Análise de Malware

“malware” (abreviação de “malicious software”)

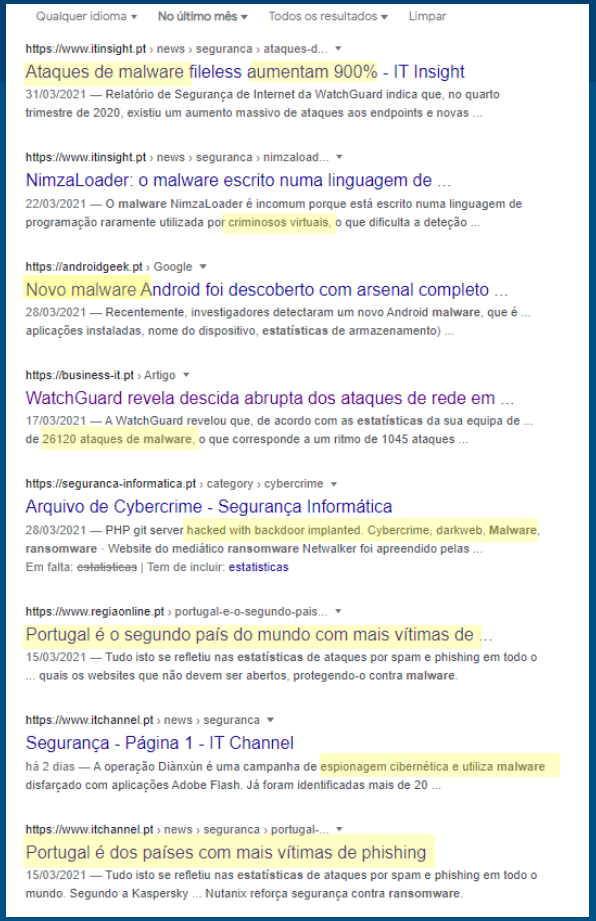
cloudsolutions

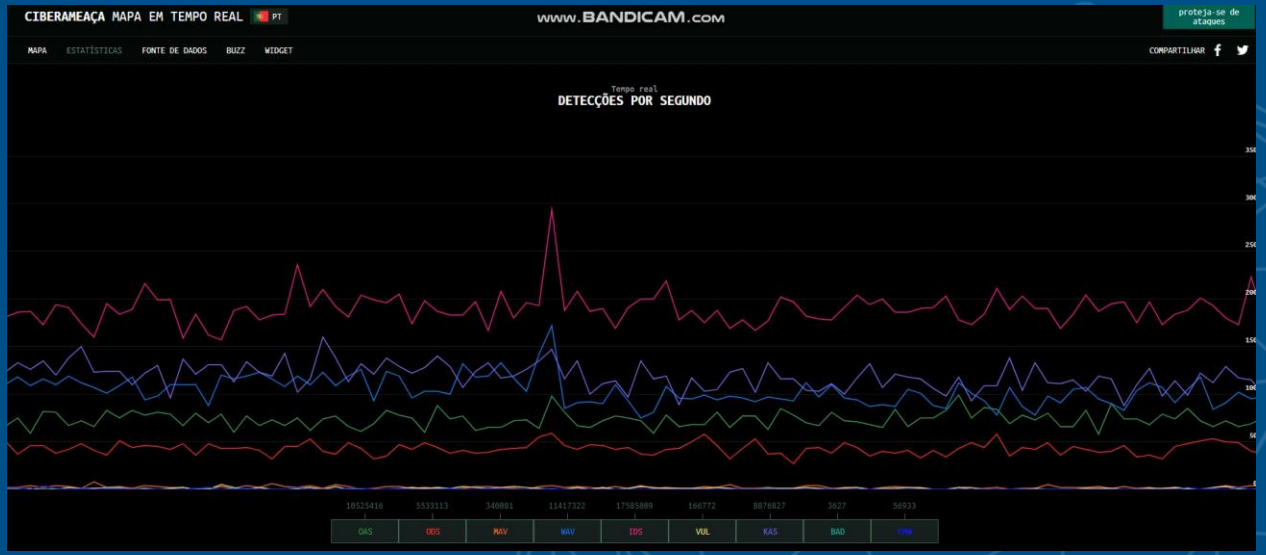
IP Telecom

IP Telecom

Malware

Estatísticas





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&region=PT

Estatísticas

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.

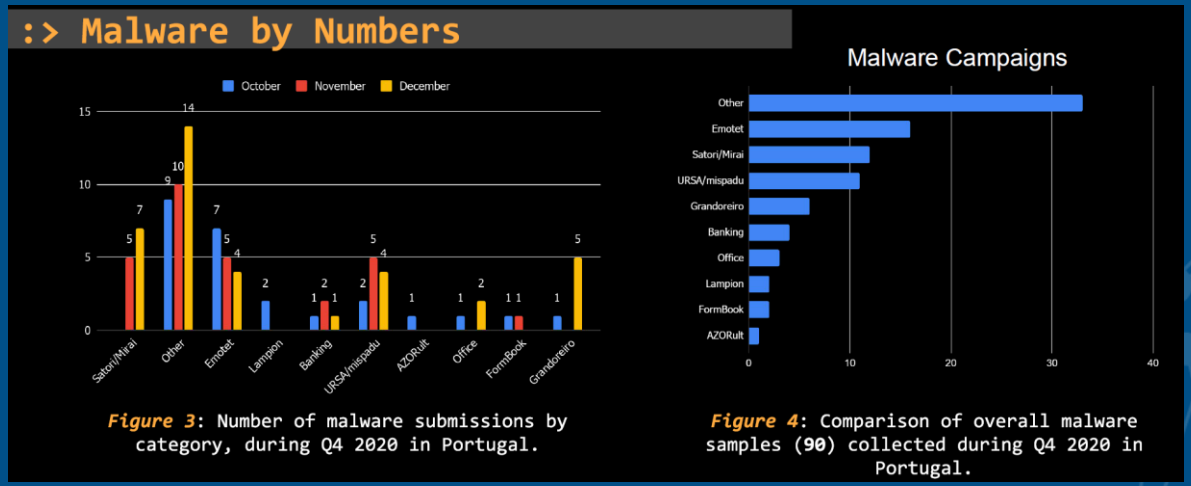


Figure 3: Number of malware submissions by category, during Q4 2020 in Portugal.

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

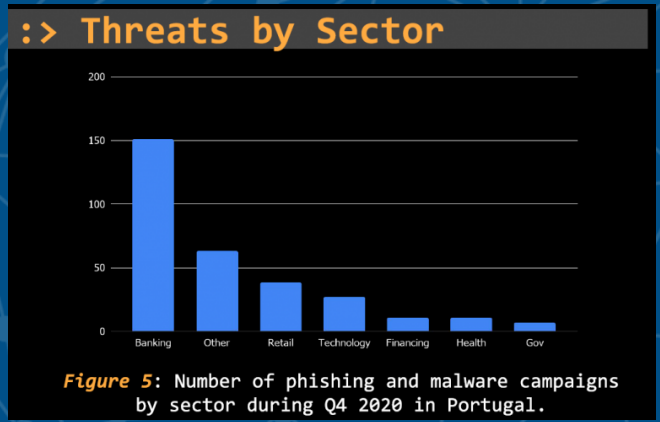


Figure 5: Number of phishing and malware campaigns by sector during Q4 2020 in Portugal.

https://seguranca-informatica.pt/threat-report-portugal-q4-2020/#.YBBX3-hKg2x

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, …

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

Tipo: Vírus

Free + Premium
=
Freemium

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

Exemplos de antivirus: Kaspersky, McAfee, AVG, Avira, Avast, Microsoft Defender, …

Malware

"malware" (abreviação de "malicious software")

IP Telecom

Sintomas

- Computador começou a ficar estranhamente lento, mensagens de erros de sistema, sem razão aparente
- Ecrã de erro com reinicio 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, alem de "shortcuts" suspeitos

IP Telecom

Tipos de Malware

2

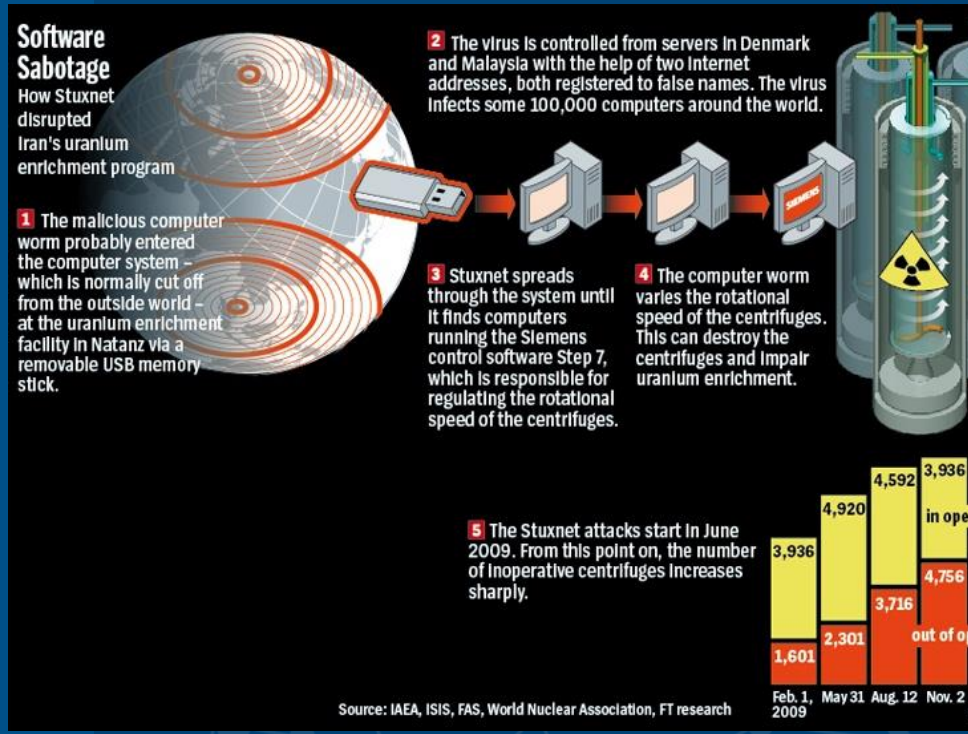
Vírus

- 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

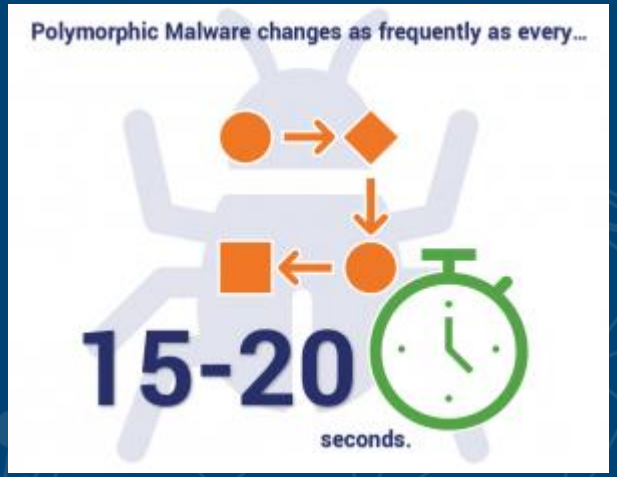


Troianos

- 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

IP Telecom

Rootkits

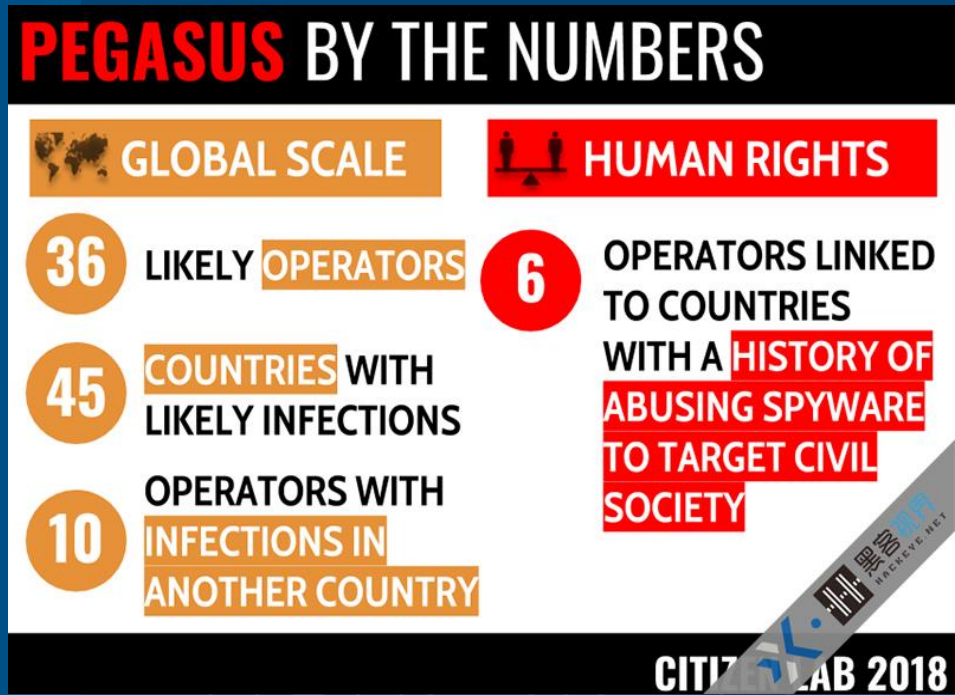
- Permite o controlo remoto ao sistema infetado;
- Permite abrir aplicações sem serem apresentadas no ecrã;
- Utilizado para gerar receitas através de anúncios na internet ou mineração de moedas digitais.

Keyloggers

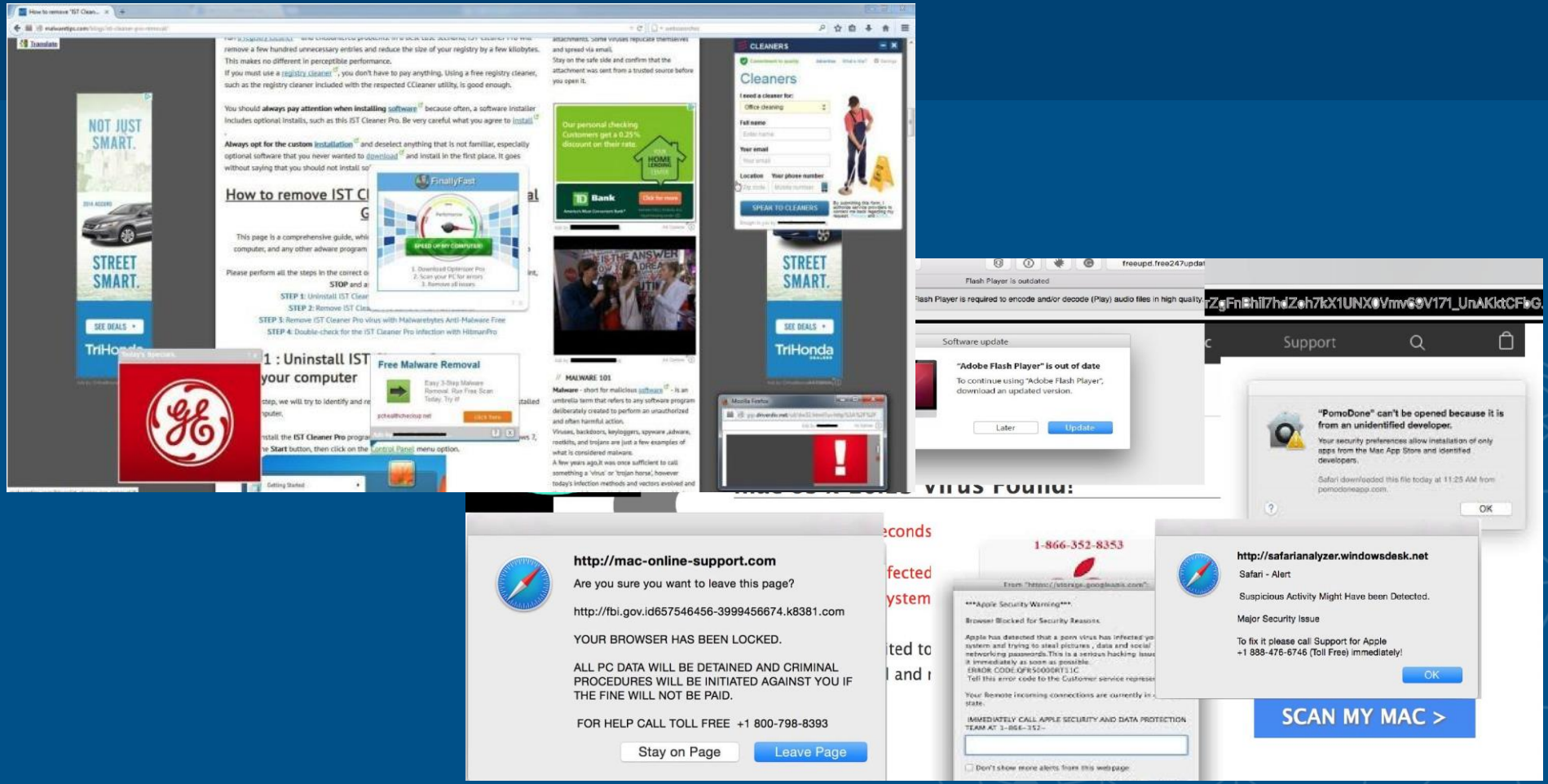
- Monitoriza as teclas selecionadas pelo utilizador;
- Objetivo é roubar informações confidências (Ex.: palavras-passe);
- Funciona em segundo plano sem ser detetado pelo utilizador.

Spyware e Adware

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



Exemplos de Adware



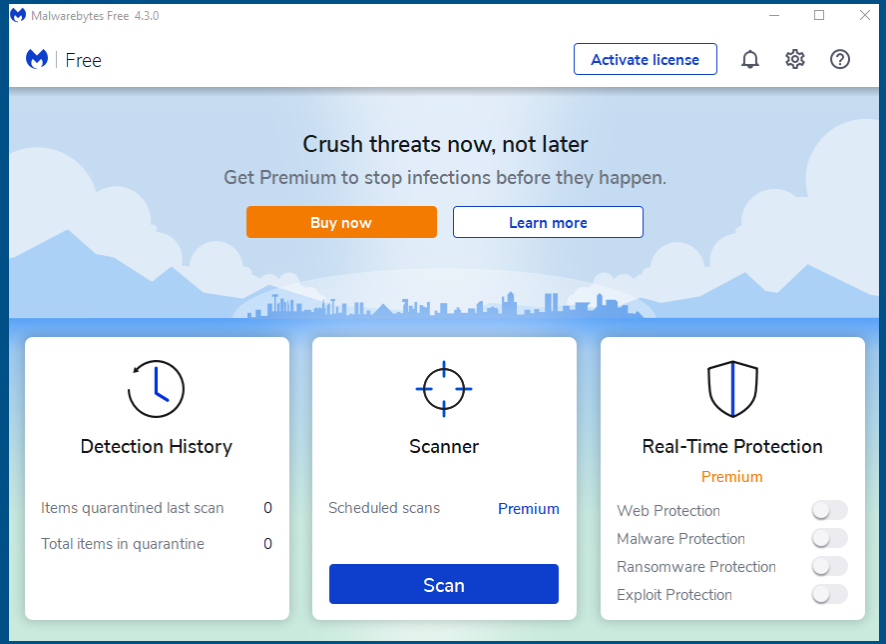
IP Telecom

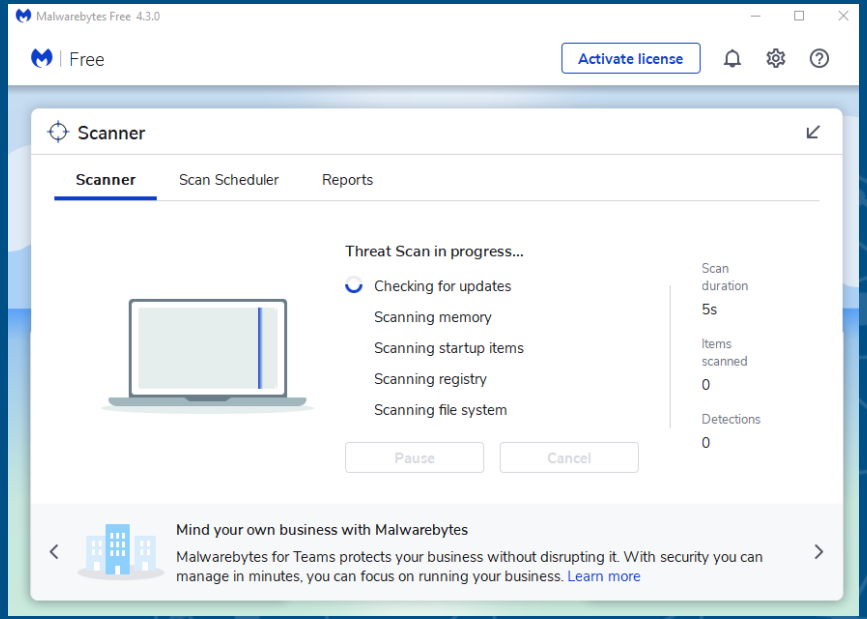
Ferramentas para análise de Malware

3

MalwareBytes

IP Telecom

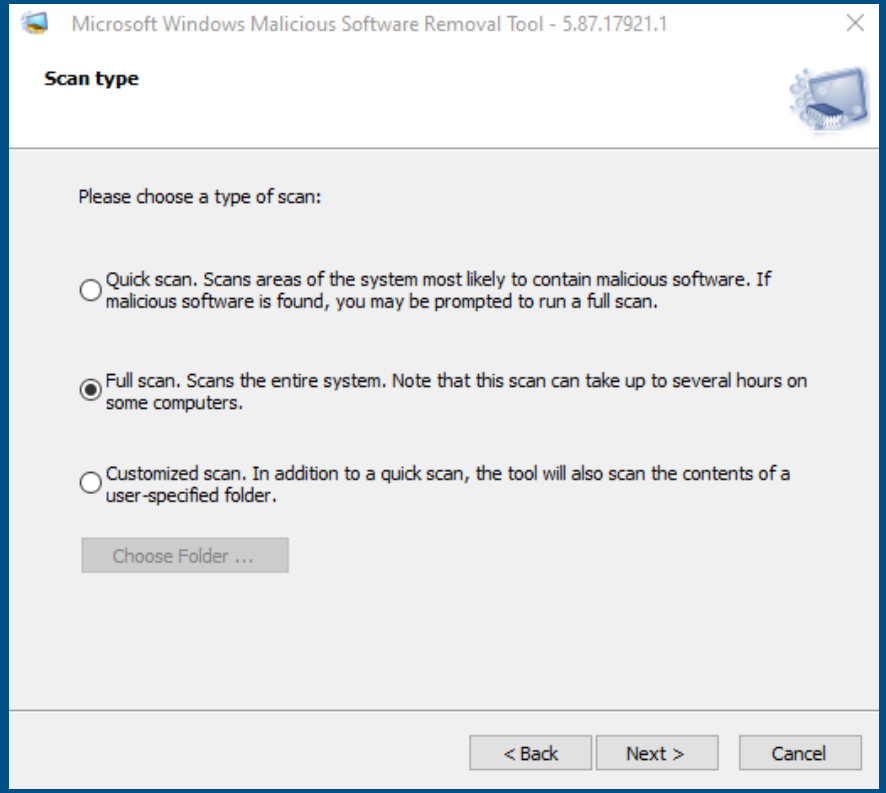


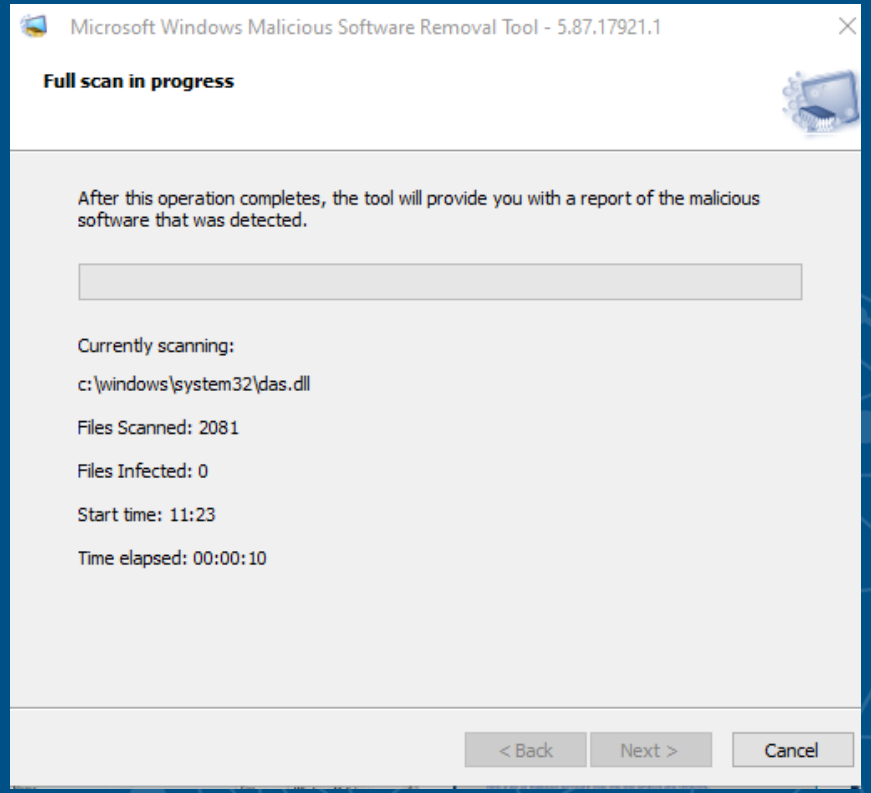


https://pt.malwarebytes.com/

Windows Malicious Software Removal Tool

IP Telecom

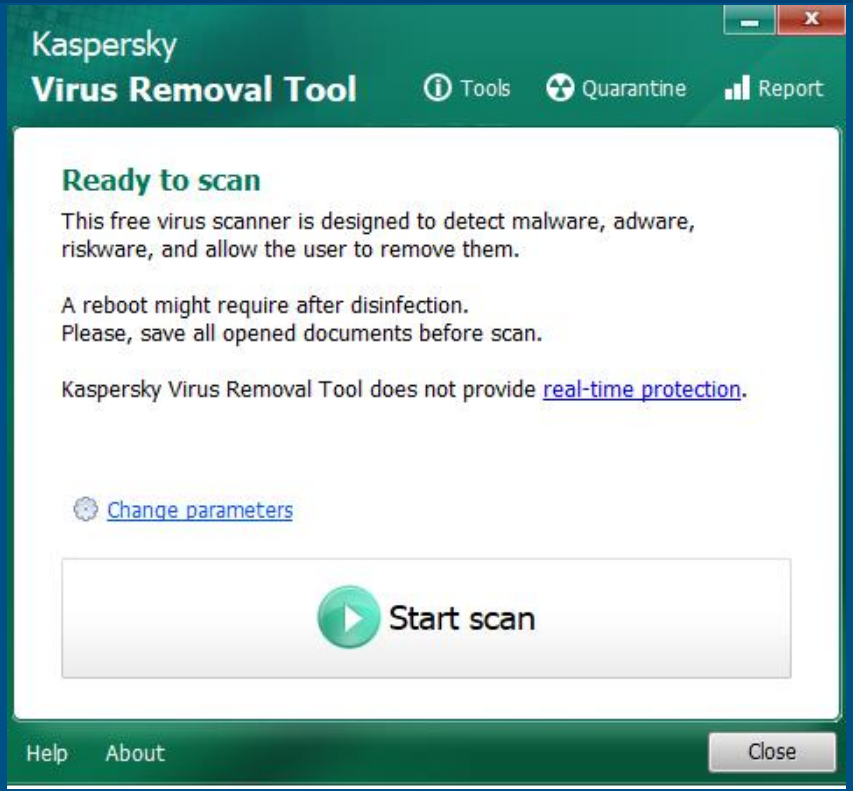


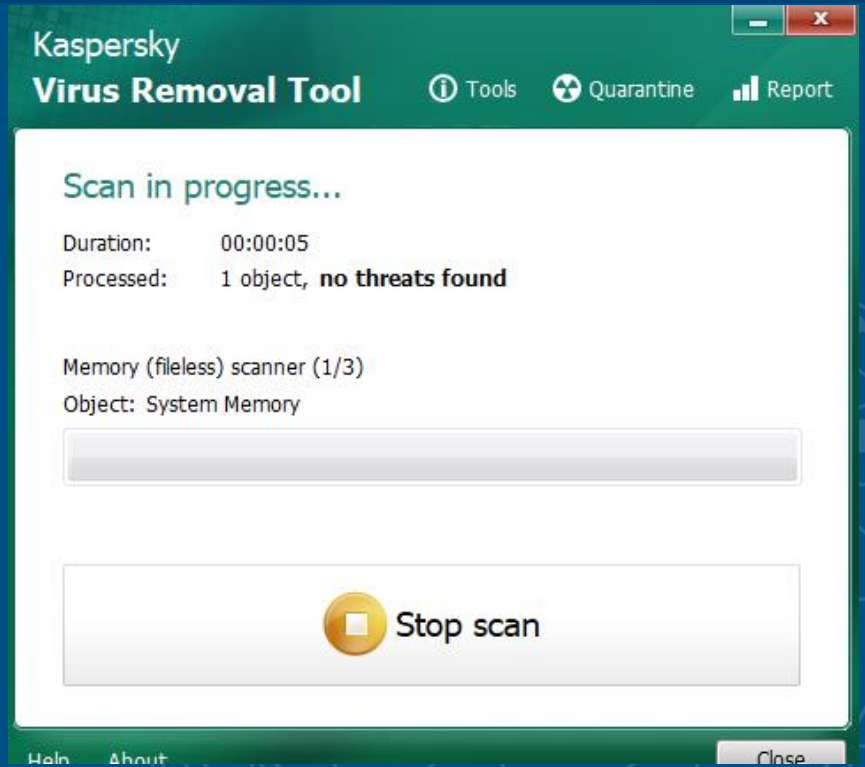


https://www.microsoft.com/en-us/download/details.aspx?id=9905

Kaspersky Virus Removal Tool

IP Telecom





https://www.kaspersky.com/downloads/thank-you/free-virus-removal-tool

IP Telecom

Boas práticas

Boas Práticas

IP Telecom

Atualizações

- Sistema Operativo
- Aplicações
- Antivirus

Compras online

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

Links e Anexos

- Verificar a autenticidade dos anexos e links que seleciona

WI-FI Público

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

Boas Práticas

IP Telecom

Backups

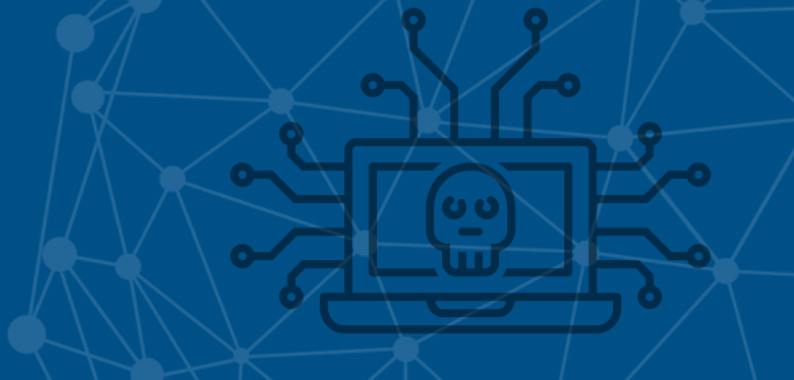
- Criar uma política de salvaguarda de dados noutra localização diferente
- Se possível efetuar um backup no mínimo diário da informação crítica

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



Boas Práticas - Ransomware

IP Telecom

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, desconentando-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.

Boas Práticas - Ransomware

IP Telecom

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

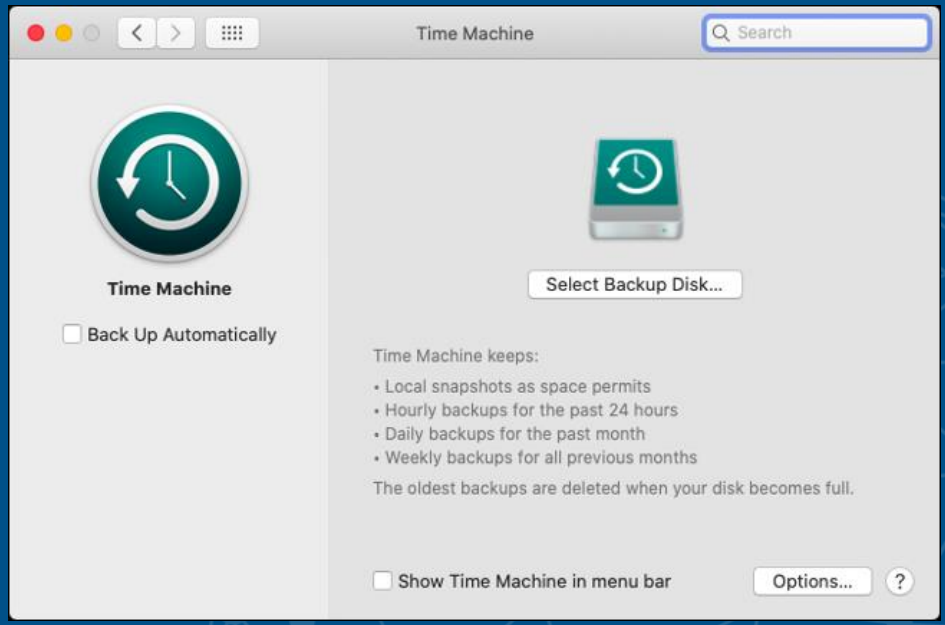
Ransomware data recovery

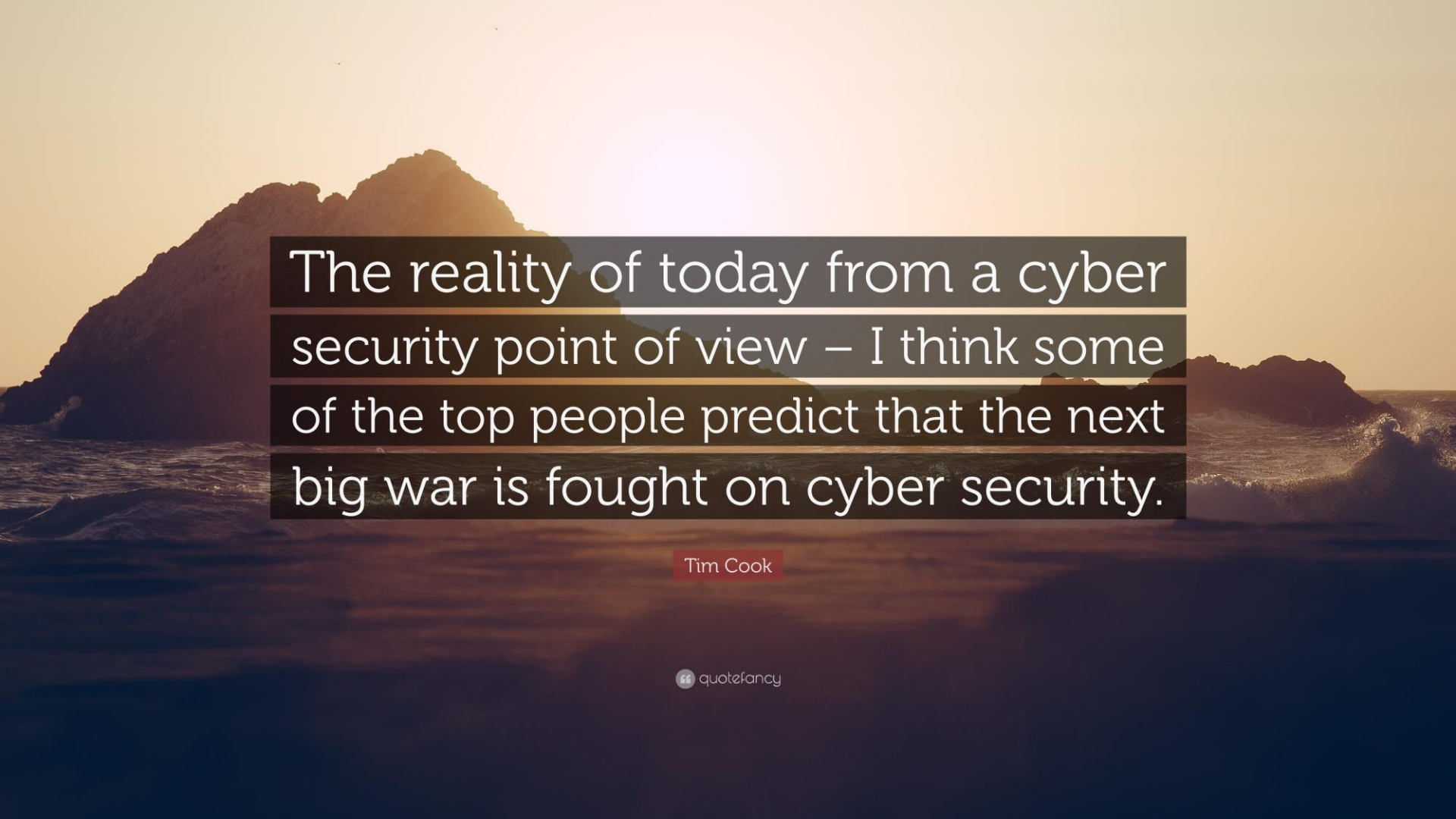
You may be able to recover files in these accounts in case of a ransomware attack.

[redacted]

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
quotefancy

Obrigado!

Alguma Questão?

- @jose.sgoncalves
- @pedro.magalhaes

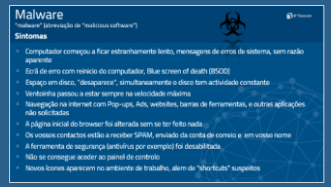
IP Telecom
Ligamos Negócios

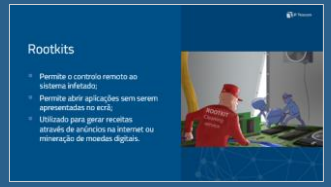
cloudsolutions

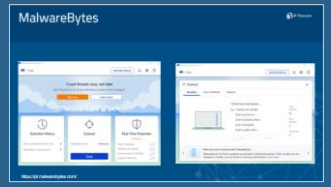
Próximas Sessões:

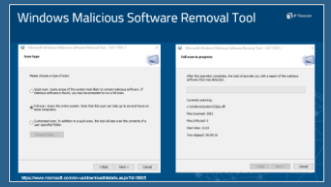
- **Gestores de Passwords**; (26 de Abril)
- **Resposta a Incidentes;** (10 de Maio)
- **Engenharia Social**. (24 de Maio)

IP Telecom









IP Telecom

Ligamos Negócios

www.iptelecom.pt

IP Telecom Portugal

/company/ip-telecom-portugal/