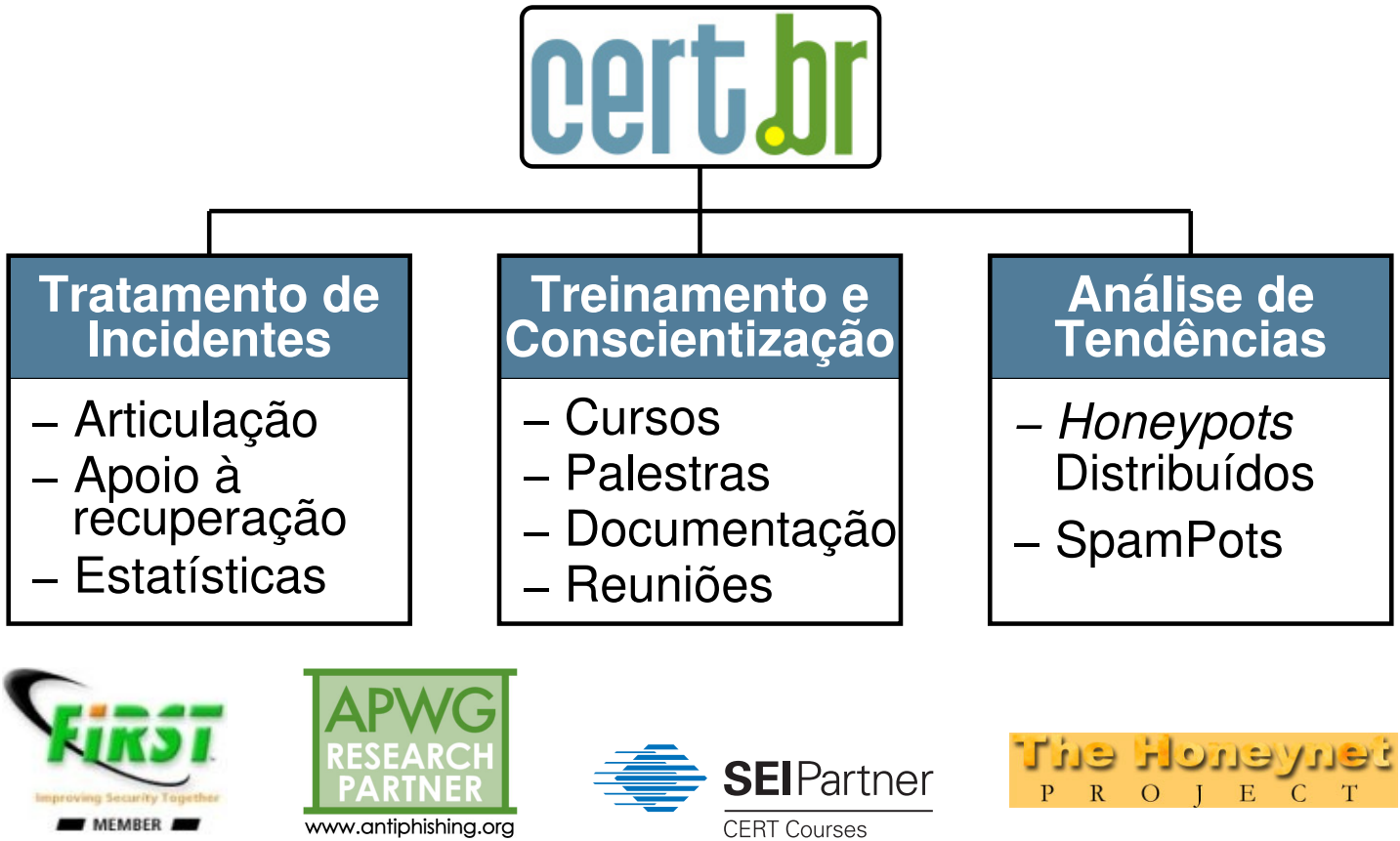
Como conviver com tantas senhas

Miriam von Zuben
miriam@cert.br

Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
Núcleo de Informação e Coordenação do Ponto br
Comitê Gestor da Internet no Brasil

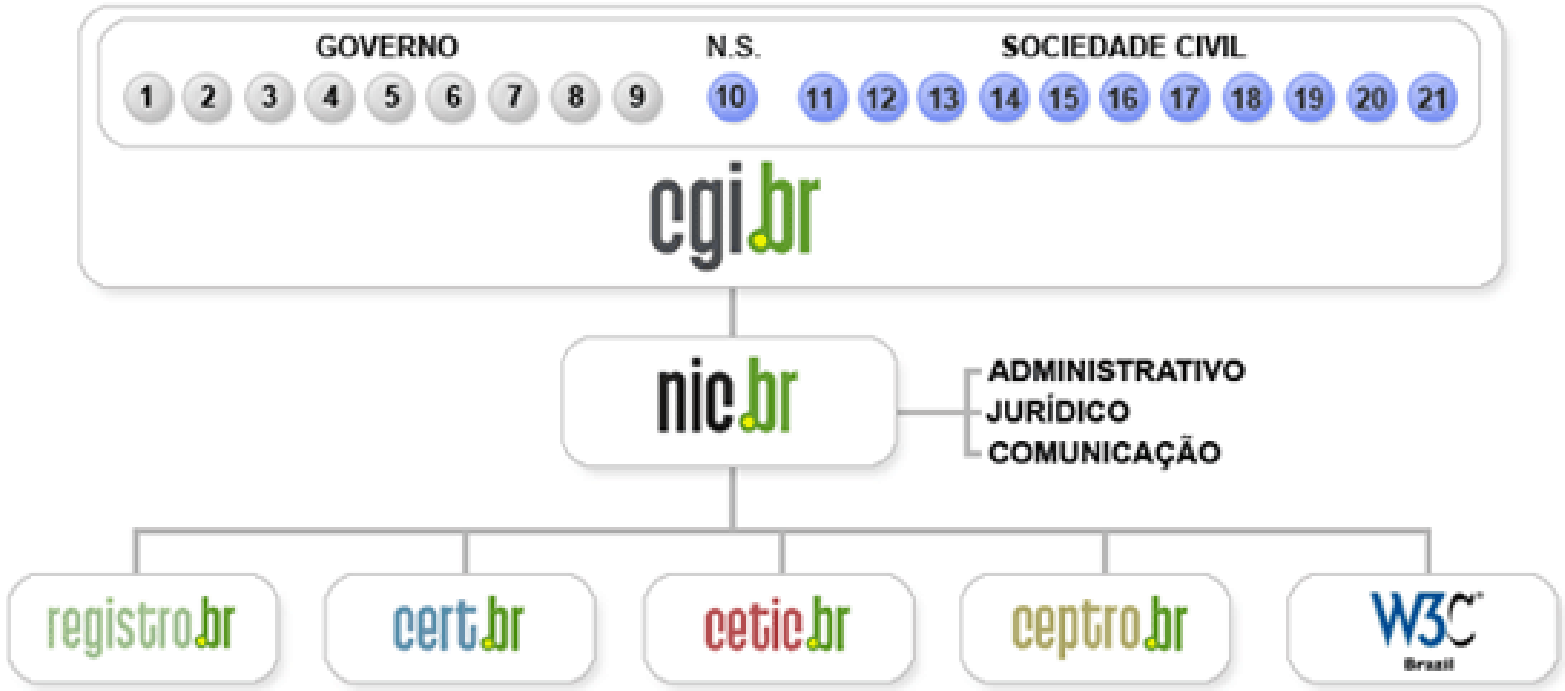
Sobre o CERT.br

Criado em 1997 como ponto focal nacional para tratar incidentes de segurança relacionados com as redes conectadas à Internet no Brasil



http://www.cert.br/sobre/

Estrutura do CGI.br



01- Ministério da Ciência e Tecnologia
02- Ministério das Comunicações
03- Casa Civil da Presidência da República
04- Ministério do Planejamento, Orçamento e Gestão
05- Ministério do Desenvolvimento, Indústria e Comércio Exterior
06- Ministério da Defesa
07- Agência Nacional de Telecomunicações
08- Conselho Nacional de Desenvolvimento Científico e Tecnológico
09- Conselho Nacional de Secretários Estaduais para Assuntos de Ciência e Tecnologia

10- Notório Saber
11- Provedores de Acesso e Conteúdo
12- Provedores de Infra-estrutura de Telecomunicações
13- Indústria TICs (Tecnologia da Informação e Comunicação) e Software
14- Empresas Usuárias
15-18- Terceiro Setor
19-21- Academia

Atribuições do CGI.br

Entre as diversas atribuições e responsabilidades definidas no Decreto Presidencial nº 4.829, destacam-se:

- a proposição de normas e procedimentos relativos à regulamentação das atividades na internet
- a recomendação de padrões e procedimentos técnicos operacionais para a internet no Brasil
- o estabelecimento de diretrizes estratégicas relacionadas ao uso e desenvolvimento da internet no Brasil
- **a promoção de estudos e padrões técnicos para a segurança das redes e serviços no país**
- a coordenação da atribuição de endereços internet (IPs) e do registro de nomes de domínios usando `<.br>`
- **a coleta, organização e disseminação de informações sobre os serviços internet, incluindo indicadores e estatísticas**

Agenda

Senhas, senhas e mais senhas

Recomendações
- O que não utilizar
- O que utilizar

Gerenciamento

Outros cuidados

Referências

Senhas, senhas e mais senhas

Uso de senhas (1/2)

Permitem acesso a:

- serviços de *e-mail*
- redes sociais
- *blogs*
- jogos *on-line*
- dispositivos móveis
- serviços bancários
- *sites* de comércio eletrônico
- computadores pessoais
- *sites* de notícias
- serviços de hospedagem
- compartilhamentos de rede
- equipamentos de rede

Uso de senhas (2/2)

Por que alguém iria querer obter suas senhas?

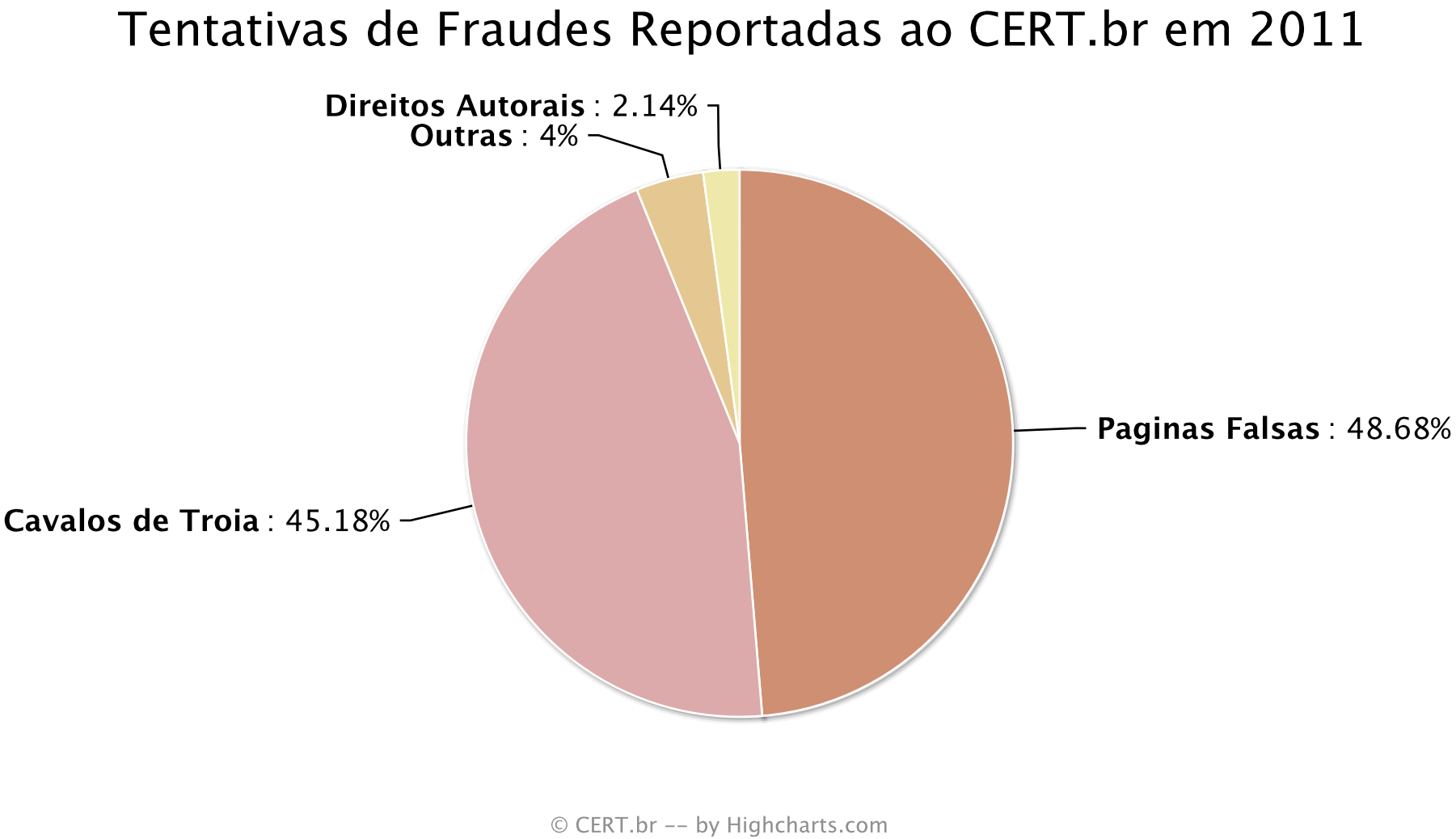
- acessar informações confidencias
- aplicar golpes de engenharia social
- propagar códigos maliciosos
- disseminar *spam*
- enviar mensagens contendo *phishing*
- invadir o computador e utilizá-lo para desferir ataques
- impedir o acesso do usuário à conta invadida

Como podem ser descobertas

Senhas podem ser descobertas através de:

- observação
- técnicas de engenharia social
- *sniffers*
- acesso ao arquivo onde elas estão armazenadas
- uso em computadores infectados (*spyware*)
- uso no acesso a *sites* falsos (*phishing*)
- ataques de força bruta

Tentativas de fraude

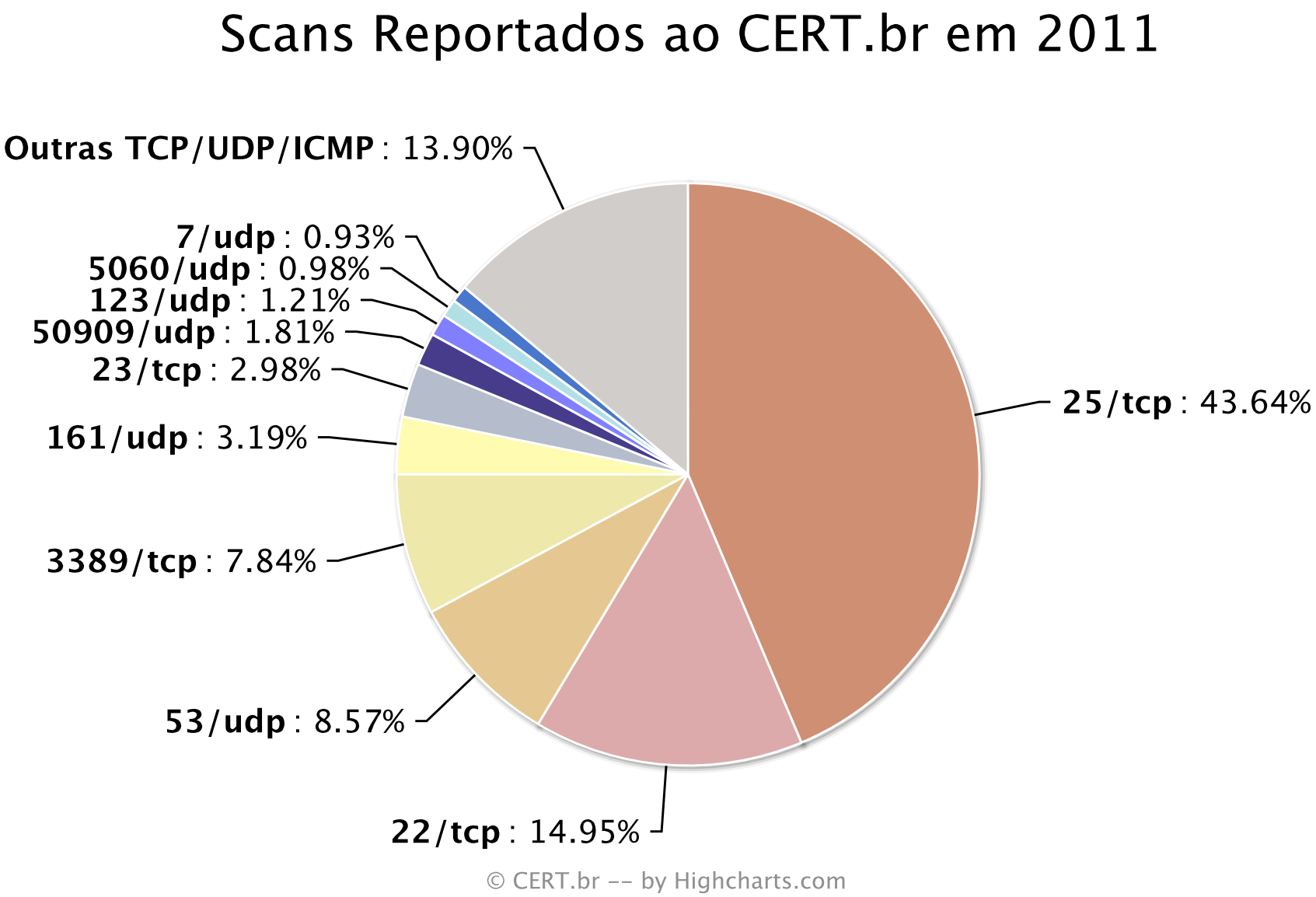


Ataques de força bruta (1/2)

Tentativas de adivinhar senhas através de:

- palavras existentes em dicionários
  - de diferentes idiomas
  - facilmente obtidos na Internet
- listas de palavras comumente usadas
- substituições óbvias de caracteres
- sequências de teclado
- informações pessoais
  - coletadas em redes sociais, *blogs*
  - de conhecimento prévio do atacante

Ataques de força bruta (2/2)



Recomendações

Recomendações

- Dados coletados pelo Projeto Honeypots Distribuídos
- Referentes a 45 sensores
- Ataques de força bruta sobre o serviço de ssh
- Período de julho a dezembro/2011

Tentativas	23.613.674
Contas únicas	155.259
Senhas únicas	347.513
Contas e senhas únicas	732.383

O que não utilizar

Dados pessoais

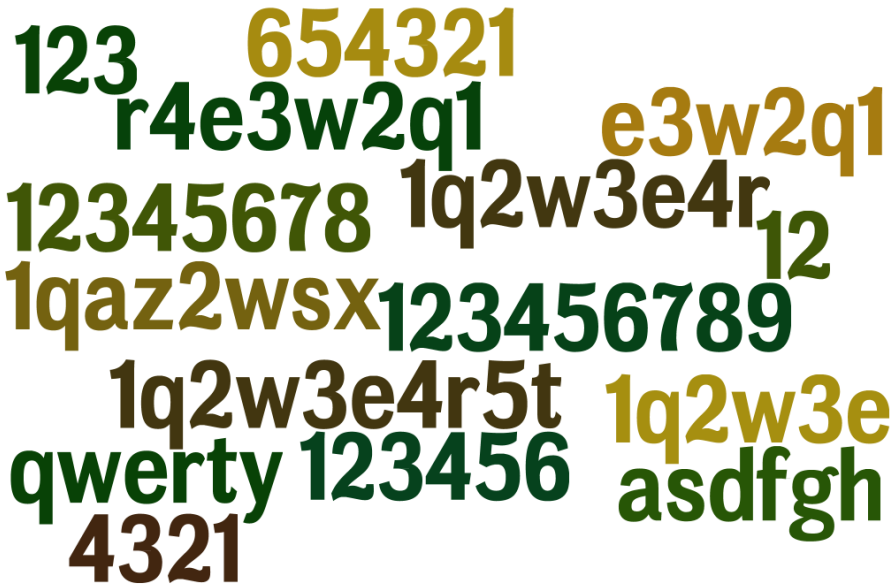
Senha igual a conta	29.18%
Senha parte da conta	11.45%
Porcentagem sobre o total	40.62%

Caracteres do mesmo tipo

Apenas dígitos	12.35%
Apenas caracteres alfabéticos	54.14%
Caracteres alfanuméricos	27.64%
Caracteres alfanuméricos e símbolos	5.86%
Senha vazia	0.01%

Sequências de teclado

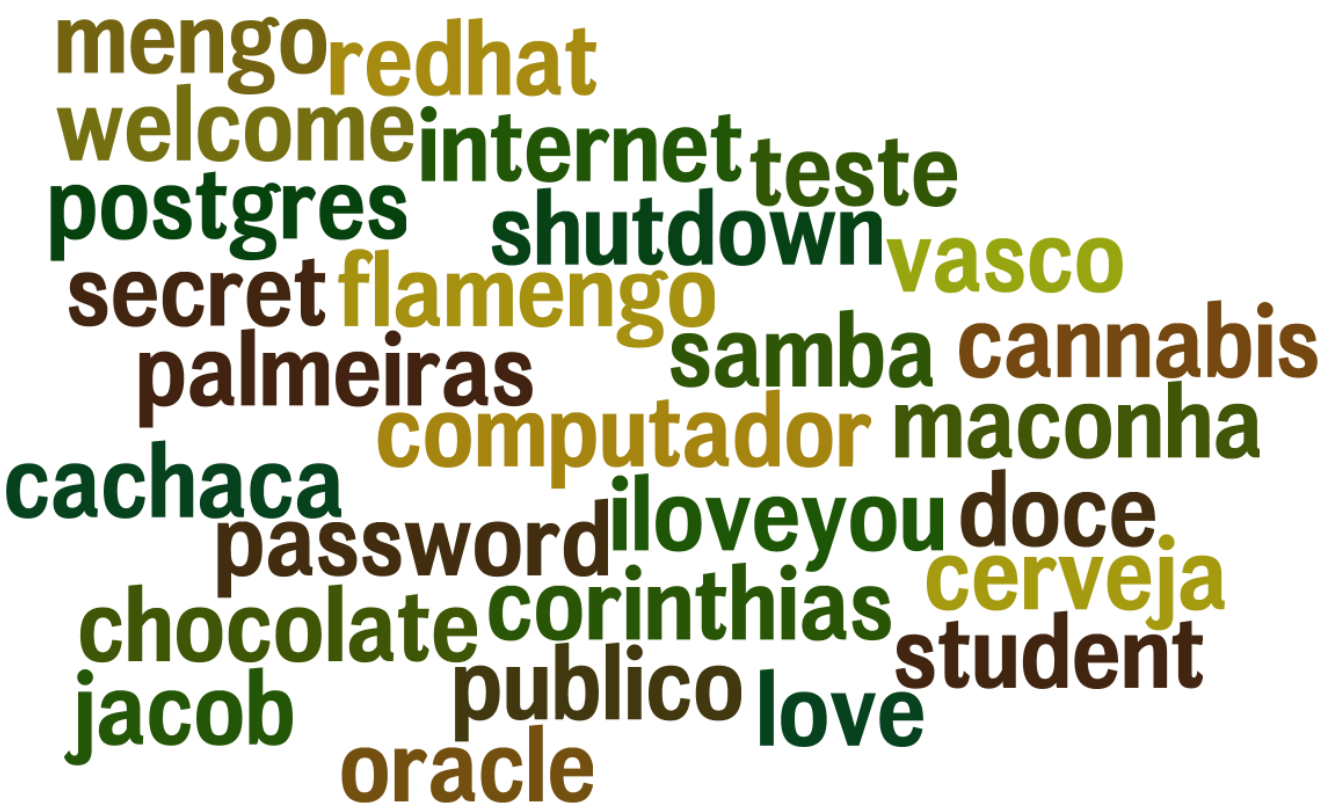
Apenas dígitos	9.17%
Apenas caracteres alfabéticos	1.49%
Caracteres alfanúmericos	2.69%
Caracteres alfanúmericos e símbolos	0.02%
Porcentagem sobre o total	13.38%



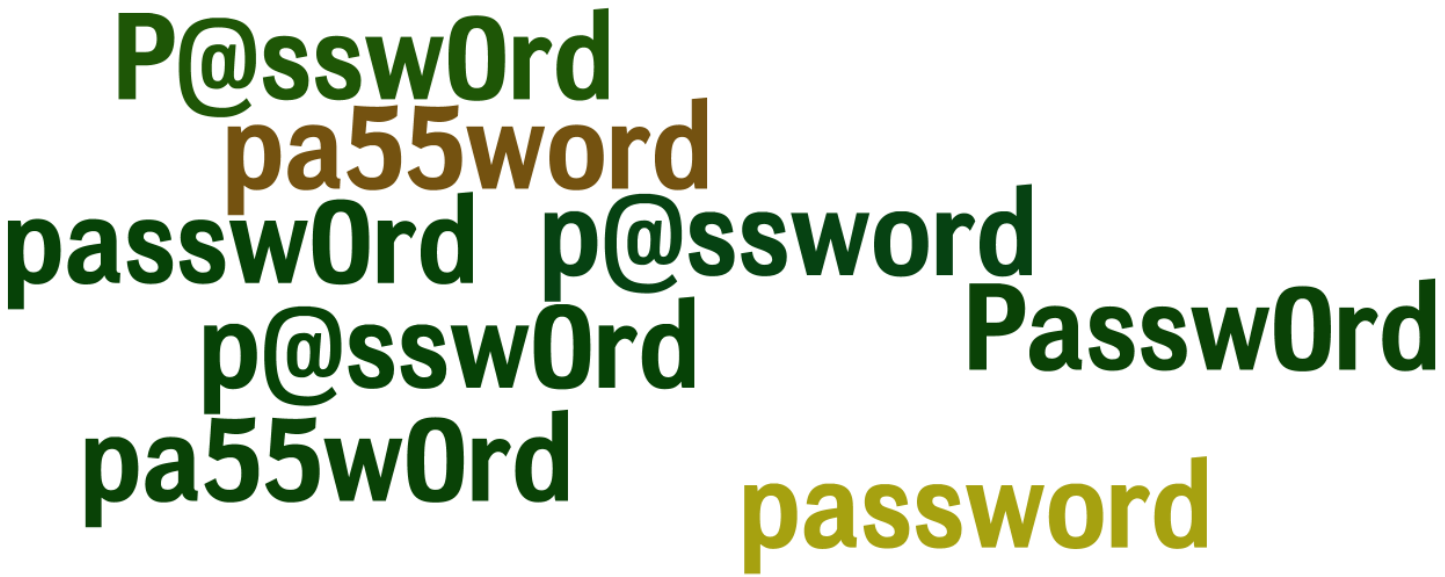
Repetições do mesmo caracter

Apenas dígitos	1.18%
Apenas caracteres alfabéticos	0.60%
Apenas símbolos	0.08%
Porcentagem sobre o total	1.86%

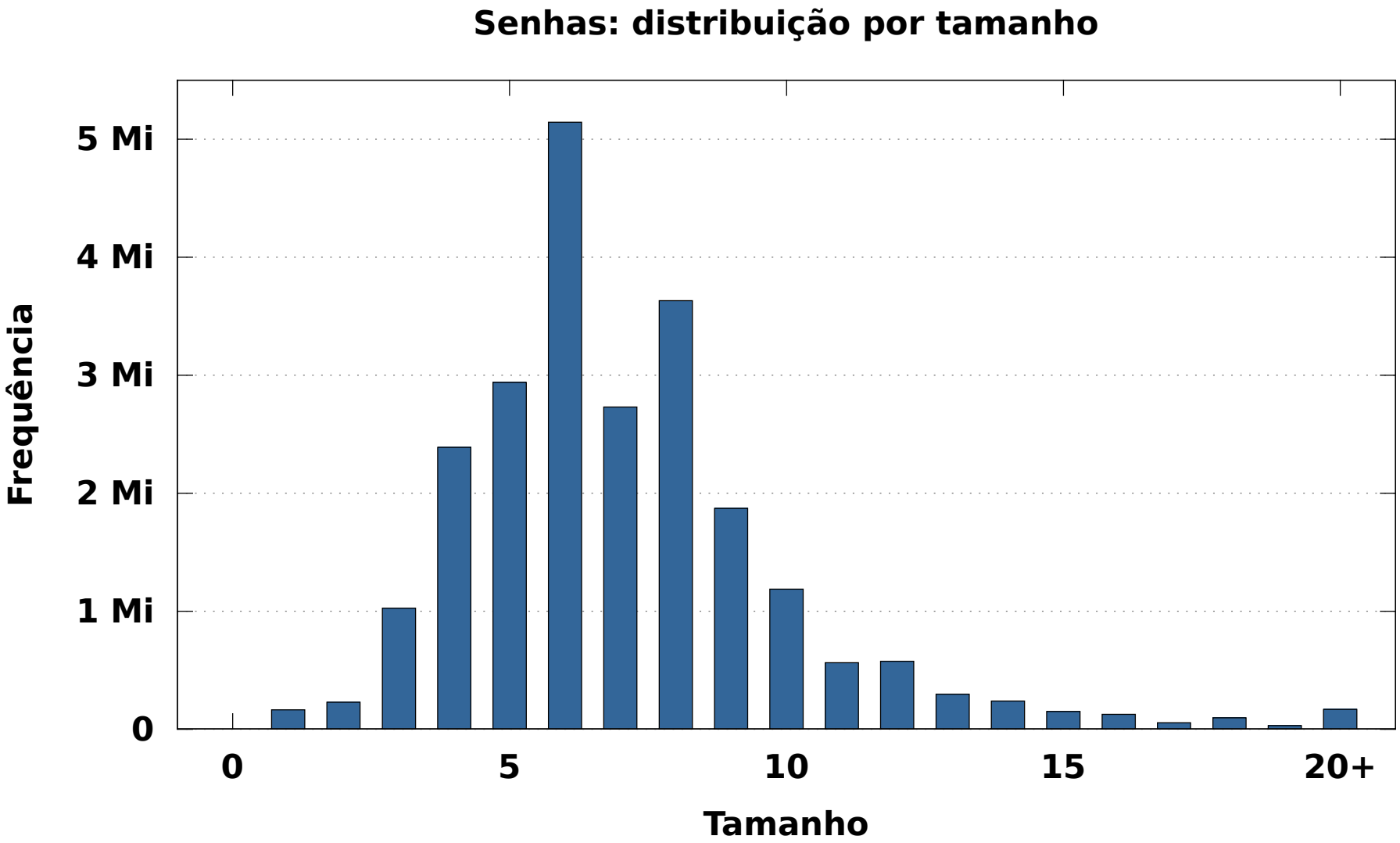
Palavras que fazem parte de listas



Substituições óbvias de caracteres



Senhas curtas

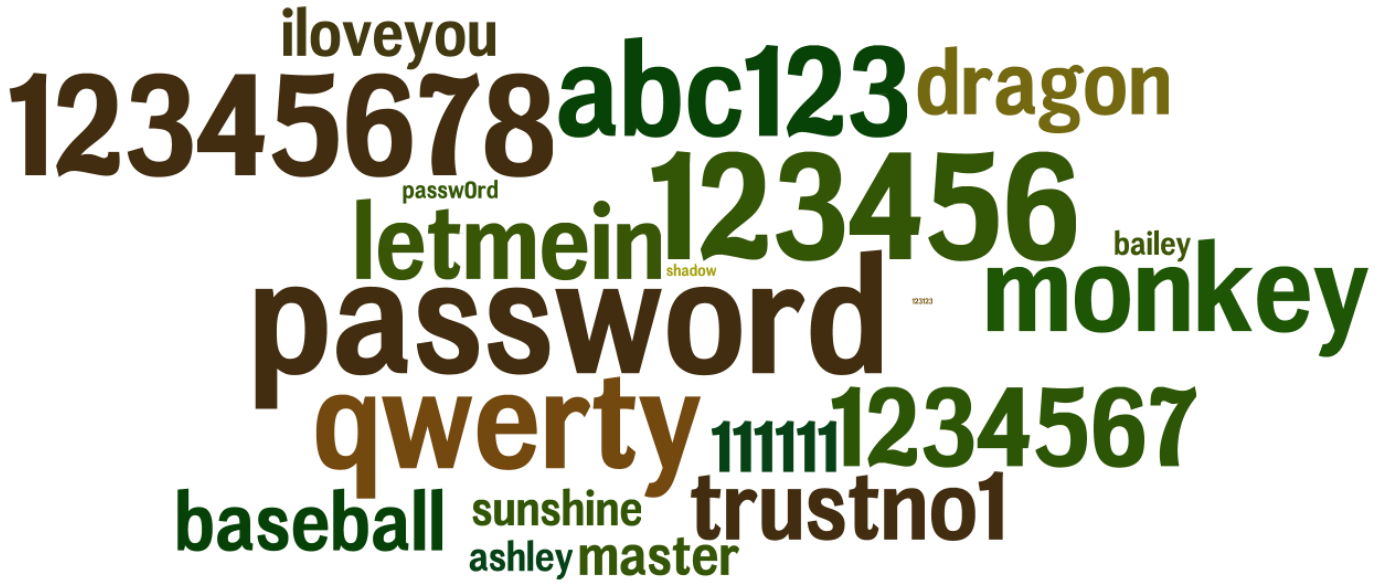


Senhas mais testadas

1	123456
2	password
3	12345
4	1234
5	123
6	654321
7	abc123
8	q1w2e3
9	1q2w3e
10	senha
11	123mudar
12	qwe123
13	mudar123
14	chocolate
15	qwerty
16	1234567
17	1q2w3e4r
18	test
19	teste
20	q1w2e3r4

Como estas tentativas podem se tornar invasões?

Senhas mais usadas (1/2)



1	password
2	123456
3	12345678
4	qwerty
5	abc123
6	monkey
7	1234567
8	letmein
9	trustno1
10	dragon
11	baseball
12	111111
13	iloveyou
14	master
15	sunshine
16	ashley
17	bailey
18	passw0rd
19	shadow
20	123123

Fonte: SplashData “25 Worst Passwords of the Year”, 2011

Senhas mais usadas (2/2)

1	123456
2	12345
3	123456789
4	Password
5	iloveyou
6	princess
7	rockyou
8	1234567
9	12345678
10	abc123
11	Nicole
12	Daniel
13	babygirl
14	monkey
15	Jessica
16	Lovely
17	michael
18	Ashley
19	654321
20	Qwerty

Fonte: Zone Alarm - “How to Avoid the Most Common and Dangerous Passwords”

O que utilizar

O que utilizar

Senhas longas

- quanto maior a senha mais difícil será descobrí-la
- com o uso frequente acabam sendo facilmente digitadas

Números aleatórios

- quanto mais aleatórios melhor
- principalmente em sistemas que aceitem **exclusivamente** caracteres numéricos

Diferentes tipos de caracteres

- quanto mais “bagunçada” mais difícil será descobrí-la

Dicas para elaboração

Selecionar caracteres de uma frase:

"Nos vemos novamente na Campus Party 2013"
"!_NvnnCP2013_!"

Utilizar uma frase longa:

"Conectando gerações e ensinando uns aos outros: sid2012"

Inventar um padrão próprio de substituição de caracteres:

"Descobrindo o mundo digital juntos... com seguranca"
"Desccobrr1nddo o munddo dd1g1t@l juntos::: ccom segurr@ncc@"

Não use estas senhas

Apenas você pode definir se sua senha é realmente boa

Gerenciamento

Métodos de gerenciamento (1/2)

Pouco indicados:

- Usar uma mesma senha para diversos serviços
  - basta que o atacante consiga uma senha para acessar diversas contas
- Salvar no navegador *Web*
  - podem ser acessadas por códigos maliciosos, ladrões e atacantes, caso não estejam criptografadas

Métodos de gerenciamento (2/2)

Mais indicados:

- Anotar em um papel e guardá-lo em local seguro
  - preferível a ter que optar por usar senhas fracas
  - segurança das senhas depende diretamente da dificuldade de acesso ao local onde o papel está guardado
- Usar serviços de hospedagem de contas/senhas
  - senhas hospedadas em servidores remotos
  - verificar políticas de privacidade
  - garantir que as senhas trafeguem criptografada
- Usar programas gerenciadores de contas/senhas
  - senhas gravadas em arquivo local
  - acessadas através de uma chave mestra
  - **não esqueça sua chave mestra**

Quando alterar a senha

Imediatamente:

- ao desconfiar que ela tenha sido descoberta
- ao usá-la em um computador comprometido
- caso o dispositivo onde ela está armazenada seja furtado

Rapidamente:

- quando usar um padrão de formação e desconfiar que uma delas tenha sido descoberta (**trocar também o padrão**)
- ao adquirir equipamentos acessíveis via rede

Regularmente:

- nos demais casos
- periodicidade de troca depende
  - de quanto a senha é exposta
  - de quão boa ela é

Como recuperar uma senha

Questões de segurança

- procure criar sua própria questão
- cuidado com questões pessoais e facilmente adivinháveis

Envio por *e-mail*

- procure alterá-la rapidamente
- cadastre um *e-mail* que você acesse frequentemente

Outros cuidados

Proteger o computador

Mantenha seu computador atualizado

- sistema operacional, aplicativos e *hardware*

Utilize e mantenha atualizados mecanismos de segurança

- *firewall* pessoal
- *antimalware*
- complementos e *plugins* em navegadores *Web*

Seja cuidadoso ao instalar aplicativos desenvolvidos por terceiros

- procure selecionar os mais usados
- denuncie caso verifique alguma ação maliciosa

Melhorar a Postura On-line

Não acessar *sites* ou seguir *links*

- recebidos por mensagem eletrônicas
- em páginas sobre as quais não se saiba a procedência

Não baseie-se na informação de remetente

- receber um *link* ou arquivo de pessoa ou instituição conhecida não é garantia de confiabilidade
- códigos maliciosos se propagam a partir das contas de máquinas infectadas
- fraudadores se fazem passar por instituições confiáveis

Informar-se e Manter-se Atualizado (1/2)

http://cartilha.cert.br/

http://internetsegura.br/

http://www.cert.br/rss/certbr-rss.xml

http://twitter.com/certbr

Informar-se e Manter-se Atualizado (2/2)

- **Site Antispam.br – Vídeos Educacionais no escopo das atividades da CT Anti-Spam do CGI.br**
  http://www.antispam.br/

Referências

- Esta apresentação pode ser encontrada em:
  http://www.cert.br/docs/palestras/
- Comitê Gestor da Internet no Brasil – CGI.br
  http://www.cgi.br/
- Núcleo de Informação e Coordenação do Ponto br – NIC.br
  http://www.nic.br/
- Centro de Estudo, Resposta e Tratamento de Incidentes no Brasil – CERT.br
  http://www.cert.br/