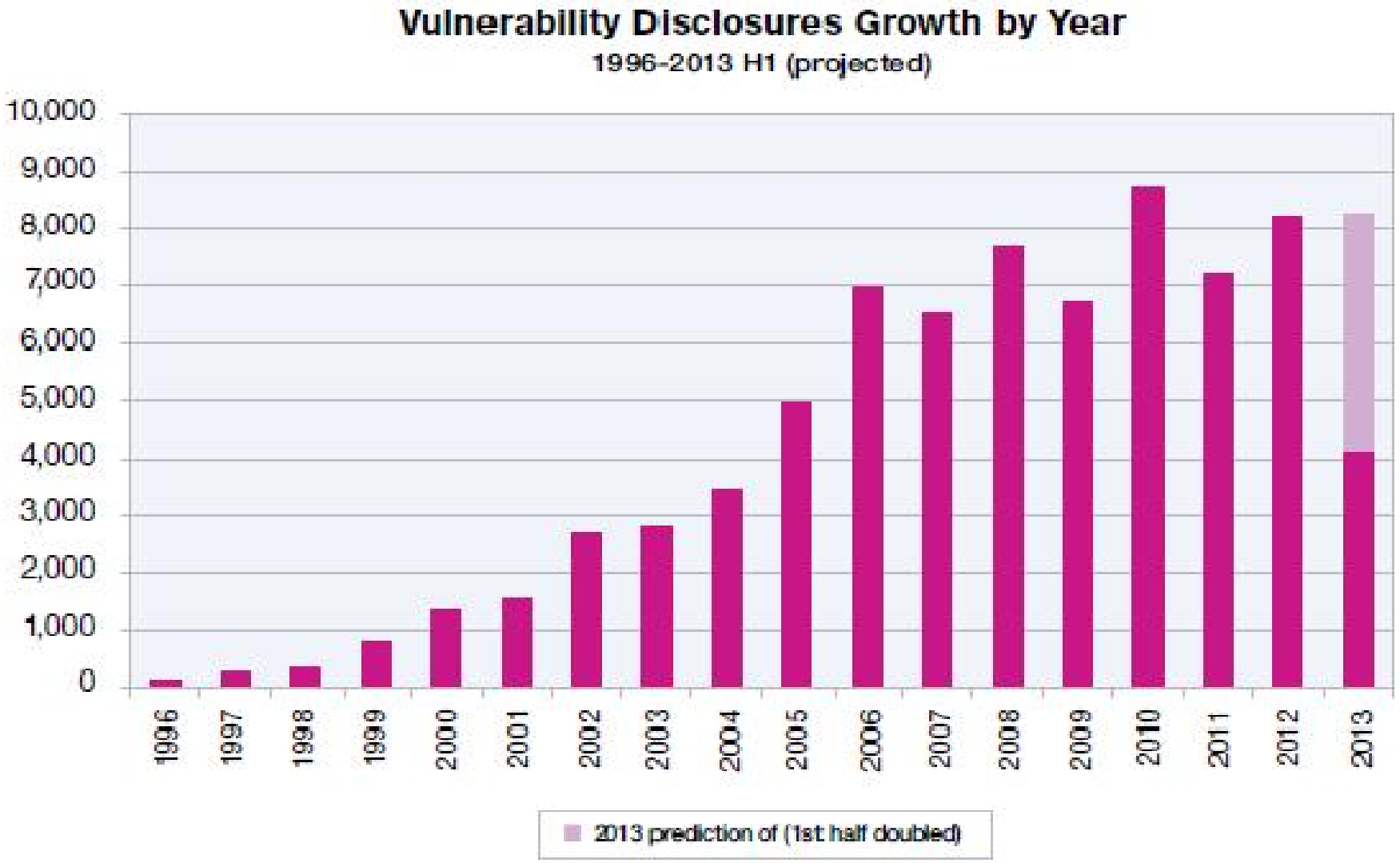
- Anonymous
  - Movimento ideológico mundial descentralizado.
  - Liderou ataques cibernéticos a diversas entidades e organizações americanas
  - Ações contra: SOPA e agora o CISPA

- Anonymous Brasil
  - Movendo campanhas contra corrupção
    - Atacou diversos sites públicos e privados:
      - DDoS:
        - bmfbovespa.com.br; bb.com.br; bcb.gov.br e camara.gov.br.
      - Invasão:
        - www.seduc.ro.gov.br; ancine.gov.br e irc.embaixadaamericana.org.br/

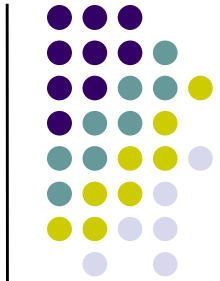
Alguns Números



Alguns Números



Revisão sobre TCP

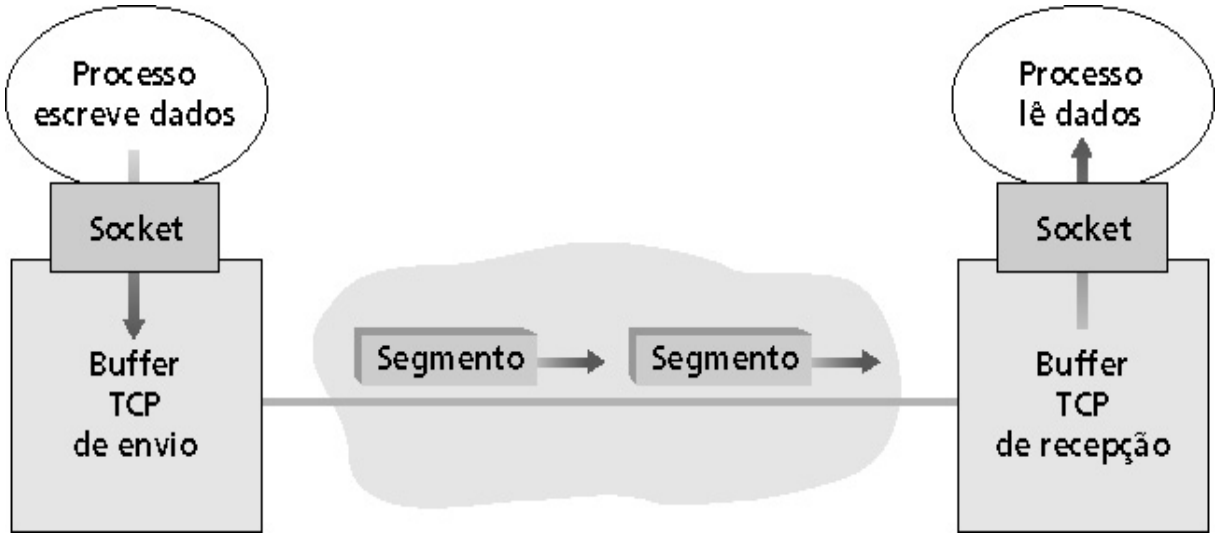


TCP: overview

- **Ponto-a-ponto:**
  - Um transmissor, um receptor
- **Confiável, sequencial byte stream**

- **Buffers de transmissão e de recepção**

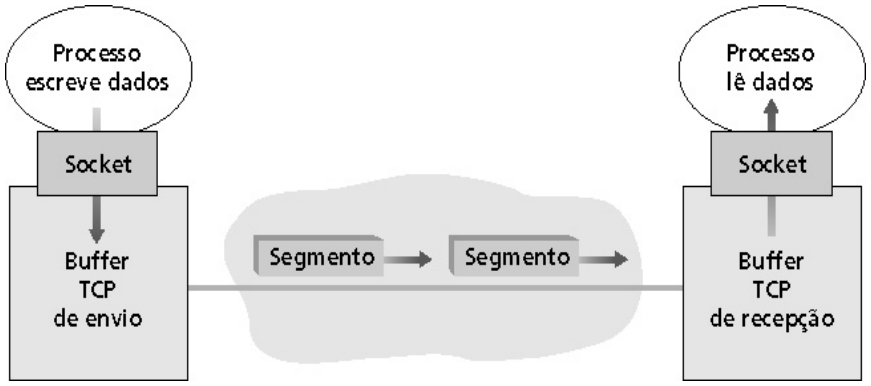
- **Paralelismo:** (transmissão de vários pacotes sem confirmação)
  - Controle de congestionamento e de fluxo definem ***tamanho das janelas de transmissão e recepção.***



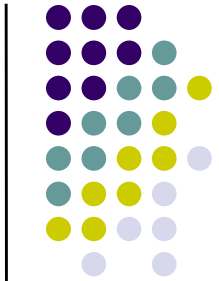
RFCs: 793, 1122, 1323, 2018, 2581

TCP: overview

- Dados full-duplex:
  - Transmissão bidirecional na mesma conexão
  - MSS: maximum segment size
- Orientado à conexão:
  - Apresentação (troca de mensagens de controle) inicia o estado do transmissor e do receptor antes da troca de dados
- Controle de fluxo:
  - Transmissor não esgota a capacidade do receptor



Estrutura Original do segmento TCP



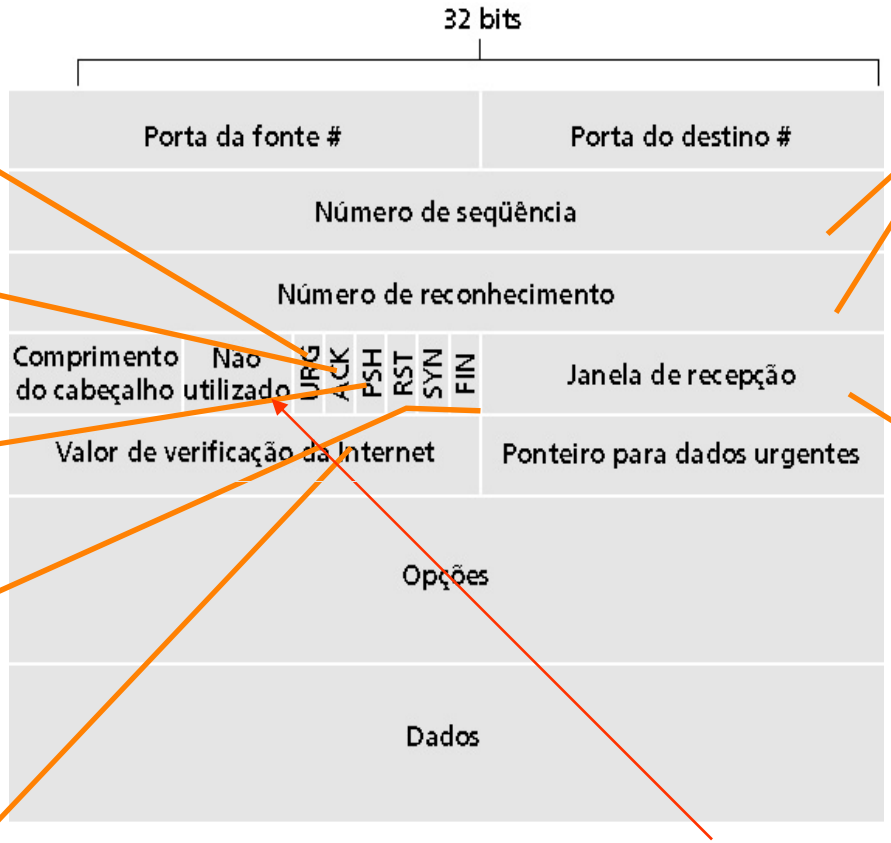
URG: dados urgentes (pouco usados)

ACK: campo de ACK é válido

PSH: produz envio de dados (pouco usado)

RST, SYN, FIN: estabelec. de conexão (comandos de criação e término)

Internet checksum (como no UDP)

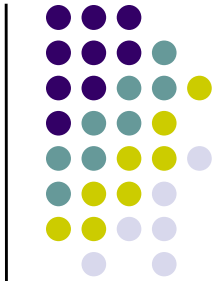


contagem por bytes de dados (não segmentos!)

número de bytes receptor está pronto para aceitar

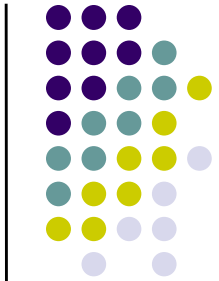
Duas flags (2 bits) foram adicionadas para auxliar no controle de congestioamento de rede (RFC 3168, 2001)
ECE – ECN-Echo : IP Explicit Congestion Notification (CE)
CWR – Window Congestion Reduced

Ataque DoS com TCP Flooding



- Ataque de DoS comum para estabelecer inúmeras conexões TCP com servidor qualquer.
- Envia inúmeros pacotes com destinos a diferentes portas ou apenas uma específica.
- Enche os buffers de recepção do receptor, inviabilizando novas conexões.
- Inviabiliza todos os serviços em cima do TCP.

Atividade 01

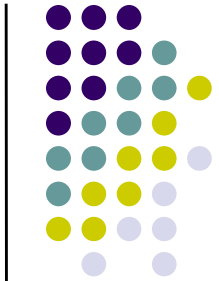


- Desenvolva uma aplicação para realizar um ataque de negação de serviço a um servidor http utilizando flooding TCP.

- Dica, tente esconder seu IP nesse tipo de ataque (spoofing).

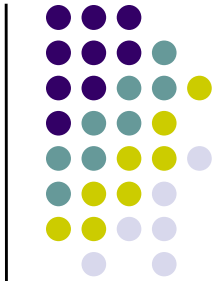
- Linguagem de programação Java, C++.
- Alvo: 172.21.210.209

Attaque DoS em HTTP



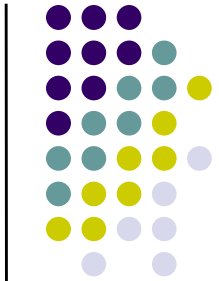
- Podemos atacar serviços específicos.
- Por exemplo um servidor Web.
- SlowLoris: é um ataque específico para webservers, inicia requisições HTTP e as mantém ativas pelo máximo de tempo possível.
- Explora vulnerabilidade de protocolo.
- Não inviabiliza outras aplicações que usam TCP na mesma máquina.

Atividade 02



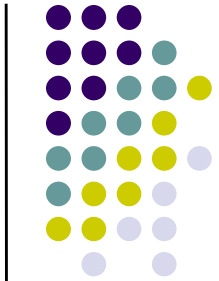
- Desenvolva uma aplicação que implemente um ataque de negação de serviço para servidores web utilizando a mesma tecnica do slowloris.
  - http://ha.ckers.org/slowloris/slowloris.pl
- Linguagem de programação Java/C++.

Ataque TCP Syn Flood



- Ataque de DoS comum para iniciar inúmeras conexões TCP com servidor qualquer, mas sem finalizar a conexão.
- Ataque que explora vulnerabilidade do protocolo de transporte.
- Tem as mesmas consequencias do TCP flooding.

Atividade Extra



- Desenvolva uma aplicação que implemente um ataque de negação de serviço utilizando a tecnica de Syn flooding.

- Linguagem de programação Java/C++.