



Análise de Malware

“malware” (abreviação de “malicious software”)



Malware



Estatísticas

Qualquer idioma ▾ No último mês ▾ Todos os resultados ▾ Limpar

<https://www.itinsight.pt/news/seguranca/ataques-d-...>

Ataques de malware fileless aumentam 900% - IT Insight

31/03/2021 — Relatório de Segurança de Internet da WatchGuard indica que, no quarto trimestre de 2020, existiu um aumento massivo de ataques aos endpoints e novas ...

<https://www.itinsight.pt/news/seguranca/nimzaloader-...>

NimzaLoader: o malware escrito numa linguagem de ...

22/03/2021 — O malware NimzaLoader é incomum porque está escrito numa linguagem de programação raramente utilizada por criminosos virtuais, o que dificulta a deteção ...

<https://androidgeek.pt/google-...>

Novo malware Android foi descoberto com arsenal completo ...

28/03/2021 — Recentemente, investigadores detectaram um novo Android malware, que é ... aplicações instaladas, nome do dispositivo, estatísticas de armazenamento) ...

<https://business-it.pt/artigo-...>

WatchGuard revela descida abrupta dos ataques de rede em ...

17/03/2021 — A WatchGuard revelou que, de acordo com as estatísticas da sua equipa de ... de 26120 ataques de malware, o que corresponde a um ritmo de 1045 ataques ...

<https://seguranca-informatica.pt/category/cybercrime-...>

Arquivo de Cybercrime - Segurança Informática

28/03/2021 — PHP git server hacked with backdoor implanted. Cybercrime, darkweb, Malware, ransomware - Website do mediático ransomware Netwalker foi apreendido pelas ...
Em falta: estatísticas | Tem de incluir: estatísticas

<https://www.regiaoonline.pt/portugal-e-o-segundo-pais-...>

Portugal é o segundo país do mundo com mais vítimas de ...

15/03/2021 — Tudo isto se refletiu nas estatísticas de ataques por spam e phishing em todo o ... quais os websites que não devem ser abertos, protegendo-o contra malware.

<https://www.itchannel.pt/news/seguranca-...>

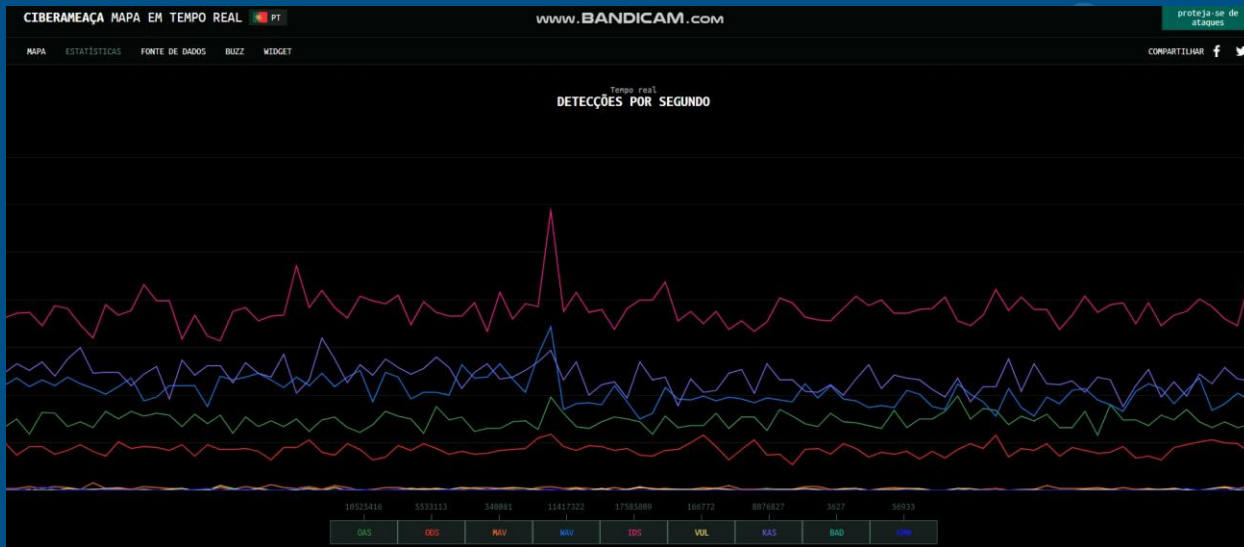
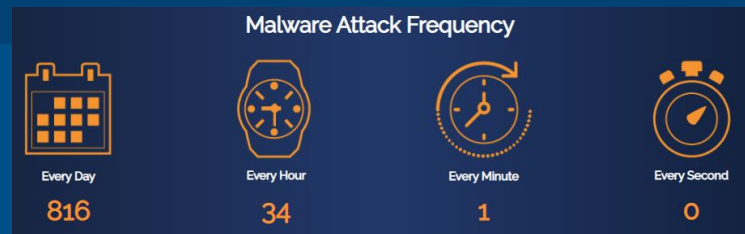
Segurança - Página 1 - IT Channel

há 2 dias — A operação Diànxùn é uma campanha de espionagem cibernética e utiliza malware disfarçado com aplicações Adobe Flash. Já foram identificadas mais de 20 ...

<https://www.itchannel.pt/news/seguranca/portugal-...>

Portugal é dos países com mais vítimas de phishing

15/03/2021 — Tudo isto se refletiu nas estatísticas de ataques por spam e phishing em todo o mundo. Segundo a Kaspersky ... Nutanix reforça segurança contra ransomware.



<https://cybermap.kaspersky.com/pt/stats#country=221&type=OAS&period=m>

<https://www.secplicity.org/threat-landscape/?s=2021-01-01&e=2021-03-31&type=all®ion=PT>

:> Phishing and Malware Q4 2020

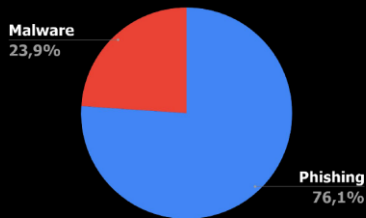


Figure 1: Volume of phishing and malware submissions (376) during Sep - Dec 2020 in Portugal.

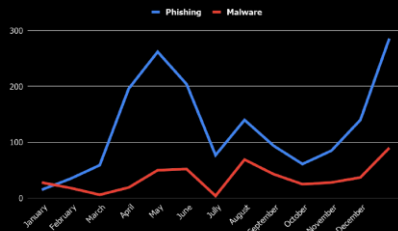


Figure 2: Number of phishing and malware campaigns from Jan to Dec of the year 2020.

:> Malware by Numbers

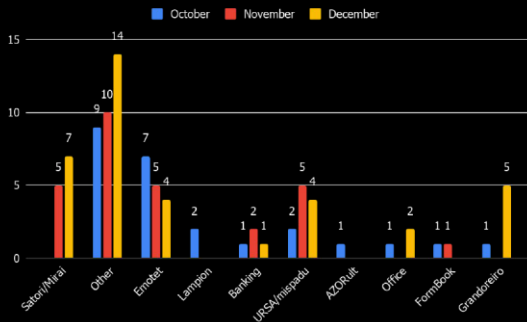


Figure 3: Number of malware submissions by category, during Q4 2020 in Portugal.

Malware Campaigns

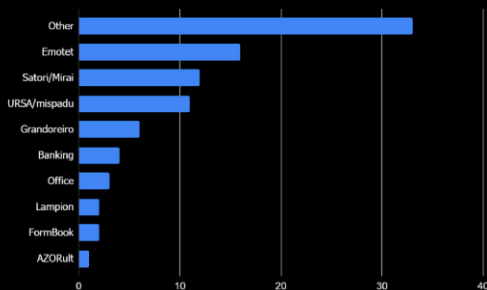


Figure 4: Comparison of overall malware samples (90) collected during Q4 2020 in Portugal.

:> Threats by Sector

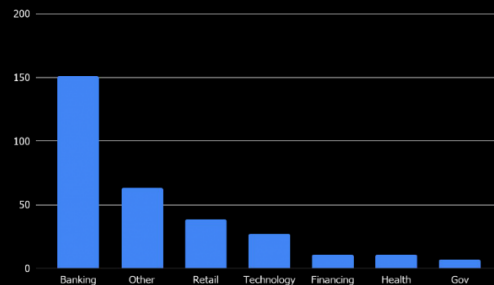


Figure 5: Number of phishing and malware campaigns by sector during Q4 2020 in Portugal.

Malware

“malware” (abreviação de “malicious software”)

Malware ou vírus?



Uma aplicação (intrusiva) que prejudica o desempenho do computador, sendo hostil

Tipo: Vírus, spyware, worms, Trojans, ransomware, adware, ...

Exemplos de antimalware: Malwarebytes, SpyBot Search and Destroy, Windows Malicious Software Removal Tool, ...



Uma aplicação capaz de se copiar e que tem um efeito prejudicial, por exemplo corrompendo o sistema e/ou destruindo dados

Tipo: Vírus

Exemplos de antivírus: Kaspersky, McAfee, AVG, Avira, Avast, Microsoft Defender, ...

Free + Premium
= Free Premium

Malware

"malware" (abreviação de "malicious software")



Sintomas

- Computador começou a ficar estranhamente lento, mensagens de erros de sistema, sem razão aparente
- Ecrã de erro com reinício do computador, Blue screen of death (BSOD)
- Espaço em disco, "desaparece", simultaneamente o disco tem actividade constante
- Ventoinha passou a estar sempre na velocidade máxima
- Navegação na internet com Pop-ups, Ads, websites, barras de ferramentas, e outras aplicações não solicitadas
- A página inicial do browser foi alterada sem se ter feito nada
- Os vossos contactos estão a receber SPAM, enviado da conta de correio e em vosso nome
- A ferramenta de segurança (antivírus por exemplo) foi desabilitada
- Não se consegue aceder ao painel de controlo
- Novos ícones aparecem no ambiente de trabalho, além de "shortcuts" suspeitos

Tipos de Malware

A large, light blue number '2' is positioned on the right side of the slide. Behind it is a faint, light blue network diagram consisting of numerous small circular nodes connected by thin lines, creating a web-like structure that fills the right half of the slide.

Vírus

- Subclasse de Malware;
- Modifica ficheiros ;
- Incluído dentro de outro programa ou ficheiro;
- Auto replica-se;
- Necessita de ser executado.

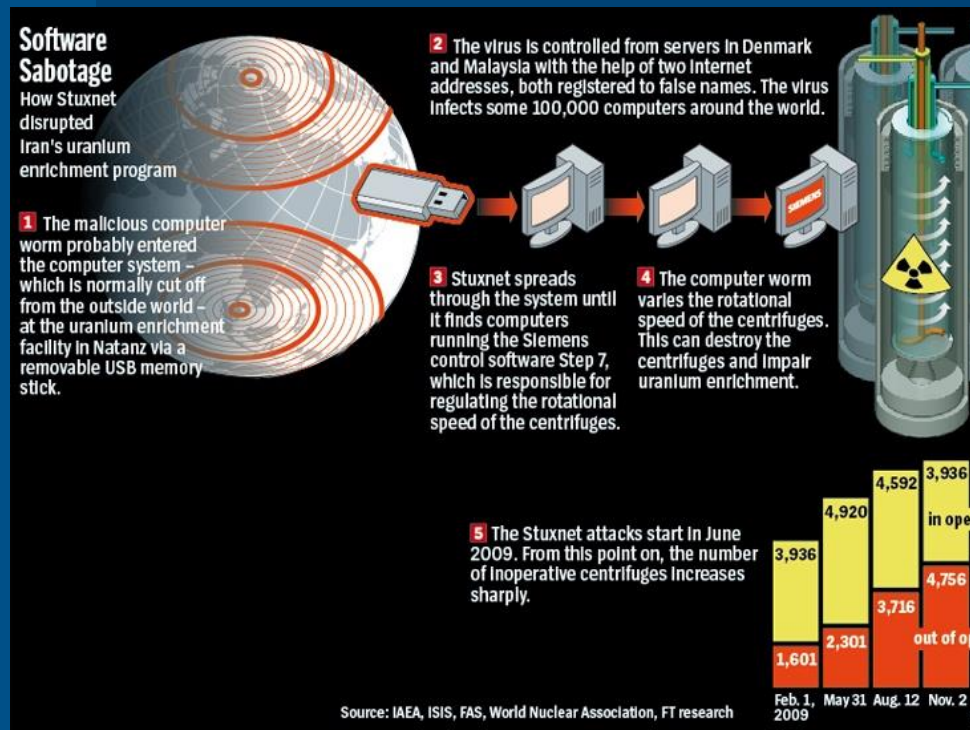
– Exemplo : ILOVEYOU



Worms

- ❑ Subclasse de Malware;
- ❑ Modifica ficheiros ;
- ❑ Incluído dentro de outro programa ou ficheiro;
- ❑ Auto replica-se;
- ❑ **Não necessita de ser executado.**

– Exemplo : STUXNET



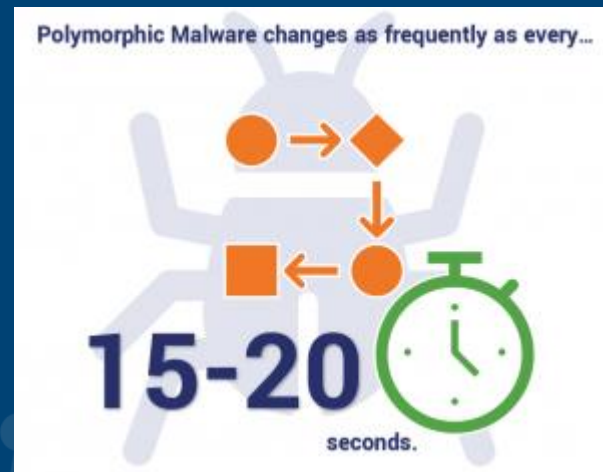
Troianos

- ▣ Incluído dentro de outro programa ou ficheiro;
- ▣ Permite o acesso ao sistema infetado;
- ▣ Permite aceder, bloquear e eliminar dados.
- ▣ Não se replicam.
 - Exemplo : PLUGX



Malware Pólimorfico

- Muda constantemente a sua assinatura;
- Dificilmente é detetável pelo antivírus;
- É necessário uma análise dos padrões do malware para ser detetado.



Ransomware

- É a classe de malware mais destrutiva atualmente;
 - Encripta os dados;
 - Bloqueia totalmente o sistema;
 - Pedido de resgate na maioria dos casos.
-
- Exemplo : WannaCry



Exemplos de Ransomware



Wana Decrypt0r 2.0

Ooops, your files have been encrypted! English

What Happened to My Computer?
Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time. You can decrypt some of your files for free. Try now by clicking <Decrypt>. But if you want to decrypt all your files, you need to pay. You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever. We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>. Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>. And send the correct amount to the address specified in this window. After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

[About bitcoin](#)
[How to buy bitcoins?](#)
[Contact Us](#)

Send \$300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw Copy

Check Payment **Decrypt**



Cryptolocker v3

Your personal files are encrypted!

Your files have been safely encrypted on this PC: photos, videos, documents, etc. Click "Show encrypted files" button to view a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a unique public key RSA-2048 generated for this computer. To decrypt files you need to obtain the **private key**.

The only copy of the private key, which will allow you to decrypt your files, is located on a secret server in the Internet; the server will eliminate the key after a time period specified in this window. **Once this has been done, nobody will ever be able to restore files...**

In order to decrypt the files open your personal page on site <https://34r6h26g2h4jz2.tor2web.fi> and follow the instruction.

Use your Bitcoin address to enter the site:
1AFU4rTQUJy2E1Omga9R1ssn8SSd4uFWdV

Click to copy Bitcoin address to clipboard

If <https://34r6h26g2h4jz2.tor2web.org> is not opening, please follow the steps: You must install this browser: www.torproject.org/projects/orbrowsers.html.en. After installation, run the browser and enter address 34r6h26g2h4jz2.tor2web.org. Follow the instruction on the web-site. We remind you that the sooner you do, the more chances are left to recover the files.

Any attempt to remove or corrupt this software will result in immediate elimination of the private key by the server.

Rootkits

- ▣ Permite o controlo remoto ao sistema infetado;
- ▣ Permite abrir aplicações sem serem apresentadas no ecrã;
- ▣ Utilizado para gerar receitas através de anúncios na internet ou mineração de moedas digitais.



Keyloggers

- Monitoriza as teclas selecionadas pelo utilizador;
- Objetivo é roubar informações confidências (Ex.: palavras-passe);
- Funciona em segundo plano sem ser detetado pelo utilizador.



Spyware e Adware



- ▣ Permite espiar a atividade do utilizador;
- ▣ Objetivo de obter informação;
- ▣ Abertura de publicidade sem autorização.
 - Exemplo : PEGASUS

PEGASUS BY THE NUMBERS

GLOBAL SCALE

36 LIKELY OPERATORS

45 COUNTRIES WITH LIKELY INFECTIONS

10 OPERATORS WITH INFECTIONS IN ANOTHER COUNTRY

HUMAN RIGHTS

6 OPERATORS LINKED TO COUNTRIES WITH A HISTORY OF ABUSING SPYWARE TO TARGET CIVIL SOCIETY

Exemplos de Adware

How to remove 'IST Cleaner'...

remove a few hundred unnecessary entries and reduce the size of your registry by a few kilobytes. This makes no difference in perceptible performance.

You should always pay attention when installing software because often, a software installer includes optional installs, such as this IST Cleaner Pro. Be very careful what you agree to install.

Always opt for the custom installation and deselect anything that is not familiar, especially optional software that you never wanted to download and install in the first place. It goes without saying that you should not install so...

How to remove IST Cleaner

This page is a comprehensive guide, while computer, and any other adware program.

Please perform all the steps in the correct order:

STEP 1: Uninstall IST Cleaner

STEP 2: Remove IST Cleaner

STEP 3: Remove IST Cleaner Pro virus with Malwarebytes Anti-Malware Free

STEP 4: Double-check for the IST Cleaner Pro infection with HitmanPro

1 : Uninstall IST Cleaner from your computer

your computer, we will try to identify and remove it.

Install the IST Cleaner Pro program. Click the Start button, then click on the Control Panel menu option.

Free Malware Removal

Easy 3-Day Malware Removal. Run Free Scan Today. Try it!

MALWARE 101

Malware - short for malicious software - is an umbrella term that refers to any software program deliberately created to perform an unauthorized and often harmful action.

Viruses, backdoors, keyloggers, spyware, adware, rootkits, and trojans are just a few examples of what is considered malware.

A few years ago it was once sufficient to call something a "virus" or "trojan horse", however today's infection methods and vectors evolved and

attachments, some viruses replicate themselves and spread via email. Stay on the safe side and confirm that the attachment was sent from a trusted source before you open it.

CLEANERS

Get a cleaner for your office cleaning.

Full name: [text input]
Your email: [text input]
Location: [text input] Your phone number: [text input]
SPEAK TO CLEANERS

STREET SMART.

SEE DEALS

TriHonda

GE

FinallyFast

Our personal checking Customers get a 0.25% discount on their rates.

Free Malware Removal

Easy 3-Day Malware Removal. Run Free Scan Today. Try it!

MALWARE 101

Malware - short for malicious software - is an umbrella term that refers to any software program deliberately created to perform an unauthorized and often harmful action.

Viruses, backdoors, keyloggers, spyware, adware, rootkits, and trojans are just a few examples of what is considered malware.

A few years ago it was once sufficient to call something a "virus" or "trojan horse", however today's infection methods and vectors evolved and

freeupdt.free247updat

Flash Player is outdated

Flash Player is required to encode and/or decode (Play) audio files in high quality.

Software update

"Adobe Flash Player" is out of date

To continue using "Adobe Flash Player", download an updated version.

Later Update

"PomoDone!" can't be opened because it is from an unidentified developer.

Your security preferences allow installation of only apps from the Mac App Store and identified developers.

Safari downloaded this file today at 11:25 AM from pomodoneapp.com.

OK

VIRUS FOUND!

http://mac-online-support.com

Are you sure you want to leave this page?

<http://fbi.gov.id657546456-3999456674.k8381.com>

YOUR BROWSER HAS BEEN LOCKED.

ALL PC DATA WILL BE DETAINED AND CRIMINAL PROCEDURES WILL BE INITIATED AGAINST YOU IF THE FINE WILL NOT BE PAID.

FOR HELP CALL TOLL FREE +1 800-798-8393

Stay on Page Leave Page

Safari - Alert

Suspicious Activity Might Have been Detected.

Major Security Issue

To fix it please call Support for Apple +1 888-476-6746 (Toll Free) immediately!

OK

Apple Security Warning

Browsers Blocked for Security Reasons.

Apple has detected that a piece of software has infected your system and is trying to steal pictures, data and social networking passwords. This is a serious hacking issue. It is immediately as soon as possible. ERROR CODE: QP6500873.1C. Tell this error code to the Customer service representative.

Your browsing connections are currently in a state.

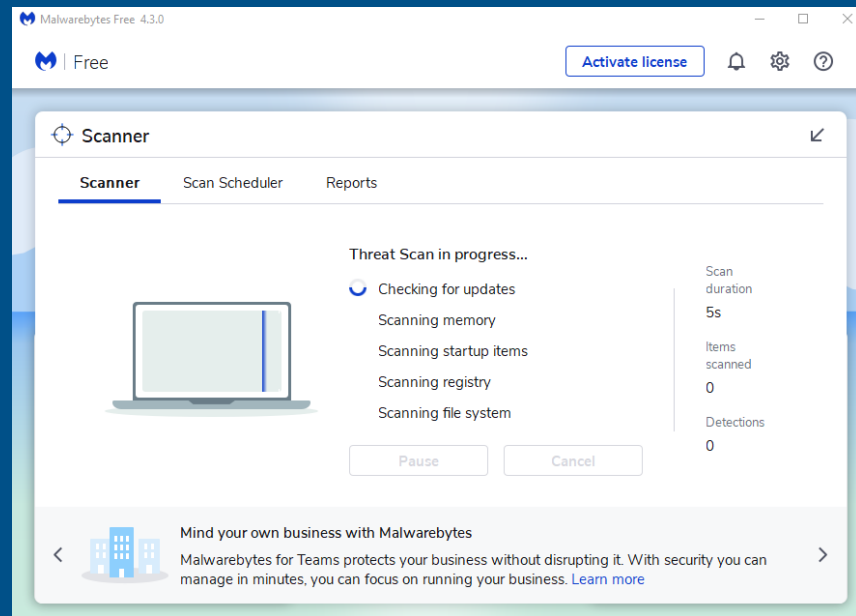
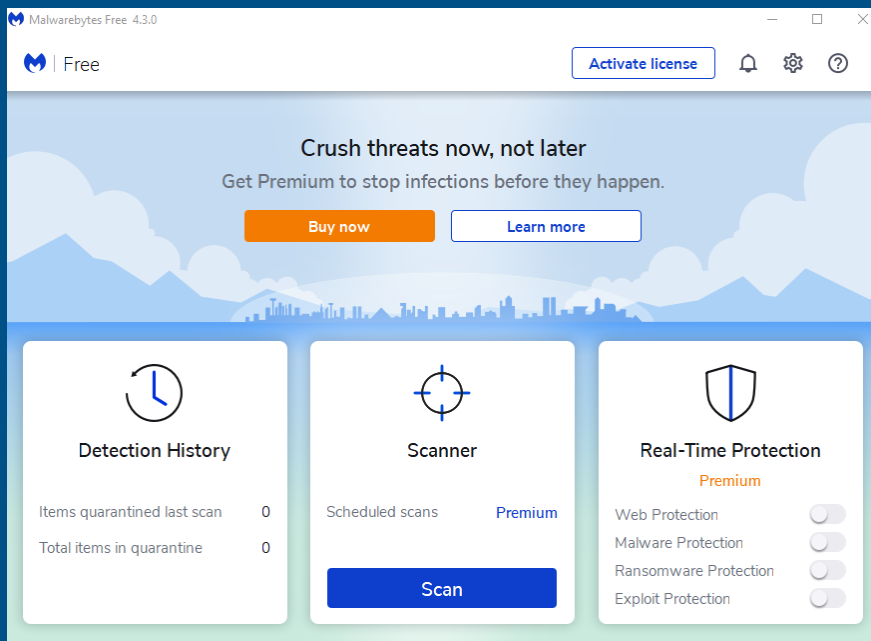
IMMEDIATELY CALL APPLE SECURITY AND DATA PROTECTION TEAM AT: 1-866-352-3532

Don't show more alerts from this webpage.

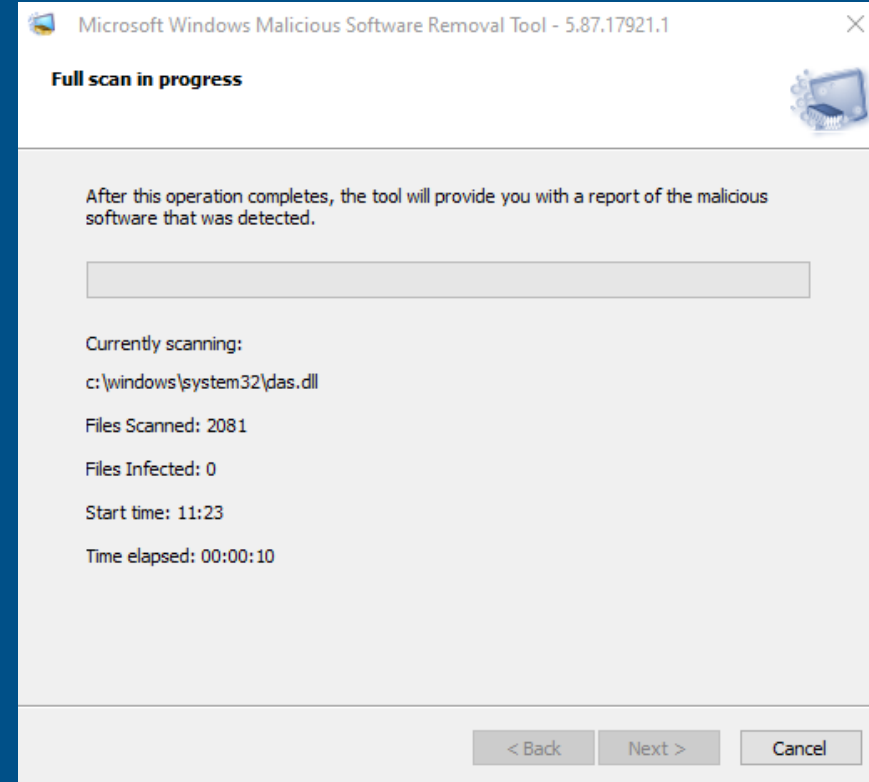
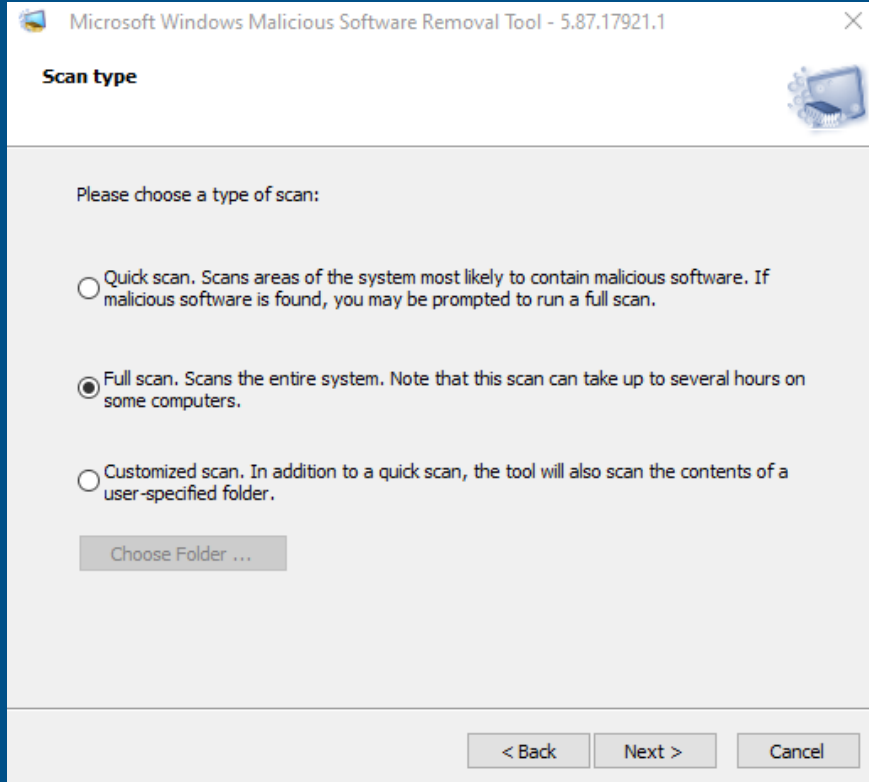
SCAN MY MAC >

Ferramentas para análise de Malware

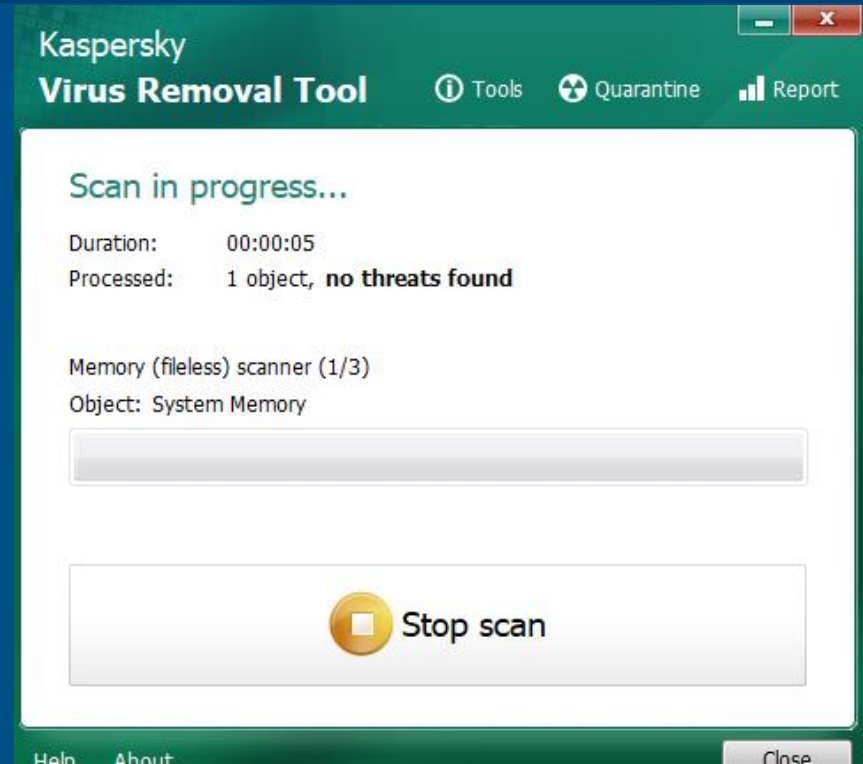
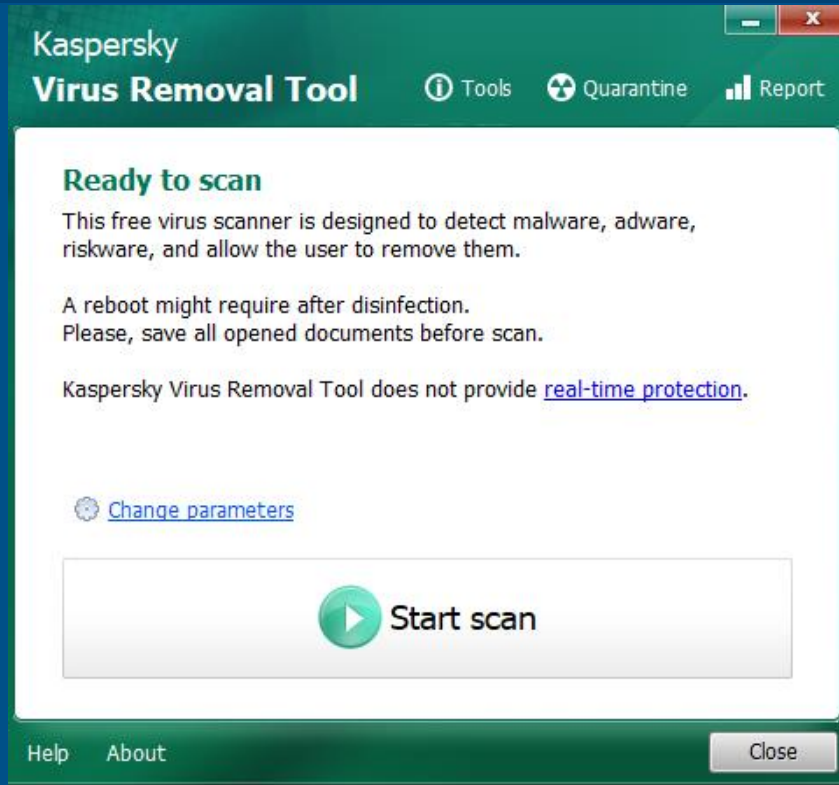
A large, light blue number '3' is positioned on the right side of the slide. Behind it is a faint, light blue network diagram consisting of numerous nodes connected by lines, creating a complex web-like structure.



Windows Malicious Software Removal Tool



Kaspersky Virus Removal Tool



Boas práticas



4

Atualizações

- Sistema Operativo
- Aplicações
- Antivirus

WI-FI Público

- Ao conectar-se a uma rede pública efetue essa ligação através de uma VPN

Compras online

- Verificar se o vendedor é confiável
- Ter em atenção os dados partilhados

Links e Anexos

- Verificar a autenticidade dos anexos e links que seleciona



Backups

- Criar uma política de salvaguarda de dados noutra localização diferente
- Se possível efetuar um backup no mínimo diário da informação crítica

Passwords

- Implementar credenciais de acesso com um grau elevado de complexidade e tamanho.

Dispositivos Externos

- Ter em atenção quais os dispositivos externos que conecta ao computador



Nunca pagar o Resgate

- É importante nunca efetuar o pagamento do resgate caso seja alvo de um ataque de ransomware

Isolar o Computador

- Deve-se isolar completamente o computador, desconectando-o da rede.

Processo de Análise

- Iniciar o processo de análise e recuperação do ataque de ransomware para tentar obter de novo os dados encriptados.



Ransomware protection

Protect your files against threats like ransomware, and see how to restore files in case of an attack.

Controlled folder access

Protect files, folders, and memory areas on your device from unauthorized changes by unfriendly applications.



On

[Block history](#)

[Protected folders](#)

[Allow an app through Controlled folder access](#)

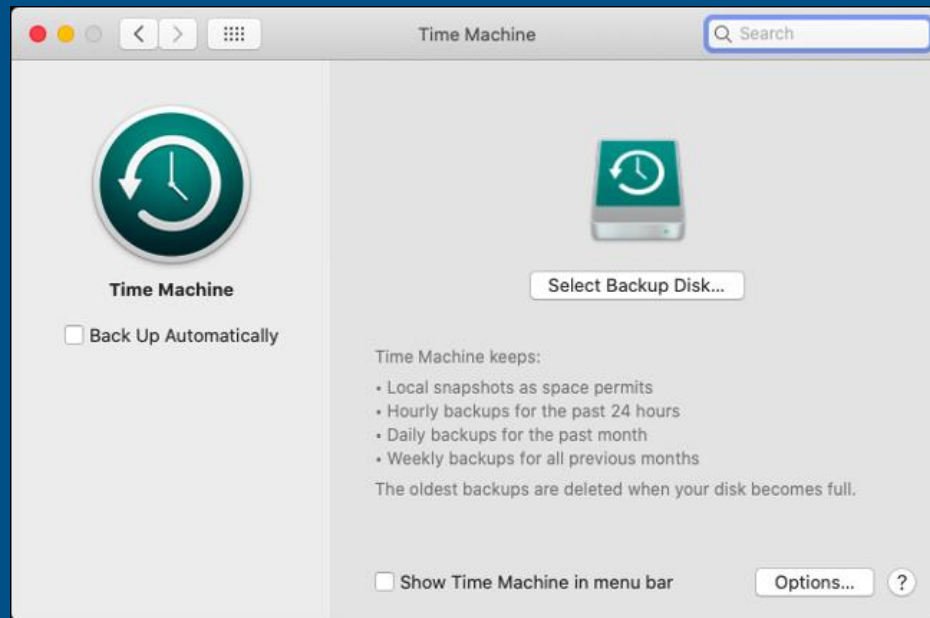
Ransomware data recovery

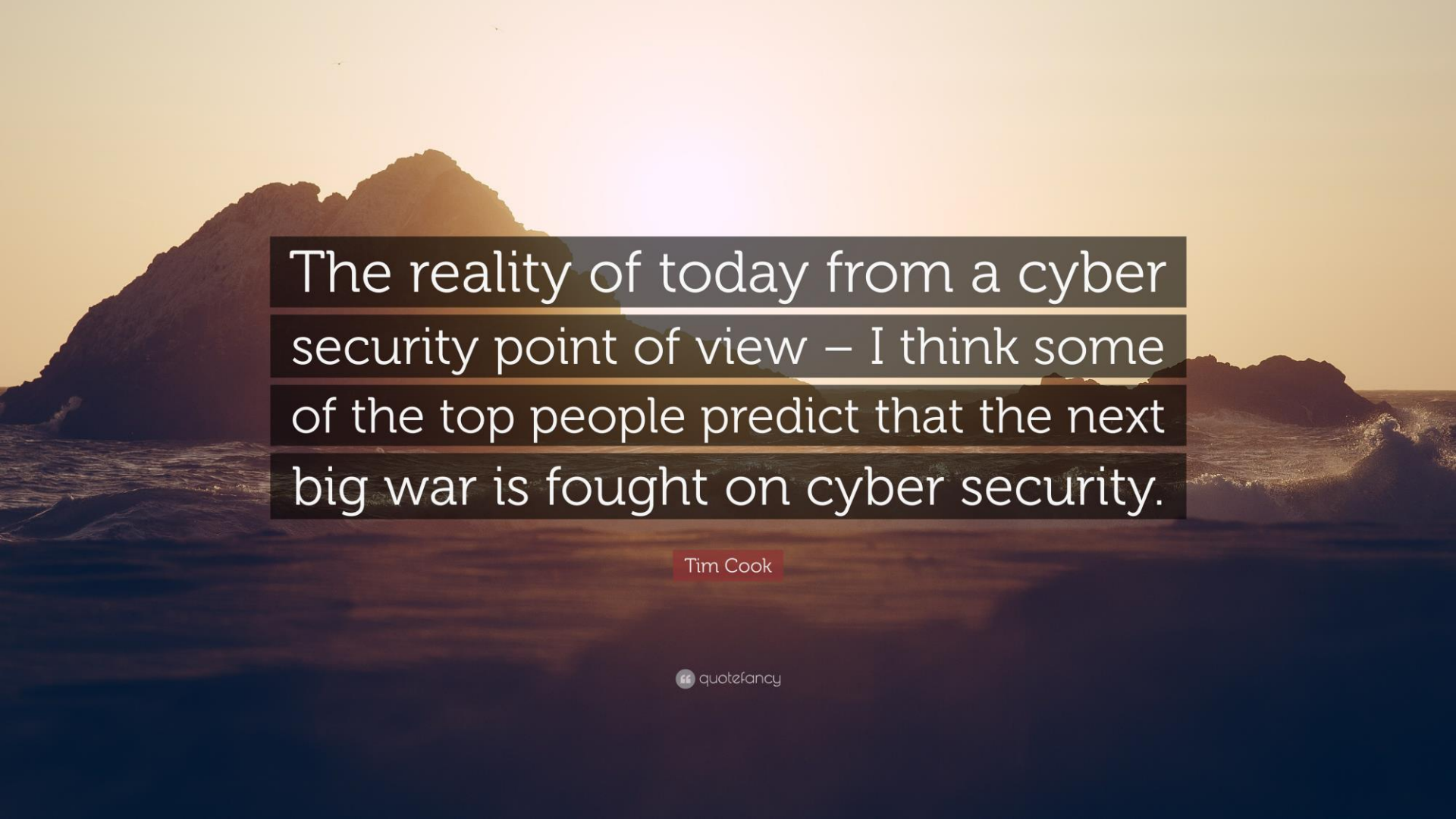
You may be able to recover files in these accounts in case of a ransomware attack.



Premium account with recovery using Files restore.

[View files](#)





The reality of today from a cyber security point of view – I think some of the top people predict that the next big war is fought on cyber security.

Tim Cook

Obrigado!

Alguma Questão?

- @jose.sgoncalves
- @pedro.magalhaes

Próximas Sessões:

- **Gestores de Passwords;** (26 de Abril)
- **Resposta a Incidentes;** (10 de Maio)
- **Engenharia Social.** (24 de Maio)





Malware

"malware" (abreviação de "malignos software")

Malware ou vírus?

Uma aplicação (malware) que prejudica o funcionamento do computador, sendo local.

Uma aplicação capaz de se replicar e que tem um efeito prejudicial, por exemplo corrompendo e destruindo seus dados (malware).

Tipos: Vírus, worms, trojans, ransomware, etc.

Exemplos de malware: Malwarebytes, Spybot, Avast, Avira, Norton, McAfee, etc.

Malware

"malware" (abreviação de "malignos software")

Sintomas

- Computador começa a ficar extremamente lento, mensagens de erros de sistema, sem razão aparente.
- Erros de erro com reinício do computador, Blue screen of death (BSOD).
- Tipagem em "disques" (malware) e desligamento de disco com atividade constante.
- Verificação de erros, a cada tempo na velocidade máxima.
- Navegação na internet com Pop-ups, Ads, banners, janelas de ferramentas, e outras aplicações de malware.
- A página inicial do navegador foi alterada sem ser feito nada.
- De vez em quando recebe SPAM, enviado de conta de correio e em nome de nome.
- Aumento de segurança (malware) por exemplo) foi desativado.
- Não se consegue acessar os dados do sistema.
- Novos ícones aparecem no ambiente de trabalho, além de "shortcuts" suspeitos.

Vírus

- Subclasse de Malware.
- Modifica arquivos.
- Incluído dentro de outro programa ou arquivo.
- Auto replicar-se.
- Necessário de ser executado.

Exemplo: ILOVEYOU

Worms

- Subclasse de Malware.
- Modifica arquivos.
- Incluído dentro de outro programa ou arquivo.
- Auto replicar-se.
- Não necessita de ser executado.

Exemplo: STUNNET

Trojanos

- Incluído dentro de outro programa ou arquivo.
- Permite o acesso ao sistema infetado.
- Permite aceder, bloquear e eliminar dados.
- Não se replicam.

Exemplo: PLUCK

Malware Pólimorfo

- Muda constantemente a sua assinatura.
- Difícilmente é detectado pelo antivírus.
- É necessário uma análise dos padrões do malware para ser detetado.

Ransomware

- É a classe de malware mais destrutiva atualmente.
- Encifra os dados.
- Bloqueia totalmente o sistema.
- Pedido de resgate na maioria dos casos.

Exemplo: WannaCry

Exemplos de Ransomware



Rootkits

- Permite o controle remoto ao sistema infetado.
- Permite a instalação de aplicativos sem serem apresentadas no ecrã.
- Utilizado para gerar receitas através de cartões de crédito ou mineração de moedas digitais.

Keyloggers

- Monitoriza as teclas selecionadas pelo utilizador.
- Objetivo é roubar informações confidenciais (Banco, palavra-passe).
- Funciona em segundo plano sem ser detetado pelo utilizador.

Spyware e Adware

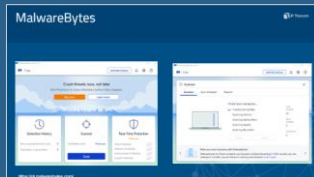
- Permite espiar a atividade do utilizador.
- Objetivo de obter informações.
- Abertura de publicidade sem autorização.

Exemplo: PEGASUS

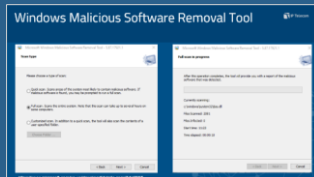
Exemplos de Adware



MalwareBytes



Windows Malicious Software Removal Tool



Boas Práticas

Atualizações

- Sistema Operativo
- Aplicações
- Antivírus

Wi-Fi Público

- Ativar o firewall
- Verificar se a conexão é segura
- Evitar a utilização de redes públicas

Boas Práticas

Backups

- Criar uma política de backup regular
- Armazenar os dados em locais diferentes
- Verificar a integridade dos dados

Senhas

- Implementar credenciais de acesso com um grau elevado de complexidade e tamanho.

Boas Práticas - Ransomware

Nunca pagar o Resgate

- É importante nunca efetuar o pagamento de resgate caso seja alvo de um ataque de ransomware.

Isolar o Computador

- Desligar o computador e desconectar da rede.

Processo de Análise

- Iniciar o processo de análise e recuperação do ataque de ransomware para tentar obter os dados, criptografados.

Boas Práticas - Ransomware

Ransomware protection