UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
DIRETORIA DE PESQUISA E PÓS-GRADUAÇÃO
DEPARTAMENTO ACADÊMICO DE ELETRÔNICA
CURSO DE ESPECIALIZAÇÃO SEMIPRESENCIAL EM CONFIGURAÇÃO E GERENCIAMENTO DE SERVIDORES E EQUIPAMENTOS DE REDES

HEMURYEL LENNON LEONEL DA SILVA

SEGURANÇA DA INFORMAÇÃO: ESTUDO DE CASO SOBRE O VAZAMENTO DE SENHAS – ANO DE 2017

MONOGRAFIA DE ESPECIALIZAÇÃO

CURITIBA
2018

HEMURYEL LENNON LEONEL DA SILVA

SEGURANÇA DA INFORMAÇÃO: ESTUDO DE CASO SOBRE O VAZAMENTO DE SENHAS – ANO DE 2017

Monografia de Especialização, apresentada ao Curso de Especialização Semipresencial em Configuração e Gerenciamento de Servidores e Equipamentos de Redes, do Departamento Acadêmico de Eletrônica – DAELN, da Universidade Tecnológica Federal do Paraná – UTFPR, como requisito parcial para obtenção do título de Especialista.

Orientador: Prof. M.Sc. Christian Carlos Souza Mendes

CURITIBA

2018

Ministério da Educação
Universidade Tecnológica Federal do Paraná
Câmpus Curitiba

Diretoria de Pesquisa e Pós-Graduação
Departamento Acadêmico de Eletrônica
Curso de Especialização Semipresencial em Configuração e Gerenciamento de Servidores e Equipamentos de Redes

TERMO DE APROVAÇÃO

SEGURANÇA DA INFORMAÇÃO: ESTUDO DE CASO SOBRE O VAZAMENTO DE SENHAS – ANO DE 2017

por

HEMURYEL LENNON LEONEL DA SILVA

Esta monografia foi apresentada em 25 de setembro de 2018 como requisito parcial para a obtenção do título de Especialista em Configuração e Gerenciamento de Servidores e Equipamentos de Redes. O candidato foi arguido pela Banca Examinadora composta pelos professores abaixo assinados. Após deliberação, a Banca Examinadora considerou o trabalho aprovado.

_____
Prof. M.Sc. Christian Carlos Souza Mendes
Orientador

_____
Prof. Dr. Kleber Kendy Horikawa Nabas
Membro titular

_____
Prof. M. Sc. Omero Francisco Bertol
Membro titular

- O Termo de Aprovação assinado encontra-se na Coordenação do Curso -

Gostaria de dedicar este trabalho produzido à todas as pessoas que fazem parte da minha vida, principalmente à minha família.

AGRADECIMENTOS

Agradeço à minha família pelo apoio na minha jornada acadêmica.

Agradeço também ao meu orientador Prof. Christian C. S. Mendes, pela orientação e conhecimento que me norteou nesta trajetória.

Aos meus colegas de sala.

A Secretaria do Curso, pela cooperação.

Enfim, a todos que contribuíram na realização e no apoio deste trabalho.

“Uma senha simples é tão perigosa quanto não ter senha alguma” (KISSELL, 2017).

RESUMO

SILVA, Hemuryel Lennon Leonel da. **Segurança da informação: estudo de caso sobre o vazamento de senhas - ano de 2017**. 2018. 90 p. Monografia de Especialização em Configuração e Gerenciamento de Servidores e Equipamentos de Redes, Departamento Acadêmico de Eletrônica, Universidade Tecnológica Federal do Paraná. Curitiba, 2018.

O uso de senhas é importante para restringir o acesso, garantir a confidencialidade e a autenticidade, no entanto, a sua má elaboração ou o uso constante de uma única senha para os mais variados serviços pode comprometer sua privacidade. O objetivo desta monografia é realizar uma análise das senhas que foram vazadas em 2017 através de um estudo de caso, mostrando sua entropia e como uma senha mesmo que criptografada, se torna fraca se utilizada de uma palavra-chave de poucos caracteres. A metodologia utilizada neste trabalho é de natureza exploratória e explicativa, e foi realizado através de fontes bibliográficas e secundárias, tratada de maneira quantitativa e qualitativa, surgiu pela necessidade de analisar a divulgação de dados sensíveis na internet como as senhas pessoais. Como resultado desta monografia, foi constatado como é possível calcular a força de uma senha, isto é, sua entropia, quais senhas devem ser memorizadas e como criá-las de maneira mais seguras e como utilizar gerenciadores para criação e armazenamento seguro de senhas aleatórias para as outras centenas de serviços.

Palavras-chave: Senha. Criptografia. Segurança. Entropia. Confidencialidade.

ABSTRACT

SILVA, Hemuryel Lennon Leonel da. **Information security: case study on password leakage - year 2017**. 2018. 90 p. Monografia de Especialização em Configuração e Gerenciamento de Servidores e Equipamentos de Redes, Departamento Acadêmico de Eletrônica, Universidade Tecnológica Federal do Paraná. Curitiba, 2018.

The use of passwords is important to restrict access, ensure confidentiality and authenticity, however, poorly crafted or constantly using a single password for the most varied services can compromise your privacy. The objective of this monograph is to perform an analysis of the passwords that were leaked in 2017 through a case study, showing its entropy and as a password even if encrypted, becomes weak if used for a keyword of few characters. The methodology used in this work is exploratory and explanatory, and was carried out through bibliographic and secondary sources, treated in a quantitative and qualitative way, arose from the need to analyze the disclosure of sensitive data on the Internet as personal passwords. As a result of this monograph, it was found how it is possible to calculate the strength of a password, that is, its entropy, which passwords should be memorized and how to create them in a more secure way, and how to use managers to create and secure random the other hundreds of services.

Keywords: Password. Encryption. Security. Entropy. Confidentiality.

LISTA DE QUADROS

LISTA DE FIGURAS

LISTA DE SIGLAS

ASCII	*American Standard Code for Information Interchange*
Bit	*Binary digit*
cert.br	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
CPU	*Central Processing Unit*
GHz	GIGA-HERTZ
GPU	*Graphics Processing Unit*
HIBP	*Have I Been Pwned*
SHA	*Secure Hash Algorithms*
UCP	Unidade Central de Processamento

LISTA DE ACRÔNIMOS

CIA	*Confidentiality, Integrity, Availability*
RFC	*Request for Comments*

LISTA DE SÍMBOLOS

log	Logaritmo
^	Expoente
<	Menor do que
x	Multiplicação
+-	Aproximadamente
±	Aproximadamente
+	Soma

SUMÁRIO

1 INTRODUÇÃO

Senha é uma informação privada, onde a pessoa que a criou e a entidade responsável pelo seu gerenciamento somente deve ter acesso. Ela é importante para restringir o acesso, garantir a confidencialidade e a autenticidade ao se utilizar os mais variados tipos de serviço (CERT.BR, 2012).

No entanto, o uso inadequado dela, isto é, a sua má elaboração ou divulgação, pode gerar sérias consequências, como ter os dados pessoais usados por terceiros, caso ocorram tentativas de invasões de acesso (MITNICK; SIMON, 2003).

A estrutura desta monografia é tratada da seguinte forma:

- O capítulo 1 é composto pela introdução, objetivos, justificativa e metodologia;
- O capítulo 2 trata do referencial teórico utilizado, mostrando os conceitos básicos relacionados ao tema proposto, englobando as definições de informação, Segurança de Informação e criptografia e apresenta os fundamentos essenciais para o entendimento de elaboração de senhas mais seguras;
- O capítulo 3 contém o Estudo de Caso da análise da entropia de senhas “vazadas” e as mais utilizadas em 2017;
- O capítulo 4 exibe as considerações na proteção de senhas, explica o problema de utilizar uma mesma senha para várias contas e como saber se as suas senhas já foram descobertas;
- O capítulo 5 trata das considerações finais a respeito do trabalho.

1.1 OBJETIVOS

1.1.1 Objetivo Geral

O objetivo geral desta monografia de especialização é realizar uma análise referente as senhas descobertas e divulgadas através de sites na internet durante o ano de 2017, no âmbito de simplicidade e robustez.

1.1.2 Objetivos Específicos

Para atender ao objetivo geral neste trabalho de conclusão de curso os seguintes objetivos específicos serão abordados:

- Identificar o perfil de senhas mais “vazadas”;
- Realizar o levantamento das características das contas, relacionadas ao usuário e ao serviço utilizado;
- Abordar os principais meios e serviços de divulgação;
- Propor sugestões para o aumento da segurança em relação a estrutura das senhas.

1.2 JUSTIFICATIVA

A grande maioria dos usuários possuem diversas contas nos mais variados tipos de serviços e para cada uma, há uma senha, com isto surge a dúvida: como é possível lembrar de todas as palavras chaves utilizadas? Com este problema, o usuário passa a se utilizar de senhas mais simples podendo conter dados pessoais, repetições de teclas no computador, chegando até a estabelecer um padrão, que facilite sua descoberta por adivinhação, ou até mesmo a utilizar a mesma senha para todas as contas como aponta Kissell (2017, p. 14):

> Inventar novas senhas aleatórias e memorizá-las de forma segura não é uma tarefa possível para o cérebro humano. Diante dessa dificuldade as pessoas normalmente procuram por atalhos. Assim, elas escolhem senhas fáceis, como o nome dos seus filhos ou um padrão de teclas do teclado. Mesmo que elas se deem ao trabalho de criar uma senha mais complexa, elas acabam a utilizando em todos os lugares, pois assim é necessário memorizar apenas uma senha em vez de dezenas.

Com isto surgem outras questões, se o cérebro humano não consegue memorizar dezenas ou até mesmo centenas de senhas aleatórias como então será possível elaborar senhas mais seguras criadas de forma randômica? E o que define uma senha ser forte?

Levando em consideração a capacidade limitada de nosso cérebro em memorizar, às vezes, não só uma, mas as diversas senhas que possuímos, o uso de ferramentas que ajudem nesse trabalho de gravar as chaves é pertinente, portanto o recomendado é utilizar gerenciadores de senhas para não ter que se preocupar em decorar diversas senhas e sim se preocupar com apenas uma única senha mestre para acessar as demais contas, com isto evita o problema de utilizar uma mesma senha para serviços diferentes, os gerenciadores possuem a base de dados criptografada para proteger seu armazenamento conforme relata Kissell (2017):

> [...] os algoritmos de criptografia utilizados pela maioria (se não por todos) dos gerenciadores de senhas passaram por uma verificação rigorosa e pública realizada por criptógrafos profissionais, mesmo que seu código fonte não seja aberto.

Cada senha possui uma força, através do cálculo de entropia é possível calcular o quanto a segura é segura, no entanto, deve ser levado em consideração que deve ser criada de forma randômica (KISSELL, 2017).

Geralmente as pessoas tendem a não levar a sério a criação de uma nova conta em um novo serviço, pois elas acham que nunca acontecerão com elas um acesso por terceiros no futuro, dessa forma, se utilizam de práticas inseguras, só tendem a se preocupar com seus dados pessoas, quando o inevitável acontece (MITNICK; SIMON, 2003).

Práticas inseguras se tratam de elaborar uma senha com poucos caracteres, utilizar dados pessoais, palavras de dicionários, que facilitem a adivinhação por pessoas não autorizadas (MITNICK; SIMON, 2003).

Utilizar senhas de acesso é importante para poder autenticar em um determinado serviço, conforme afirma Kissell (2017, p. 65):

> [...] termo autenticar – que significa, literalmente, “provar a sua identidade” – com o sentido de “acessar um dispositivo ou serviço utilizando o seu nome de usuário e senha”. Ou seja, ao se autenticar em um computador ou website, você está provando que é quem diz ser. Não é possível realizar uma autenticação em um serviço que não o conhece, pois é necessário possuir uma conta já armazenada. Toda a noção de autenticação se baseia na ideia de que a parte que está realizando a sua autenticação precisa saber quem é você.

A justificativa para este trabalho é fornecer um estudo de caso das análises de senhas mais utilizadas e que foram vazadas no ano de 2017 para conscientizar sobre a importância de utilizar boas práticas na elaboração e na utilização de senhas.

1.3 METODOLOGIA

A metodologia utilizada neste trabalho é de pesquisa exploratória, visando fornecer mais informações para a investigação do tema, e explicativa, identificando os fatores que apoiam os acontecimentos dos fenômenos (PRODANOV; FREITAS, 2013).

De acordo com Prodanov e Freitas (2013, p. 52):

> [...] A pesquisa exploratória possui planejamento flexível, o que permite o estudo do tema sob diversos ângulos e aspectos. Em geral, envolve:
> - levantamento bibliográfico; [...] - análise de exemplos que estimulem a compreensão. [...] Pesquisa explicativa: quando o pesquisador procura explicar os porquês das coisas e suas causas, por meio do registro, da análise, da classificação e da interpretação dos fenômenos observados.

Quanto à natureza utilizada foram escolhidas a básica, para gerar novos conhecimentos úteis, e a aplicada, para gerar novos conhecimentos na solução de problemas específicos (PRODANOV; FREITAS, 2013).

Referente à forma de abordagem do problema foram optadas pela quantitativa e qualitativa. Prodanov e Freitas (2013, p. 69-70) afirmam que:

> [...] Pesquisa quantitativa: considera que tudo pode ser quantificável, o que significa traduzir em números opiniões e informações para classificá-las e analisá-las. [...] No desenvolvimento da pesquisa de natureza quantitativa, devemos formular hipóteses e classificar a relação entre as variáveis para garantir a precisão dos resultados, evitando contradições no processo de análise e interpretação. [...] Pesquisa qualitativa: considera que há uma relação dinâmica entre o mundo real e o sujeito, isto é, um vínculo indissociável entre o mundo objetivo e a subjetividade do sujeito que não pode ser traduzido em números. A interpretação dos fenômenos e a atribuição de significados são básicas no processo de pesquisa qualitativa.

Em relação aos procedimentos foram adotados:

- O bibliográfico se utilizando do tipo de instrumento de fontes bibliográficas para fundamentação do estudo através de material já publicado (PRODANOV; FREITAS, 2013).
- O documental se utilizando de fontes secundárias de dados para materiais que não receberam tratamento analítico (PRODANOV; FREITAS, 2013);
- E o estudo de caso para compor e analisar as senhas mais utilizadas e divulgadas no ano de 2017. Ao todo foram encontradas 100 senhas mais utilizadas no ano de 2017 e uma base de dados que foi exposta do serviço Instagram através do compartilhamento pelo Pastebin na internet no ano de 2017 (PRODANOV; FREITAS, 2013).

2 REFERENCIAL TEÓRICO

Neste capítulo aborda todos os fundamentos que serviram de base para a análise das senhas do estudo de caso proposto.

Explica sobre os conceitos básicos de segurança da informação e criptografia, logo após fala sobre os fatores que podem ser levados na elaboração, na análise e na auditoria de senhas, tais como:

- Conjunto de caracteres;
- Entropia;
- Comprimento;
- Tempo de processamento;
- Máscara.

Ainda no último tópico será aborda as principais ameaças que devem ser consideradas quando o assunto é a utilização de senhas.

2.1 SEGURANÇA DA INFORMAÇÃO

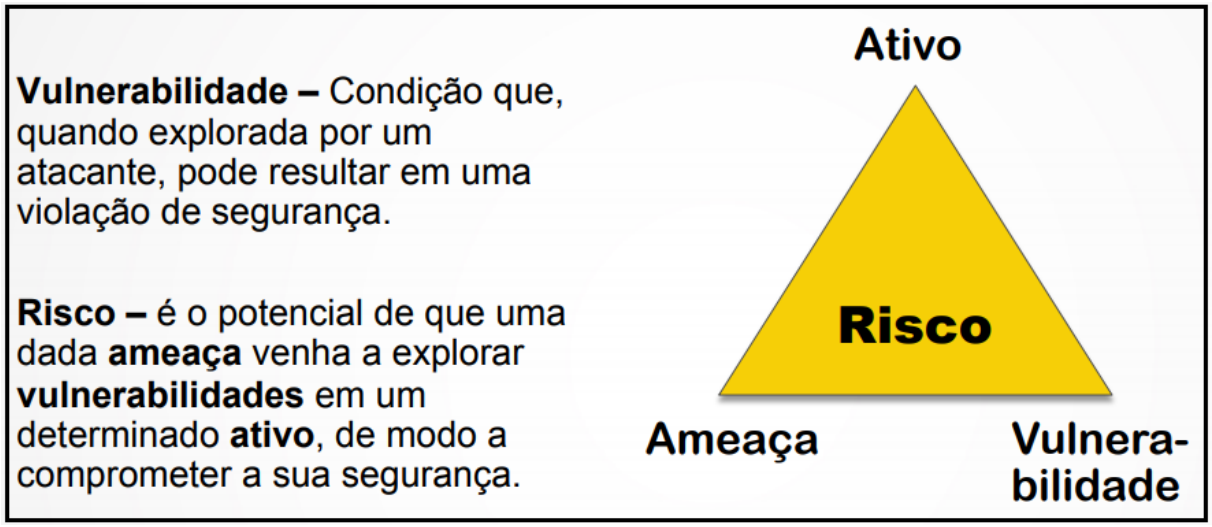
Para se iniciar sobre o tema proposto é necessário, antes de tudo, começar pela definição de informação, segundo a norma ABNT NBR ISO/IEC 27002 (ABNT, 2005) “a informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e consequentemente necessita ser adequadamente protegida”.

De acordo com Coelho, Araújo e Bezerra (2014, p. 2):

> [...] Ativo: qualquer coisa que tenha valor para a organização e para os seus negócios. [...] Incidente de segurança: corresponde a qualquer evento adverso relacionado à segurança; por exemplo vazamento e obtenção de acesso não autorizado a informações. [...] Segurança da Informação compreende a proteção das informações, sistemas, recursos e demais ativos contra desastres, erros (intencionais ou não) e manipulação não autorizada, objetivando a redução da probabilidade e do impacto de incidentes de segurança.

Após se falar sobre ativo, é importante introduzir (Figura 1) sobre o que vem a ser risco e vulnerabilidade na segurança da informação.

Figura 1 - Risco e vulnerabilidade



Fonte: Cert.br (2012). Disponível em: <https://www.cert.br/docs/palestras/certbr-egi2014.pdf>. Acesso em: 07 set. 2018.

Observa-se, ainda na Figura 1, que ativo está diretamente relacionado a risco, uma vez que tem um valor importante na organização (STALLINGS, 2015).

Na imagem, apresentada na Figura 2, é mostrado os principais exemplos de riscos, atacantes (ameaças) e vulnerabilidades.

Figura 2 - Exemplo de riscos

Fonte: Cert.br (2012). Disponível em: <https://www.cert.br/docs/palestras/certbr-egi2014.pdf>. Acesso em: 07 set. 2018.

Para a proteção dos ativos, a segurança da informação se fundamenta em três conceitos básicos: Confidencialidade, Integridade e Disponibilidade (do acrônimo em inglês para *Confidentiality, Integrity, Availability*) que fazem parte da Tríade CIA apresentada na Figura 3 (STALLINGS, 2015).

Figura 3 - Tríade CIA (*Confidentiality*, *Integrity*, *Availability*)

Fonte: Henderson (2017).

A imagem, ainda da Figura 3, exibe o triângulo representando a tríade, onde a Segurança da Informação (do inglês, *Information Security*) está localizada na região central, sendo composta ao seu redor pela tríade CIA (STALLINGS, 2015).

Confidencialidade está relacionada a dois fatores como: a confidencialidade de dados e a privacidade. O primeiro diz respeito que as informações privadas não estejam disponíveis as pessoas não autorizadas e o segundo, que as informações privadas sejam controladas pelo próprio dono. Partindo deste princípio, entende-se que o inverso de confidencialidade é quando suas informações são expostas ou acessíveis à outras pessoas (STALLINGS, 2015).

Integridade é o fato da informação permanecer integra, ou melhor dizendo, que não seja modificada ou destruída por pessoas não autorizadas, assegurando que a informação seja alterada somente quando autorizada (STALLINGS, 2015).

Disponibilidade é a informação estar acessível para o sujeito autorizado, e indisponível para pessoas sem permissão (STALLINGS, 2015).

Os objetivos principais da criação de uma senha são fornecer a confidencialidade e a autenticidade ao indivíduo. Estas duas características fazem parte dos pilares fundamentais da segurança da informação, a tríade CIA (STALLINGS, 2015).

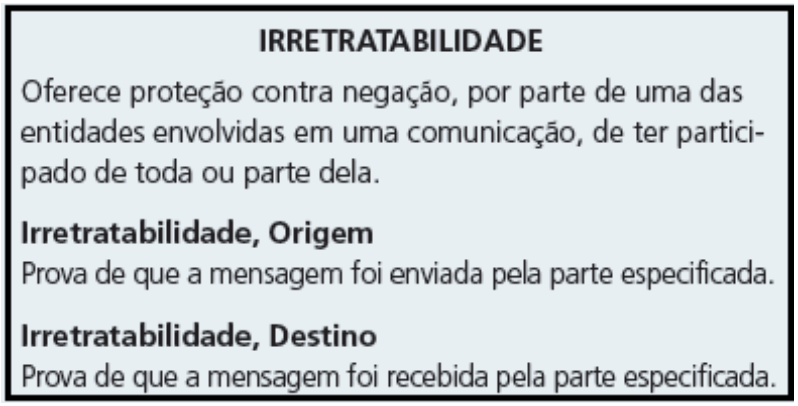
Além destes conceitos básicos, também são importantes mencionar para complementar os conceitos da tríade CIA: a Autenticidade, a Responsabilização e a Irretratabilidade (STALLINGS, 2015).

Conforme relatado pelo Stallings (2015):

> [...] Autenticidade: a propriedade de ser genuíno e capaz de ser verificado e confiável; confiança na validação de uma transmissão, em uma mensagem ou na origem de uma mensagem. Isso significa verificar que os usuários são quem dizem ser e, além disso, que cada entrada no sistema vem de uma fonte confiável. [...] Responsabilização: a meta de segurança que gera o requisito para que ações de uma entidade sejam atribuídas exclusivamente a ela.

O conceito da “irretratabilidade” é mostrado na Figura 4.

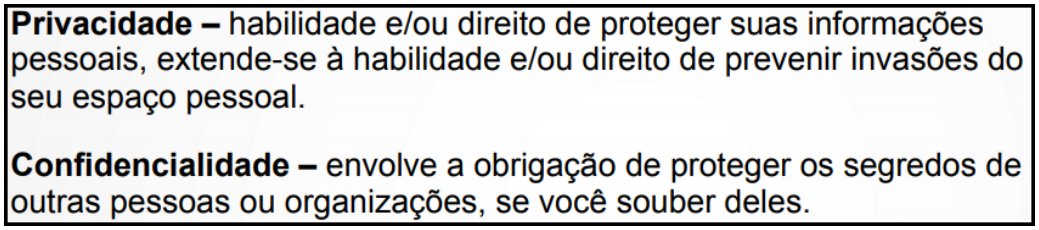
Figura 4 - Definição de irretratabilidade



Fonte: Stallings (2015).

Na Segurança da Informação, ao se comparar o conceito de Confidencialidade com Privacidade, tem-se o resultado apresentado na Figura 5.

Figura 5 - Comparação: confidencialidade e privacidade



Fonte: Cert.br (2012). Disponível em: <https://www.cert.br/docs/palestras/certbr-egi2014.pdf>. Acesso em: 07 set. 2018.

E também é válido ressaltar sobre o que vem a ser auditoria em Segurança da Informação, segundo Fonseca (2012):

> A auditoria de sistemas de informação visa verificar a conformidade não dos aspectos contábeis da organização, mas sim do próprio ambiente informatizado, garantindo a integridade dos dados manipulados pelo computador. Assim, ela estabelece e mantém procedimentos documentados para planejamento e utilização dos recursos computacionais da empresa, verificando aspectos de segurança e qualidade.

2.2 CRIPTOGRAFIA

Segundo Tanenbaum e Wetherall (2011, p. 481), “a palavra criptografia vem de palavras gregas que significam ‘escrita secreta’”.

Na criptografia se tem o conceito de cifra, que é uma modificação de caractere por caractere e código, que troca uma palavra por uma outra, consiste em transformar o texto simples em um texto cifrado, isto é, em um texto embaralhado, que só é possível realizar a leitura sabendo a chave secreta, chamado de criptologia e através da criptoanálise é possível tentar descobrir as palavras secretas para desvendar a criptografia por trás de algum texto cifrado (TANENBAUM; WETHERALL, 2011, p. 481).

Como exemplo se pode citar o algoritmo cifra de césar, que consiste em substituir cada caractere por outra, como modificar a letra “A” por “D” conforme ilustra a Figura 6 (RIBEIRO; LOURENÇANO; COSTA, 2013).

Figura 6 - Cifra de César

Uma mensagem como: “ALGORITMO” seria cifrado como “DOJRULXPR”. A equivalência entre as letras pode ser facilmente identificada quando ambos os conjuntos de letras são sobrepostos, como na figura 3:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X	W	Y	Z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X	W	Y	Z	A	B	C

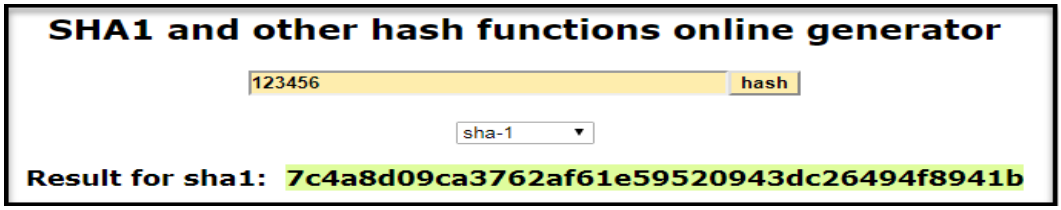
Fonte: Ribeiro, Lourençano e Costa (2013).

Na criptografia também se tem o conceito de *hashes*, que são valores únicos usados para comprovar a integridade do conteúdo, *hash* segundo Mitnick e Simon (2003, p. 56) é “Uma *string* de coisas ininteligíveis que resulta do processamento de uma senha por meio de um processo de criptografia de uma via. O processo deve ser irreversível”.

Um exemplo de *hash* é o SHA-1, um tipo de algoritmo de criptografia que utiliza uma função *hash* que gera um valor único com base em uma função matemática. SHA significa *Secure Hash Algorithm*, ou seja, Algoritmo de *Hash* Seguro (STALLINGS, 2015).

No conversor SHA-1 *online*, apresentado na Figura 7, é possível visualizar a representação da senha “123456” em *hash*.

Figura 7 - Senha “123456” em SHA-1



Fonte: Autoria própria. Disponível em: <http://www.sha1-online.com/>. Acesso em: 10 set. 2018.

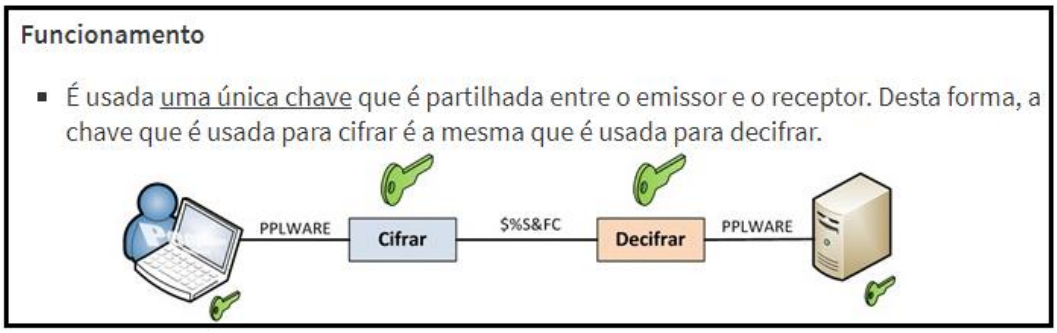
De acordo com a Cert.br (2012), existem duas categorias para os métodos criptográficos: a) criptografia de chave simétrica; e b) criptografia de chave assimétrica.

Segundo a Cert.br (2012), a definição de criptografia de chave simétrica é:

> [...] chamada de criptografia de chave secreta ou única, utiliza uma mesma chave tanto para codificar como para decodificar informações, sendo usada principalmente para garantir a confidencialidade dos dados. Casos nos quais a informação é codificada e decodificada por uma mesma pessoa não há necessidade de compartilhamento da chave secreta. Entretanto, quando estas operações envolvem pessoas ou equipamentos diferentes, é necessário que a chave secreta seja previamente combinada por meio de um canal de comunicação seguro (para não comprometer a confidencialidade da chave). Exemplos de métodos criptográficos que usam chave simétrica são: AES, Blowfish, RC4, 3DES e IDEA.

Na imagem, apresentada na Figura 8, é possível observar o funcionamento da criptografia de chave simétrica.

Figura 8 - Funcionamento da criptografia de chave simétrica



Fonte: Pinto (2010).

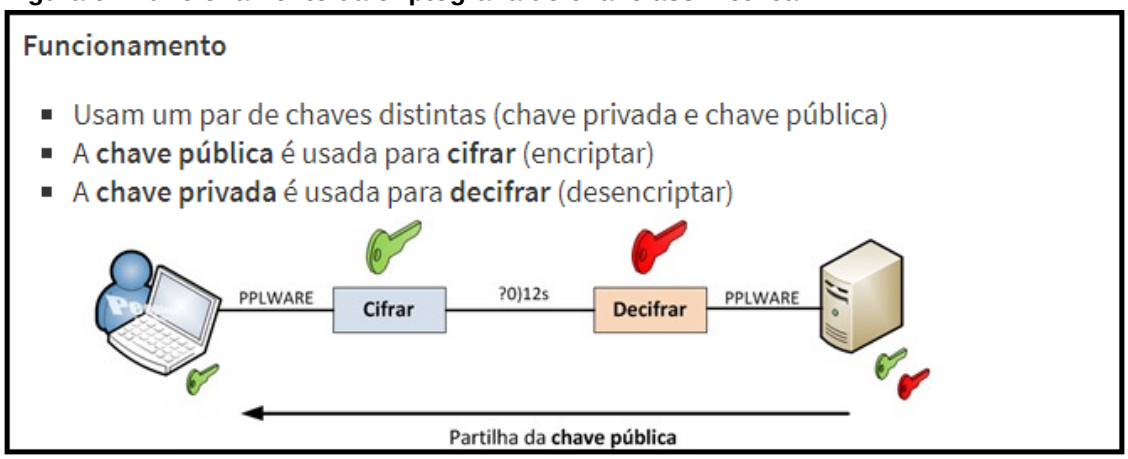
E a definição de criptografia de chave assimétrica conforme relata Cert.br (2012):

> [...] conhecida como criptografia de chave pública, utiliza duas chaves distintas: uma pública, que pode ser livremente divulgada, e uma privada, que deve ser mantida em segredo por seu dono. Quando uma informação é codificada com uma das chaves, somente a outra chave do par pode decodificá-la. Qual chave usar para codificar depende da proteção que se deseja, se confidencialidade

> ou autenticação, integridade e não-repúdio. A chave privada pode ser armazenada de diferentes maneiras, como um arquivo no computador, um *smartcard* ou um *token*. Exemplos de métodos criptográficos que usam chaves assimétricas são: RSA, DSA, ECC e Diffie-Hellman.

O funcionamento da criptografia de chave assimétrica é apresentado na Figura 9.

Figura 9 - Funcionamento da criptografia de chave assimétrica



Fonte: Pinto (2010).

Na criptografia, o processo inverso é chamado de criptoanálise, que é a arte de tentar adivinhar o texto cifrado, sem o conhecimento do algoritmo de criptografia utilizado na codificação do texto cifrado, através da utilização de técnicas de diferentes cifras para obter o texto original, mesmo que de forma parcial (QUARESMA; PINHO, 2009).

Os responsáveis por este processo são chamados de Criptoanalistas, eles utilizam da criptoanálise para testar e até mesmo melhorar um algoritmo de criptografia (STALLINGS, 2015).

Segundo Quaresma e Pinho (2009), “Os sistemas criptográficos surgiram então como forma de garantir a confidencialidade da informação, a criptoanálise surgiu como forma de “quebrar” essa mesma confidencialidade.”

2.3 CONJUNTO DE CARACTERES

Para se entender o conjunto de caracteres que pode ser utilizado na construção de senhas é necessário entender algumas definições como: caractere, *bit*, *byte* e ASCII.

Caractere é um grupo de 8 *bits* representados por 1 *byte* (VASCONCELOS, 2012).

Bit, se trata da menor unidade de informação que é representado por 0 ou 1, do inglês *BInary digitT*, que significa digito binário (VASCONCELOS, 2012).

Byte, de acordo com Vasconcelos (2012):

> Os *bytes* podem ser usados para representar números, caracteres, figuras, ou qualquer outro tipo de dado armazenado ou processado em um computador. Para representar caracteres, por exemplo, basta estabelecer um código que indique um número associado a cada caractere. Um código muito utilizado é o ASCII.

Para mais detalhes sobre *bit* e *byte*, pode-se consultar: VASCONCELOS, L. Hardware total. 1 ed. São Paulo: Makron Books, 2012. 2117 p.

ASCII (do inglês, *American Standard Code for Information Interchange)* é o código padrão americano para o intercâmbio de informação, serve para padronizar a maneira que os computadores compõem e trocam a informação (RFC20, 1969).

A partir destas definições, em um teclado padrão, considera-se 95 a quantidade de caracteres total (KISSELL, 2017). Estes 95 caracteres, numerados de 32 a 126 na tabela ASCII (Figura 10), são a quantidade possível de imprimir e os caracteres de 0 a 31 e 127 na tabela ASCII são reservados para funções de controle para o computador (RFC20, 1969).

Figura 10 - Tabela ASCII

Decimal	Hex	Char	Decimal	Hex	Char	Decimal	Hex	Char	Decimal	Hex	Char
0	0	[NULL]	32	20	[SPACE]	64	40	@	96	60	`
1	1	[START OF HEADING]	33	21	!	65	41	A	97	61	a
2	2	[START OF TEXT]	34	22	"	66	42	B	98	62	b
3	3	[END OF TEXT]	35	23	#	67	43	C	99	63	c
4	4	[END OF TRANSMISSION]	36	24	$	68	44	D	100	64	d
5	5	[ENQUIRY]	37	25	%	69	45	E	101	65	e
6	6	[ACKNOWLEDGE]	38	26	&	70	46	F	102	66	f
7	7	[BELL]	39	27	'	71	47	G	103	67	g
8	8	[BACKSPACE]	40	28	(	72	48	H	104	68	h
9	9	[HORIZONTAL TAB]	41	29	)	73	49	I	105	69	i
10	A	[LINE FEED]	42	2A	*	74	4A	J	106	6A	j
11	B	[VERTICAL TAB]	43	2B	+	75	4B	K	107	6B	k
12	C	[FORM FEED]	44	2C	,	76	4C	L	108	6C	l
13	D	[CARRIAGE RETURN]	45	2D	-	77	4D	M	109	6D	m
14	E	[SHIFT OUT]	46	2E	.	78	4E	N	110	6E	n
15	F	[SHIFT IN]	47	2F	/	79	4F	O	111	6F	o
16	10	[DATA LINK ESCAPE]	48	30	0	80	50	P	112	70	p
17	11	[DEVICE CONTROL 1]	49	31	1	81	51	Q	113	71	q
18	12	[DEVICE CONTROL 2]	50	32	2	82	52	R	114	72	r
19	13	[DEVICE CONTROL 3]	51	33	3	83	53	S	115	73	s
20	14	[DEVICE CONTROL 4]	52	34	4	84	54	T	116	74	t
21	15	[NEGATIVE ACKNOWLEDGE]	53	35	5	85	55	U	117	75	u
22	16	[SYNCHRONOUS IDLE]	54	36	6	86	56	V	118	76	v
23	17	[ENG OF TRANS. BLOCK]	55	37	7	87	57	W	119	77	w
24	18	[CANCEL]	56	38	8	88	58	X	120	78	x
25	19	[END OF MEDIUM]	57	39	9	89	59	Y	121	79	y
26	1A	[SUBSTITUTE]	58	3A	:	90	5A	Z	122	7A	z
27	1B	[ESCAPE]	59	3B	;	91	5B	[	123	7B	{
28	1C	[FILE SEPARATOR]	60	3C	<	92	5C	\	124	7C	|
29	1D	[GROUP SEPARATOR]	61	3D	=	93	5D	]	125	7D	}
30	1E	[RECORD SEPARATOR]	62	3E	>	94	5E	^	126	7E	~
31	1F	[UNIT SEPARATOR]	63	3F	?	95	5F	_	127	7F	[DEL]

Fonte: Sugai (2015).

Considerando apenas os 95 caracteres imprimíveis tem-se o conjunto de caracteres apresentados no Quadro 1.

Quadro 1 - Conjunto de caracteres

26 letras minúsculas	a b c d e f g h i j k l m n o p q r s t u v w x y z
26 letras maiúsculas	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
10 números	0 1 2 3 4 5 6 7 8 9
33 caracteres especiais	[SPACE] ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~

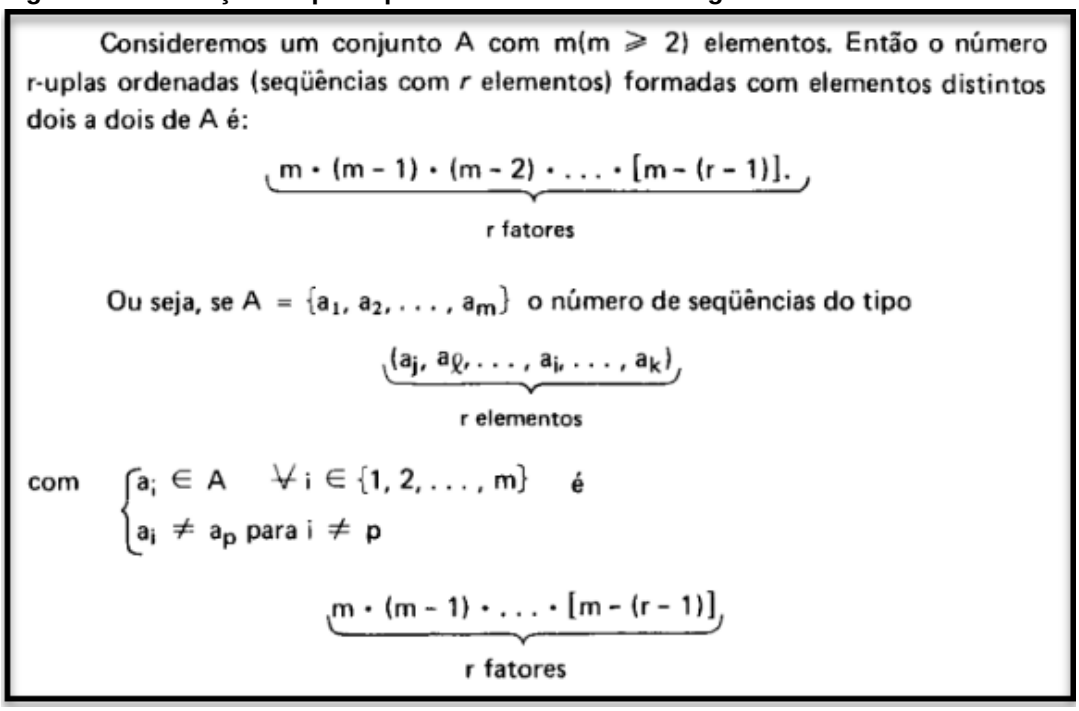
Fonte: Autoria própria.

Este conjunto de caracteres será importante na utilização do cálculo de entropia do próximo tópico, pois ele impactará diretamente no cálculo da força da senha ao se utilizar a análise combinatória: princípio fundamental de contagem (HAZZAN, 1997).

Segundo Hazzan (1977), "A análise combinatória visa desenvolver métodos que permitam contar o número de elementos de um conjunto, sendo estes elementos, agrupamentos formados por certas condições".

O princípio fundamental de contagem é apresentado na Figura 11.

Figura 11 - Definição do princípio fundamental de contagem



Consideremos um conjunto A com m(m ⩾ 2) elementos. Então o número r-uplas ordenadas (seqüências com *r* elementos) formadas com elementos distintos dois a dois de A é:

$$\underbrace{m \cdot (m-1) \cdot (m-2) \cdot \ldots \cdot [m-(r-1)]}_{r \text{ fatores}}.$$

Ou seja, se $A = \{a_1, a_2, \ldots, a_m\}$ o número de seqüências do tipo

$$\underbrace{(a_j, a_\ell, \ldots, a_i, \ldots, a_k)}_{r \text{ elementos}}$$

com $\begin{cases} a_i \in A \quad \forall\, i \in \{1, 2, \ldots, m\} \quad \text{é} \\ a_i \neq a_p \text{ para } i \neq p \end{cases}$

$$\underbrace{m \cdot (m-1) \cdot \ldots \cdot [m-(r-1)]}_{r \text{ fatores}}$$

Fonte: Hazzan (1977, p. 7-E).

Na Figura 12, são mostrados exemplos do princípio fundamental de contagem, para mais detalhes, pode-se consultar: HAZZAN, S. Fundamentos de Matemática Elementar volume 5: Combinatória e Probabilidade, 3. ed. São Paulo: Atual Editora, 1977. 149 p.

Figura 12 - Exemplos do princípio fundamental de contagem

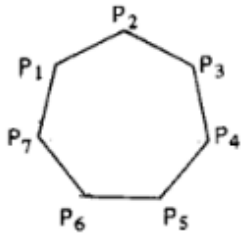
1º) A é o conjunto de números de dois algarismos distintos formados a partir dos dígitos 1, 2 e 3.

$A = \{12, 13, 21, 23, 31, 32\}$ e $\#A = 6$

2º) B é o conjunto das diagonais de um heptágono

$B = \{\overline{P_1P_3}, \overline{P_1P_4}, \overline{P_1P_5}, \overline{P_1P_6}, \overline{P_2P_4}, \overline{P_2P_5}, \overline{P_2P_6}, \overline{P_2P_7}, \overline{P_3P_5}, \overline{P_3P_6}, \overline{P_3P_7}, \overline{P_4P_6}, \overline{P_4P_7}, \overline{P_5P_7}\}$

e $\#B = 14$.



3º) C é o conjunto das seqüências de letras que se obtêm, mudando-se a ordem das letras da palavra ARI (anagramas da palavra ARI).

$C = \{ARI, AIR, IRA, IAR, RAI, RIA\}$ e $\#C = 6$

4º) D é o conjunto de números de três algarismos, todos distintos, formados a partir dos dígitos 1, 2, 3, 4, 5, 6, 7, 8.

$D = \{123, 124, 125, \ldots, 875, 876\}$

Fonte: Hazzan (1977, p. 1-E).

2.4 ENTROPIA

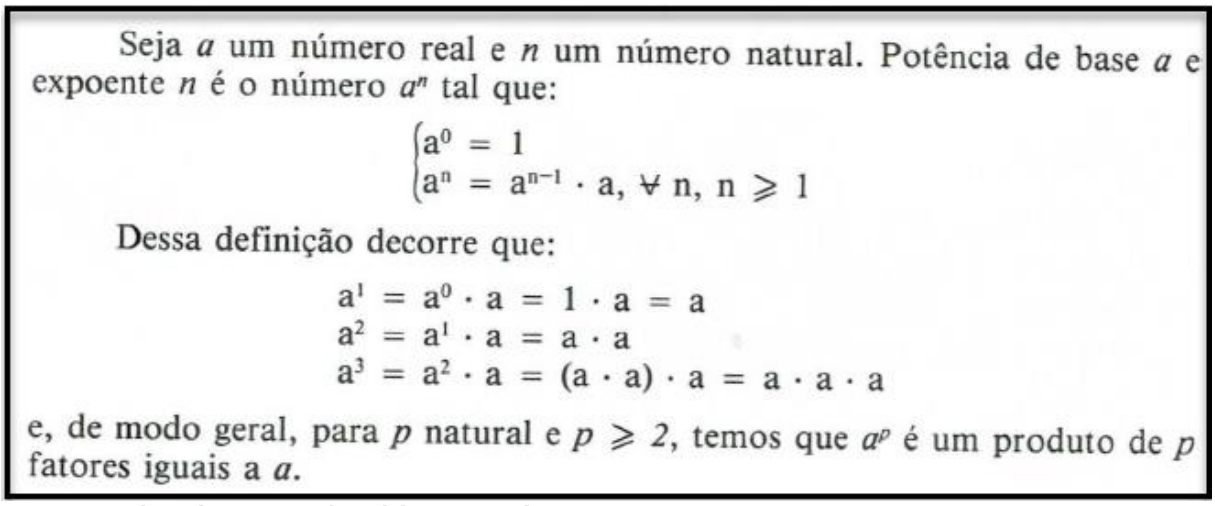
Através dos caracteres possíveis elevado ao expoente do tamanho obtém-se o número máximo de tentativas, que se refere todas as possíveis combinações até adivinhar a senha. No entanto é importante ressaltar que ao se trabalhar com entropia, deve considerar que o conjunto de caracteres que foi escolhida de forma randômica na elaboração da senha, ou seja, não houve nenhum padrão em sua construção que possa enfraquecer a força de sua senha (KISSELL, 2017).

Como exemplo, Kissell (2017, p. 161) afirma que:

> [...] Se você tiver uma senha construída a partir de letras minúsculas, possuindo 6 caracteres, então o número total de possibilidades é 26 x 26 x 26 x 26 x 26 x 26 ou 26^6, ou 308.915.776. Vamos dizer que você precisaria de 300 milhões de tentativas para adivinhar a senha. Esse é o número máximo de tentativas que você precisaria.

A definição de potenciação, logaritmo e exponenciação são mostradas nas: a) Figura 13 (potenciação), b) Figura 14 (logaritmo), e c) Figura 15 (exponenciação); para mais detalhes, pode-se consultar: IEZZI, G.; DOLCE, O.; MURAKAMI, C. Fundamentos de Matemática Elementar volume 2: logaritmos. 9. ed. São Paulo: Atual Editora, 2004. 198 p.

Figura 13 - Definição de potenciação de expoente natural



Seja a um número real e n um número natural. Potência de base a e expoente n é o número a^n tal que:

$$\begin{cases} a^0 = 1 \\ a^n = a^{n-1} \cdot a, \forall\ n,\ n \geqslant 1 \end{cases}$$

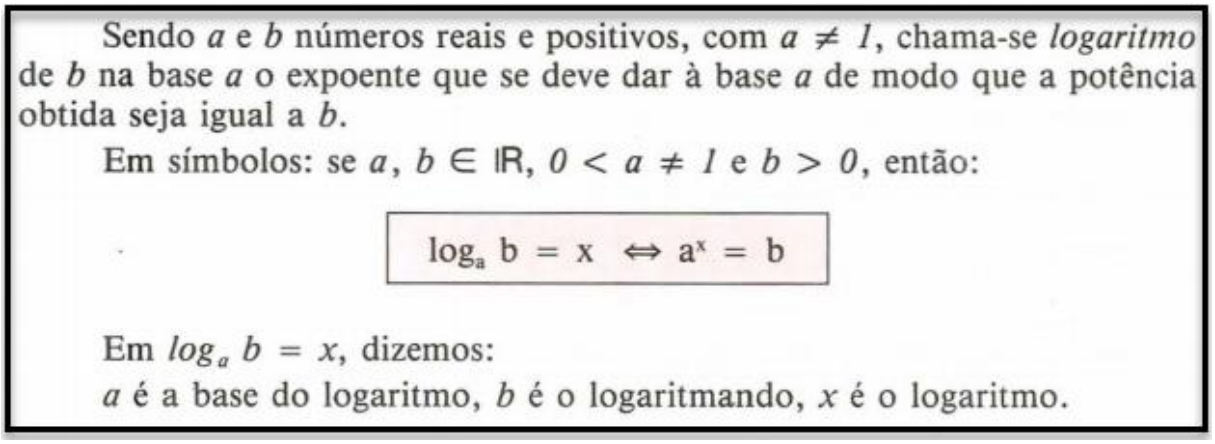
Dessa definição decorre que:

$$a^1 = a^0 \cdot a = 1 \cdot a = a$$
$$a^2 = a^1 \cdot a = a \cdot a$$
$$a^3 = a^2 \cdot a = (a \cdot a) \cdot a = a \cdot a \cdot a$$

e, de modo geral, para p natural e $p \geqslant 2$, temos que a^p é um produto de p fatores iguais a a.

Fonte: Iezzi, Dolce e Murakami (2004, p. 1).

Figura 14 - Definição de logaritmo



Sendo a e b números reais e positivos, com $a \neq 1$, chama-se *logaritmo* de b na base a o expoente que se deve dar à base a de modo que a potência obtida seja igual a b.

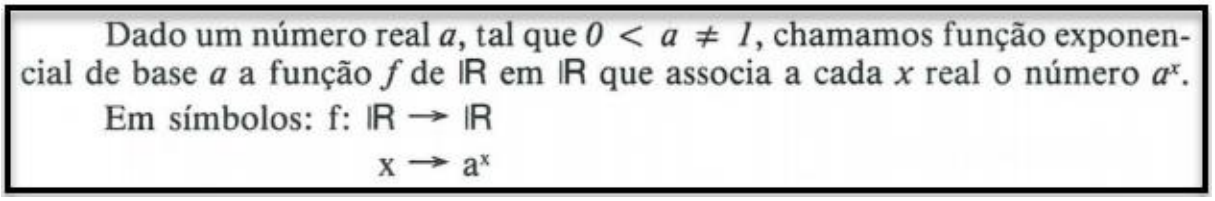
Em símbolos: se $a, b \in \mathbb{R}$, $0 < a \neq 1$ e $b > 0$, então:

$$\log_a b = x \iff a^x = b$$

Em $\log_a b = x$, dizemos:
a é a base do logaritmo, b é o logaritmando, x é o logaritmo.

Fonte: Iezzi, Dolce e Murakami (2004, p. 57).

Figura 15 - Definição de exponenciação



Dado um número real a, tal que $0 < a \neq 1$, chamamos função exponencial de base a a função f de $\mathbb{R}$ em $\mathbb{R}$ que associa a cada x real o número a^x.

Em símbolos: $f: \mathbb{R} \to \mathbb{R}$

$$x \to a^x$$

Fonte: Iezzi, Dolce e Murakami (2004, p. 27).

De acordo com Kissell (2017):

> A entropia é a resistência que uma senha apresenta para ser adivinhar [...] A palavra entropia significa desordem, aleatoriedade, imprevisibilidade. Criptógrafos utilizam o termo entropia para se referir à aproximação matemática da complexidade de uma senha baseada no método utilizado para cria-la. Uma senha que possui uma entropia mais elevada possui uma chance menor de ser adivinhada por uma pessoa (e mais importante ainda, a senha possui uma chance menor de ser adivinhar por uma máquina). Logo, quando falamos sobre senhas, quanto maior a entropia, melhor. [...] Criptógrafos

> medem a entropia de uma senha por meio de bits. Um número mais elevado de bits indica uma entropia mais elevada

A entropia é medida em bits, a fórmula da entropia de acordo com Kissell (2017) é $\log_2(caracteres\_possiveis^{tamanho})$ resultando em $\log_2(\text{número\_máximo\_de\_tentativas})$, onde os caracteres possíveis são a variação de caracteres contida na senha e o tamanho é a quantidade de caracteres que compõem a senha (KISSELL, 2017).

2.5 COMPRIMENTO

Comprimento da senha é a quantidade de caracteres que foram utilizados na elaboração da senha (MITNICK; SIMON, 2003).

Segundo Mitnick e Simon (2003, p. 25) uma senha "deve ter pelo menos 12 caracteres de comprimento".

Com o estudo da entropia do tópico anterior, obtém-se os resultados apresentados no Quadro 2, ao se comparar com a quantidade de caracteres.

Quadro 2 - Comprimento x tentativas x entropia

Comprimento	Tentativas	Entropia
1 caractere	$95^1 = 95$	$\log_2(95^1) = \pm 6{,}57\ bits$
2 caracteres	$95^2 = 9.025$	$\log_2(95^2) = \pm 13{,}14\ bits$
3 caracteres	$95^3 = 857.375$	$\log_2(95^3) = \pm 19{,}71\ bits$
4 caracteres	$95^4 = 81.450.625$	$\log_2(95^4) = \pm 26{,}28\ bits$
5 caracteres	$95^5 = 7.737.809.375$	$\log_2(95^5) = \pm 32{,}85\ bits$
6 caracteres	$95^6 = 735.091.890.625$	$\log_2(95^6) = \pm 39{,}41\ bits$
7 caracteres	$95^7 = 6.983373\text{e} + 13$	$\log_2(95^7) = \pm 45{,}99\ bits$
8 caracteres	$95^8 = 6.6342043\text{e} + 15$	$\log_2(95^8) = \pm 52{,}56\ bits$
9 caracteres	$95^9 = 6.3024941\text{e} + 17$	$\log_2(95^9) = \pm 59{,}13\ bits$
10 caracteres	$95^{10} = 5.9873694\text{e} + 19$	$\log_2(95^{10}) = \pm 69{,}70\ bits$
11 caracteres	$95^{11} = 5.6880009\text{e} + 21$	$\log_2(95^{11}) = \pm 72{,}27\ bits$
12 caracteres	$95^{12} = 5.4036009\text{e} + 23$	$\log_2(95^{12}) = \pm 78{,}84\ bits$

Fonte: Autoria própria.

Uma senha composta por mais de 75 *bits* é a recomendada pelo Kissell (2017). Observe que a quantidade de caracteres influencia diretamente em relação ao número de tentativas e ao cálculo de entropia, que quanto maior for o número de caracteres, mais forte será a entropia, considerando que foram escolhidas de forma aleatória, com apenas a adição de um caractere a mais na senha já a torna mais forte (KISSELL, 2017).

2.6 TEMPO DE PROCESSAMENTO

Para falar a respeito do tempo de processamento, antes é necessário introduzir os conceitos de CPU e *clock*.

Segundo Vasconcelos (2012), a definição de CPU é:

> [...] chamada de Unidade Central de Processamento (UCP). Em inglês, usamos a sigla CPU, que é abreviatura de *Central Processing Unit*. Nos computadores de grande porte, a CPU é formada por uma ou várias placas. Cada uma dessas placas contém vários chips. Nos microcomputadores a CPU nada mais é que o próprio processador.

Segundo Sumares (2017), a definição de *clock* é:

> [...] O *clock* é o número de ações (ou "pulsos de clock") que o processador consegue executar por segundo. [...] Um computador que fizesse uma ação por segundo teria *clock* de um hertz (1 Hz). Mas os processadores atuais têm clocks de cerca de 2 GHz. Isso significa que eles são capazes de realizar cerca de dois bilhões de pulsos de *clock* por segundo. Ou seja, nos cerca de 250 milissegundos que um piscar de olhos leva, o processador consegue realizar cerca de 500 milhões de ações. [...] O *clock* é o indicador mais imediato da "velocidade" de um processador.

Com base no artigo “Ars Technica 25-GPU ClusterCracks Every Standard Windows Password in <6Hours”, Kissell (2017, p. 26-27) afirma que:

> Uma senha de 8 dígitos contendo maiúscula e minúsculas, números e caracteres especiais poderia ser quebrada, através de um ataque de força bruta, em cerca de cinco horas e trinta minutos. [...] Atualmente uma quebra de uma senha assim certamente ocorre muito mais rapidamente [...] através da checagem de 350 bilhões de senhas por segundo. [...] Isso indica que uma senha de nove caracteres levaria 475 horas para ser quebrada, no máximo. Ou seja, menos de 20 dias.

Esta possibilidade de processar 350 bilhões de senhas por segundo ocorre devido a capacidade de aproveitar 25 GPUs AMD Radeon (do inglês, *Graphics Processing Unit*), unidades gráficas de processamento, em um pacote de virtualização com cinco servidores (GOODIN, 2012).

Na Figura 16, é exibido um dos cinco servidores que compõem as 25 GPUs.

Figura 16 - Um dos cinco servidores com GPUs

Fonte: Goodin (2012).

Para se comparar a velocidade de processamento desta supermáquina, constituída de 5 servidores com um total de 25 GPUs, de forma simples se utilizará as configurações abaixo de um computador acessível no mercado:

- Placa mãe: Intel
- HD: 500 GB
- Memória RAM: 4 GB
- Sistema Operacional: Linux
- Modelo do Processador: Intel Core i3 3.3 *GHz*

A comparação ocorrerá apenas com base na frequência do *clock* de 3.3 GHz (do inglês *GIGA-HERTZ*, onde cada impulso gera um ciclo, e cada ciclo executa 3,3 bilhões de instruções por segundo no processador) desconsiderando outros fatores como arquitetura, núcleo, modelo e memória que podem influenciar na velocidade de processamento e se torna difícil de mensurar caso considere estes fatores (VASCONCELOS, 2012).

Dessa forma, será considerado no cálculo:

- Comprimento da senha;
- Entropia com 95 caracteres possíveis de um teclado padrão;
- Quantidade de tentativas para a quebra;
- Tempo de quebra sendo o número de tentativas dividido pela quantidade de checagem por segundo;

- 350 bilhões de checagem por segundo através de 25 GPUs funcionando em conjunto, que equivale à 350x(10^9);
- 3,3 bilhões de checagem por segundo através do *clock* de 3.3 *GHz*, que equivale à 3,3x(10^9).

Realizando os cálculos sugeridos obtém-se os resultados apresentados no Quadro 3.

Quadro 3 - Tentativas x tempo

Qt. de caracteres	Tentativas (caracteres ^ comprimento)	Tempo de quebra com 25 GPUs (350 bilhões por segundo)	Tempo de quebra com 3.3 GHz (3,3 bilhões por segundo)
1	$95^1 = 95$	+- 0,27 nanosegundos	+- 28,79 nanosegundos
2	$95^2 = 9.025$	+- 0,03 microssegundos	+- 2,73 microssegundos
3	$95^3 = 857.375$	+- 2,45 microssegundos	+- 0,26 milissegundos
4	$95^4 = 81.450.625$	+- 0,23 milissegundos	+- 0,02 segundos
5	$95^5 = 7.737.809.375$	+- 0,02 segundos	+- 0,04 minutos
6	$95^6 = 735.091.890.625$	+- 2,10 segundos	+- 3,71 minutos
7	$95^7 = 6.983373\text{e} + 13$	+- 3,33 minutos	+- 5,88 horas
8	$95^8 = 6.6342043\text{e} + 15$	+- 5,27 horas	+- 23,27 dias
9	$95^9 = 6.3024941\text{e} + 17$	+- 20,84 dias	+- 6,05 anos
10	$95^{10} = 5.9873694\text{e} + 19$	+- 5,42 anos	+- 57.493 décadas
11	$95^{11} = 5.6880009e + 21$	+- 51,49 décadas	+- 546,1875 séculos
12	$95^{12} = 5.4036009\text{e} + 23$	+- 489,228 séculos	+- 51887,8115 séculos

Fonte: Autoria própria.

Note que o conjunto de caracteres e o comprimento da senha são fatores importantes, pois quanto maior o comprimento e a variação dos caracteres, mais tempo de processamento levará. Caso o comprimento da senha seja enorme, isto é, levando séculos para a decifragem, se tornará inviável realizar o ataque de força bruta (MITNICK; SIMON, 2003).

2.7 MÁSCARA

Expressão regular é utilizado para representar o padrão em um texto. A partir destas expressões regulares, se cria máscaras padrões para a utilização em validação de formulários, algumas das formas de representação são mostradas nas figuras abaixo (JARGAS, 2012).

De acordo com Jargas (2012):

> [...] é uma composição de símbolos, caracteres com funções especiais, que, agrupados entre si e com caracteres literais, formam uma sequência, uma expressão. Essa expressão é interpretada como uma regra que indicará sucesso se uma entrada de dados qualquer casar com essa regra, ou seja, obedecer exatamente a todas as suas condições.

Na Figura 17, é representado as equivalências das expressões regulares, na coluna da esquerda contém a expressão regular e na coluna da direita o seu respectivo significado (JARGAS, 2009).

Figura 17 - Expressões regulares

Similar	Significa
[A-Z]	Letras maiúsculas
[a-z]	Letras minúsculas
[A-Za-z]	Maiúsculas e minúsculas
[A-Za-z0-9]	Letras e números
[0-9]	Números
[0-9A-Fa-f]	Números hexadecimais
[.,!?:...]	Caracteres de pontuação
[\t]	Espaço em branco e TAB
[\t\n\r\f\v]	Caracteres brancos
[^ \t\n\r\f\v]	Caracteres imprimíveis
[^\t\n\r\f\v]	Imprimíveis e o espaço

Fonte: Jargas (2009).

Na Figura 18, tem-se alguns exemplos simples de expressões regulares para melhor entendimento do assunto.

Figura 18 - Exemplos de expressões regulares

Metacaractere	Repetições
{1,3}	De 1 a 3
{3,}	Pelo menos 3 (3 ou mais)
{0,3}	Até 3
{3}	Exatamente 3
{1}	Exatamente 1
{0,1}	Zero ou 1 (igual ao opcional)
{0,}	Zero ou mais (igual ao asterisco)
{1,}	Um ou mais (igual ao mais)

Fonte: Jargas (2012, p. 45).

Na expressão regular existe o conceito de metacaracteres (Quadro 4 e Quadro 5), que representam funções específicas e podem associar entre si formando criações mais complexas (JARGAS, 2012).

Quadro 4 - Exemplos de metacaracteres, parte 1 de 2

Metacaractere	Nome	Função
.	Ponto	Um caractere qualquer
[...]	Lista	Lista de caracteres permitidos
[^...]	Lista Negada	Lista de caracteres proibidos

Fonte: Jargas (2012, p. 26).

Quadro 5 - Exemplos de metacaracteres, parte 2 de 2

Metacaractere	Nome	Função
?	Opcional	Zero ou um
*	Asterisco	Zero, um ou mais
+	Mais	Um ou mais
{n, m}	Chaves	De n até m

Fonte: Jargas (2012, p. 26).

O Quadros 6 e o Quadro 7, mostram exemplos de utilizações dos metacaracteres, por exemplo a expressão “n.o” equivale as duas correspondentes “não” ou “não”, quando uma expressão corresponde à alguma palavra, se diz “casa com” (JARGAS, 2012).

Quadro 6 - Utilização de metacaracteres, parte 1 de 2

Expressão	Casa com
n.o	não, não, ...
.eclado	teclado, Teclado, ...
e.tendido	estendido, extendido, eztendido, ...

Fonte: Jargas (2012, p. 28).

Quadro 7 - Utilização de metacaracteres, parte 2 de 2

Expressão	Casa com
n[ãa]o	não, nao
[Tt]eclado	Teclado, teclado
e[sx]tendido	estendido, extendido
12[:.]45	12:45, 12.45, 12 45
<[BIP]>	<B>, <I>, <P>

Fonte: Jargas (2012, p. 30).

Para mais detalhes sobre expressões regulares e metacaracteres, pode-se consultar: JARGAS, A. M. Livro Expressões Regulares - Uma abordagem divertida, 4. ed. São Paulo: Novatec, 2012. 224 p.

Nesta monografia será utilizado a expressão regular com o intuito de demonstrar os tipos de caracteres que compõem as senhas que foram analisadas.

2.8 TIPOS DE AMEAÇAS PARA SENHA

2.8.1 Anotações em Bloco de Notas

Anotações em bloco de notas são considerados ameaças, pois de acordo com Kissell (2017, p. 6), “Não adianta possuir a senha mais complexa do mundo se você a deixa escrita em uma nota adesiva colada em seu monitor, pois qualquer pessoa pode caminhar até a sua mesa e descobrir sua senha”.

Da mesma forma, se estiver anotado em algum caderno, no computador ou em qualquer lugar sem nenhuma proteção, pode prejudicar na descoberta da senha por mais elaborada que seja (MITNICK; SIMON, 2003).

De acordo com Mitnick e Simon (2003):

> [...] no caso de um empregado que tem diversas contas em diferentes sistemas de computadores. [..] Todas as senhas escritas devem estar seguras em um local longe do computador. Sob nenhuma circunstância uma senha pode ser armazenada sob o teclado ou pregada no monitor do computador.

2.8.2 Keystroke Logging

Acessar sites que requerem autenticação em computadores públicos é um risco, pois é possível estes computadores estarem com softwares maliciosos instalados, já que é público e qualquer pessoa pode ter acesso, como o *Keystroke logger*, que registra todas as teclas digitadas e capaz de enviar capturas de telas para terceiros, uma vez captura as teclas digitadas de sua senha, por mais segura que seja, será enviada à outra pessoa não autorizada (MITNICK; SIMON, 2003).

2.8.3 Sniffing

O *Sniffing* é uma forma de monitorar o tráfego da rede através de capturas de pacotes de rede, ao se utilizar de redes públicas, ou seja, geralmente redes Wi-Fi sem senhas, podem haver pessoas mal-intencionadas que estejam tentando descobrir nomes de usuários e senhas ao enviar estas informações para o servidor, por isto, é importante evitar acessar contas pessoais em redes de terceiros, caso contrário, pode também ocorrer um risco de ter seus dados capturados pelo analisador de pacotes (MITNICK; SIMON, 2005).

2.8.4 Engenharia Social

Segundo Mitnick e Simon (2003):

> A engenharia social usa a influência e a persuasão para enganar as pessoas e convencê-las de que o engenheiro social é alguém que na verdade ele não e, ou pela manipulação. Como resultado, o engenheiro social pode aproveitar-se das pessoas para obter as informações com ou sem o uso da tecnologia.

Um exemplo de ataque usando Engenharia social é o *Phishing*, que se trata de enviar e-mails falsos, mas que são cópias idênticas aos originais, se passando por outra identidade, como bancos, sites de compras confiáveis ou pessoas conhecidas (MITNICK; SIMON, 2003).

Os e-mails falsos de acordo com Mitnick e Simon (2003) são:

> [...] quando uma oferta aparece na sua caixa de correio eletrônico, uma oferta que chama a sua atenção. Isso pode ser um jogo de graça, uma oferta de fotos do seu astro preferido, um programa de agenda grátis ou um *shareware* barato que protege o seu computador contra vírus. Independente de qual seja a oferta, a mensagem direciona você para fazer o *download* do arquivo com os bens que a mensagem o convenceu a experimentar.

E um outro exemplo consiste em se aproximar de alguma forma da vítima para observar os seus dedos enquanto ela digita a senha, por mais simples que isto possa aparecer, se não for cuidadoso, corre-se o risco de ter sua senha observada e assim fornecida para pessoas não autorizadas (MITNICK; SIMON, 2003).

2.8.5 Força Bruta

Força bruta, em inglês *Brute Force*, é um método que envolve inúmeras tentativas para descobrir determinadas senhas, que possuem acessos privilegiados. Os ataques, isto é, tentativas de descoberta, podem ser realizadas de maneira manual ou automatizada por ferramentas (SCHARDONG; ÁVILA, 2012).

O *Wordlist*, que significa lista de palavras, que junto a uma ferramenta de força bruta, pode decifrar com facilidade caso sua senha esteja nesta lista (ROCHA et al., 2016).

Mitnick e Simon (2005, p. 111) afirmam que:

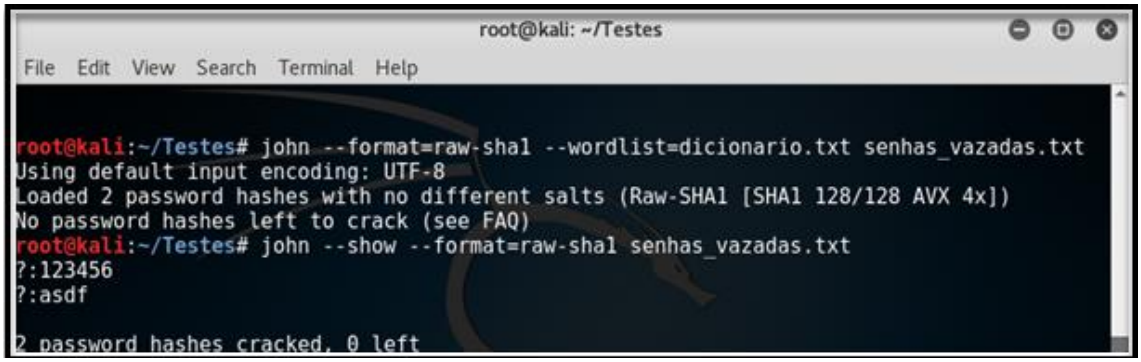
> Uma vez que a maioria dos usuários escolhe uma senha que é um nome ou uma simples palavra de dicionário, um atacante geralmente começa instalando 10phtCrack (ou o programa que está usando) para efetuar um 'ataque de

> dicionário' — testando cada palavra do dicionário para descobrir se alguma é a senha do usuário. Se o programa não tiver sucesso com o ataque do dicionário, o atacante então começará um 'ataque força-bruta', em que o programa tenta toda combinação possível (por exemplo, AAA, AAB, AAC ... ABA, ABB, ABC, e assim por diante) e então verifica combinações que incluem letras maiúsculas, minúsculas, numerais e símbolos.

Uma das ferramentas para determinar senhas usando o método de força bruta que pode-se citar é a “John The Ripper”, disponível em: <https://www.kitploit.com/2014/12/john-ripper-180-jumbo-1-fast-password.html>, acesso em: 11 set. 2018.

Na Figura 19, é demonstrado a utilização através de um exemplo simples com o arquivo “dicionario.txt” contendo uma lista de palavras chaves e o arquivo criptografado “senhas.txt” contendo senhas em SHA-1 como “123456” sendo “7c4a8d09ca3762af61e59520943dc26494f8941b” e “asdf” sendo “3da541559918a808c2402bba5012f6c60b27661c”. Após executar os comandos do “John The Ripper” para decifrar SHA-1 com “--format=raw-sha1”, utilizando a lista de palavras com “--wordlist=dicionario.txt” para o arquivo “senhas_vazadas.txt”, tem-se relevado com o comando “--show” as 2 senhas contidas em nossa lista.

Figura 19 - Comprovação de decifragem pelo John The Ripper



Fonte: Autoria própria.

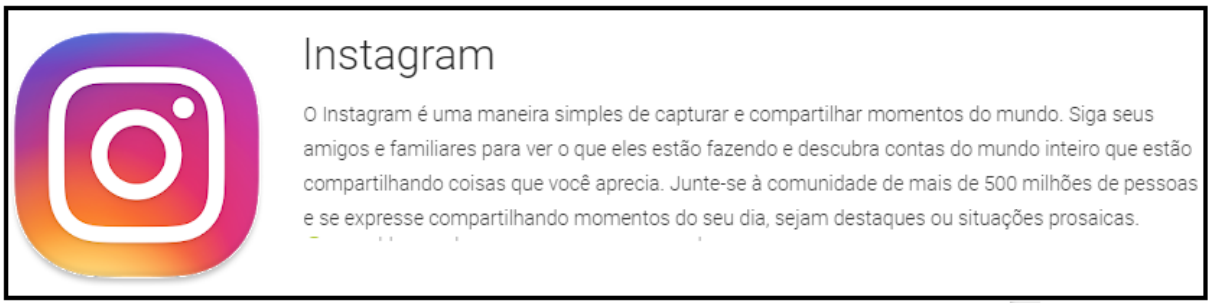
3 ESTUDO DE CASO

Neste estudo de caso é demonstrado a análise de senhas com base no conjunto de caracteres, entropia, comprimento, máscara e tempo de processamento que foram vistos no capítulo do referencial teórico:

- Sobre base de dados das senhas coletadas:
  - 100 senhas vazadas do Instagram disponível no Apêndice A: Figura 46, Figura 47, Figura 48 e Figura 49;
  - 100 senhas mais utilizadas em 2017 disponível no Apêndice B: Figura 50, Figura 51, Figura 52 e Figura 53.
- Os dados analisados foram:
  - As 25 senhas do serviço do Instagram vazadas em 2017;
  - As 25 senhas mais utilizadas em 2017;
  - 8 tipos de padrão de senha obtidos da base de 200 senhas;
  - Comparativo do comprimento das 200 senhas coletadas.

Na Figura 20, é mostrado no que consiste o serviço do Instagram.

Figura 20 - Serviço Instagram



Fonte: Autoria própria. Disponível em: <https://play.google.com/store/apps/details?id=com.instagram.android&hl=pt_BR>. Acesso em: 11 set. 2018.

As análises de senhas foram baseadas no estudo de entropia (considerando a aleatoriedade da senha). As fontes utilizadas neste estudo de caso foram: a) Pastebin, e b) SplashData.

O Pastebin (Figura 21) é uma ferramenta *online* que permite compartilhar trechos de código e saídas de terminal, determinando o tempo que o código ficará disponível. Existem muitas outras como Pastie, Paste2, Codepad, FrubarPaste, YourPaste, LodgeIt, Slexy.org ou Gist.

Figura 21 - Logo do site Pastebin

Fonte: Autoria própria. Disponível em: <https://pastebin.com>. Acesso em: 11 set. 2018.

O SplashData (Figura 22), fundada em 2000 na Califórnia, que é responsável por um trabalho de líder de aplicativos e serviços de segurança, divulga anualmente uma lista das piores senhas utilizadas com o intuito de conscientizar a população sobre o perigo de utilizá-las e terem os seus dados vazados na internet.

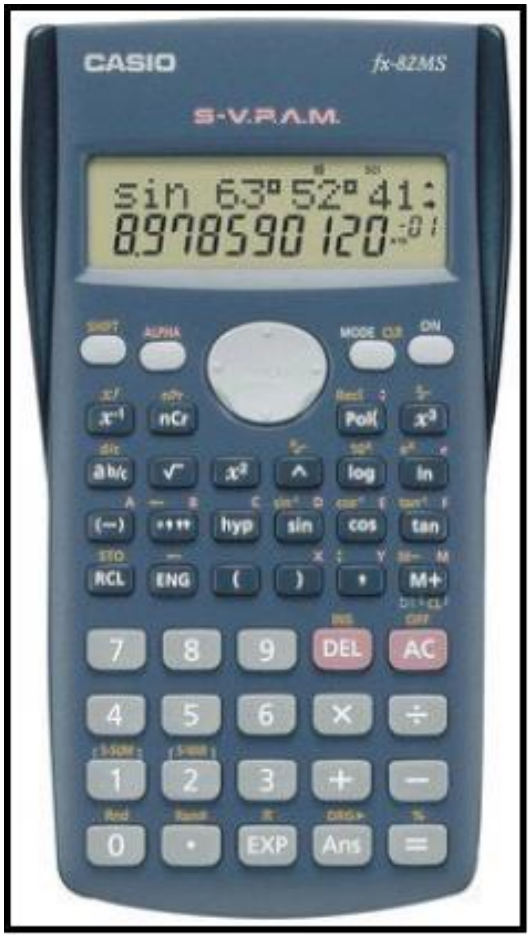
Figura 22 - Empresa Splashdata

Fonte: Autoria própria. Disponível em: <http://www.splashdata.com/index.htm>. Acesso em: 11 set. 2018.

Para a realização dos cálculos de entropia, comprimento e tempo de processamento foi utilizado a Calculadora Científica CASIO conforme mostrado na Figura 23, a especificação da calculadora é:

- Marca CASIO;
- Modelo FX-82MS;
- 240 funções;
- 2 linhas 10+2 dígitos;
- 9 Memórias de Variáveis;
- S-VPAM: Super Visualização das Fórmulas Algébricas.

Figura 23 - Calculadora científica CASIO

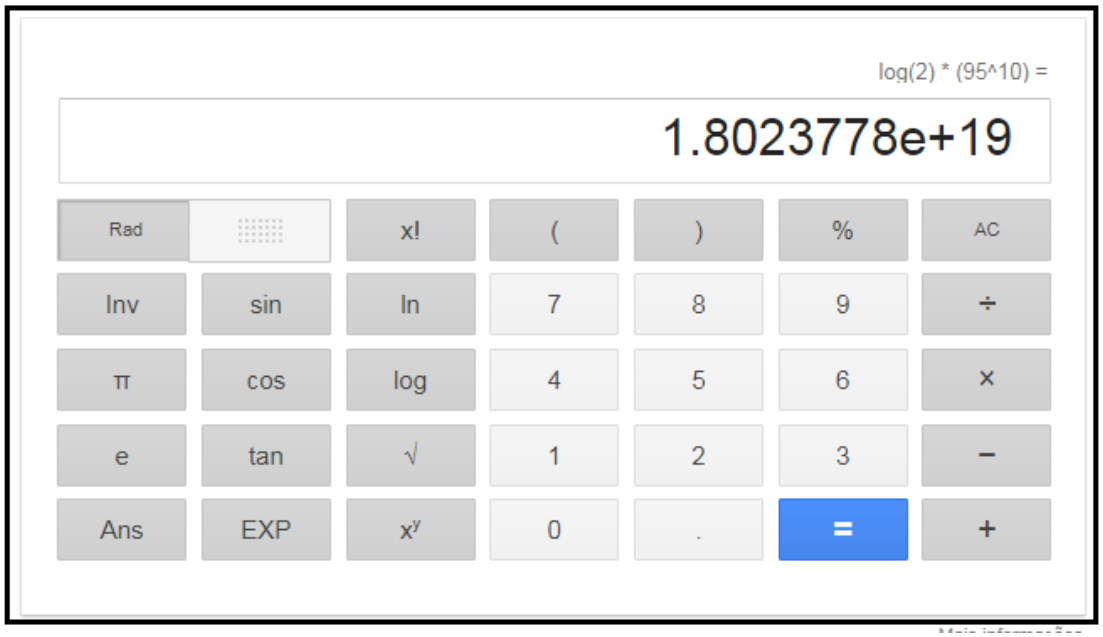


Fonte: Autoria própria. Disponível em: <https://www.kabum.com.br/produto/31744/calculadora-cientifica-casio-240-funcoes-fx-82ms>. Acesso em: 11 set. 2018.

Para poder simular o logaritmo base 2 ($\log_2$) na Calculadora Científica CASIO foi necessário utilizar a divisão pelo log de 2, por exemplo, a equação $\log_2(95^2)$ foi realizada da seguinte maneira: $\log(95^2) / \log_2$.

Para agilizar grande parte dos cálculos foi utilizado a cálculo do Google, disponível na própria barra de busca ao digitar a equação através do link “https://www.google.com.br”. A Figura 24, mostra um exemplo de utilização da calculador do Google.

Figura 24 - Calculadora do Google



Fonte: Autoria própria.

Durante a realização dos cálculos, em alguns resultados mostram o valor “e”, que corresponde à base dos logaritmos naturais, que se trata de uma constante com valor aproximado de 2,71828182845904523536028747135266249775 7, a Figura 25 mostra mais detalhes sobre esta constante (SONDRÉ, 2007).

Figura 25 - Constante de Euler

Existe uma importantíssima constante matemática, denotada por e e definida através da função exponencial por $e = \exp(1)$. O número e é irracional e positivo, está relacionado à função logaritmo por $\log(e) = 1$. Em homenagem ao matemático suíço Leonhard Euler (1707-1783)

Fonte: Sondré (2007).

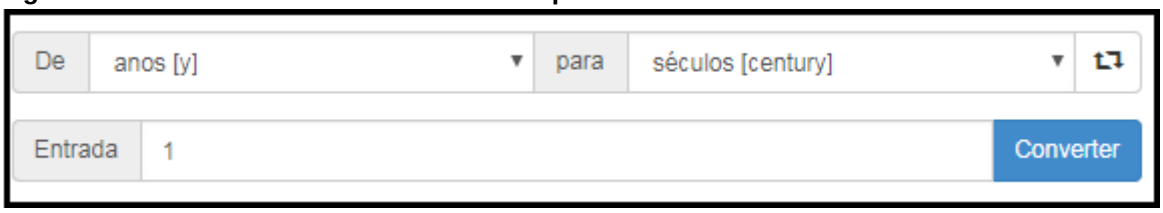
E para simplificar os cálculos, convertendo os segundos em séculos, anos, meses, semanas, dias, horas, minutos, milissegundos, microssegundos ou nanossegundos foi utilizado a tabela de conversão de tempo *online* através das ferramentas:

- Ferramenta 1: Figura 26, disponível em: <https://www.convertworld.com/pt/tempo>, acesso em: 12 set. 2018;
- Ferramenta 2: Figura 27, disponível em: <http://extraconversion.com/pt/tempo/anos/anos-para-seculos.html>, acesso em: 12 set. 2018.

Figura 26 - Ferramenta 1: conversão de tempo

Fonte: Autoria própria. Disponível em: <https://www.convertworld.com/pt/tempo/>. Acesso em: 12 set. 2018.

Figura 27 - Ferramenta 2: conversão de tempo



Fonte: Autoria própria. Disponível em: <http://extraconversion.com/pt/tempo/anos/anos-para-seculos.html>. Acesso em: 12 set. 2018.

3.1 VAZAMENTO DE SENHAS

3.1.1 Tipos de Análise de Senhas

Ao observar as senhas vazadas e as senhas que foram mais utilizadas em 2017 que se encontram no Apêndice A: Figura 46, Figura 47, Figura 48 e Figura 49; e Apêndice B: Figura 50, Figura 51, Figura 52 e Figura 53, é possível notar que existem alguns padrões de senhas constituídas que são apresentados no Quadro 8.

Quadro 8 - Tipos de padrões de senhas

Padrão de senha	Quantidade identificada	% Percentual
somente números	20	10,00%
somente letras minúsculas	85	42,50%
números e letras minúsculas	78	39,00%
números e letras maiúsculas	1	0,50%
números, letras minúsculas e maiúsculas	10	5,00%
letras minúsculas e outros caracteres	1	0,50%
números, letras minúsculas e outros caracteres imprimíveis	2	1,00%
números, letras minúsculas e maiúsculas e outros caracteres imprimíveis	3	1,50%
TOTAL	**200**	**100,00%**

Fonte: Autoria própria.

Com base no referencial teórico desta pesquisa e utilizando os seguintes critérios de:

- Conjunto de caracteres;
- Entropia;
- Comprimento;
- Tempo de processamento;
- Máscara.

As senhas que serão analisadas estão disponíveis no Quadro 9.

Quadro 9 - Senhas escolhidas para os padrões

Padrão de senha	Senha
somente números	13707377509
somente letras minúsculas	snowball
números e letras minúsculas	nakamura1933
números e letras maiúsculas	YUE2551998
números, letras minúsculas e maiúsculas	Cacademy678
letras minúsculas e outros caracteres imprimíveis	dhave.com
números, letras minúsculas e outros caracteres imprimíveis	g00dbyte$
números, letras minúsculas e maiúsculas e outros caracteres imprimíveis	Felipe1996.

Fonte: Autoria própria.

Ao analisar a máscara do padrão de senhas, obtém-se a equivalência apresentada no Quadro 10. Para mais detalhes, pode-se consultar a seção “2.7 MÁSCARA”.

Quadro 10 - Máscara do padrão de senha

Padrão de senha	Equivalência de Máscara
somente números	[0-9]
somente letras minúsculas	[a-z]
números e letras minúsculas	[0-9][a-z]
números e letras maiúsculas	[0-9][A-Z]
números, letras minúsculas e maiúsculas	[0-9][a-z][A-Z]
letras minúsculas e outros caracteres imprimíveis	[a-z][^\t\n\r\f\v]
números, letras minúsculas e outros caracteres imprimíveis	[0-9][a-z][^\t\n\r\f\v]
números, letras minúsculas e maiúsculas e outros caracteres imprimíveis	[0-9][a-z][A-Z][^\t\n\r\f\v]

Fonte: Autoria própria.

Analisando as máscaras das senhas apresentadas no Quadro 10, obtém-se os resultados apresentados no Quadro 11.

Quadro 11 - Análise de máscara das senhas

Senha	Máscara
13707377509	[0-9][0-9][0-9][0-9][0-9][0-9][0-9][0-9][0-9][0-9][0-9]
Snowball	[a-z][a-z][a-z][a-z][a-z][a-z][a-z][a-z]
nakamura1933	[a-z][a-z][a-z][a-z][a-z][a-z][a-z][a-z][0-9][0-9][0-9][0-9]
YUE2551998	[A-Z][A-Z][A-Z][0-9][0-9][0-9][0-9][0-9][0-9][0-9]
Cacademy678	[A-Z][a-z][a-z][a-z][a-z][a-z][a-z][a-z][0-9][0-9][0-9]
dhave.com	[a-z][a-z][a-z][a-z][a-z][^\t\n\r\f\v][a-z][a-z][a-z]
g00dbyte$	[a-z][0-9][0-9][a-z][a-z][a-z][a-z][a-z][^\t\n\r\f\v]
Felipe1996.	[A-Z][a-z][a-z][a-z][a-z][a-z][0-9][0-9][0-9][0-9][^\t\n\r\f\v]

Fonte: Autoria própria.

Ao analisar o comprimento de cada senha, isto é, contando a quantidade de caracteres que cada uma possui, resulta nos dados apresentados no Quadro 12. Para mais detalhes, pode-se consultar a seção “2.5 COMPRIMENTO”.

Quadro 12 - Análise de comprimento

Senha	Comprimento
13707377509	11 caracteres
snowball	8 caracteres
nakamura1933	12 caracteres
YUE2551998	10 caracteres
Cacademy678	11 caracteres
dhave.com	9 caracteres
g00dbyte$	9 caracteres
Felipe1996.	11 caracteres

Fonte: Autoria própria.

Em relação à base de dados coletada, foi identificada a relação de comprimento das senhas apresentada no Quadro 13.

Quadro 13 - Análise de comprimento base de dados

Comprimento	Quantidade de senhas	% Percentual
4 caracteres	9	4,50%
5 caracteres	5	2,50%
6 caracteres	48	24,00%
7 caracteres	23	11,50%
8 caracteres	52	26,00%
9 caracteres	18	9,00%
10 caracteres	12	6,00%
11 caracteres	13	6,50%
12 caracteres	11	5,50%
13 caracteres	6	3,00%
15 caracteres	2	1,00%
16 caracteres	1	0,50%
TOTAL	**200**	**100,00%**

Fonte: Autoria própria.

Quanto ao conjunto de caracteres para os padrões de senhas e as senhas escolhidas, chega-se aos dados apresentados no Quadro 14. Para mais detalhes, pode-se consultar a seção “2.3 CONJUNTO DE CARACTERES”.

Quadro 14 - Análise de conjunto de caracteres

Item	Padrão de senha	Senha	Possibilidades por caractere	Explicação
1	somente números	13707377509	10	Números variam de 0 a 9, então se tem 10 possibilidades.
2	somente letras minúsculas	snowball	26	O alfabeto contém 26 letras, de “a” à “z”, logo se tem 26 possibilidades
3	números e letras minúsculas	nakamura1933	10+26=36	Somando as explicações do item 1 e 2, resulta em 36 possibilidades.
4	números e letras maiúsculas	YUE2551998	10+26=36	Idem item 1 e 2.
5	números, letras minúsculas e maiúsculas	Cacademy678	10+26+26=62	Como o alfabeto tem 26 letras, no entanto, este valor pode ser duplicado ao contar as minúsculas e as maiúsculas, somados ao item 1.
6	letras minúsculas e outros caracteres imprimíveis	dhave.com	26+33=59	Os caracteres imprimíveis consistem em 33 possibilidades somados ao item 2.
7	números, letras minúsculas e outros caracteres imprimíveis	g00dbyte$	10+26+33=69	Idem item 1, 2 e 6.
8	números, letras minúsculas e maiúsculas e outros caracteres imprimíveis	Felipe1996.	10+26+26+33=95	Idem todas as explicações anteriores.

Fonte: Autoria própria.

Usando as fórmulas para calcular a força da senha e o número de tentativas possíveis vista na seção “2.4 ENTROPIA” e utilizando a análise do conjunto de caracteres do Quadro 14, chega-se aos dados apresentados no Quadro 15.

Quadro 15 - Análise de entropia

Senha / Comprimento	**Conjunto de caracteres (por caractere)**	**Tentativas**	**Entropia**
13707377509 / 11 caracteres	10 possibilidades	$10^{11} = 100000000000$	$\log_2(10^{11}) = \pm 36,54 bits$
Snowball / 8 caracteres	26 possibilidades	$26^8 = 208827064576$	$\log_2(26^8) = \pm 37{,}60\ bits$
nakamura1933 / 12 caracteres	36 possibilidades	$36^{12} = 4.7383813e + 18$	$\log_2(36^{12}) = \pm 62{,}04\ bits$
YUE2551998 / 10 caracteres	36 possibilidades	$36^{10} = 3.6561584e + 15$	$\log_2(36^{10}) = \pm 51{,}70\ bits$
Cacademy678 / 11 caracteres	62 possibilidades	$62^{11} = 5.2036561e + 19$	$\log_2(62^{11}) = \pm 65{,}50\ bits$
dhave.com / 9 caracteres	59 possibilidades	$59^9 = 8.6629958e + 15$	$\log_2(59^9) = \pm 52{,}94\ bits$
g00dbyte$ / 9 caracteres	69 possibilidades	$69^9 = 3.5452088e + 16$	$\log_2(69^9) = \pm 54{,}98\ bits$
Felipe1996. / 11 caracteres	95 possibilidades	$95^{11} = 5.6880009e + 21$	$\log_2(95^{11}) = \pm 72{,}27\ bits$

Fonte: Autoria própria.

Calculando o tempo de processamento com base na análise de entropia e na simulação de 25 GPUs e o *clock* de 3.3 GHz. Considerando que 25 GPUs equivalem ao processamento de 350 bilhões de instruções por segundo e 3,3 GHz equivale ao processamento de 3,3 bilhões de instruções por segundo (Quadro 16). Para mais detalhes pode-se consultar a seção “2.6 TEMPO DE PROCESSAMENTO”.

Quadro 16 - Análise de tempo de processamento

Senha	**Tentativas (caracteres ^ comprimento)**	**Tempo de quebra com 25 GPUs (350 bilhões por segundo)**	**Tempo de quebra com 3.3 GHz (3,3 bilhões por segundo)**
13707377509	$10^{11} = 100000000000$	+- 0,29 segundos	+- 30,3 segundos
Snowball	$26^8 = 208827064576$	+- 0,6 segundos	+- 1,05 minutos
nakamura1933	$36^{12} = 4.7383813e + 18$	+- 5,15 meses	+- 45,5 anos
YUE2551998	$36^{10} = 3.6561584e + 15$	+- 2,9 horas	+- 1,83 semanas
Cacademy678	$62^{11} = 5.2036561e + 19$	+- 4,71 anos	+- 4,9968 séculos
dhave.com	$59^9 = 8.6629958e + 15$	+- 6,88 horas	+- 1 mês
g00dbyte$	$69^9 = 3.5452088e + 16$	+- 28,14 horas	+- 4,09 meses
Felipe1996.	$95^{11} = 5.6880009e + 21$	+- 51,49 décadas	+- 546,1875 séculos

Fonte: Autoria própria.

Como resultados finais tem-se os dados apresentados nos quadros: a) Quadro 17 (Senha: “13707377509”); b) Quadro 18 (Senha: “snowball”); c) Quadro 19 (Senha: “nakamura1933”); d) Quadro 20 (Senha: “YUE2551998”); e) Quadro 21 (Senha: “Cacademy678”); f) Quadro 22 (Senha: “dhave.com”); g) Quadro 23 (Senha: “g00dbyte$”); e h) Quadro 24 (Senha: “Felipe1996.”).

Quadro 17 - Análise de senhas, parte 1 de 8

Senha	13707377509
Comprimento	11 caracteres
Máscara	[0-9][0-9][0-9][0-9][0-9][0-9][0-9][0-9][0-9][0-9][0-9]
Conjunto de caracteres	10 possibilidades por caractere
Entropia	$\log_2(10^{11}) = \pm 36,54\ bits$
Tentativas para quebra	$10^{11} = 100000000000$
Tempo de quebra 25 GPUs	+- 0,29 segundos
Tempo de quebra 3.3 GHz	+- 30,3 segundos

Fonte: Autoria própria.

Quadro 18 - Análise de senhas, parte 2 de 8

Senha	snowball
Comprimento	8 caracteres
Máscara	[a-z][a-z][a-z][a-z][a-z][a-z][a-z][a-z]
Conjunto de caracteres	26 possibilidades por caractere
Entropia	$\log_2(26^8) = \pm 37,60\ bits$
Tentativas para quebra	$26^8 = 208827064576$
Tempo de quebra 25 GPUs	+- 0,6 segundos
Tempo de quebra 3.3 GHz	+- 1,05 minutos

Fonte: Autoria própria.

Quadro 19 - Análise de senhas, parte 3 de 8

Senha	nakamura1933
Comprimento	12 caracteres
Máscara	[a-z][a-z][a-z][a-z][a-z][a-z][a-z][a-z][0-9][0-9][0-9][0-9]
Conjunto de caracteres	36 possibilidades por caractere
Entropia	$\log_2(36^{12}) = \pm 62,04\ bits$
Tentativas para quebra	$36^{12} = 4.7383813e + 18$
Tempo de quebra 25 GPUs	+- 5,15 meses
Tempo de quebra 3.3 GHz	+- 45,5 anos

Fonte: Autoria própria.

Quadro 20 - Análise de senhas, parte 4 de 8

Senha	YUE2551998
Comprimento	10 caracteres
Máscara	[A-Z][A-Z][A-Z][0-9][0-9][0-9][0-9][0-9][0-9][0-9]
Conjunto de caracteres	36 possibilidades por caractere
Entropia	$\log_2(36^{10}) = \pm 51,70\ bits$
Tentativas para quebra	$36^{10} = 3.6561584e + 15$
Tempo de quebra 25 GPUs	+- 2,9 horas
Tempo de quebra 3.3 GHz	+- 1,83 semanas

Fonte: Autoria própria.

Quadro 21 - Análise de senhas, parte 5 de 8

Senha	Cacademy678
Comprimento	11 caracteres
Máscara	[A-Z][a-z][a-z][a-z][a-z][a-z][a-z][a-z][0-9][0-9][0-9]
Conjunto de caracteres	62 possibilidades
Entropia	$\log_2(62^{11}) = \pm 65{,}50\ bits$
Tentativas para quebra	$62^{11} = 5.2036561e + 19$
Tempo de quebra 25 GPUs	+- 4,71 anos
Tempo de quebra 3.3 GHz	+- 4,9968 séculos

Fonte: Autoria própria.

Quadro 22 - Análise de senhas, parte 6 de 8

Senha	dhave.com
Comprimento	9 caracteres
Máscara	[a-z][a-z][a-z][a-z][a-z][^\t\n\r\f\v][a-z][a-z][a-z]
Conjunto de caracteres	59 possibilidades por caractere
Entropia	$\log_2(59^9) = \pm 52{,}94\ bits$
Tentativas para quebra	$59^9 = 8.6629958e + 15$
Tempo de quebra 25 GPUs	+- 6,88 horas
Tempo de quebra 3.3 GHz	+- 1 mês

Fonte: Autoria própria.

Quadro 23 - Análise de senhas, parte 7 de 8

Senha	g00dbyte$
Comprimento	9 caracteres
Máscara	[a-z][0-9][0-9][a-z][a-z][a-z][a-z][a-z][^\t\n\r\f\v]
Conjunto de caracteres	69 possibilidades por caractere
Entropia	$\log_2(69^9) = \pm 54{,}98\ bits$
Tentativas para quebra	$69^9 = 3.5452088e + 16$
Tempo de quebra 25 GPUs	+- 28,14 horas
Tempo de quebra 3.3 GHz	+- 4,09 meses

Fonte: Autoria própria.

Quadro 24 - Análise de senhas, parte 8 de 8

Senha	Felipe1996.
Comprimento	11 caracteres
Máscara	[A-Z][a-z][a-z][a-z][a-z][a-z][0-9][0-9][0-9][0-9][^\t\n\r\f\v]
Conjunto de caracteres	95 possibilidades por caractere
Entropia	$\log_2(95^{11}) = \pm 72{,}27\ bits$
Tentativas para quebra	$95^{11} = 5.6880009e + 21$
Tempo de quebra 25 GPUs	51,49 décadas
Tempo de quebra 3.3 GHz	546,1875 séculos

Fonte: Autoria própria.

No entanto, nota-se que grande parte das senhas da lista acima não foram elaboradas de forma aleatória, podendo enfraquecer consideravelmente seu poder de entropia e o tempo de processamento devido a sua mal elaboração ao se utilizar de padrões conhecidos como informações pessoais ou palavras de dicionários não sendo considerados boas práticas na elaboração de senhas, pois a senha:

- "snowball" foi retirada do dicionário da língua inglesa;

- "nakamura1933" e "Felipe1996." contém o nome de uma pessoa (informação pessoal) e o ano (pode ser de nascimento, placa de carro, ano de nascimento do avô);
- "Cacademy678" possui a palavra "academy" retirada do dicionário da língua inglesa e a sequência numérica "678";
- "dhave.com" foi elaborada utilizando as palavras "have" e ".com" retiradas do dicionário da língua inglesa;
- "g00dbyte$" foi construída com base em 2 palavras do dicionário da língua inglesa que são "good" e "byte".

3.1.2 Análise das Senhas Vazadas (Serviço Instagram)

Na Figura 28, é mostrado um pequeno pedaço do resultado de busca no Pastebin ao pesquisar por "*password leak*" (que significa vazamento de senha) resultou em 2930 registros. Nesta pesquisa, é possível observar a exposição de senhas, inclusive de 2017.

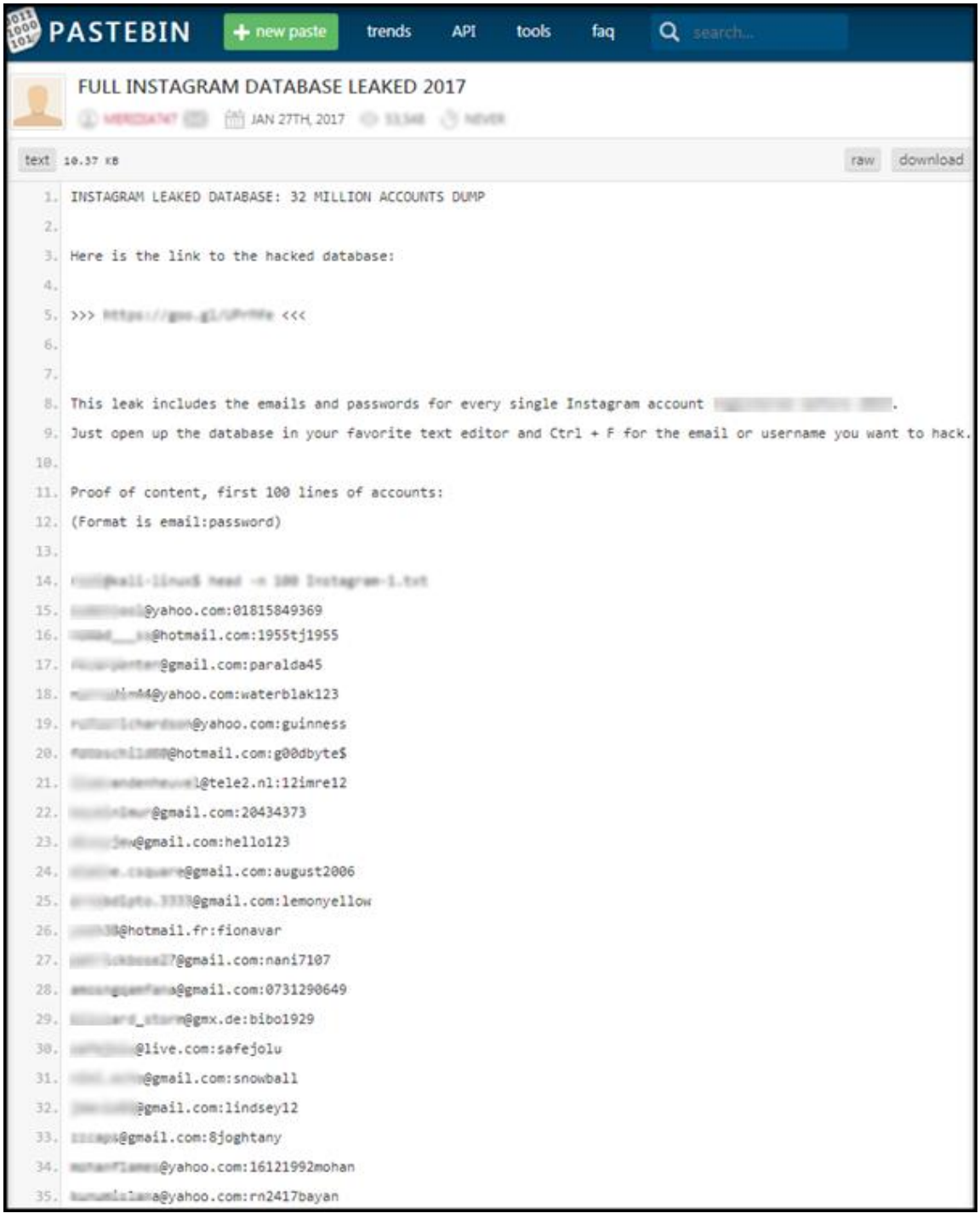
Figura 28 - Pesquisa de vazamento de senhas no Pastebin

Fonte: Autoria própria. Disponível em: <https://pastebin.com/search?q=passwords+leaks>. Acesso em: 12 set. 2018.

Através do Pastebin, foi possível obter uma pequena amostra de 100 senhas vazadas em 2017 referentes ao Instagram.

Os e-mails da Figura 29, foram borrados propositalmente para manter o anonimato da exposição de dados sensíveis e reais. Todas as imagens encontram-se localizadas no Apêndice A: Figura 46, Figura 47, Figura 48 e Figura 49.

Figura 29 - Vazamento de senhas do Instagram



Fonte: Autoria própria. Disponível em: <https://pastebin.com>. Acesso em: 12 set. 2018.

Ao analisar as primeiras 25 senhas vazadas do Instagram, obtém-se os dados apresentos nos quadros: 1) Quadro 25 (Senha: “01815849369”); 2) Quadro 26 (Senha: “1955tj1955”); 3) Quadro 27 (Senha: “paralda45”); 4) Quadro 28 (Senha: “waterblak123”); 5) Quadro 29 (Senha: “guinness”); 6) Quadro 30 (Senha: “g00dbyte$”); 7) Quadro 31 (Senha: “12imre12”); 8) Quadro 32 (Senha: “20434373”); 9) Quadro 33 (Senha: “hello123”); 10) Quadro 34 (Senha: “august2006”); 11) Quadro

35 (Senha: “lemonyellow”); 12) Quadro 36 (Senha: “fionavar”); 13) Quadro 37 (Senha: “nani7107”); 14) Quadro 38 (Senha: “0731290649”); 15) Quadro 39 (Senha: “bibo1929”); 16) Quadro 40 (Senha: “safejolu”); 17) Quadro 41 (Senha: “snowball”); 18) Quadro 42 (Senha: “lindsey12”); 19) Quadro 43 (Senha: “8joghtany”); 20) Quadro 44 (Senha: “16121992mohan”); 21) Quadro 45 (Senha: “rn2417bayan”); 22) Quadro 46 (Senha: “underground69”); 23) Quadro 47 (Senha: “CHIecher875”); 24) Quadro 48 (Senha: “kK1119132175”); e 25) Quadro 49 (Senha: “1952vnf”).

Quadro 25 - Senhas vazadas do Instagram, análise da 1º senha

Senha	01815849369
Comprimento	11 caracteres
Máscara	[0-9][0-9][0-9][0-9][0-9][0-9][0-9][0-9][0-9][0-9][0-9]
Conjunto de caracteres	10 possibilidades por caractere
Entropia	$\log_2(10^{11}) = \pm 36,54\ bits$
Tentativas para quebra	$10^{11} = 100000000000$
Tempo de quebra 25 GPUs	+- 0,29 segundos
Tempo de quebra 3.3 GHz	+- 30,3 segundos

Fonte: Autoria própria.

Quadro 26 - Senhas vazadas do Instagram, análise da 2º senha

Senha	1955tj1955
Comprimento	10 caracteres
Máscara	[0-9] [0-9] [0-9] [0-9][a-z][a-z] [0-9] [0-9] [0-9] [0-9]
Conjunto de caracteres	36 possibilidades por caractere
Entropia	$\log_2(36^{10}) = \pm 51,70\ bits$
Tentativas para quebra	$36^{10} = 3.6561584e + 15$
Tempo de quebra 25 GPUs	+- 2,9 horas
Tempo de quebra 3.3 GHz	+- 1,83 semanas

Fonte: Autoria própria.

Quadro 27 - Senhas vazadas do Instagram, análise da 3º senha

Senha	paralda45
Comprimento	9 caracteres
Máscara	[a-z][a-z][a-z][a-z][a-z][a-z][a-z][a-z][0-9][0-9]
Conjunto de caracteres	26+10=36 possibilidades por caractere
Entropia	$\log_2(36^9) = \pm 46,529325013\ bits$
Tentativas para quebra	$36^9 = 1.0155996e + 14$
Tempo de quebra 25 GPUs	+- 4,84 minutos
Tempo de quebra 3.3 GHz	+- 8,55 horas

Fonte: Autoria própria.

Quadro 28 - Senhas vazadas do Instagram, análise da 4º senha

Senha	waterblak123
Comprimento	12 caracteres
Máscara	[a-z][a-z][a-z][a-z][a-z][a-z][a-z][a-z][a-z][0-9][0-9][0-9]
Conjunto de caracteres	26+10=36 possibilidades por caractere
Entropia	$\log_2(36^{12}) = \pm 62,04\ bits$
Tentativas para quebra	$36^{12} = 4.7383813e + 18$
Tempo de quebra 25 GPUs	+- 5,15 meses
Tempo de quebra 3.3 GHz	+- 45,5 anos

Fonte: Autoria própria.

Quadro 29 - Senhas vazadas do Instagram, análise da 5º senha

Senha	guinness
Comprimento	8 caracteres
Máscara	[a-z][a-z][a-z][a-z][a-z][a-z][a-z][a-z]
Conjunto de caracteres	26 possibilidades por caractere
Entropia	$\log_2(26^8) = \pm 37{,}6035177451$ bits
Tentativas para quebra	$26^8 = 208.827.064.576$
Tempo de quebra 25 GPUs	+- 0,6 microssegundos
Tempo de quebra 3.3 GHz	+- 0,06 segundos

Fonte: Autoria própria.

Quadro 30 - Senhas vazadas do Instagram, análise da 6º senha

Senha	g00dbyte$
Comprimento	9 caracteres
Máscara	[a-z][0-9][0-9][a-z][a-z][a-z][a-z][a-z][^\t\n\r\f\v]
Conjunto de caracteres	26+10+33=69 possibilidades por caractere
Entropia	$\log_2(69^9) = \pm 54{,}98\ bits$
Tentativas para quebra	$69^9 = 3.5452088e + 16$
Tempo de quebra 25 GPUs	+- 28,14 horas
Tempo de quebra 3.3 GHz	+- 4,09 meses

Fonte: Autoria própria.

Quadro 31 - Senhas vazadas do Instagram, análise da 7º senha

Senha	12imre12
Comprimento	8 caracteres
Máscara	[0-9][0-9][a-z][a-z][a-z][a-z][0-9][0-9]
Conjunto de caracteres	26+10=36 possibilidades por caractere
Entropia	$\log_2(36^8) = \pm 41{,}3594000115$ bits
Tentativas para quebra	$36^8 = 2{,}8211099e + 12$
Tempo de quebra 25 GPUs	+- 8,060314 segundos
Tempo de quebra 3.3 GHz	+- 14,25 minutos

Fonte: Autoria própria.

Quadro 32 - Senhas vazadas do Instagram, análise da 8º senha

Senha	20434373
Comprimento	8 caracteres
Máscara	[0-9][0-9][0-9][0-9][0-9][0-9][0-9][0-9]
Conjunto de caracteres	10 possibilidades por caractere
Entropia	$\log_2(10^8) = \pm 26{,}5754247591$ bits
Tentativas para quebra	$10^8 = 100.000.000$
Tempo de quebra 25 GPUs	+- 0,29 microssegundos
Tempo de quebra 3.3 GHz	+- 30,3 microssegundos

Fonte: Autoria própria.

Quadro 33 - Senhas vazadas do Instagram, análise da 9º senha

Senha	hello123
Comprimento	8 caracteres
Máscara	[a-z][a-z][a-z][a-z][a-z][0-9][0-9][0-9]
Conjunto de caracteres	26+10=36 possibilidades por caractere
Entropia	$\log_2(36^8) = \pm 41{,}3594000115$ bits
Tentativas para quebra	$36^8 = 2{,}8211099e + 12$
Tempo de quebra 25 GPUs	+- 8,060314 segundos
Tempo de quebra 3.3 GHz	+- 14,25 minutos

Fonte: Autoria própria.

Quadro 34 - Senhas vazadas do Instagram, análise da 10º senha

Senha	august2006
Comprimento	10 caracteres
Máscara	[a-z][a-z][a-z][a-z][a-z][a-z][0-9][0-9][0-9][0-9]
Conjunto de caracteres	26+10=36 possibilidades por caractere
Entropia	$\log_2(36^{10}) = \pm 51{,}70\ bits$
Tentativas para quebra	$36^{10} = 3.6561584e + 15$
Tempo de quebra 25 GPUs	+- 2,9 horas
Tempo de quebra 3.3 GHz	+- 1,83 semanas

Fonte: Autoria própria.

Quadro 35 - Senhas vazadas do Instagram, análise da 11º senha

Senha	lemonyellow
Comprimento	11 caracteres
Máscara	[a-z][a-z][a-z][a-z][a-z][a-z][a-z][a-z][a-z][a-z][a-z]
Conjunto de caracteres	26 possibilidades por caractere
Entropia	$\log_2(26^{11}) = \pm 51{,}7048368996\ bits$
Tentativas para quebra	$26^{11} = 3{,}6703445e + 15$
Tempo de quebra 25 GPUs	+- 2,91 horas
Tempo de quebra 3.3 GHz	+- 308,95 horas

Fonte: Autoria própria.

Quadro 36 - Senhas vazadas do Instagram, análise da 12º senha

Senha	fionavar
Comprimento	8 caracteres
Máscara	[a-z][a-z][a-z][a-z][a-z][a-z][a-z][a-z]
Conjunto de caracteres	26 possibilidades por caractere
Entropia	$\log_2(26^8) = \pm 37{,}6035177451$ bits
Tentativas para quebra	$26^8 = 208.827.064.576$
Tempo de quebra 25 GPUs	+- 0,6 microssegundos
Tempo de quebra 3.3 GHz	+- 0,06 segundos

Fonte: Autoria própria.

Quadro 37 - Senhas vazadas do Instagram, análise da 13º senha

Senha	nani7107
Comprimento	8 caracteres
Máscara	[a-z][a-z][a-z][a-z][0-9][0-9][0-9][0-9]
Conjunto de caracteres	26+10=36 possibilidades por caractere
Entropia	$\log_2(36^8) = \pm 41{,}3594000115$ bits
Tentativas para quebra	$36^8 = 2{,}8211099e + 12$
Tempo de quebra 25 GPUs	+- 8,060314 segundos
Tempo de quebra 3.3 GHz	+- 14,25 minutos

Fonte: Autoria própria.

Quadro 38 - Senhas vazadas do Instagram, análise da 14º senha

Senha	0731290649
Comprimento	10 caracteres
Máscara	[0-9][0-9][0-9][0-9][0-9][0-9][0-9][0-9][0-9][0-9]
Conjunto de caracteres	10 possibilidades por caractere
Entropia	$\log_2(10^{10}) = \pm 33{,}2192809489\ bits$
Tentativas para quebra	$10^{10} = 10000000000$
Tempo de quebra 25 GPUs	+- 28,57 milissegundos
Tempo de quebra 3.3 GHz	+- 3,03 segundos

Fonte: Autoria própria.

Quadro 39 - Senhas vazadas do Instagram, análise da 15º senha

Senha	bibo1929
Comprimento	8 caracteres
Máscara	[a-z][a-z][a-z][a-z][0-9][0-9][0-9][0-9]
Conjunto de caracteres	26+10=36 possibilidades por caractere
Entropia	$\log_2(36^8) = \pm 41{,}3594000115$ bits
Tentativas para quebra	$36^8 = 2{,}8211099e + 12$
Tempo de quebra 25 GPUs	+- 8,060314 segundos
Tempo de quebra 3.3 GHz	+- 14,25 minutos

Fonte: Autoria própria.

Quadro 40 - Senhas vazadas do Instagram, análise da 16º senha

Senha	safejolu
Comprimento	8 caracteres
Máscara	[a-z][a-z][a-z][a-z][a-z][a-z][a-z][a-z]
Conjunto de caracteres	26 possibilidades por caractere
Entropia	$\log_2(26^8) = \pm 37{,}6035177451$ bits
Tentativas para quebra	$26^8 = 208.827.064.576$
Tempo de quebra 25 GPUs	+- 0,6 microssegundos
Tempo de quebra 3.3 GHz	+- 0,06 segundos

Fonte: Autoria própria.

Quadro 41 - Senhas vazadas do Instagram, análise da 17º senha

Senha	snowball
Comprimento	8 caracteres
Máscara	[a-z][a-z][a-z][a-z][a-z][a-z][a-z][a-z]
Conjunto de caracteres	26 possibilidades por caractere
Entropia	$\log_2(26^8) = \pm 37{,}6035177451$ bits
Tentativas para quebra	$26^8 = 208.827.064.576$
Tempo de quebra 25 GPUs	+- 0,6 microssegundos
Tempo de quebra 3.3 GHz	+- 0,06 segundos

Fonte: Autoria própria.

Quadro 42 - Senhas vazadas do Instagram, análise da 18º senha

Senha	lindsey12
Comprimento	9 caracteres
Máscara	[a-z][a-z][a-z][a-z][a-z][a-z][a-z][0-9][0-9]
Conjunto de caracteres	26+10=36 possibilidades por caractere
Entropia	$\log_2(36^9) = \pm 46{,}529325013\ bits$
Tentativas para quebra	$36^9 = 1.0155996e + 14$
Tempo de quebra 25 GPUs	+- 4,84 minutos
Tempo de quebra 3.3 GHz	+- 8,55 horas

Fonte: Autoria própria.

Quadro 43 - Senhas vazadas do Instagram, análise da 19º senha

Senha	8joghtany
Comprimento	9 caracteres
Máscara	[0-9][a-z][a-z][a-z][a-z][a-z][a-z][a-z][a-z]
Conjunto de caracteres	26+10=36 possibilidades por caractere
Entropia	$\log_2(36^9) = \pm 46{,}529325013\ bits$
Tentativas para quebra	$36^9 = 1.0155996e + 14$
Tempo de quebra 25 GPUs	+- 4,84 minutos
Tempo de quebra 3.3 GHz	+- 8,55 horas

Fonte: Autoria própria.

Quadro 44 - Senhas vazadas do Instagram, análise da 20º senha

Senha	16121992mohan
Comprimento	13 caracteres
Máscara	[0-9][0-9][0-9][0-9][0-9][0-9][0-9][0-9][a-z][a-z][a-z][a-z][a-z]
Conjunto de caracteres	26+10=36 possibilidades por caractere
Entropia	$\log_2(36^{13}) = \pm 67{,}2090250188$ bits
Tentativas para quebra	$36^{13} = 1.7058173\text{e} + 20$
Tempo de quebra 25 GPUs	+- 15,44 anos
Tempo de quebra 3.3 GHz	+- 16,38 séculos

Fonte: Autoria própria.

Quadro 45 - Senhas vazadas do Instagram, análise da 21º senha

Senha	rn2417bayan
Comprimento	11 caracteres
Máscara	[a-z][0-9][0-9][0-9][0-9][a-z][a-z][a-z][a-z][a-z][a-z]
Conjunto de caracteres	26+10=36 possibilidades por caractere
Entropia	$\log_2(36^{11}) = \pm 56{,}8691750159\ bits$
Tentativas para quebra	$36^{11} = 1{,}316217e + 17$
Tempo de quebra 25 GPUs	+- 4,35 dias
Tempo de quebra 3.3 GHz	+- 1,26 anos

Fonte: Autoria própria.

Quadro 46 - Senhas vazadas do Instagram, análise da 22º senha

Senha	underground69
Comprimento	13 caracteres
Máscara	[a-z][a-z][a-z][a-z][a-z][a-z][a-z][a-z][a-z][a-z][a-z][0-9][0-9]
Conjunto de caracteres	26+10=36 possibilidades por caractere
Entropia	$\log_2(36^{13}) = \pm 67{,}2090250188$ bits
Tentativas para quebra	$36^{13} = 1.7058173\text{e} + 20$
Tempo de quebra 25 GPUs	+- 15,44 anos
Tempo de quebra 3.3 GHz	+- 16,38 séculos

Fonte: Autoria própria.

Quadro 47 - Senhas vazadas do Instagram, análise da 23º senha

Senha	CHIecher875
Comprimento	11 caracteres
Máscara	[A-Z][A-Z][A-Z][a-z][a-z][a-z][a-z][a-z][0-9][0-9][0-9]
Conjunto de caracteres	26+26+10=62 possibilidades por caractere
Entropia	$\log_2(62^{11}) = \pm 65{,}4961594143\ bits$
Tentativas para quebra	$62^{11} = 5.2036561e + 19$
Tempo de quebra 25 GPUs	+- 4,71 anos
Tempo de quebra 3.3 GHz	+- 4,9968 séculos

Fonte: Autoria própria.

Quadro 48 - Senhas vazadas do Instagram, análise da 24º senha

Senha	kK1119132175
Comprimento	12 caracteres
Máscara	[a-z][A-Z][0-9][0-9][0-9][0-9][0-9][0-9][0-9][0-9][0-9][0-9]
Conjunto de caracteres	26+26+10=62 possibilidades por caractere
Entropia	$\log_2(62^{12}) = \pm 71{,}4503557246\ bits$
Tentativas para quebra	$62^{12} = 3{,}2262668e + 21$
Tempo de quebra 25 GPUs	+- 2,921 séculos
Tempo de quebra 3.3 GHz	+- 309,8007 séculos

Fonte: Autoria própria.

Quadro 49 - Senhas vazadas do Instagram, análise da 25º senha

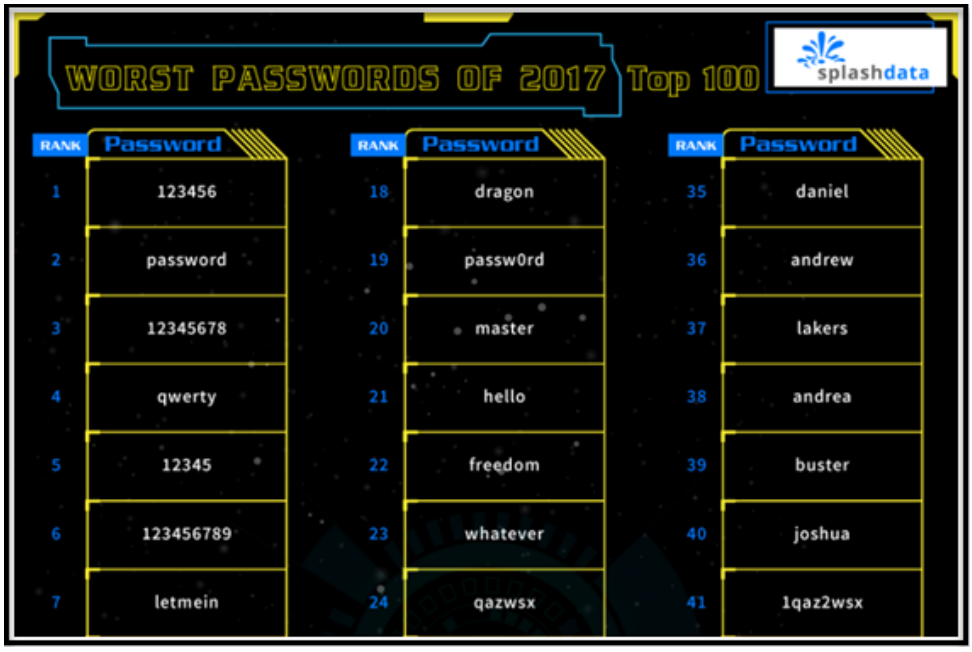
Senha	1952vnf
Comprimento	7 caracteres
Máscara	[0-9][0-9][0-9][0-9][a-z][a-z][a-z]
Conjunto de caracteres	26+10=36 possibilidades por caractere
Entropia	$\log_2(36^7) = \pm 36{,}1894750101\ bits$
Tentativas para quebra	$36^7 = 78364164096$
Tempo de quebra 25 GPUs	+- 0,22 segundos
Tempo de quebra 3.3 GHz	+- 23,75 segundos

Fonte: Autoria própria.

3.1.3 Análise das Senhas mais Utilizadas em 2017

A Figura 30, apresenta a lista das piores senhas utilizadas em 2017. Segundo a SplashData, são as piores, pois foram as senhas mais utilizadas em 2017. Todas as imagens encontram-se localizadas no Apêndice B: Figura 50, Figura 51, Figura 52 e Figura 53.

Figura 30 - Senhas mais utilizadas em 2017



Fonte: Autoria própria. Disponível em: <https://s13639.pcdn.co/wp-content/uploads/2017/12/Top-100-Worst-Passwords-of-2017a.pdf>. Acesso em: 12 set. 2018.

Ao analisar as 25 senhas mais utilizadas em 2017, obtém-se os dados apresentados nos quadros: 1) Quadro 50 (Senha: “123456”); 2) Quadro 51 (Senha: “password”); 3) Quadro 52 (Senha: “12345678”); 4) Quadro 53 (Senha: “qwerty”); 5) Quadro 54 (Senha: “12345”); 6) Quadro 55 (Senha: “123456789”); 7) Quadro 56 (Senha: “letmein”); 8) Quadro 57 (Senha: “1234567”); 9) Quadro 58 (Senha: “football”); 10) Quadro 59 (Senha: “iloveyou”); 11) Quadro 60 (Senha: “admin”); 12) Quadro 61

(Senha: “welcome”); 13) Quadro 62 (Senha: “monkey”); 14) Quadro 63 (Senha: “login”); 15) Quadro 64 (Senha: “abc123”); 16) Quadro 65 (Senha: “starwars”); 17) Quadro 66 (Senha: “123123”); 18) Quadro 67 (Senha: “dragon”); 19) Quadro 68 (Senha: “passw0rd”); 20) Quadro 69 (Senha: “master”); 21) Quadro 70 (Senha: “hello”); 22) Quadro 71 (Senha: “freedom”); 23) Quadro 72 (Senha: “whatever”); 24) Quadro 73 (Senha: “qazwsx”); e 25) Quadro 74 (Senha: “trustno1”).

Quadro 50 - Senhas mais utilizadas, análise da 1º posição

Senha	123456
Comprimento	6 caracteres
Máscara	[0-9][0-9][0-9][0-9][0-9][0-9]
Conjunto de caracteres	10 possibilidades por caractere
Entropia	$\log_2(10^6) = \pm 19{,}9315685693$ bits
Tentativas para quebra	$10^6 = 1.000.000$
Tempo de quebra 25 GPUs	+- 2,86 nanosegundos
Tempo de quebra 3.3 GHz	+- 0,3 microssegundos

Fonte: Autoria própria.

Quadro 51 - Senhas mais utilizadas, análise da 2º posição

Senha	password
Comprimento	8 caracteres
Máscara	[a-z][a-z][a-z][a-z][a-z][a-z][a-z][a-z]
Conjunto de caracteres	26 possibilidades por caractere
Entropia	$\log_2(26^8) = \pm 37{,}6035177451$ bits
Tentativas para quebra	$26^8 = 208.827.064.576$
Tempo de quebra 25 GPUs	+- 0,6 microssegundos
Tempo de quebra 3.3 GHz	+- 0,06 segundos

Fonte: Autoria própria.

Quadro 52 - Senhas mais utilizadas, análise da 3º posição

Senha	12345678
Comprimento	8 caracteres
Máscara	[0-9][0-9][0-9][0-9][0-9][0-9][0-9][0-9]
Conjunto de caracteres	10 possibilidades por caractere
Entropia	$\log_2(10^8) = \pm 26{,}5754247591$ bits
Tentativas para quebra	$10^8 = 100.000.000$
Tempo de quebra 25 GPUs	+- 0,29 microssegundos
Tempo de quebra 3.3 GHz	+- 30,3 microssegundos

Fonte: Autoria própria.

Quadro 53 - Senhas mais utilizadas, análise da 4º posição

Senha	qwerty
Comprimento	6 caracteres
Máscara	[a-z][a-z][a-z][a-z][a-z][a-z]
Conjunto de caracteres	26 possibilidades por caractere
Entropia	$\log_2(26^6) = \pm 28{,}2026383088$ bits
Tentativas para quebra	$26^6 = 308915776$
Tempo de quebra 25 GPUs	+- 0,88 milissegundos
Tempo de quebra 3.3 GHz	+- 96,61 milissegundos

Fonte: Autoria própria.

Quadro 54 - Senhas mais utilizadas, análise da 5º posição

Senha	12345
Comprimento	5 caracteres
Máscara	[0-9][0-9][0-9][0-9][0-9]
Conjunto de caracteres	10 possibilidades por caractere
Entropia	$\log_2(10^5) = \pm 16{,}6096404744$ bits
Tentativas para quebra	$10^5 = 100000$
Tempo de quebra 25 GPUs	+- 0,29 microssegundos
Tempo de quebra 3.3 GHz	+- 30,3 microssegundos

Fonte: Autoria própria.

Quadro 55 - Senhas mais utilizadas, análise da 6º posição

Senha	123456789
Comprimento	9 caracteres
Máscara	[0-9][0-9][0-9][0-9][0-9][0-9][0-9][0-9][0-9]
Conjunto de caracteres	10 possibilidades por caractere
Entropia	$\log_2(10^9) = \pm 29{,}897352854$ bits
Tentativas para quebra	$10^9 = 1000000000$
Tempo de quebra 25 GPUs	+- 2,86 milissegundos
Tempo de quebra 3.3 GHz	+- 303,3 milissegundos

Fonte: Autoria própria.

Quadro 56 - Senhas mais utilizadas, análise da 7º posição

Senha	letmein
Comprimento	7 caracteres
Máscara	[a-z][a-z][a-z][a-z][a-z][a-z][a-z]
Conjunto de caracteres	26 possibilidades por caractere
Entropia	$\log_2(26^7) = \pm 32{,}903078027$ bits
Tentativas para quebra	$26^7 = 8031810176$
Tempo de quebra 25 GPUs	+- 0,02 segundos
Tempo de quebra 3.3 GHz	+- 2,43 segundos

Fonte: Autoria própria.

Quadro 57 - Senhas mais utilizadas, análise da 8º posição

Senha	1234567
Comprimento	7 caracteres
Máscara	[0-9][0-9][0-9][0-9][0-9][0-9][0-9]
Conjunto de caracteres	10 possibilidades por caractere
Entropia	$\log_2(10^7) = \pm 23{,}2534966642$ bits
Tentativas para quebra	$10^7 = 10000000$
Tempo de quebra 25 GPUs	+- 28,57 microssegundos
Tempo de quebra 3.3 GHz	+- 3,03 milissegundos

Fonte: Autoria própria.

Quadro 58 - Senhas mais utilizadas, análise da 9º posição

Senha	football
Comprimento	8 caracteres
Máscara	[a-z][a-z][a-z][a-z][a-z][a-z][a-z][a-z]
Conjunto de caracteres	26 possibilidades por caractere
Entropia	$\log_2(26^8) = \pm 37{,}6035177451$ bits
Tentativas para quebra	$26^8 = 208.827.064.576$
Tempo de quebra 25 GPUs	+- 0,6 microssegundos
Tempo de quebra 3.3 GHz	+- 0,06 segundos

Fonte: Autoria própria.

Quadro 59 - Senhas mais utilizadas, análise da 10º posição

Senha	iloveyou
Comprimento	8 caracteres
Máscara	[a-z][a-z][a-z][a-z][a-z][a-z][a-z][a-z]
Conjunto de caracteres	26 possibilidades por caractere
Entropia	$\log_2(26^8) = \pm 37{,}6035177451$ bits
Tentativas para quebra	$26^8 = 208.827.064.576$
Tempo de quebra 25 GPUs	+- 0,6 microssegundos
Tempo de quebra 3.3 GHz	+- 0,06 segundos

Fonte: Autoria própria.

Quadro 60 - Senhas mais utilizadas, análise da 11º posição

Senha	admin
Comprimento	5 caracteres
Máscara	[a-z][a-z][a-z][a-z][a-z]
Conjunto de caracteres	26 possibilidades por caractere
Entropia	$\log_2(26^5) = \pm 23{,}5021985907$ bits
Tentativas para quebra	$26^5 = 11881376$
Tempo de quebra 25 GPUs	+- 0,03 milissegundos
Tempo de quebra 3.3 GHz	+- 3,6 milissegundos

Fonte: Autoria própria.

Quadro 61 - Senhas mais utilizadas, análise da 12º posição

Senha	welcome
Comprimento	7 caracteres
Máscara	[a-z][a-z][a-z][a-z][a-z][a-z][a-z]
Conjunto de caracteres	26 possibilidades por caractere
Entropia	$\log_2(26^7) = \pm 32{,}903078027$ bits
Tentativas para quebra	$26^7 = 8031810176$
Tempo de quebra 25 GPUs	+- 0,02 segundos
Tempo de quebra 3.3 GHz	+- 2,43 segundos

Fonte: Autoria própria.

Quadro 62 - Senhas mais utilizadas, análise da 13º posição

Senha	monkey
Comprimento	6 caracteres
Máscara	[a-z][a-z][a-z][a-z][a-z][a-z]
Conjunto de caracteres	26 possibilidades por caractere
Entropia	$\log_2(26^6) = \pm 28{,}2026383088$ bits
Tentativas para quebra	$26^6 = 308915776$
Tempo de quebra 25 GPUs	+- 0,88 milissegundos
Tempo de quebra 3.3 GHz	+- 96,61 milissegundos

Fonte: Autoria própria.

Quadro 63 - Senhas mais utilizadas, análise da 14º posição

Senha	login
Comprimento	5 caracteres
Máscara	[a-z][a-z][a-z][a-z][a-z]
Conjunto de caracteres	26 possibilidades por caractere
Entropia	$\log_2(26^5) = \pm 23{,}5021985907$ bits
Tentativas para quebra	$26^5 = 11881376$
Tempo de quebra 25 GPUs	+- 0,03 milissegundos
Tempo de quebra 3.3 GHz	+- 3,6 milissegundos

Fonte: Autoria própria.

Quadro 64 - Senhas mais utilizadas, análise da 15º posição

Senha	abc123
Comprimento	6 caracteres
Máscara	[a-z][a-z][a-z][0-9][0-9][0-9]
Conjunto de caracteres	26+10=36 possibilidades por caractere
Entropia	$\log_2(36^6) = \pm 31{,}0195500087$ bits
Tentativas para quebra	$36^6 = 2176782336$
Tempo de quebra 25 GPUs	+- 6,22 milissegundos
Tempo de quebra 3.3 GHz	+- 659,63 milissegundos

Fonte: Autoria própria.

Quadro 65 - Senhas mais utilizadas, análise da 16º posição

Senha	starwars
Comprimento	8 caracteres
Máscara	[a-z][a-z][a-z][a-z][a-z][a-z][a-z][a-z]
Conjunto de caracteres	26 possibilidades por caractere
Entropia	$\log_2(26^8) = \pm 37{,}6035177451$ bits
Tentativas para quebra	$26^8 = 208.827.064.576$
Tempo de quebra 25 GPUs	+- 0,6 microssegundos
Tempo de quebra 3.3 GHz	+- 0,06 segundos

Fonte: Autoria própria.

Quadro 66 - Senhas mais utilizadas, análise da 17º posição

Senha	123123
Comprimento	6 caracteres
Máscara	[0-9][0-9][0-9][0-9][0-9][0-9]
Conjunto de caracteres	10 possibilidades por caractere
Entropia	$\log_2(10^6) = \pm 19{,}9315685693$ bits
Tentativas para quebra	$10^6 = 1.000.000$
Tempo de quebra 25 GPUs	+- 2,86 nanosegundos
Tempo de quebra 3.3 GHz	+- 0,3 microssegundos

Fonte: Autoria própria.

Quadro 67 - Senhas mais utilizadas, análise da 18º posição

Senha	dragon
Comprimento	6 caracteres
Máscara	[a-z][a-z][a-z][a-z][a-z][a-z]
Conjunto de caracteres	26 possibilidades por caractere
Entropia	$\log_2(26^6) = \pm 28{,}2026383088$ bits
Tentativas para quebra	$26^6 = 308915776$
Tempo de quebra 25 GPUs	+- 0,88 milissegundos
Tempo de quebra 3.3 GHz	+- 96,61 milissegundos

Fonte: Autoria própria.

Quadro 68 - Senhas mais utilizadas, análise da 19º posição

Senha	passw0rd
Comprimento	8 caracteres
Máscara	[a-z][a-z][a-z][a-z][a-z][0-9][a-z][a-z]
Conjunto de caracteres	26+10=36 possibilidades por caractere
Entropia	$\log_2(36^8) = \pm 41{,}3594000115$ bits
Tentativas para quebra	$36^8 = 2{,}8211099e + 12$
Tempo de quebra 25 GPUs	+- 8,060314 segundos
Tempo de quebra 3.3 GHz	+- 14,25 minutos

Fonte: Autoria própria.

Quadro 69 - Senhas mais utilizadas, análise da 20º posição

Senha	master
Comprimento	6 caracteres
Máscara	[a-z][a-z][a-z][a-z][a-z][a-z]
Conjunto de caracteres	26 possibilidades por caractere
Entropia	$\log_2(26^6) = \pm 28{,}2026383088$ bits
Tentativas para quebra	$26^6 = 308915776$
Tempo de quebra 25 GPUs	+- 0,88 milissegundos
Tempo de quebra 3.3 GHz	+- 96,61 milissegundos

Fonte: Autoria própria.

Quadro 70 - Senhas mais utilizadas, análise da 21º posição

Senha	hello
Comprimento	5 caracteres
Máscara	[a-z][a-z][a-z][a-z][a-z]
Conjunto de caracteres	26 possibilidades por caractere
Entropia	$\log_2(26^5) = \pm 23{,}5021985907$ bits
Tentativas para quebra	$26^5 = 11881376$
Tempo de quebra 25 GPUs	+- 0,03 milissegundos
Tempo de quebra 3.3 GHz	+- 3,6 milissegundos

Fonte: Autoria própria.

Quadro 71 - Senhas mais utilizadas, análise da 22º posição

Senha	freedom
Comprimento	7 caracteres
Máscara	[a-z][a-z][a-z][a-z][a-z][a-z][a-z]
Conjunto de caracteres	26 possibilidades por caractere
Entropia	$\log_2(26^7) = \pm 32{,}903078027$ bits
Tentativas para quebra	$26^7 = 8031810176$
Tempo de quebra 25 GPUs	+- 0,02 segundos
Tempo de quebra 3.3 GHz	+- 2,43 segundos

Fonte: Autoria própria.

Quadro 72 - Senhas mais utilizadas, análise da 23º posição

Senha	whatever
Comprimento	8 caracteres
Máscara	[a-z][a-z][a-z][a-z][a-z][a-z][a-z][a-z]
Conjunto de caracteres	26 possibilidades por caractere
Entropia	$\log_2(26^8) = \pm 37{,}6035177451$ bits
Tentativas para quebra	$26^8 = 208.827.064.576$
Tempo de quebra 25 GPUs	+- 0,6 microssegundos
Tempo de quebra 3.3 GHz	+- 0,06 segundos

Fonte: Autoria própria.

Quadro 73 - Senhas mais utilizadas, análise da 24º posição

Senha	qazwsx
Comprimento	6 caracteres
Máscara	[a-z][a-z][a-z][a-z][a-z][a-z]
Conjunto de caracteres	26 possibilidades por caractere
Entropia	$\log_2(26^6) = \pm 28{,}2026383088$ bits
Tentativas para quebra	$26^6 = 308915776$
Tempo de quebra 25 GPUs	+- 0,88 milissegundos
Tempo de quebra 3.3 GHz	+- 96,61 milissegundos

Fonte: Autoria própria.

Quadro 74 - Senhas mais utilizadas, análise da 25º posição

Senha	trustno1
Comprimento	8 caracteres
Máscara	[a-z][a-z][a-z][a-z][a-z][a-z][a-z][0-9]
Conjunto de caracteres	26+10=36 possibilidades por caractere
Entropia	$\log_2(36^8) = \pm 41{,}3594000115$ bits
Tentativas para quebra	$36^8 = 2{,}8211099e + 12$
Tempo de quebra 25 GPUs	+- 8,060314 segundos
Tempo de quebra 3.3 GHz	+- 14,25 minutos

Fonte: Autoria própria.

Além da análise acima, pode-se observar que as senhas são compostas de padrões como:

- Sequências numéricas: 123456, 1234578, 123456789, 1234567, 12345, 1234 e 654321;
- Repetições com poucas variações: 123123, 121212, aaaaaa e 12341234;
- Sequências de caracteres do teclado: qwerty, asdf, qazwsx, zaq1zaq1, 1qaz2wsx, 1q2w3e e querty;
- Sequências com poucas variações, usando primeiras letras e primeiros números: abc123;
- Nomes comuns com poucas variações: daniel, jessica, amanda, andrew, andrea, george, jordan, charlie, jennifer, nicole, jordan, jordan23, robert, matthew, joshua, merlin, ashley, michelle, william, maggie e martin;
- Marcas de veículos: ferrari, mercedes, corvette, harley e maverick;
- Times: yankees, lakers;
- Esportes: football, hockey, soccer e golfer;
- Expressões e gírias: letmein, welcome, asshole, whatever, iloveyou, hello, fuckyou, blahblah, trustno1, sunshine e bitme;
- Anos anteriores a 2000 (provavelmente anos de nascimento): 1990, 1991, 1994, 1992 e 1989;
- Referência a própria de senha: password, passw0rd, pass, password1 e passwor;
- Referência ao próprio painel: login;
- Nomes de administradores com poucas variações: admin, master e admin123;
- Cidades: london e dallas;
- Nomes de animais: monkey e tigger;
- Nomes de filmes: starwars;
- Estações do ano: summer;

- Comida: banana, cheese, cookie, pepper e ginger;
- Referência a guarda e a bandido: bandit, hunter, ranger e rangers;
- Palavras facilmente encontradas em dicionários: test, dragon, freedom, computer, killer, buster, thunder, solo, pussy e phoenix.

Nesta lista de 2017, entrou de novo a senha “starwars”, devido ao recente filme da franquia, que fez com que muitas pessoas optassem pela escolha do nome do filme de sucesso como senha.

Observe que senhas fracas vão muito além de dados pessoais, conforme análise feita acima, existem padrões mais comuns de sequência de caracteres, nome de cidades, palavras encontradas em dicionários, repetições simples, que enfraquecem a força da entropia da senha.

Adicionalmente, ao verificar o tamanho de caracteres desta lista, nota-se que o tamanho é de 4 até 9 caracteres. Quanto menor for o tamanho da senha, mais insegura poderá ficar para decifrá-la, pois exigirá menor poder e tempo de processamento ao utilizar alguma ferramenta de força bruta por exemplo para a decifragem, isto é, para o processo de criptoanálise referente a descoberta da senha.

4 CONSIDERAÇÕES SOBRE PROTEÇÃO DE SENHAS

Muitos fatores devem ser levados na proteção de senhas, neste capítulo propõe mostrar as boas práticas em sua elaboração recomendas pela Cert.br (2012), Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil, que elaborou a Cartilha de Segurança para Internet, que é um documento com recomendações e dicas para aumentar a segurança (Figura 31) e a proteção referente ao comportamento de usuários na internet.

Figura 31 - Cartilha de segurança

Fonte: Autoria própria. Disponível em: <https://cartilha.cert.br>. Acesso em: 12 set. 2018.

E também como é possível utilizar ferramentas de:

- Analisador de senhas: para verificar se a sua senha é forte o suficiente;
- Gerenciadores de senhas: para armazenar todas suas outras dezenas de contas;
- MinhaSenha e HIBP: para analisar se as suas senhas foram descobertas e estão sendo divulgadas na internet.

4.1 BOAS PRÁTICAS PARA ELABORAÇÃO DE SENHAS

Recomenda-se como boas práticas na criação de senhas mais seguras segundo Cert.br (2012) os seguintes critérios:

- Números aleatórios: pois não tem nenhuma relação com informações pessoais (CERT.BR, 2012);
- Grande quantidade de caracteres: quanto maior for a senha, mais tempo levará de processamento, podendo chegar a anos, se tornando inviável para tentativas de descobertas (CERT.BR, 2012);

- Diferentes tipos de caracteres: recomenda-se misturar números, sinais de pontuação e letras maiúsculas e minúsculas para fortalecer a senha (CERT.BR, 2012).

De acordo com Mitnick e Simon (2003, p. 255) recomendam que as senhas:

> Contenham pelo menos um número, pelo menos um símbolo (tal como $, _, !. &). pelo menos uma letra minúscula e pelo menos uma letra maiúscula (na medida em que tais variáveis sejam suportadas pelo sistema operacional).

Além do mais, a Cert.br (2012) oferece algumas dicas práticas para a elaboração de senhas mais seguras como:

- Selecionar caracteres de uma frase: por exemplo, a frase “Segurança em primeiro lugar sempre que eu puder”, pode-se utilizar a posição de cada palavra para elaborar a senha, para ilustrar isto, se pegar o primeiro e último carácter de cada palavra da frase anterior ficaria “Saempolrseqeeupe” (CERT.BR, 2012);
- Utilizar uma frase longa: isto é, escolher uma frase fácil de memorizar que tenha diferentes tipos de caracteres e que não seja citações comuns, refrões de músicas ou frases pessoais. Exemplo: “farei este trabalho com muita dedicação e muitas pesquisas” se tornaria como senha da seguinte forma: “fareiestetrabalhocommuitadedicaçãoemuitaspesquisas” (CERT.BR, 2012);
- Substituições de caracteres: seria inventar o próprio padrão de substituição. Por exemplo, por semelhanças, por duplicações, por substituições de algumas letras por números (CERT.BR, 2012).

Outro fator relevante é evitar senhas que utilizam dados pessoais como por exemplo número do celular, número da identidade, data de nascimento, nome completo, nome de algum membro da família, ano de nascimento dos filhos, escola que frequentou, nome do animal de estimação, do desenho predileto, do filme favorito, do jogo que mais gostou, são consideradas fracas pois são informações fáceis de se obter. Muitas destas informações estão disponíveis para se coletar de maneira gratuita na própria internet através de redes sociais como Facebook, Instagram e Google+ (CERT.BR, 2012).

De acordo com Mitnick e Simon (2003, p. 256) não se deve utilizar na construção de senhas:

> [...] palavras de um dicionário de qualquer idioma; qualquer palavra que esteja relacionada com família, hobbies, veículo, trabalho, placas do veículo. número de seguro social, endereço, telefone, nome do bichinho de estimação do empregado ou frases contendo essas palavras. [...] Não sejam a variação de uma senha usada anteriormente

Importante ressaltar que estas dicas devem ser adaptadas, pois já existem muitos padrões que são de conhecimento público. Além do mais, estas dicas devem ser utilizadas em combinação para aumentar a proteção da mesma e devem ser trocadas periodicamente sempre que possível, nunca serem reveladas a ninguém, não armazenar em lugares inseguros e não elaborar senhas muito curtas (CERT.BR, 2012).

Mas o que leva uma senha ser boa? Segundo Kissell (2017, p. 44) “uma senha boa é algo que você não esquecerá e que nenhum outro humano ou computador conseguirá adivinhar”, uma vez que possuem uma sequência simples, lógica ou intuitiva que podem ser vítimas na internet de contas roubadas e posteriormente dados pessoais vazados (KISSELL, 2017).

4.2 ANALISADORES DE SENHAS

Caso tenha interesse em saber o quanto é segura sua senha, é possível utilizando analisadores de senhas.

A *Kaspersky Lab* (Figura 32), empresa russa fornecedora de serviços de softwares de segurança, oferece o serviço para fins educacionais, onde é possível avaliar o grau de segurança como também o tempo que levará de processamento para descobrir através de ataques de força bruta, para mais informações deve-se consultar o site “https://password.kaspersky.com/br”.

Figura 32 - Kaspersky Lab

Fonte: Autoria própria. Disponível em: <https://password.kaspersky.com/br/>. Acesso em: 12 set. 2018.

Na Figura 33, foi digitado a senha “12345678999” no verificador de senhas. Note que apesar da senha conter 11 dígitos, apresenta os erros comuns como: combinação muito usada e caracteres repetidos. O nível de segurança está em com

3 barras em vermelho, que representa senha fraca quase moderada. Além do vermelho, há o amarelo representado senha moderada e o verde representando senha forte. O que é interessante nesta verificação é mostrar o tempo estimado de quebra de senha de apenas 3 minutos com base no cálculo utilizado pela empresa *Kaspersky Lab*.

Figura 33 - Senha 12345678999

Fonte: Autoria própria. Disponível em: <https://password.kaspersky.com/br/>. Acesso em: 12 set. 2018.

Caso seja utilizado uma senha seguindo as recomendações de segurança como a frase “saia da matrix” com a substituição de alguns caracteres e a adição de alguns caracteres sem sentidos, ficando da seguinte forma “sai00d11mAtrix@@#”.

Haverá maior proteção, observa-se que o nível de proteção, apresentado na Figura 34, está em verde e com todas as barras preenchidas, representando senha forte. Ela também pode ser descoberta, mas levará muito tempo, em torno de 1889 séculos, se tornando inviável de realizar ataque por força bruta.

Figura 34 - Senha sai00d11mAtrix@@#”

Fonte: Autoria própria. Disponível em: <https://password.kaspersky.com/br/>. Acesso em: 12 set. 2018.

Vale ressaltar que estes analisadores de senhas nem sempre estão 100% corretos, pois ao utilizar substituição de caracteres pelo óbvio, podem representar uma falsa verificação dizendo que se trata de uma segurança forte. Por exemplo, a substituição de “E” por “3” é muito utilizado hoje em dia e pode ocorrer, dependendo da elaboração do analisador de senhas, de tratar como uma boa prática, o correto é

realizar a substituição deste exemplo por algum que não faça sentido e que seja pouco utilizado nos padrões atuais como “00” (KISSELL, 2017).

4.3 GERENCIADORES DE SENHA

Atualmente, cada pessoa dificilmente possui poucas contas para gerenciar, aqui entra o problema de reutilizar a mesma senha em várias contas, por mais que a senha seja forte, a partir do momento que utiliza a mesma senha para várias contas, se corre um risco enorme de segurança pois de acordo com Kissell (2017, p. 22):

> Se a senha de um serviço ou site for comprometida (roubada, adivinhada, hackeada) e você utiliza esta mesma senha em outros lugares, a pessoa que a comprometeu poderá tentar utilizá-la em outros serviços e conseguirá fazer um estrago muito maior. Ao utilizar a mesma senha em todos os lugares você está, essencialmente, concedendo acesso a todos os seus dados pessoais para a primeira pessoa que descobrir a sua senha.

A solução para gerenciar centenas de contas é através de gerenciadores de senhas, ou também conhecido como cofre de senhas ou chaveiro de senhas, com este recurso poderá armazenar de forma segura as senhas geradas de forma randômica com forte poder de entropia sem se preocupar em memoriza-las. Apenas precisará memorizar a senha mestre, que é a palavra secreta utilizada no gerenciador de senhas para acessar as demais senhas (CERT.BR, 2012).

De acordo com Kissell (2017, p. 75):

> Os gerenciadores de senha protegem todos os seus nomes de usuário e senhas – e algumas vezes outros dados importantes – através de um arquivo criptografado que você pode desbloquear com uma única chave-mestra.
> [...] Como você só precisa memorizar uma senha, todas as demais podem ser longas e complexas, pois não será necessário conhece-las.

Note que precisará apenas memorizar uma única senha forte para acessar o gerenciador de senhas, mas não utilizará esta mesma senha para as demais contas. A ideia é copiar a senha pelo gerenciador de senhas para acessar a conta desejada. Com isto, evita o problema de utilizar a mesma senha em várias contas. Mesmo que uma senha seja vazada, não comprometerá as demais senhas, pois os gerenciadores de conta armazenam as senhas em uma base criptografada, que geralmente passam por um processo rigoroso de avaliação elaborado por criptógrafos profissionais, mesmo se houver um vazamento de bases por parte da empresa responsável pelo

software de gerenciamento, os dados estarão protegidos pela criptografia (KISSELL, 2017).

Mesmo que muitas pessoas achem difícil confiar no uso de gerenciadores de senhas, deve ser levado em consideração o seguinte exemplo mencionado pelo Kissell (2017, p. 80):

> Tanto pessoas quanto máquinas são imperfeitas, e confiar em alguém ou em alguma coisa poderia lhe causar problemas. Mesmo assim, precisamos confiar em pessoas todos os dias para que seja possível viver normalmente. O meu chaveiro, meu contador ou meu médico, poderiam estar secretamente tentando me roubar ou me causa mal, mas não tenho motivos para pensar que eles realmente estão tentando, fazer isso. Assim, é melhor eu confiar neles do que eu mesmo tentar trocar minhas fechaduras, fazer a minha contabilidade ou realizar eu mesmo as minhas cirurgias. Da mesma forma, o meu carro poderia estar sendo monitorado através de um dispositivo localizador e a lâmpada da minha mesa poderia conter uma câmera escondida, mas não tenho motivos para suspeitar que isso é verdade porque este tipo de paranoia não serve para nada.

Existem muitas opções de gerenciadores disponíveis atualmente, na Figura 35 e na Figura 36, é mostrada um comparativo dos gerenciadores de senhas “1Password”, “Dashlane”, “Enpass”, “LastPass” e “oneSafe”, que utilizam a chave de criptografia AES-256 (KLOPPER, 2016).

Figura 35 - Gerenciadores de senhas, parte 1 de 2

	1Password	Dashlane	Enpass	LastPass	oneSafe
Demonstrador de senha segura	SIM	SIM	SIM	SIM	NÃO
Tem como adicionar novos campos às senhas?	SIM (desktop)	NÃO	SIM	SIM (na versão web)	SIM
Importa senhas que já tinham no computador antes (no Acesso às Chaves)	NÃO	SIM	NÃO	SIM	NÃO
Importar e exportar informações	SIM	SIM	SIM	SIM	SIM
Versão web	SIM (só para planos *Family* ou *Team*)	SIM (somente leitura)	NÃO	SIM (inclusive, é a única maneira de ver/editar configurações avançadas)	NÃO
Preço	**Desktop:** US$65 (uma vez só) **Mobile:** gratuito com limitações (outras categorias ou pastas, entre outros recursos podem ser adquiridos por US$10)	**Desktop e mobile:** gratuito com limitações (US$40/ano para sincronizar as plataformas, entre outros recursos)	**Desktop:** totalmente gratuito **Mobile:** gratuito com limitações (somente 20 itens ou uma vez de US$10 por plataforma)	**Desktop e mobile:** gratuito com limitações (US$12/ano para utilizar em mais de uma plataformas)	**Desktop:** US$20 **Mobile:** US$5

Fonte: Klopper (2016).

Figura 36 - Gerenciadores de senhas, parte 2 de 2

	1Password	Dashlane	Enpass	LastPass	oneSafe
Sincronização	**Offline:** SIM **Online:** iCloud e Dropbox	**Offline:** SIM **Online:** servidor próprio	**Offline:** SIM **Online:** Box, iCloud, Dropbox, Google Drive, OneDrive, WebDAV/ownCloud	**Offline:** SIM **Online:** servidor próprio	**Offline:** SIM **Online:** iCloud
Backup	**SIM** (automático e manual)	**SIM** (se desabilitado o modo de sincronização online ou exportando os dados)	**SIM** (manual)	**SIM** (manualmente pelo site)	**SIM** (com opção de backup automático)
Extensões em navegadores	**Desktop:** Safari, Chrome, Firefox e Opera **Mobile:** Safari, Chrome e Firefox	**Desktop:** Safari, Chrome, Firefox, Opera e Internet Explorer **Mobile:** Safari e Chrome	**Desktop:** Safari, Chrome, Firefox e Opera **Mobile:** Safari	**Desktop:** Safari, Chrome, Firefox e Opera **Mobile:** Safari, Google Chrome e Firefox	**Desktop:** Safari **Mobile:** Safari
Captura novas senhas de sites?	**Desktop:** SIM (popup) **Mobile:** SIM (manualmente, pela extensão do Safari — já preenche o nome do site)	**Desktop:** SIM (popup) **Mobile:** SIM (manualmente, mas não preenche o nome/endereço do site automaticamente)	**Desktop:** SIM (popup) **Mobile:** SIM (manualmente, pela extensão do Safari — já preenche o nome do site)	**Desktop:** SIM (nova aba) **Mobile:** SIM (manualmente, pela extensão do Safari — já preenche o nome do site)	**Desktop:** SIM (popup) **Mobile:** NÃO
Gera e preenche senha forte ao se cadastrar em algum site?	**SIM** (pela extensão)	**SIM** (clicando no ícone dentro campo de senha ou na extensão)	**SIM** (pela extensão)	**SIM** (clicando no ícone dentro campo de senha ou na extensão)	**SIM** (pela extensão)
Preenchimento automático em logins	**SIM** (precisa selecionar a opção nas preferências do app)	**SIM** — inclusive em sites visitados pela 1ª vez (a partir de informações já adicionadas no app)	**NÃO** (precisa selecionar na extensão ou no atalho do teclado)	**SIM**	**SIM**
Opção de entrar no site automaticamente (auto-login)	**SIM**	**SIM**	**NÃO**	**SIM** (precisa habilitar antes a opção para cada site)	**SIM**
Pergunta se quer atualizar senha já cadastrada se a mudarmos no site?	**SIM**	**SIM**	**SIM**	**SIM**	**NÃO**
Preenchimento de formulários	**SIM** (pela extensão)	**SIM**, (opções aparecem automaticamente assim que o cursor é colocado no campo do formulário)	**NÃO** (caso queira preencher, pode procurar na extensão e copiar cada campo manualmente)	**SIM** (clicando no ícone dentro campo de senha ou na extensão)	**NÃO** (em desenvolvimento)

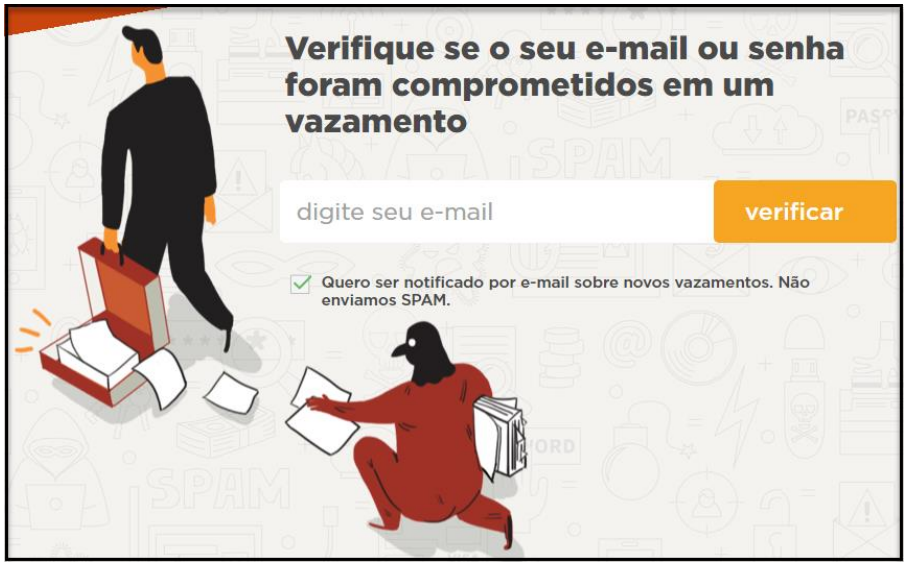
Fonte: Klopper (2016).

4.4 ANALISAR SE A SUA SENHA FOI DESCOBERTA

4.4.1 MinhaSenha

Axur, empresa responsável pelo monitoramento e reação a riscos digitais, que possui o site “minhasenha.com” (Figura 37), disponibilizando uma forma de consultar se o seu e-mail ou senha foram comprometidos.

Figura 37 - MinhaSenha



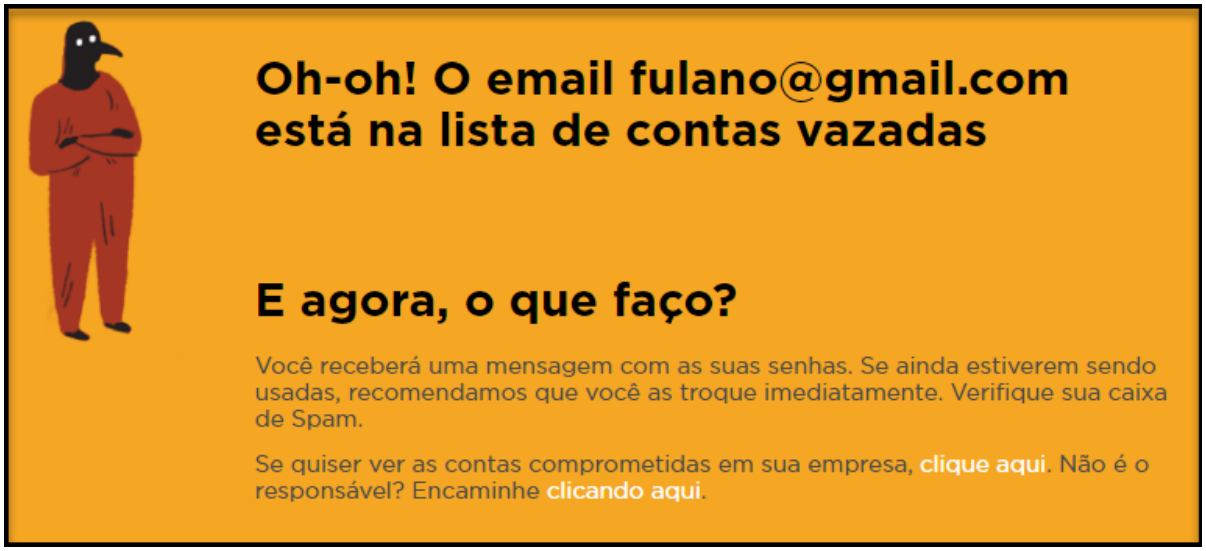
Fonte: Autoria própria. Disponível em: <https://minhasenha.com>. Acesso em: 12 set. 2018.

No portal “minhasenha.com”, permite verificar se o e-mail foi comprometimento em algum vazamento de dados, o serviço é grátis. A empresa por trás deste serviço é uma empresa brasileira chamada Axur.

Nesta verificação de e-mail são enviadas apenas as senhas que estiverem associadas ao próprio e-mail. A principal especialidade da Axur é o monitoramento de riscos digitais. Atualmente, este site conta com uma base de 1,4 bilhões de senhas vazadas até 13/12/2017.

A Figura 38, apresenta a verificação do e-mail “fulano@gmail.com”, mostrando que houve violações, pois consta na lista de contas vazadas e orienta para trocar senha imediatamente.

Figura 38 - MinhaSenha - verificando e-mail



Fonte: Autoria própria. Disponível em: <https://minhasenha.com>. Acesso em: 12 set. 2018.

Na Figura 39, é mostrado a quantidade em que houve vazamento de senhas pela “minhasenha.com”.

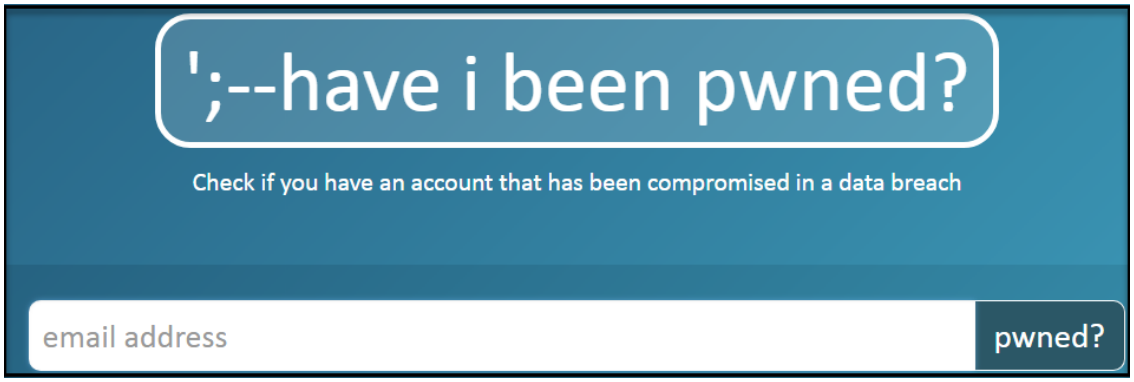
Figura 39 - MinhaSenha - vazamento de senhas

Fonte: Autoira própria. Disponível em: <https://minhasenha.com>. Acesso em: 12 set. 2018.

4.4.2 Hibp

O HIBP (*Have I been pwned*), apresentado na Figura 40, cujo significado pode ser traduzido como “Eu fui descoberto?”, “Eu tive meus dados comprometidos” ou “Eu tive meus dados vazados?”, a palavra *pwned* na tradução literal significa dominado, criado por Troy Hunt, diretor regional da Microsoft, disponibiliza no site “haveibeenpwned.com” um recurso que permite verificar se os seus dados estão em risco, isto é, foram comprometidos.

Figura 40 - HIBP



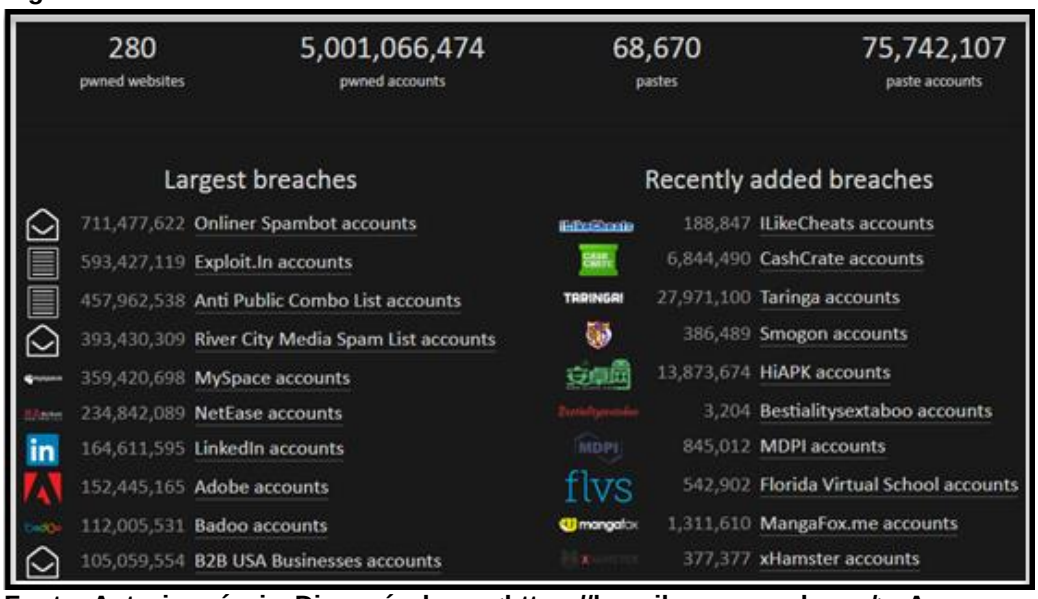
Fonte: Autoria própria. Disponível em: <https://haveibeenpwned.com>. Acesso em: 12 set. 2018.

No site “haveibeenpwned.com”, além de verificar sobre o vazamento de senhas em e-mail, também é possível verificar se alguma senha consta na lista de vazamento de dados como também obter todos os dados que foram vazados.

Ao todo são quase 5 bilhões de contas vazadas, envolvendo vazamento de diversos sites como: LinkedIn, Badoo, MySpace e Adobe.

A Figura 41, mostra os serviços em que houve grande vazamento de senhas ao lado esquerdo e que foram recentemente adicionados ao lado direito.

Figura 41 - HIBP: vazamento de senhas



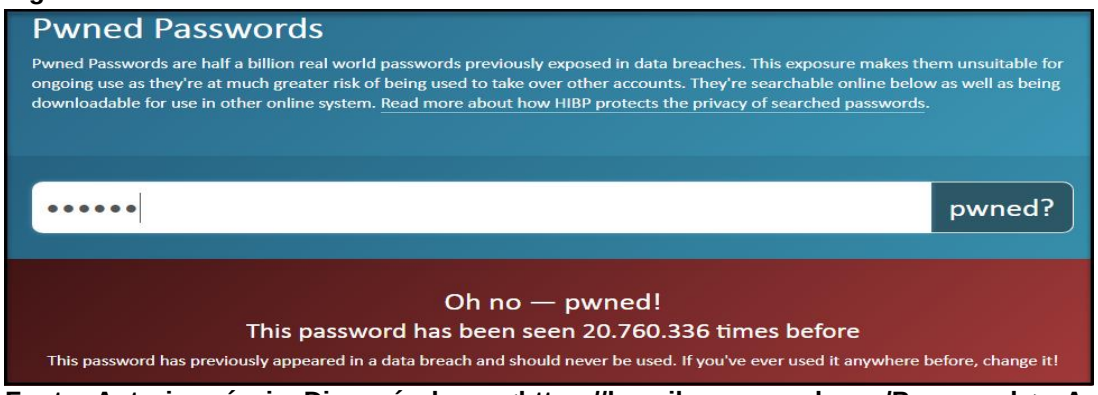
Fonte: Autoria própria. Disponível em: <https://haveibeenpwned.com/>. Acesso em: 12 set. 2018.

Esta base também pode ser integrada a outros sistemas para utilizá-lo como forma de verificação se alguma senha consta na lista de dados vazados.

Na Figura 42, é apresentada a tela em que é possível verificar se uma determinada senha foi comprometida, isto é, consta nos dados vazados, basta digitar

a senha no campo *password* (senha) e clicar em *pwned* (descoberto). No exemplo foi digitado 123456 e retornou que foi visto mais de 20 milhões de vezes.

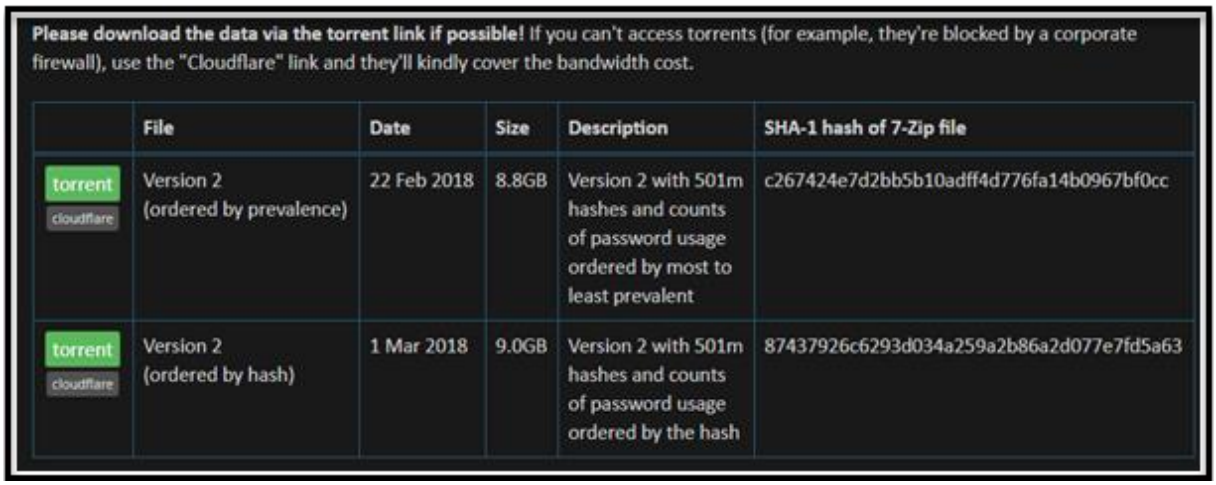
Figura 42 - HIBP: verificando senha



Fonte: Autoria própria. Disponível em: <https://haveibeenpwned.com/Passwords>. Acesso em: 12 set. 2018.

Na Figura 43, é apresentada a localização de como obter todos os dados que foram vazados, são em torno 9 Gigabytes compactados no formato 7z[1] até março de 2018.

Figura 43 - Base de senhas vazadas até março de 2018



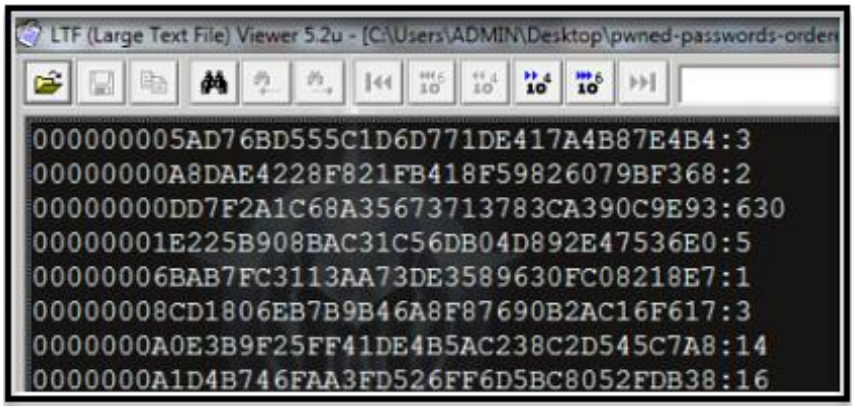
Fonte: Autoria própria. Disponível em: <https://haveibeenpwned.com/Passwords>. Acesso em: 12 set. 2018.

Os dados, ainda na Figura 43, correspondem a 30 Gigabytes descompactados, no entanto, para não expor estes dados sensíveis, isto é, que contém informações de senhas reais de pessoas, todos estão criptografados com SHA-1.

[1] 7z é um tipo de arquivo compactado de especificação de código aberto e padrões de codificação de dados utilizando para reduzir o tamanho de um determinado arquivo para que se possa compartilhar com mais facilidade e menor tempo (PAVLOV, 2016).

Na Figura 44, é apresentado um pequeno fragmento do arquivo, que foi aberto utilizando um editor de texto especial chamado *Large File Text*, que permite abrir enormes arquivos de texto, cada linha corresponde a uma senha em SHA-1 e ao final o número vezes que a senha aparece em uma violação de dados.

Figura 44 - Hashes de senhas vazadas



Fonte: Autoria própria. Disponível em: <https://haveibeenpwned.com/>. Acesso em: 12 set. 2018.

4.5 EXEMPLO DE CRIAÇÕES DE SENHAS

A lista de 30 senhas, apresentadas no Quadro 75, foram criadas utilizando o gerador de senhas RoboForm, como exemplo, de criação de senhas mais seguras geradas de forma randômica contendo 12 caracteres, letras maiúsculas, letras minúsculas, números e caracteres especiais.

Quadro 75 - Exemplo de senhas

Exemplo	Senha	Exemplo	Senha
1	bdW!8u@HHr2%	16	zoD#54otUTCf
2	7i@N%xiWWGce	17	7L^jUsGNxhco
3	YvzUC6H!@XJZ	18	7!%8GW@cQ!4G
4	#^ogtXu7xExX	19	H$BUKt##6sR8
5	WFv%!NcBXst4	20	#f5XBRWgd#Ex
6	jP!x3k@YsS65	21	cS5Pg88#dF92
7	P!%SU4u!6kTV	22	i^xcK2%7b%Re
8	aU%a#5zr7xGo	23	57bh$ASHBGAd
9	eWJYh^t5%CVX	24	%@8VMmApJ8
10	Kq#9i7ruDrfi	25	fa5q$dZAA6rJ
11	cDp34L3!35Mb	26	x@Bc!Cu5gt@g
12	og3oH5moX#8e	27	3hGvrq3Au$qr
13	z^6x^kERaZ2#	28	uBtCfY5ZwLB!
14	3EC%w6zAJLUT	29	^$edm8Ht@9Dn
15	Ns^s@Y6tJBsN	30	x76!%mya#bT!

Fonte: Autoria própria. Geradas em: <https://www.roboform.com/br/password-generator>. Acesso em: 12 set. 2018.

O RoboForm, apresentado na Figura 45, é um gerenciador de senhas que disponibiliza gratuitamente o gerador de senhas através do seguinte link: “https://www.roboform.com/br/password-generator”.

Figura 45 - Gerador de senhas RoboForm

Fonte: Autoria própria. Disponível em: <https://www.roboform.com/br/password-generator>. Acesso em: 12 set. 2018.

5 CONSIDERAÇÕES FINAIS

No desenvolvimento deste trabalho, foi observado a importância de apresentar como é possível realizar um cálculo de força para senhas, como obter um tempo de processamento estimado para a criptoanálise e como as pessoas descuidam e utilizam a mesma senha para os mais diversos serviços. Espera-se que este trabalho possa ajudar as pessoas a tomarem consciência de elaborar senhas mais eficientes e principalmente como gerenciá-las.

Foi constatado que uma senha composta de números, letras minúsculas e maiúsculas, caracteres imprimíveis, com tamanho mínimo de 12 caracteres e gerada de forma randômica aumenta consideravelmente a segurança da senha.

Os limitantes desta pesquisa foram a falta de tempo para realizar as simulações em máquinas com diferentes arquiteturas e núcleos, bem como carecer de uma supermáquina composta de 5 servidores com 25 GPUs no total, pois este tipo de equipamento, não foi possível simular a criptoanálise de senhas mais robustas. As dificuldades encontradas foram: procurar informações para coletar as senhas vazadas, obter o conhecimento para analisar a força das senhas e como estimar o tempo de processamento da criptoanálise.

A continuação deste trabalho seria realizar simulações de criptoanálise com base no processamento de dados e comparar o tempo que foi obtido pelos cálculos de entropia.

Por fim, o pesquisador observou a importância de realizar uma auditoria em todas suas senhas criadas até o momento, utilizar uma ferramenta para gerenciá-las e orientar outras pessoas sempre que possível sobre o quão importante este assunto se trata.

5.1 TRABALHOS FUTUROS

Com base no estudo do referencial teórico, este trabalho se restringiu a analisar o conjunto de caracteres, a entropia, o comprimento e o tempo de processamento estimado:

- De uma base de dados do serviço do Instagram vazadas em 2017;
- Das senhas mais utilizadas de 2017 segundo a SplashData.

Os pontos que podem ser analisados futuramente são:

- Análise de uma base de dados maior dos principais meios de serviços utilizados em 2018 como o Facebook e o Linkedin;
- As senhas mais utilizadas em 2018 e quais as novidades, ou seja, quais senhas entraram de novo na lista de 2018 e as influências externas que podem estar relacionadas com esta nova lista;
- Realizar simulações de criptoanálise comparando com o cálculo obtido pela entropia;
- Realizar entrevistas que levam as pessoas em geral a continuarem utilizando senhas fracas e os motivos pelas quais continuam.

REFERÊNCIAS

ABNT. **NBR ISO/IEC 27002: tecnologia da informação - técnicas de segurança - código de prática para a gestão da segurança da informação**. Rio de Janeiro: Associação Brasileira de Normas Técnicas (ABNT), 2005. 140 p.

CERT.BR. **Contas e senhas**. Cartilha de segurança para internet, versão 4.0 / cert.br. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br). São Paulo: Comitê Gestor da Internet no Brasil, 2012. Disponível em: <https://cartilha.cert.br/senhas/>. Acesso em: 25 mar. 2018.

COELHO, F. E. S.; ARAÚJO, L. G. S.; BEZERRA, E. K. **Gestão da segurança da informação NBR 27001 e NBR 27002**. Rio de Janeiro: Escola Superior de Redes, 2014. 220 p.

FONSECA, G. **Auditoria de sistemas de informação: conheça mais sobre o assunto**. Profissionais TI, publicado em: 19 abr. 2012. Disponível em: <https://www.profissionaisti.com.br/2012/04/auditoria-de-sistemas-de-informacao-conheca-mais-sobre-o-assunto/>. Acesso em: 10 set. 2018.

GOODIN, D. **25-GPU cluster cracks every standard windows password in < 6 hours**. Copyright by art Tecnica, publicado em: 12 set. 2012. Disponível em: <https://arstechnica.com/information-technology/2012/12/25-gpu-cluster-cracks-every-standard-windows-password-in-6-hours/>. Acesso em: 26 de abril de 2018.

HAZZAN, S. **Fundamentos de matemática elementar volume 5: combinatória e probabilidade**. 3. ed. São Paulo: Atual Editora, 1977. 149 p.

HENDERSON, A. **The CIA triad: confidentiality, integrity, availability**. Copyright by Panmore Institute, alterado em: 25 mar. 2017. Disponível em: <http://panmore.com/the-cia-triad-confidentiality-integrity-availability>. Acesso em: 10 set. 2018.

IEZZI, G.; DOLCE, O.; MURAKAMI, C. **Fundamentos de matemática elementar volume 2: logaritmos**. 9. ed. São Paulo: Atual Editora, 2004. 198 p.

JARGAS, A. M. **Livro expressões regulares - uma abordagem divertida**. 3. ed. São Paulo: Novatec, 2009. 208 p.

JARGAS, A. M. **Livro expressões regulares - uma abordagem divertida**. 4. ed. São Paulo: Novatec, 2012. 224 p.

KISSELL, J. **Aprendendo a proteger suas senhas**. Tradução: BrodTec. 1. ed. São Paulo: Novatec, 2017. 176 p.

KLOPPER, P. **Comparativo: saiba qual é o gerenciador de senhas que mais se adequa às suas prioridades**. Copyright© MacMagazine, publicado em: 11/07/2016. Disponível em: <https://macmagazine.com.br/2016/07/11/comparativo-saiba-qual-e-o-gerenciador-de-senhas-que-mais-se-adequa-as-suas-prioridades/>. Acesso em: 12 set. 2018.

MITNICK, K. D.; SIMON, W. L. **A arte de enganar**. São Paulo: Pearson, 2003. 286 p.

MITNICK, K. D.; SIMON, W. L. **A arte de invadir**. São Paulo: Pearson, 2005. 245 p.

PINTO, P. **Criptografia simétrica e assimétrica. Sabe a diferença?** Copyright by pplware, publicado em: 07 dez. 2010. Disponível em: <https://pplware.sapo.pt/tutoriais/networking/criptografia-simetrica-e-assimetrica-sabe-a-diferenca/>. Acesso em: 10 set. 2018.

PRODANOV, C. C.; FREITAS, E. C. D. **Metodologia do trabalho científico: métodos e técnicas da pesquisa e do trabalho acadêmico**. 2. ed. Rio Grande do Sul: Universiade Freevale, 2013. 277 p.

QUARESMA, P.; PINHO, A. **Criptoanálise**. Gazeta de Matemática # 157, p. 22-31. Portugal: Universidade de Coimbra, 2009.

RFC20. **ASCII format for network interchange**. Publicado em: 16 out. 1969. Disponível em: <http://www.faqs.org/rfcs/rfc20.html>. Acesso em: 10 set. 2018.

RIBEIRO, D. F.; LOURENÇANO, P. G. P.; COSTA, A. D. **Criptografia: uma aplicação da matemática discreta através da implementação da cifra de César em visualg**. Interface Tecnológica, v. 10, n. 1, p. 17-26, 2013. São Paulo: Interface Tecnológica, 2013.

ROCHA, A. T. Q.; COSTA, B. N. L.; GIUZEPPE, K. V. L.; MARTINS, G. H. P. **Pentest para quebra de criptografia wireless**. Caderno de Estudos Tecnológicos, v. 4, n. 1, 2016. São Paulo: Faculdade de Tecnologia de Bauru, 2016.

SCHARDONG. F.; ÁVILA. R. B. **Interface de apoio para ataques de força bruta com o GPU MD5 crack**. In: Sessão de Iniciação Científica. ANAIS da 12ª Escola Regional de Alto Desempenho: ERAD 2012, 20 à 23 de Março de 2012, Erechim, RS. Rio Grande do Sul: Universidade do Vale do Rio dos Sinos, 2012.

SONDRÉ, U. **Elementos de matemática: funções exponenciais e logarítmicas**. Versão compilada. Londrina: Departamento de Matemática, 2007. 25 p.

STALLINGS, W. **Criptografia e segurança de redes: princípios e práticas**. Tradução: Daniel Vieira. 6. ed. São Paulo: Pearson Education do Brasil, 2015. 578 p.

SUGAI, A. **O que é o código ASCII e para que serve? Descubra**. Copyright by techtudo, atualizado em: 15 fev. 2015. Disponível em: <https://www.techtudo.com.br/noticias/noticia/2015/02/o-que-e-o-codigo-ascii-e-para-que-serve-descubra.html>. Acesso em: 10 set. 2018.

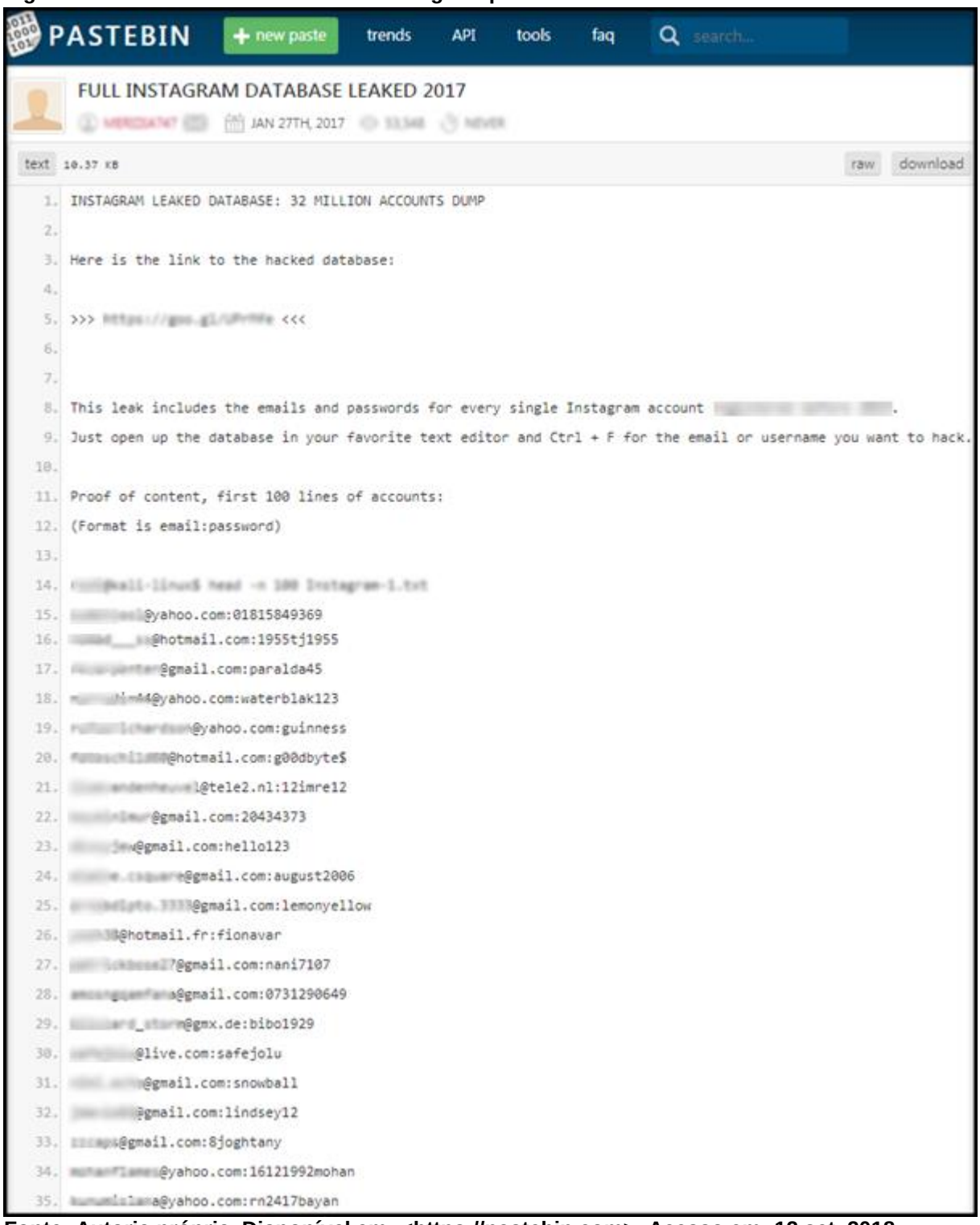
SUMARES, G. **Clock, cache e núcleos: saiba como eles afetam o desempenho do processador**. Copyright by Olha Digital, publicado em: 10 fev. 2017. Disponível em: <https://olhardigital.com.br/noticia/clock-cache-e-nucleos-saiba-como-eles-afetam-o-desempenho-do-processador/66010/>. Acesso em: 10 set. 2018.

TANENBAUM, A. S.; WETHERALL, D. **Redes de computadores**. Tradução: Daniel Vieira. 5. ed. São Paulo: Pearson Prentice-Hall, 2011. 600 p.

VASCONCELOS, L. **Hardware total**. 1. ed. São Paulo: Makron Books, 2012. 2117 p.

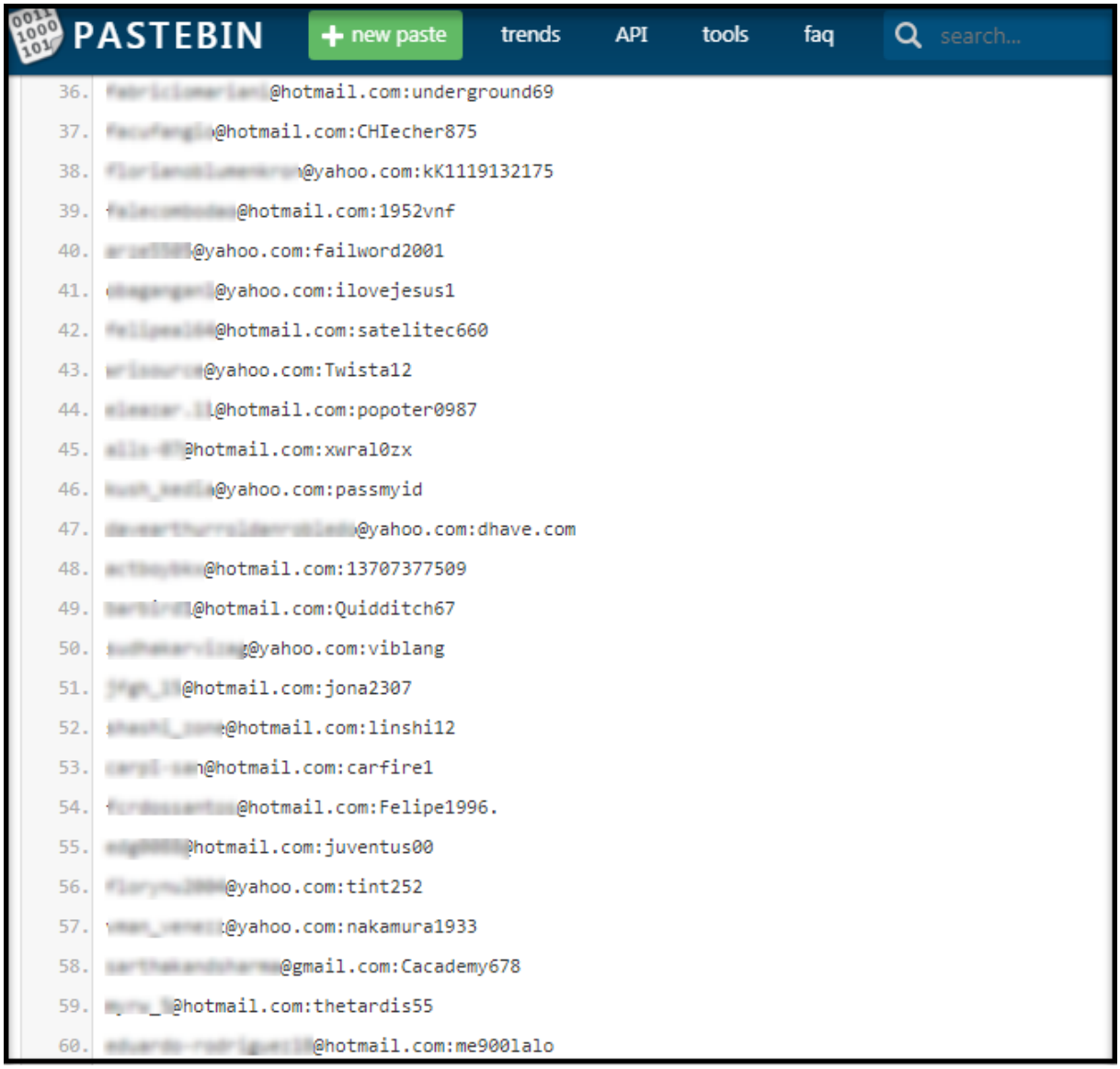
APÊNDICE A - VAZAMENTO DE SENHAS DO INSTAGRAM

Figura 46 - Vazamento de senhas do Instagram parte 1 de 4



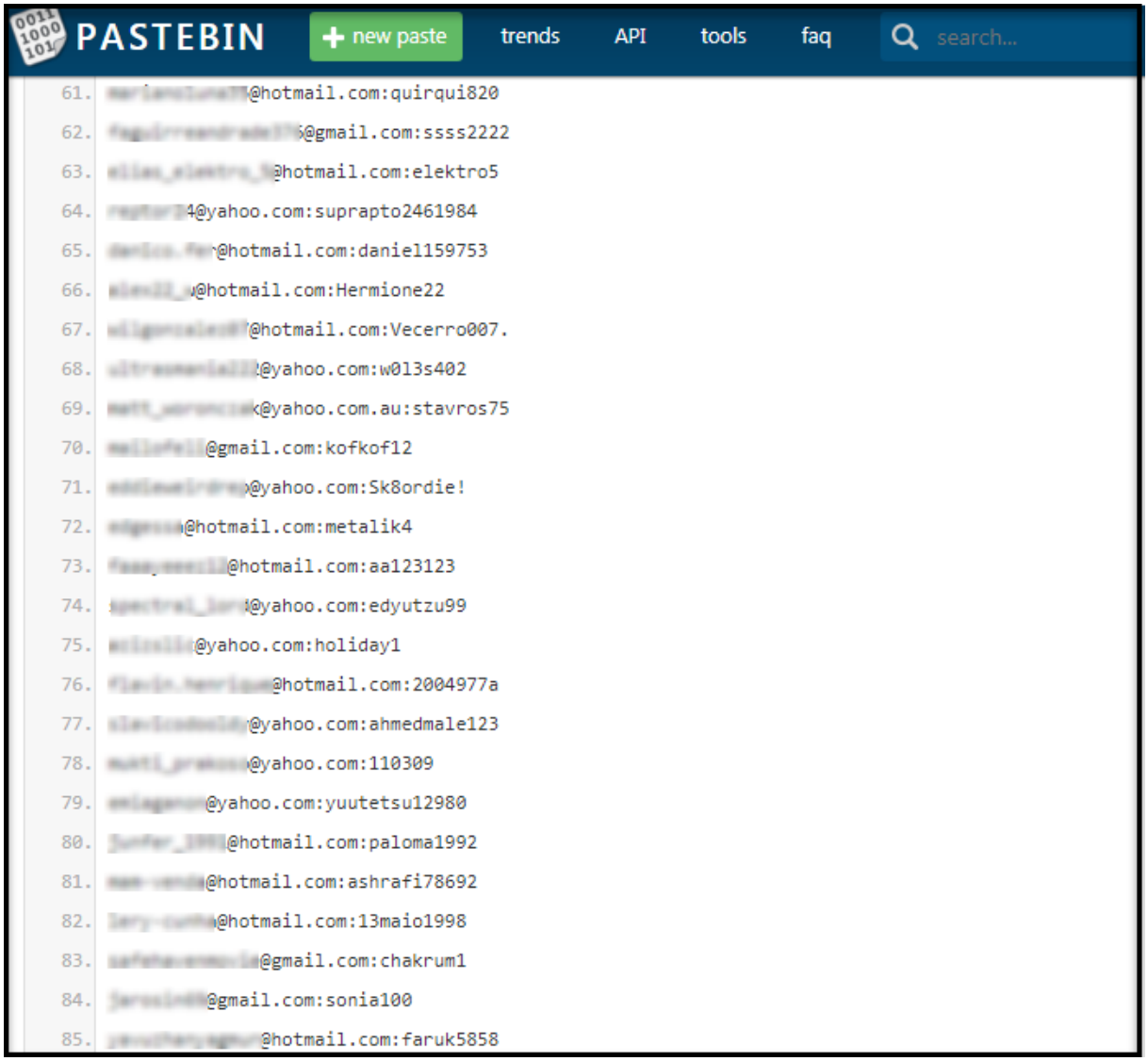
Fonte: Autoria própria. Disponível em: <https://pastebin.com>. Acesso em: 12 set. 2018.

Figura 47 - Vazamento de senhas do Instagram parte 2 de 4



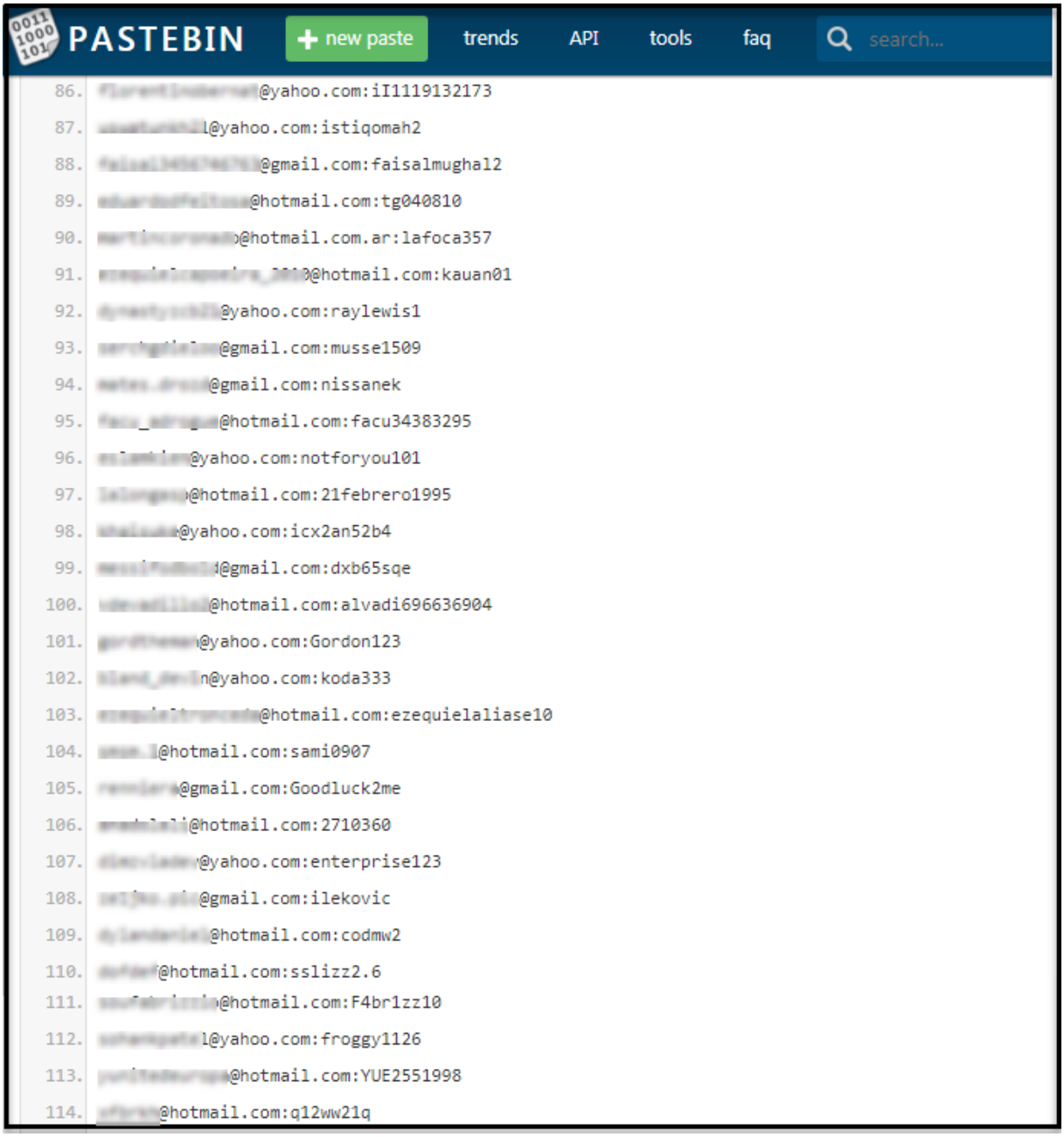
Fonte: Autoria própria. Disponível em: <https://pastebin.com>. Acesso em: 12 set. 2018.

Figura 48 - Vazamento de senhas do Instagram parte 3 de 4



Fonte: Autoria própria. Disponível em: <https://pastebin.com>. Acesso em: 12 set. 2018.

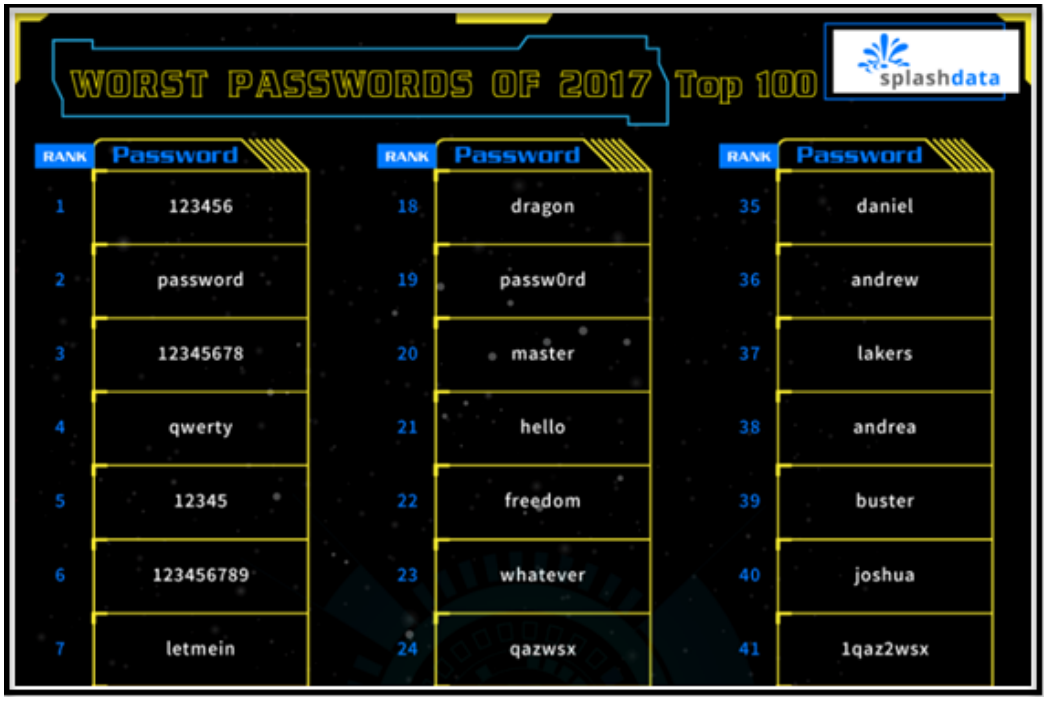
Figura 49 - Vazamento de senhas do Instagram parte 4 de 4



Fonte: Autoria própria. Disponível em: <https://pastebin.com>. Acesso em: 12 set. 2018.

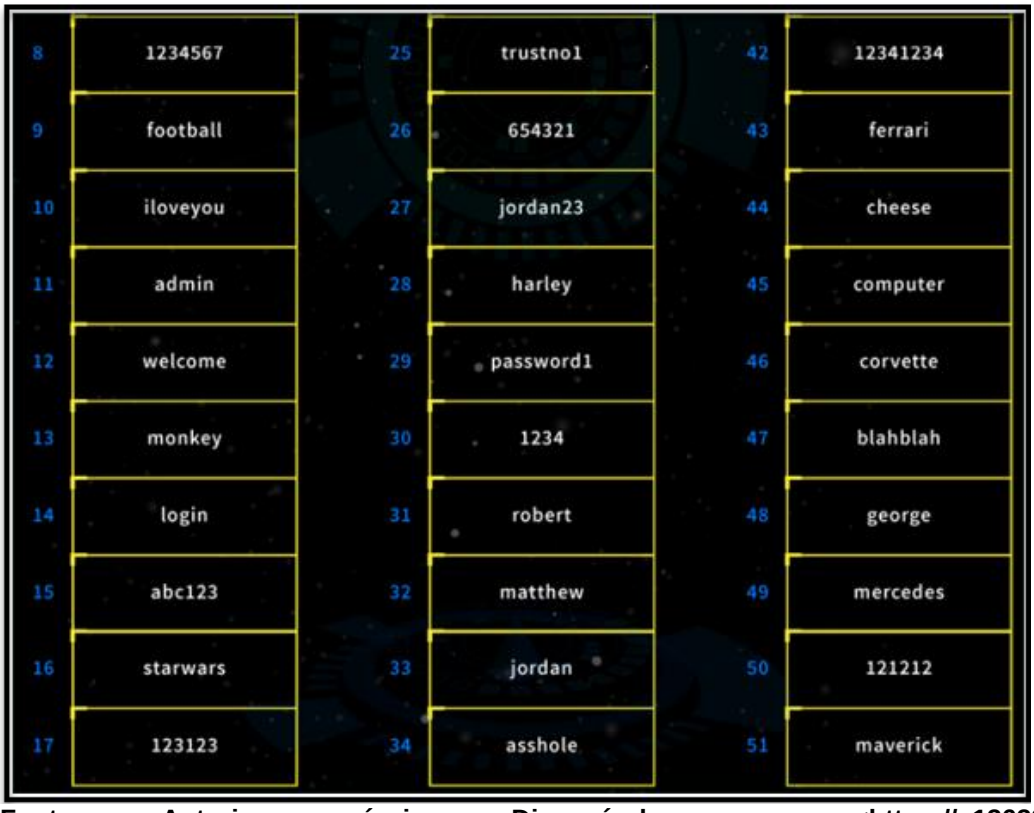
APÊNDICE B - SENHAS MAIS UTILIZADAS EM 2017

Figura 50 - Senhas mais utilizadas em 2017, parte 1 de 4



Fonte: Autoria própria. Disponível em: <https://s13639.pcdn.co/wp-content/uploads/2017/12/Top-100-Worst-Passwords-of-2017a.pdf>. Acesso em: 12 set. 2018.

Figura 51 - Senhas mais utilizadas em 2017, parte 2 de 4



Fonte: Autoria própria. Disponível em: <https://s13639.pcdn.co/wp-content/uploads/2017/12/Top-100-Worst-Passwords-of-2017a.pdf>. Acesso em: 12 set. 2018.

Figura 52 - Senhas mais utilizadas em 2017, parte 3 de 4

RANK	Password	RANK	Password	RANK	Password
52	fuckyou	69	ashley	86	william
53	nicole	70	bandit	87	soccer
54	hunter	71	killer	88	london
55	sunshine	72	aaaaaa	89	1q2w3e
56	tigger	73	pepper	90	1992
57	1989	74	jessica	91	biteme
58	merlin	75	zaq1zaq1	92	maggie
59	ranger	76	jennifer	93	querty

Fonte: Autoria própria. Disponível em: <https://s13639.pcdn.co/wp-content/uploads/2017/12/Top-100-Worst-Passwords-of-2017a.pdf>. Acesso em: 12 set. 2018.

Figura 53 - Senhas mais utilizadas em 2017, parte 4 de 4

60	solo	77	test	94	rangers
61	banana	78	hockey	95	charlie
62	chelsea	79	dallas	96	martin
63	summer	80	passwor	97	ginger
64	1990	81	michelle	98	golfer
65	1991	82	admin123	99	yankees
66	phoenix	83	pussy	100	thunder
67	amanda	84	pass		
68	cookie	85	asdf		

Fonte: Autoria própria. Disponível em: <https://s13639.pcdn.co/wp-content/uploads/2017/12/Top-100-Worst-Passwords-of-2017a.pdf>. Acesso em: 12 set. 2018.