



1



2



FIAP

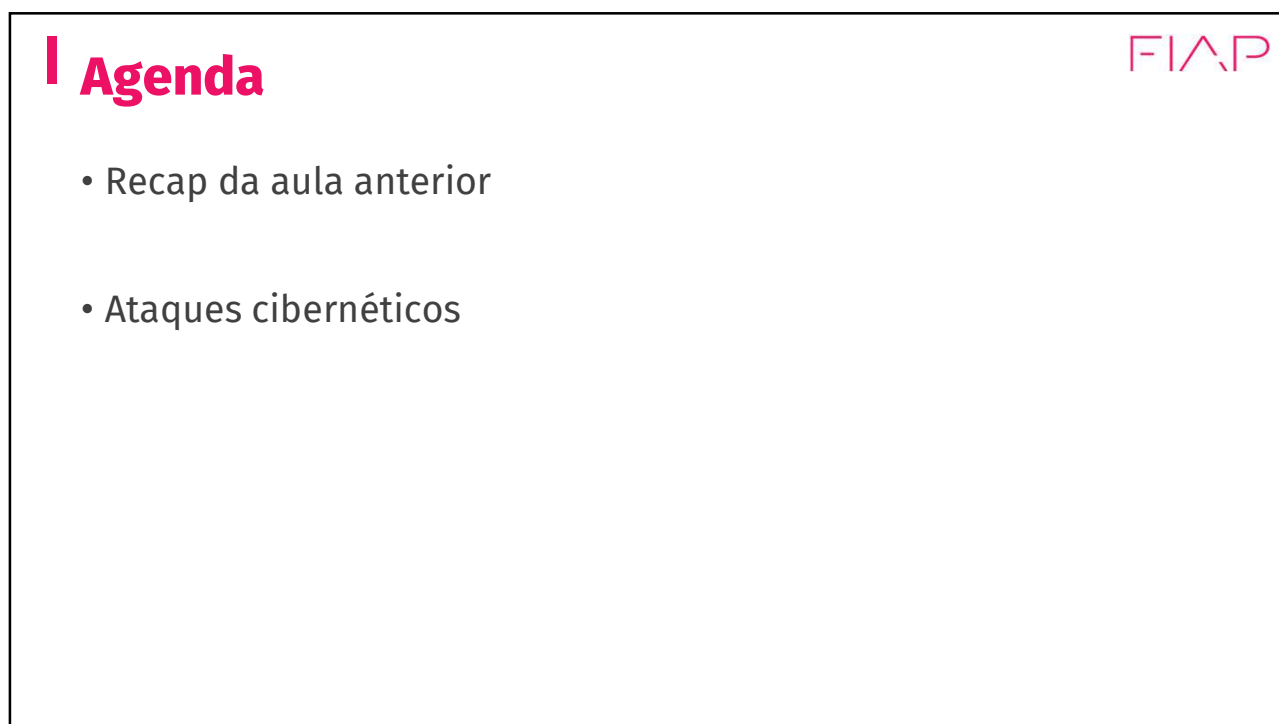
FIAP GRADUAÇÃO

Cognitive Cybersecurity

Prof. Leonardo Orabona
E-mail: profleonardo.orabona@fiap.com.br

Prof. Dr. Noris Junior
E-mail: profnoris.junior@fiap.com.br

3



I Agenda

- Recap da aula anterior
- Ataques cibernéticos

4



AMEAÇAS E ATAQUES

5

I Ameaças digitais

- Uma vez conectados, todos estão sujeitos a ameaças digitais
- Quem já foi alvo de ataque?
- Quem já recebeu um conteúdo falso em meio digital?

6

Ataques

FIAP



Brasil é vice-campeão em ataques cibernéticos, com 1.379 golpes por minuto, aponta estudo

Especialista orienta que além de tecnologia, usuários devem investir em capacitação

João Nakamura, da CNN, em São Paulo
30/10/2024 às 08:15

Brasil é 2º maior alvo mundial de ciberataques, revela estudo
País supera 439 mil ataques em 2021 e fica atrás apenas dos Estados Unidos em ranking feito por empresa de cibersegurança

Olhar Digital > Segurança e Privacidade > Hacker vende maior lista de senhas roubadas da história

SEGURANÇA E PRIVACIDADE

Hacker vende maior lista de senhas roubadas da história

Arquivo chamado "RockYou2024" é o maior pacote de senhas comprometidas já visto até aqui, afirma página de segurança cibernética

Gabriel Sêrvio | 12/07/2024 12h51



7

Ataques

FIAP

exame.

Home > Tecnologia

Brasil segue como país mais atacado por hackers na América Latina, diz Kaspersky

Mesmo com queda de 26% em comparação a 2023, o país registrou mais de 487 mil detecções de ataques em um ano

Política

Incidentes cibernéticos em sistemas do governo dobram no primeiro semestre de 2024

Órgão do governo federal registrou 4,4 mil incidentes até junho; no mesmo período do ano passado foram 2 mil

8

I Vazamento de dados

FIAP

Banco Neon confirma vazamento de dados, mas nega 30 milhões de clientes afetados

Informações foram publicadas em um fórum cibercriminoso, de acordo com um site especializado

Banco Central comunica vazamento de dados de 150 cadastros feitos na Shopee

Segundo o BC, dados vazados não incluem informações sensíveis dos usuários. Vazamento ocorreu por 'falha pontual' em sistemas da plataforma.

Por **Thiago Resende**, TV Globo — Brasília
19/09/2024 19h37 - Atualizado há 5 meses

Clientes do Neon têm dados vazados, e banco alerta para tentativas de golpes

Instituição enviou comunicado a seus clientes nesta quarta-feira (12) e garantiu que a segurança das contas foi preservada. Ao g1, banco diz que adotou as medidas para cessar acessos indevidos e que vai realizar uma avaliação do cenário.

Por **Redação g1** — São Paulo
12/02/2025 18h20 - Atualizado há 4 semanas

9

I Outros ataques

FIAP

Após ataque hacker, Renner nega que pagou US\$ 20 milhões aos criminosos

A extorsão inicial dos hackers visava a quantia de 1 bilhão de reais em criptomoedas para restabelecer os sistemas da empresa

10

I Atacantes

FIAP

Grupo de hackers 'Anonymous' declara 'guerra cibernética' à Rússia



O grupo hacker Anonymous disse ter invadido os canais de TV russos *Russia 24*, *Channel 1* e *Moscow 24*, e os serviços de *streaming* Wink e Ivi. No lugar da programação regular, vídeos da Ucrânia e mensagens antiguerra foram exibidos.

“O coletivo de hacker Anonymous hoje invadiu os serviços de streaming russos Wink e Ivi (como Netflix) e canais de TV ao vivo ‘Russia 24’, ‘Channel 1’ e ‘Moscow 24’ para transmitir imagens de guerra da Ucrânia”, escreveu no [Twitter](#) na noite de domingo (6.mar.2022).

O Anonymous, um grupo de hackers, declarou uma “guerra cibernética” contra o governo do presidente russo, Vladimir Putin. O objetivo do coletivo, segundo a mídia internacional, é desativar vários sites do governo russo. A RT.com, uma rede de televisão internacional controlada pelo Estado russo, também foi alvo da quadrilha.

11

I Atacantes

FIAP

MOSCOU

Grupo de hackers Anonymous reivindica ciberataque contra imprensa russa

12



MALWARE

13

Malware

O que é um vírus de computador?

Há muitas informações (inclusive erradas) circulando online sobre o termo “vírus”, então vamos esclarecer e definir de uma vez por todas o vírus de computador: **ele é um programa ou parte de um código malicioso capaz de se autorreplicar que se infiltra no seu dispositivo sem o seu conhecimento ou permissão.**



Vírus de computador

Origem: Wikipédia, a enciclopédia livre.

Em **informática**, um **vírus de computador** é um **software** malicioso que é desenvolvido por programadores geralmente inescrupulosos. Tal como um **vírus biológico**, o programa infecta o sistema, faz cópias de si e tenta se espalhar para outros computadores e dispositivos de informática.



MALWARE 101: WHAT IS A VIRUS?

Escrito por um funcionário da NortonLifeLock

Um vírus de computador, assim como um vírus da gripe, tem a habilidade de se replicar e foi desenvolvido para se propagar de um host para outro. Da mesma forma como os vírus não se reproduzem sem uma célula hospedeira, os vírus de computador também não se reproduzem ou se propagam sem programação, como um arquivo ou documento.

14

I Malware

FIAP

- Malware, derivado de "malicious software" é um tipo de software que pode causar danos em dispositivos, roubar dados e causar o caos em sistemas digitais
- Leitura para casa:
 - Definição de malware da Microsoft:
 - <https://www.microsoft.com/pt-br/security/business/security-101/what-is-malware>

15

I Softwares anti-malware (antivirus)

FIAP

- Nome atual: endpoint protection
- Conjunto de softwares integrados ao sistema operacional
 - Essa integração impede (ou tenta dificultar ao máximo) o acesso do malware aos recursos do núcleo do sistema
- Por onde chegam os malwares?

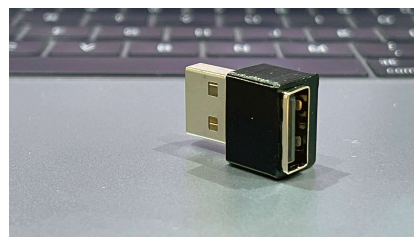
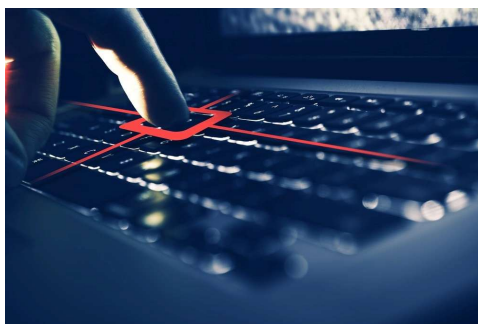
16

I Keylogger

FIAP

O principal objetivo de um keylogger é **interceptar** todas as informações que são digitadas pelo usuário no PC. Assim, quando o usuário tecla senhas ou dados bancários, por exemplo, essas informações são enviadas diretamente para o responsável pela distribuição desse tipo de programa.

Os dados do usuário, como logins e e-mails, são cruzados com as senhas digitadas e o resultado é o acesso direto às suas informações. Softwares antivírus e antimalwares atualizados e em execução são as maneiras mais eficientes de bloquear keyloggers.



17

I Ransomware

FIAP



Na lista dos tipos de vírus, os ransomware estão entre os **mais nocivos em circulação na atualidade**. Eles são os principais responsáveis pelas perdas financeiras em empresas atacadas.

Isso porque o que ele faz é assumir o controle de uma base de dados.

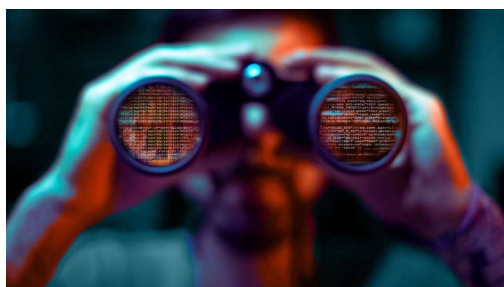
Durante a execução de um ataque de ransomware, todos os sistemas acabam sendo paralisados.

A forma de ativação é geralmente por meio de isca - um funcionário desavisado clica em um link malicioso e o estrago está feito. A melhor maneira de se prevenir contra esses ataques é instalar ferramentas de identificação de ransomwares em toda a rede.

18

I Spyware

FIAP



Os spywares têm um funcionamento bastante similar ao dos keyloggers: o objetivo aqui é **capturar informações dos usuários sem que eles saibam disso**. Porém, o que muda aqui é o modo de operação.

Os spywares modificam o conteúdo de páginas, exibindo anúncios que levem ao download de programas maliciosos.

Por essa razão, os spywares são considerados mais nocivos do que os keyloggers, uma vez que eles não apenas capturam dados pessoais como também são capazes de modificar as configurações de uma máquina remotamente. Softwares antivírus ativos impedem boa parte desses ataques, mas é necessário ter muita atenção àquilo que é baixado.

19

I Trojan

FIAP

Cavalo de Troia: são uma das ameaças mais perigosas aos usuários, **pois nem sempre é possível identificá-los**. Em termos de aparência eles são semelhantes a um software original, inclusive funcionando normalmente.

Porém, enquanto são executados, instalam em segundo plano softwares maliciosos que exploram falhas no sistema operacional. Em casos mais graves o computador se torna um "zumbi", virando um elemento de uma poderosa rede universal utilizado para atacar outras máquinas.



20

I Trojan - é coisa velha...

SEGURANÇA

Nova versão de vírus rouba senhas de centenas de programas no Windows

A variante mais avançada do malware também rouba carteiras de criptomoedas e sequencia arquivos nos PCs infectados



Por André Luiz Dias Gonçalves em 08/04/2025, 17:00



capturador de senhas para extrair credenciais de acesso de 270 aplicativos, de acordo com o relatório. Além disso, traz [recursos de ransomware](#), "sequestrando" arquivos no computador da vítima e exibindo uma página com as informações do resgate.

Como o Neptune RAT se espalha?

Segundo os pesquisadores de segurança responsáveis pela descoberta, a nova variante do malware **está sendo distribuída por meio de plataformas como GitHub, Telegram e YouTube**. Ela é oferecida para cibercriminosos iniciantes e experientes à procura de um malware pronto para ser adicionado às suas campanhas maliciosas.

O que é RAT?

Os especialistas apontam que há, ainda, uma opção paga e mais poderosa. Ela estaria sendo comercializada como um software supostamente destinado a atividades educacionais, trazendo sérios riscos para quem instala essa ferramenta acreditando se tratar de um programa legítimo.

Vale lembrar que malware é um [software malicioso](#) criado para causar danos e/ou explorar dispositivos de terceiros. Incluído nesta categoria o Neptune é um **trojan de acesso remoto (RAT, na sigla em inglês) que permite ao invasor controlar o computador infectado à distância**.

Como se proteger de malware?

Para evitar os riscos associados ao Neptune RAT e ameaças similares, os pesquisadores de segurança sugerem [baixar programas somente de fontes confiáveis](#), bem como manter o Windows e os softwares do PC atualizados. Usar antivírus e outras ferramentas de segurança e fazer backup de dados importantes também ajuda.

Outras medidas para reforçar a segurança são habilitar a [autenticação multifator](#) em serviços online e apps para dificultar o roubo de senhas, configurar firewall para bloquear conexões com domínios suspeitos e implementar políticas de controle de apps para limitar a execução do PowerShell.

<https://www.tecmundo.com.br/seguranca/403852-nova-versao-de-virus-rouba-senhas-de-centenas-de-programas-no-windows.htm>

21

I Backdoor

FIAP

- "Entrada secreta" em um sistema ou programa, criada para permitir acesso sem permissão.
- Pode ser colocada por hackers (ex.: em um software infectado) ou até por desenvolvedores (intencionalmente ou por erro), dando controle total ao invasor.
- Exemplo: Um aplicativo parece normal, mas tem um backdoor que deixa alguém roubar seus dados ou controlar seu celular.
- Perigo: É difícil de detectar e pode ser usado para espionar, instalar outros ataques (como ransomware) ou destruir o sistema.



22

I Worms

FIAP

Os worms já foram mais populares no passado, mas nem por isso deixaram de ser uma ameaça nos dias atuais. A palavra "worms" significa "Vermes" e seu modo de distribuição é bastante semelhante ao dos parasitas. Eles têm alta capacidade de se multiplicar em uma rede, mesmo que não haja intervenção humana.

Os worms são distribuídos por mensagens de spam e a partir de sites falsos. Uma vez que uma máquina fosse infectada, todos os dispositivos em contato com ela acabavam ganhando uma cópia do software malicioso. PCs de uso compartilhado estão mais susceptíveis a esse tipo de ameaça.



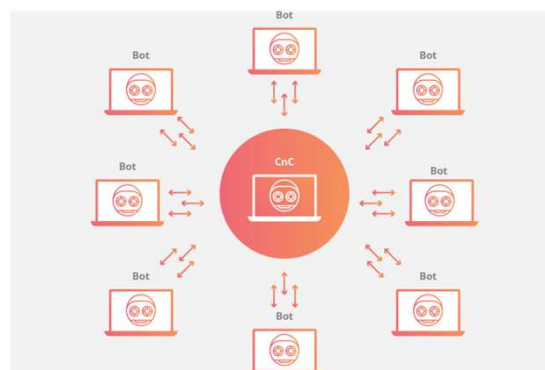
23

I Botnet

FIAP

Botnet (de bot network, ou **rede de robôs**), também conhecida como exército de zumbis, é uma rede composta por um grande número de computadores que foram infectados por malwares para atender aos comandos do hacker que a criou.

Com o controle de centenas ou mesmo milhares de computadores, as botnets são geralmente usadas para enviar spam ou vírus, roubar dados pessoais ou executar ataques de negação de serviço para um alvo (site, banco, etc). Elas são consideradas uma das maiores ameaças on-line da atualidade.



24

I Fork bomb

FIAP

- Ataque de replicação de processos no computador/servidor
- Finalidade: abrir tantos processos que o computador/servidor fica inutilizável
- Código fonte de fork bomb em diferentes linguagens (**NÃO EXECUTE NO SEU COMPUTADOR!**):
<https://github.com/aaronryank/fork-bomb>

25

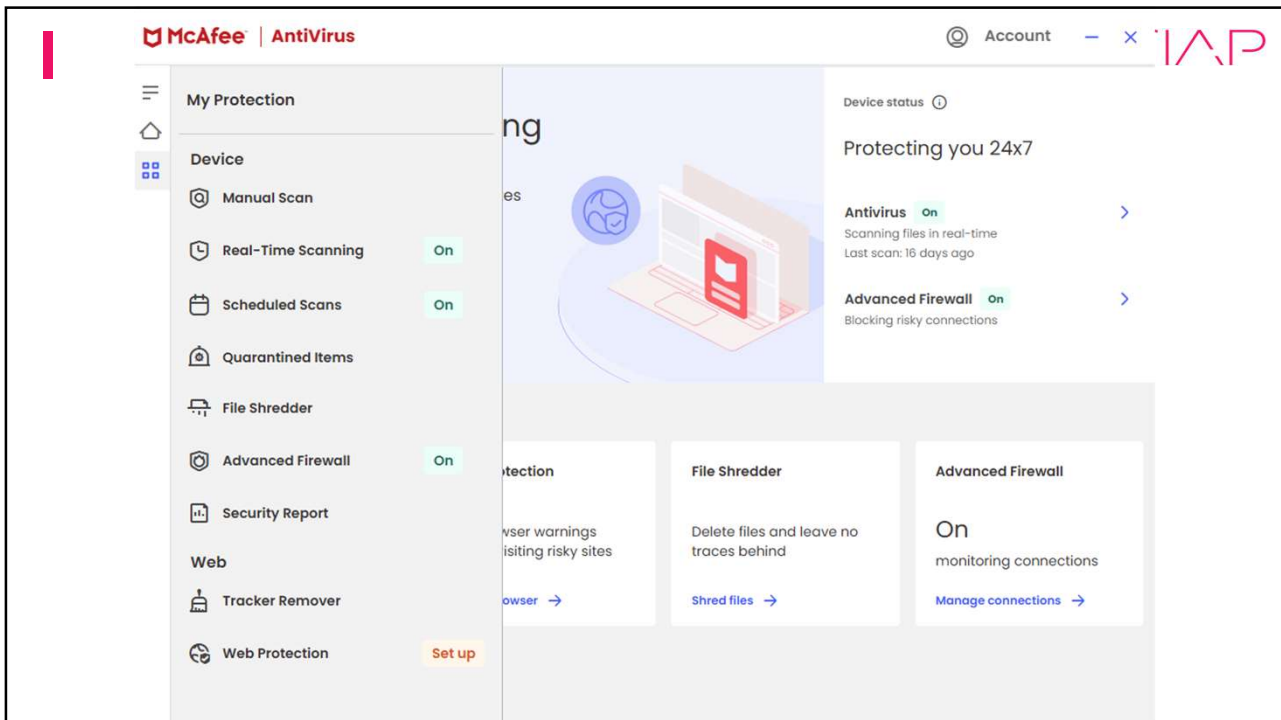
I Proteção

FIAP

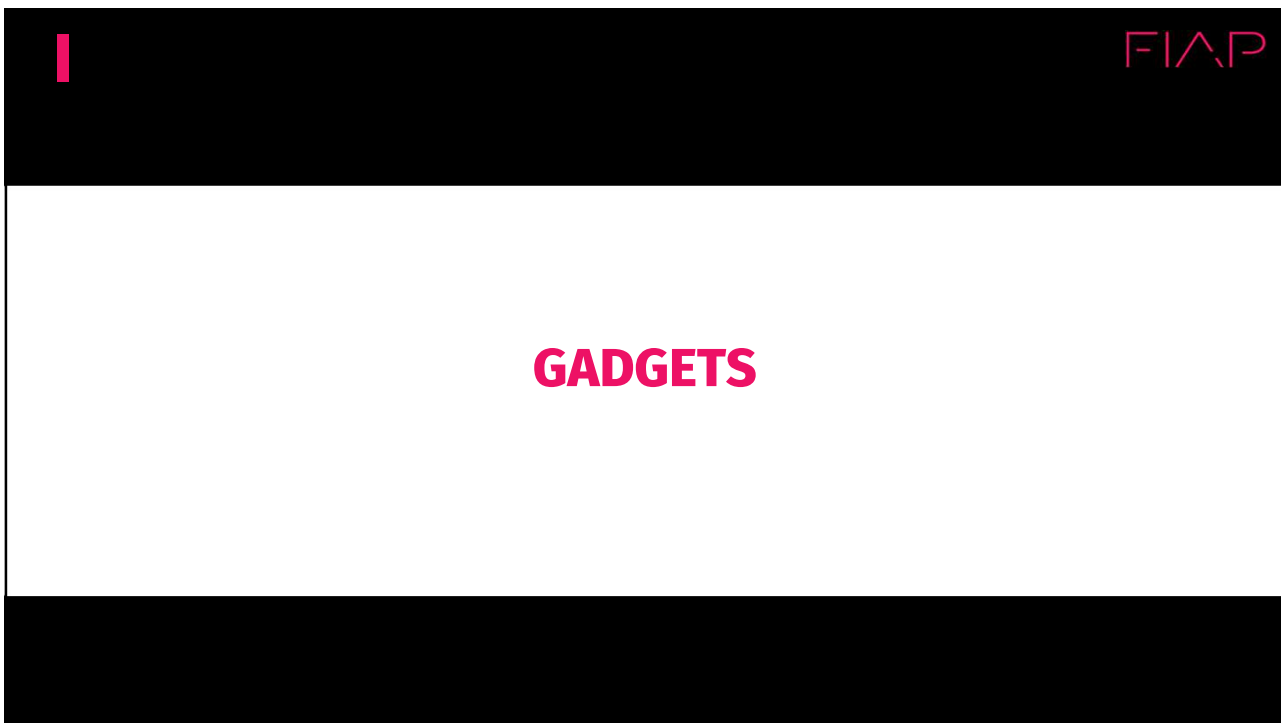
- Endpoint protection
 - O “famoso” antivírus
 - Residencial:
 - varredura de arquivos baixados da Internet, bloqueio de portas (firewall), examina cookies
 - Corporativo:
 - controla ingresso de equipamentos na rede (Network Address Control - NAC), controle de aplicações, console de gerenciamento, isolamento de dispositivo infectado, ataques de dia zero (veremos na próxima aula), detecção e resposta à incidente (EDR), prevenção à perda de dados (DLP) - ex. bloqueia um usuário de compartilhar dados/imagens para fora da empresa



26



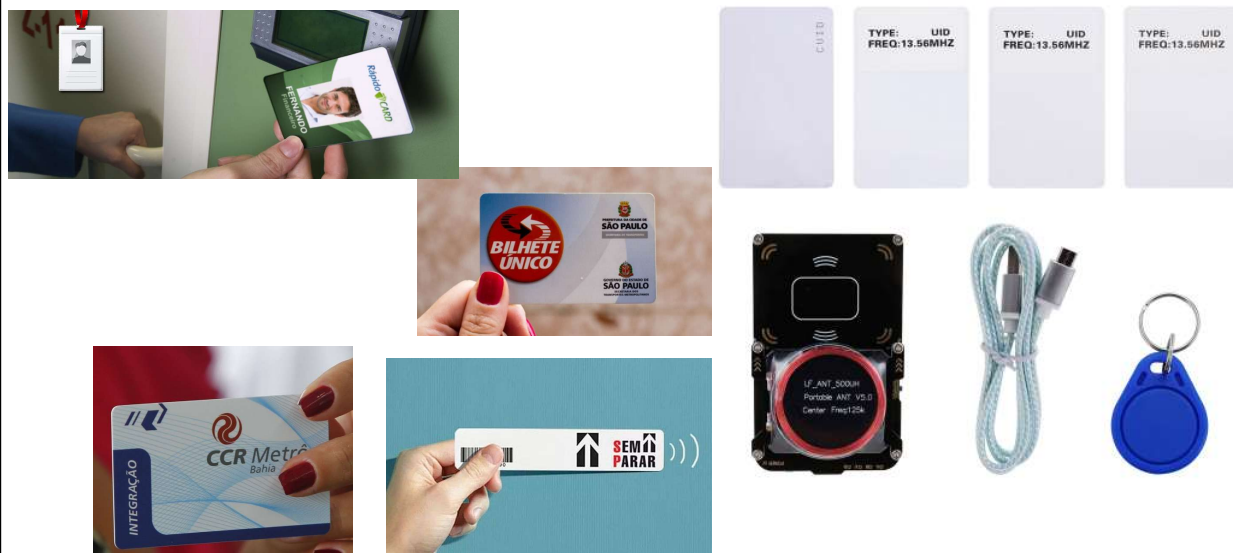
27



28

I Proxmark3

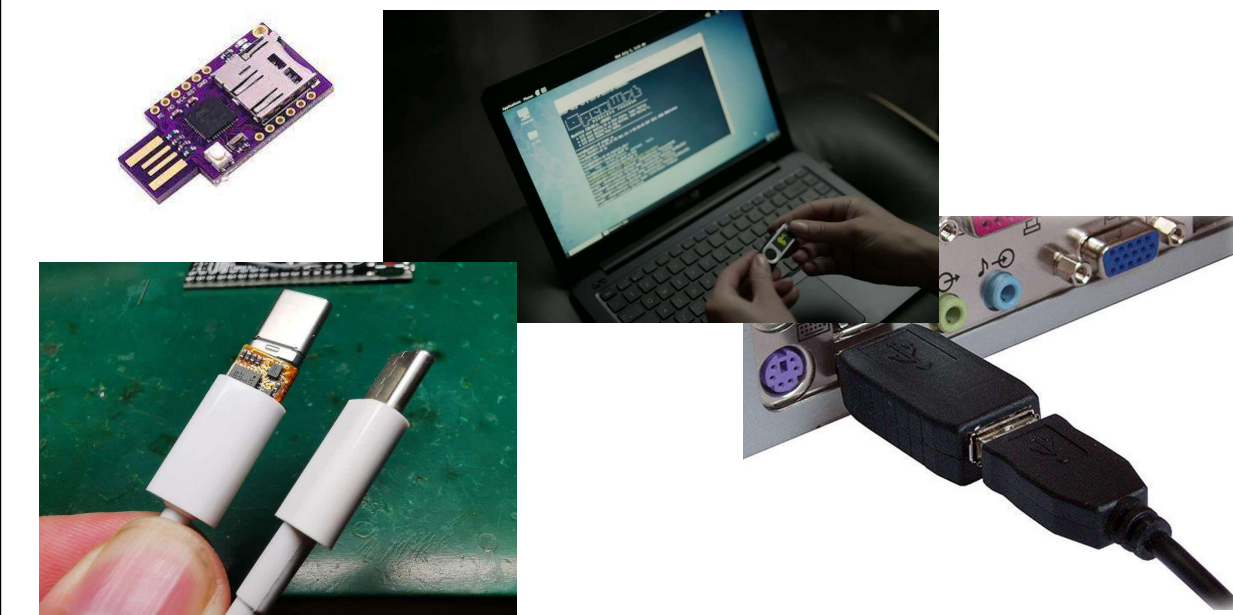
FIAP



29

I BadUSB (Rubber Ducky) e keylogger

FIAP



30

I HackRF One (1 MHz - 6 GHz)

FIAP



31

I FlipperZero

FIAP



- <https://www.youtube.com/watch?v=NsYStuMVjTE>

- 3:48 a 4:11

32



33

I

Configs

- Default
 - Vêm de fábrica
 - Importante vetor de ataque

Senhas de fábrica são as mais usadas por hackers em ataques, diz pesquisa

Segundo levantamento da F-Secure, senha "admin" é a mais usada em tentativas de ataques

Por Thiago Siqueira, para o TechTudo

08/03/2020 06h00 - Atualizado há 4 anos

f

X

34

17

I Configs

FIAP



enorme risco de segurança. Um estudo da NordPass, empresa especializada na área, mapeou as *passwords* que mais aparecem em incidentes de cibersegurança, incluindo em listas disponíveis na dark web — é possível encontrar senhas como "Mudar123" e "12345678". Nesta lista, confira as 20 senhas que não devem ser usadas online, **como criar uma senha segura** e mais.

ISACA

35

I No Brasil...

FIAP

- <https://www.youtube.com/watch?v=gmueFnCGGdY>

36



COMO SE PROTEGER?

37

I Recomendações de segurança

- 1. Não usar senhas padrão, nem senhas simples/fáceis, nem derivadas de palavras conhecidas do dicionário;
- 2. Realizar atualizações disponíveis regulares e oportunas dos sistemas em todos os dispositivos;
- 3. Ter cuidado ao abrir e-mails, ao clicar em links e anexos e principalmente se for uma mensagem inesperada de remetente desconhecido, o que não exclui o cuidado também com remetentes supostamente conhecidos;
- 4. Procurar baixar apps, programas e jogos apenas de fontes confiáveis;

38

I Recomendações de segurança

FIAP

- 5. Fazer backup (cópia de segurança) de dados importantes regularmente para se proteger contra criptografia e poder recuperar dados perdidos;
- 6. Instalar e manter atualizado programa antivírus e firewall para detectar programas mal-intencionados;
- 7. Usar contas de usuários com direitos reduzidos para que programas maliciosos não tenham direitos de administrador e, portanto, não tenham acesso a todo o sistema.

39

I

FIAP

SENHAS

40

I Senhas

FIAP

Brasil:

| | |
|----------------|------------------|
| 1. 123456 | 16. abc123 |
| 2. 123456789 | 17. q1w2e3r4t5y6 |
| 3. Brasil | 18. 101010 |
| 4. 12345 | 19. 159753 |
| 5. 102030 | 20. 123321 |
| 6. senha | 21. senha123 |
| 7. 12345678 | 22. mirantte |
| 8. 1234 | 23. flamengo |
| 9. 10203 | 24. felicidade |
| 10. 123123 | 25. qwerty |
| 11. 123 | 26. felipe |
| 12. 1234567 | 27. 121212 |
| 13. 654321 | 28. 111111 |
| 14. 1234567890 | 29. 142536 |
| 15. gabriel | 30. familia |

Codiname "password"

No Brasil, a senha mais popular é a combinação "123456", que já foi vazada mais de 1 milhão de vezes — em segundo e terceiro lugar ficaram as palavras chaves "123456789" e "brasil". Mas esse não é um problema só dos brasileiros: a senha "123456" é a mais usada ao redor do mundo com mais de 103 milhões de registros.

41

I Senhas

FIAP

- <https://gpuhash.me/>
- <http://crypt-fud.ru/>

42

I Senhas

FIAP

- Wordlists:
 - <https://blog.g0tmi1k.com/2011/06/dictionaries-wordlists/>
- Listas de senhas
 - Categorizada, organizada, limpa, duplicatas removidas, com análise de quantitativo
 - Há arquivos com 13GB de senhas!
- <https://weakpass.com/wordlist>
 - Centenas de listas de senhas

43

I Senhas

FIAP

- Analisando essa lista, chega-se às seguintes conclusões:
 - Há 50% de chance de uma senha conter uma ou mais vogais
 - Caso contenha um número, geralmente será 1 ou 2 e estará no final
 - Caso contenha letra maiúscula, estará no início da senha seguido de uma vogal



44

I Senhas

FIAP

- Analisando essa lista, chega-se às seguintes conclusões:
 - A média das pessoas tem um vocabulário de aproximadamente 50000 a 150000 palavras, e normalmente serão usadas na senha
 - Mulheres tem fama de usarem nomes pessoais nas senhas, e homens optam por senhas com seus hobbies
 - Mesmo usando símbolos, os mais comuns de aparecerem são: ~, !, @, #, \$, %, &, ?.

45

I Senhas

FIAP

BRUTEFORCE



Felipe Mendes
Colaboração para Tilt
23/06/2021 18h09 | Atualizada em 23/06/2021 18h11

No início do mês, o vazamento de um arquivo com 8,4 bilhões de senhas deixou muita gente assustada pelo grande volume de dados. Até então, não existiam tantas informações sobre o ocorrido. Nos dias seguintes a notícia do que poderia ser o maior vazamento da história, profissionais da área começaram a destrinchar o documento.

Ao que parece, o caso, conhecido como RockYou2021, reúne não apenas senhas, mas também um banco de palavras. Por isso, é tão grande (100 GB, mais do que a memória de muito celular). Além disso, o arquivo foi criado a partir de um compilado de senhas que já haviam sido vazadas anteriormente (informação que já se tinha na época da descoberta).

46

I Senhas

FIAP

<https://password.kaspersky.com/pt/><https://testedesenha.com.br/>

47

I Senhas

FIAP

Desafio

Gere um código em python para criar um arquivo contendo uma wordlist com um número de letras específico (3)

Use essa Wordlist para destravar o arquivo "arquivo_protegido_3_letras.pdf"

Leia o conteúdo

48

I Mapa mental

FIAP

- Recap da aula

49



FIAP

FIAP GRADUAÇÃO

Copyright © 2025 Prof. Leonardo Orabona e Prof. Dr. Noris Junior

Todos direitos reservados. Reprodução ou divulgação total ou parcial deste documento é expressamente proibido sem o consentimento formal, por escrito, do Professor (autor).

50