Especialização em TIESD #edu462 (Programa e Perfil)

7 Artigos | Dissertação - SISTEMAS DE INFORMAÇÃO

Disciplinas de Segurança da Informação e Teoria da Informação:

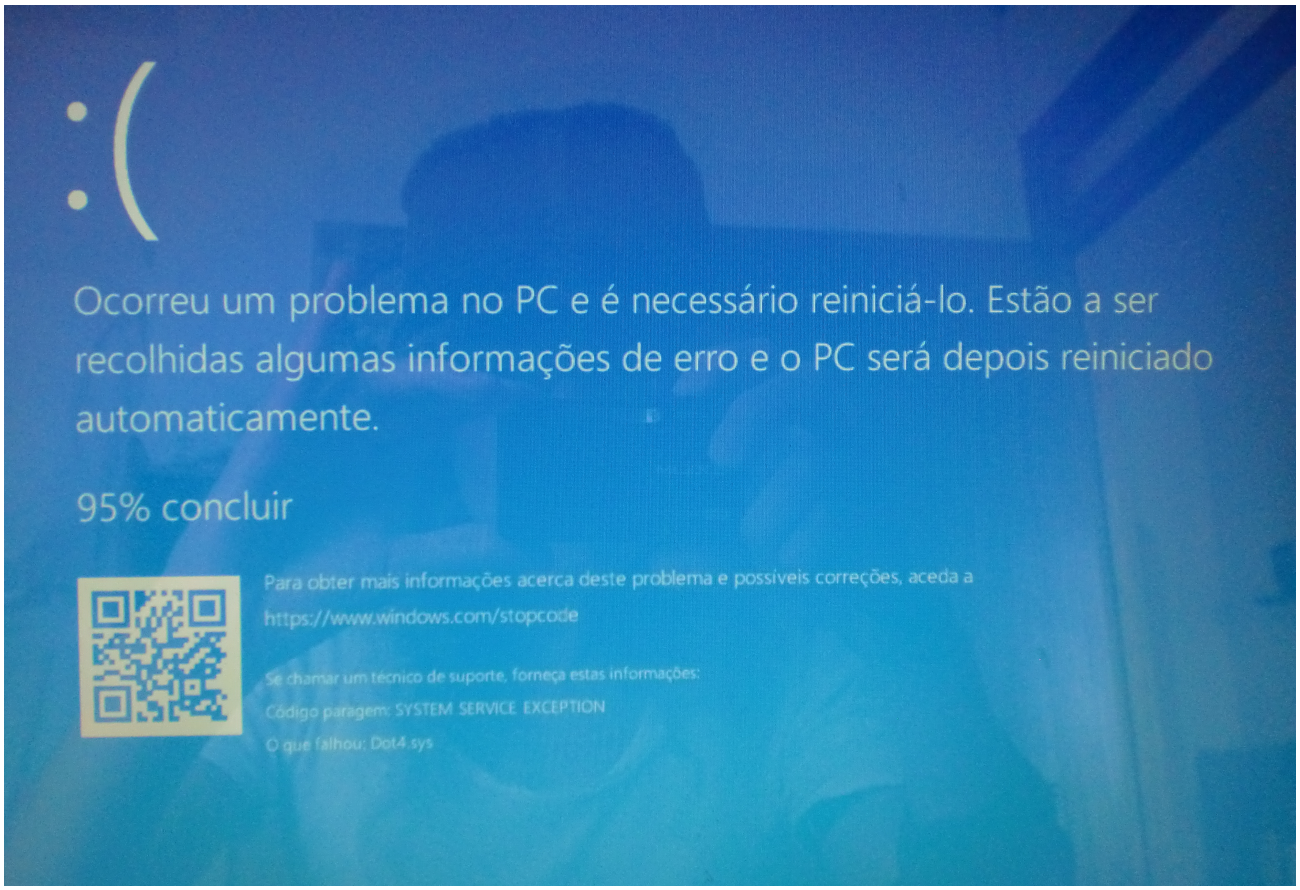
1.º Princípio básico de segurança da informação é: não usar Windows.

• Recomendações de S.O.: Ubuntu (Linux). [inclui LibreOffice suite e browser Mozilla Firefox]

ARTIGOS
~~~~~~~~

Redes de (in)Segurança da Informação no séc. XXI: a relação (dis)funcional do sistema

- Cláudia Penélope Fournier -*




```
Operações ilegais num computador podem conduzir a um "crash" do sistema. Por vezes existe
m operações de processos que geram conflitos internos ou, simplesmente, o hacker necessit
a encobrir as suas acções (que podem surtir uso abusivo da CPU) e provoca deliberadamente
um "crash" do sistema.
Um episódio que tem como objectivo apagar o rasto do "intruso".
Neste caso, a falência do sistema - o erro "blue screen of death", conforme já foi apelid
ado - está associada a um problema nas bibliotecas partilhadas...
```
~~~~~~~~

ABSTRACT

– – – – – – –

Kierkegaard escreveu que «todo o homem é uma excepção». Infelizmente, o que não é excepção é a frequência com que ocorrem estas falhas no sistema. Um indicador de que algo vai mal.
Um computador que vai abaixo, em média, 3 a 4 vezes ao dia – às vezes uma vez, às vezes cinco ou seis, raramente nenhuma – durante um dia de trabalho, não é normal. Com todo o prejuízo que isto implica no trabalho que o utilizador estava a realizar e que não fica gravado (pois que o sistema operativo desliga-se, tal e qual como se tivesse havido uma falha de energia eléctrica). Para além disto, há que considerar que estas interrupções abruptas de processos podem comprometer o correcto funcionamento do disco rígido do computador.

À falta de garantias de integridade do 'coração' do seu computador, pode ainda acontecer que o seu sistema operativo passe a iniciar em modo de linha de comandos ('DOS')!

Em todo este processo o utilizador tem de aguardar pacientemente ou impacientemente que o sistema recolha informações sobre o erro. Se somar tudo isto, o utilizador pode perder cerca de duas horas de trabalho por dia.

Adicionalmente, o sistema operativo passa a iniciar cada vez mais tarde. Isto é, desde o momento em que se liga o botão *power* do PC até que finalmente se apresente a interface gráfica pode demorar 17 minutos a abrir o computador!!

O utilizador pode questionar como é que tudo isto acontece num Sistema Operativo que diz ser eficiente, mas que se apresenta ser manifestamente ineficiente.

Se a explicação fosse assim 'tão simples' não se estaria a escrever este artigo.

Observações: Nunca a palavra de cabeçalho para este conteúdo "Abstract" esteve tão certa. E apela-se ao leitor que tenha algum sentido do abstracto.

E-mail de contacto: Qualquer apreciação crítica, contributo técnico ou testemunho poderá ser enviado para o e-mail forumsocial@o-musas.org

*ex-militar das Forças Armadas da Marinha de Guerra Portuguesa, com a especialidade de Radarista. Licenciada em Ciências da Informação e da Documentação pela Universidade Aberta.

Palavras-chave: Criminologia informática; Configurações ilegais; Estado Digital; Segurança da Informação; *data leak;* Microsoft hackers; Windows.

Estrutura-índice do artigo:

INTRODUÇÃO

_ _ _ _ _ _ _ _ _

Parte I - Corrupção informática

- **Pistas preliminares de *hacking***

Até se chegar a uma consciência crítica para podermos passar a questionar – Porquê que o sistema operativo havia de nos estar a enganar? – é preciso percorrer algum caminho de exploração. Ou seja, supervisionar o que é que o computador anda a fazer.

Nesta fase de análise inicial podemos considerar que *a tradição ainda é o que era*:

Três indicadores clássicos:

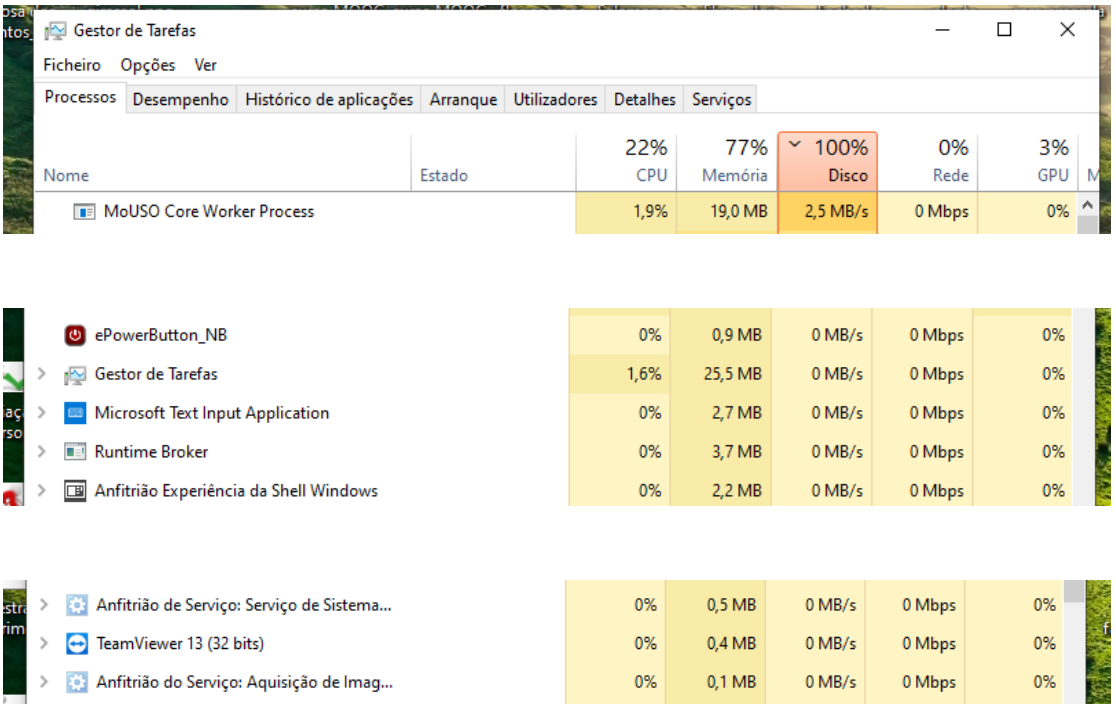
1 - Se o computador apresenta grande tráfego de rede sem que se esteja a trabalhar na internet, desconfie. Isso pode indicar um grande fluxo de transferência de dados, o que não é normal.

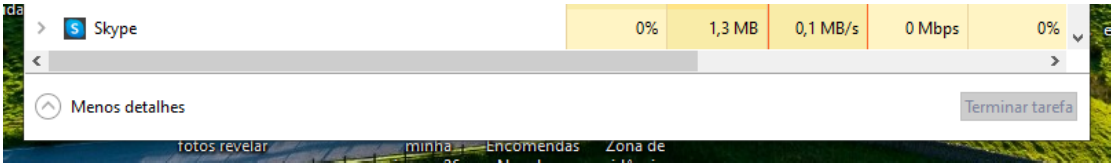
Para uma ligação por ethernet, o utilizador deverá verificar se, na parte detrás do router/modem, a luz de rede acende e desliga de forma intermitente.

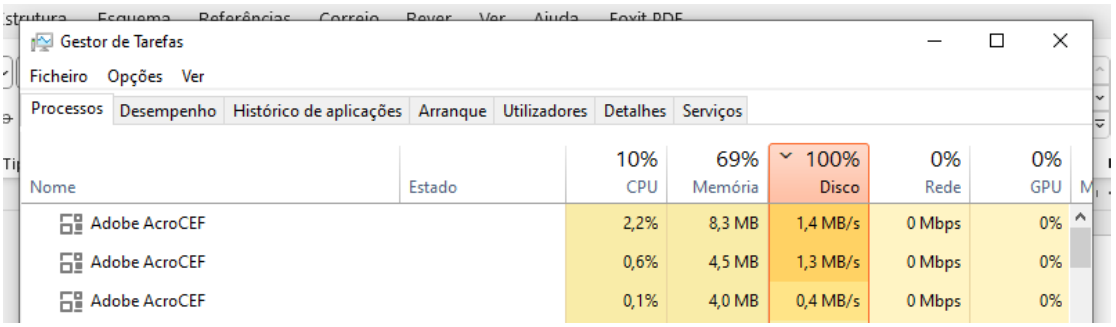
2 - Se em processos em segundo plano existem aplicações regularmente abertas que o utilizador não utiliza há décadas, desconfie ainda mais. Aplicações do tipo: Team Viewer; Skype; Programas de OCR – Optical Character Recognition (útil para ler ficheiros protegidos); Text input application, etc.

3 - Se o computador passa a estar a trabalhar sempre com o disco nos 100%, e este valor nunca desce, e, pressupondo que o disco é um disco saudável, também não é nada normal. O utilizador deve ponderar bem a possibilidade de o seu computador já estar a ser 'invadido'.

Importa salientar que é importante estar atento a estes 'detalhes' para que se possa prevenir o pior.







● Team Viewer - [programa que permite ligação remota e acesso directo a outro computador]
● Skype [programa adquirido pela Microsoft e que, na sua versão original, permite comunicação síncrona streaming via webcam]

****

NO TEXTO QUE SE SEGUE CONTINUAMOS A NOSSA VIAGEM EXPLORATÓRIA AO UNIVERSO DO COMPUTADOR, TAL COMO FARIA CARL SAGAN COM A SONDA VOYAGER NA SUA MAGNÍFICA OBRA COSMOS.

****

- **Telemetria e AI (artificial intelligence)**

Se o utilizador tiver um olhar atento, irá eventualmente encontrar no seu computador um conjunto de outras situações que poderão suscitar questões, dúvidas, interrogações, suspeitas: - “O que é isto?”.

#utilizador n.º 1

Fig. 6

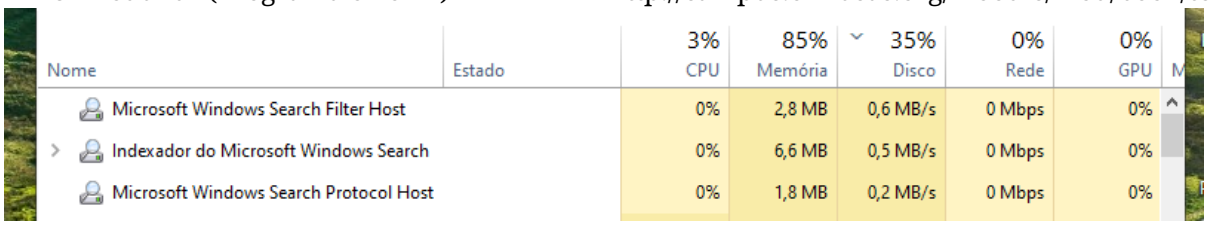


Fig. 7 - Ambiente Windows - Aplicação AI (Artificial Intelligence) associada aos ficheiros sempre que se abre um documento e “print driver host for appplications” sem que se tenha solicitado nenhuma impressão:

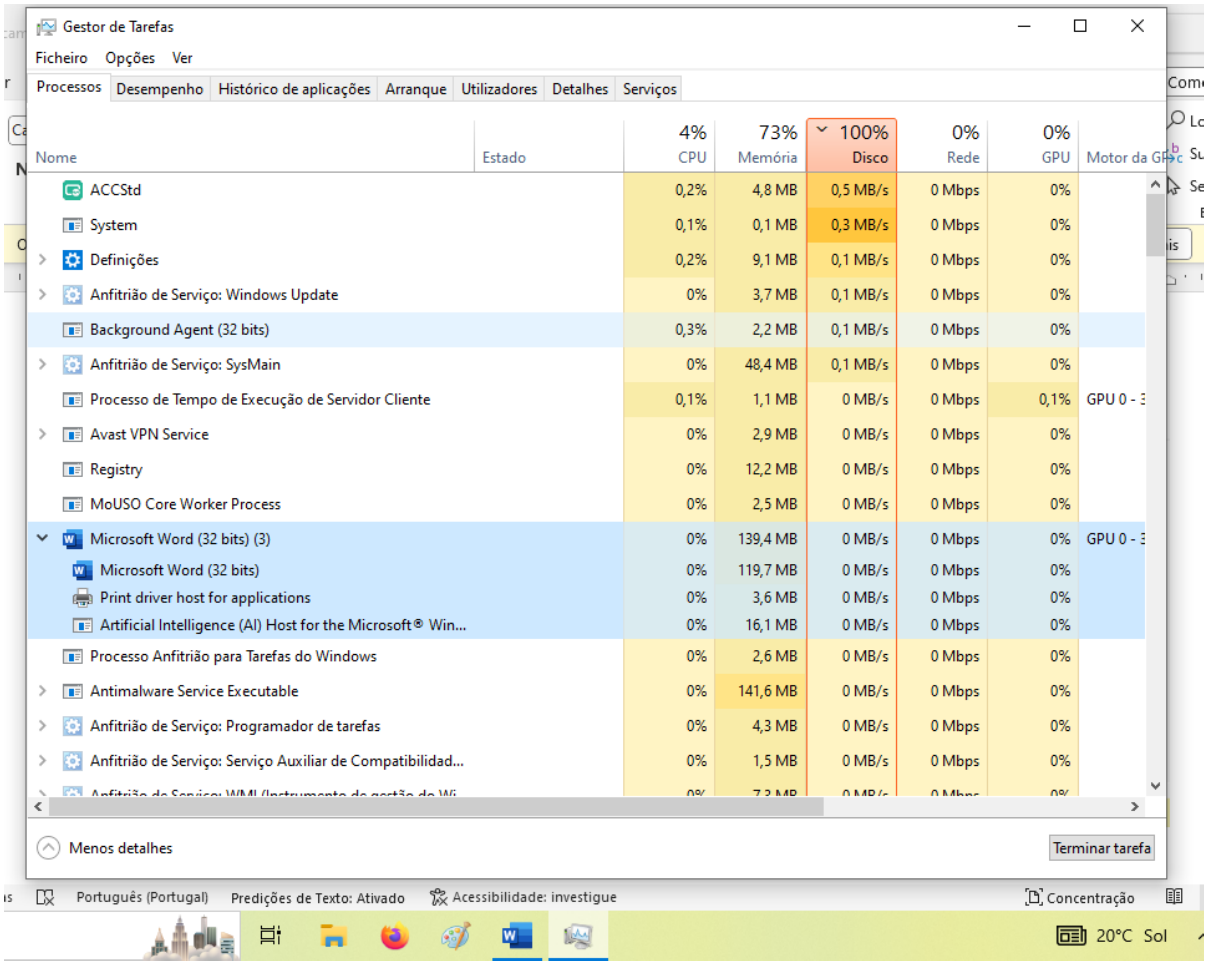
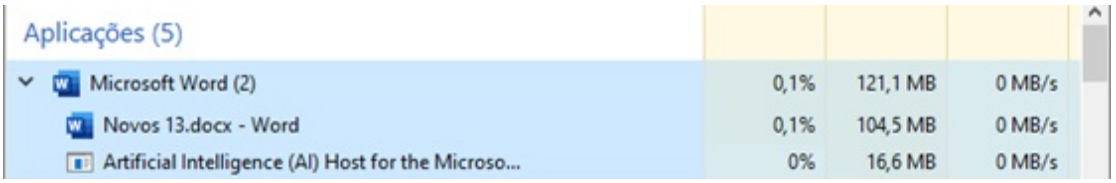
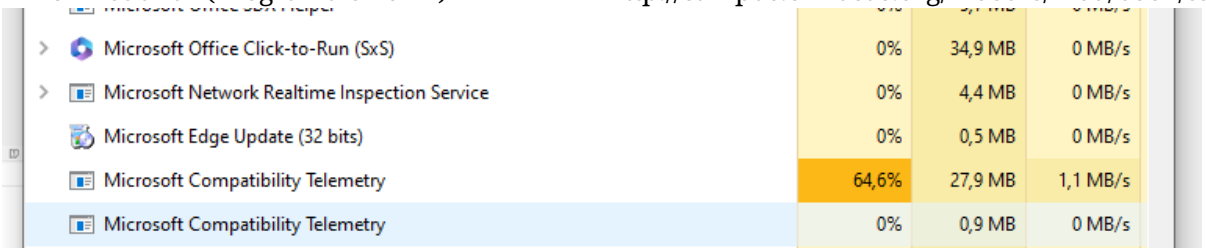


Fig. 8



Pode-se definir a "aprendizagem da máquina" como o "campo de estudo que dá aos computadores a habilidade de aprender sem serem explicitamente programados". (Arthur Samuel, 1959)

Fig. 9



#utilizador n.º 2

Fig. 10

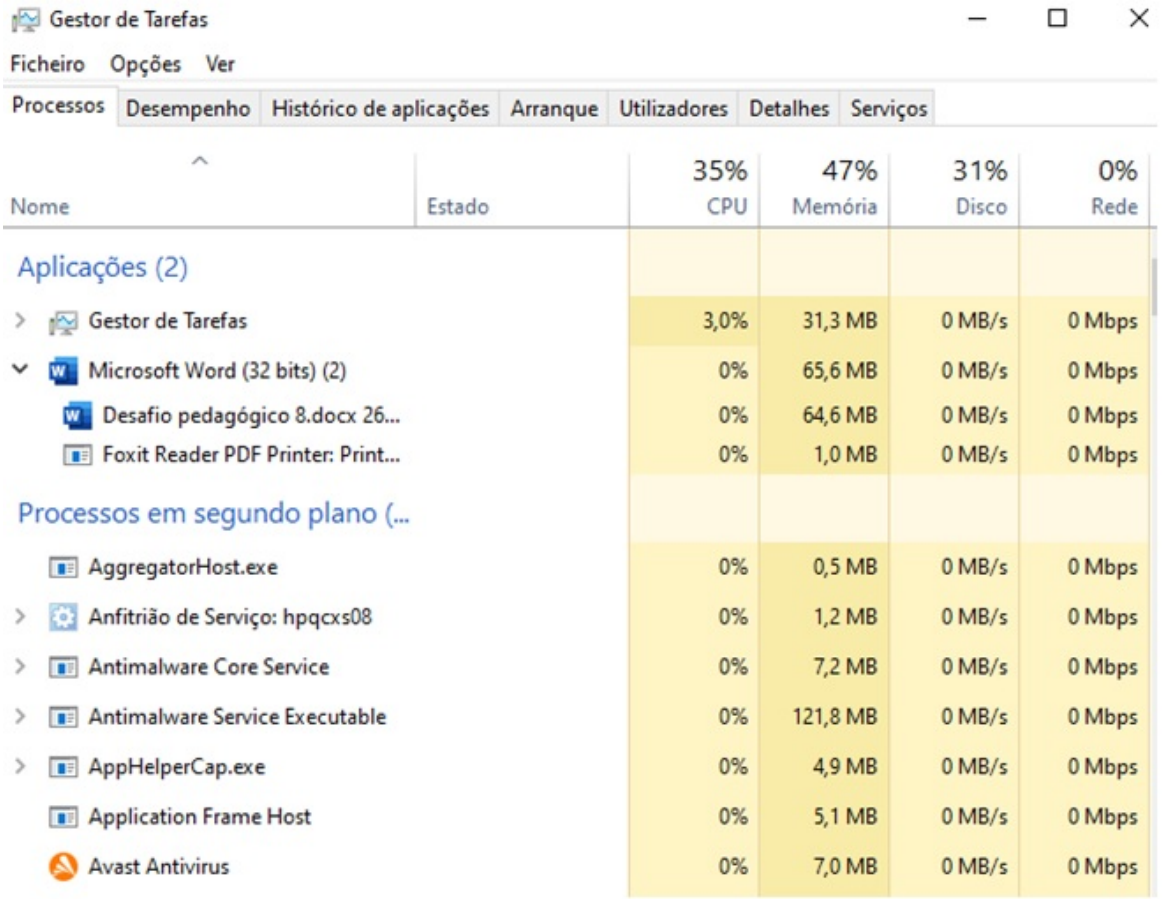


Fig. 11

Gestor de Tarefas

Ficheiro Opções Ver

Processos | Desempenho | Histórico de aplicações | Arranque | Utilizadores | Detalhes | Serviços

Nome	Estado	37% CPU	51% Memória	98% Disco	0% Rede	1% GPU	Motor da GPU
BridgeCommunication.exe		0%	4,2 MB	0 MB/s	0 Mbps	0%	
BridgeCommunication.exe		0%	3,8 MB	0 MB/s	0 Mbps	0%	
Carregador do CTF		0,2%	3,8 MB	0 MB/s	0 Mbps	0%	
COM Surrogate		0%	2,5 MB	0 MB/s	0 Mbps	0%	
COM Surrogate		0%	1,4 MB	0 MB/s	0 Mbps	0%	
Device Association Framework ...		0%	0,9 MB	0 MB/s	0 Mbps	0%	
DiagsCap.exe		0%	7,6 MB	0 MB/s	0 Mbps	0%	
Dropbox Update (32 bits)		0%	0,1 MB	0 MB/s	0 Mbps	0%	
Gestor de audio de alta definica...		0%	2,0 MB	0 MB/s	0 Mbps	0%	
Google Chrome		0%	57,1 MB	0,1 MB/s	0 Mbps	0%	
Google Chrome		0%	8,3 MB	0 MB/s	0 Mbps	0%	
Google Chrome		0%	12,2 MB	0 MB/s	0,1 Mbps	0%	
Indexador do Microsoft Windo...		0%	6,5 MB	0 MB/s	0 Mbps	0%	
Início		0%	21,7 MB	0 MB/s	0 Mbps	0%	
Microsoft Compatibility Teleme...		0%	1,4 MB	0 MB/s	0 Mbps	0%	
Microsoft Compatibility Teleme...		0,6%	15,6 MB	0,2 MB/s	0 Mbps	0%	
Microsoft Compatibility Teleme...		0%	0,2 MB	0 MB/s	0 Mbps	0%	
Microsoft Edge		0%	5,8 MB	0 MB/s	0 Mbps	0%	

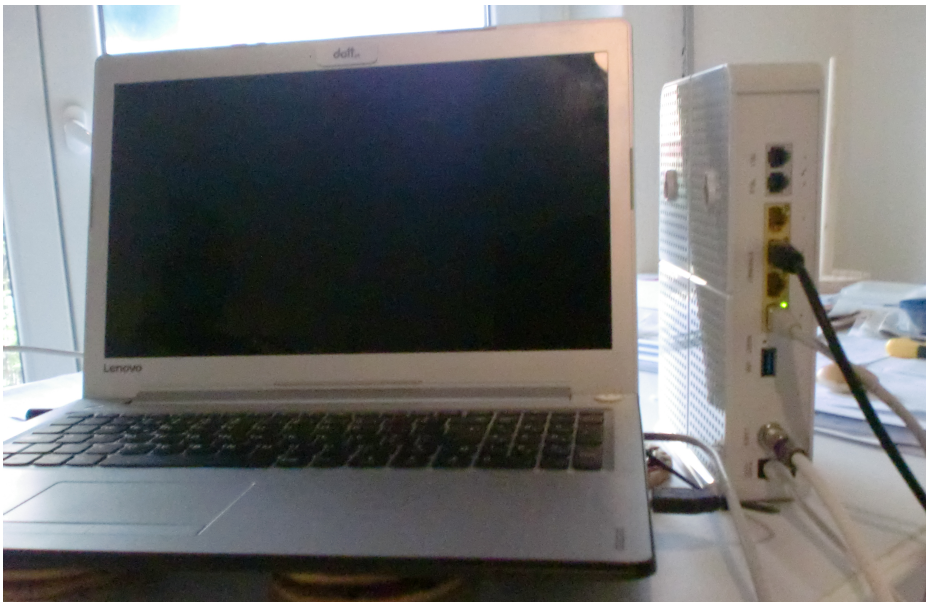
Qualquer modelo de inteligência artificial é feito com base em dados, informação e conhecimento. Para esse fim é necessário alimentar um *Data Warehouse* (armazém de dados) para promover a aprendizagem da máquina.

- **Anomalias**

“Anomalias”, chamemos-lhe assim. Neste caso, a anomalia que apresentamos não obedece à *tradição*. É algo completamente novo.

Há uma luz que você vê brilhar ao longe. Mas não se trata da estrela Sirius nem do planeta Vénus. É mesmo a luz *led* da sua rede de ethernet que permanece acesa quando o computador está desligado!
[cabo ethernet cinza claro]

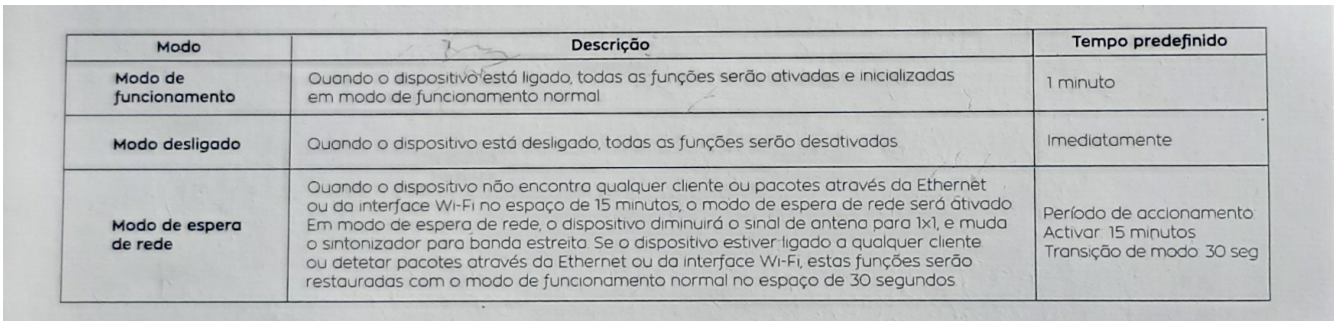
Fig. 12



- computador desligado com ligação à internet -

Instruções do router/modem:

Fig. 13



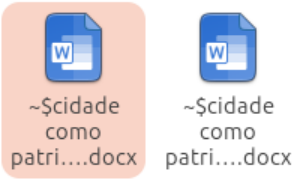
Modo	Descrição	Tempo predefinido
Modo de funcionamento	Quando o dispositivo está ligado, todas as funções serão ativadas e inicializadas em modo de funcionamento normal	1 minuto
Modo desligado	Quando o dispositivo está desligado, todas as funções serão desativadas	Imediatamente
Modo de espera de rede	Quando o dispositivo não encontra qualquer cliente ou pacotes através da Ethernet ou da interface Wi-Fi no espaço de 15 minutos, o modo de espera de rede será ativado Em modo de espera de rede, o dispositivo diminuirá o sinal de antena para 1x1, e muda o sintonizador para banda estreita Se o dispositivo estiver ligado a qualquer cliente ou detetar pacotes através da Ethernet ou da interface Wi-Fi, estas funções serão restauradas com o modo de funcionamento normal no espaço de 30 segundos	Período de accionamento Activar 15 minutos Transição de modo 30 seg

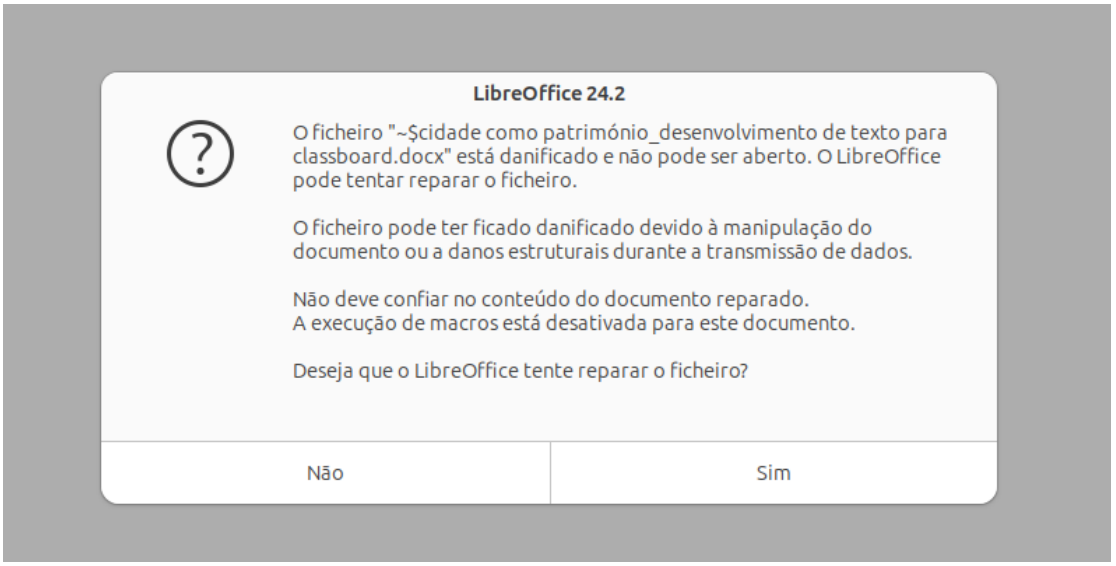
- **Tampering de *drives*** [numa pen]

```
- "Tampering" (do Inglês): Defeito deliberado causado num equipamento com o objectivo de comprometer a sua segurança e correcto funcionamento.
```

Para aumentar ainda mais as suas preocupações, coisas estranhas começam a acontecer na sua *pen* que já o estão a deixar num estado de nervos.

Ficheiros propositadamente danificados, seguido de uma mensagem muito subtil na aplicação Word: "carregue os seus documentos para a Cloud":



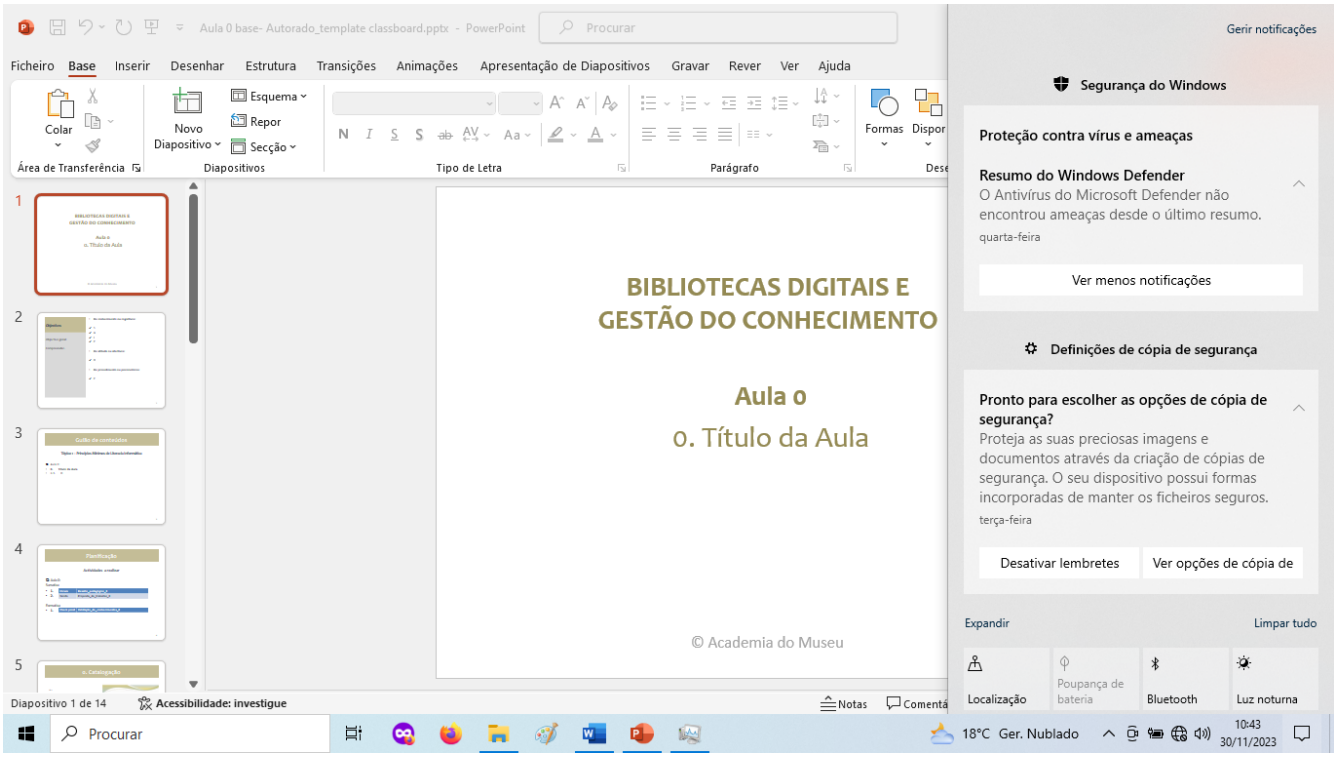


- Ficheiros danificados causado pelo tampering de drives (*pen*) no computador do utilizador:

ficheiros com til e cifrão -

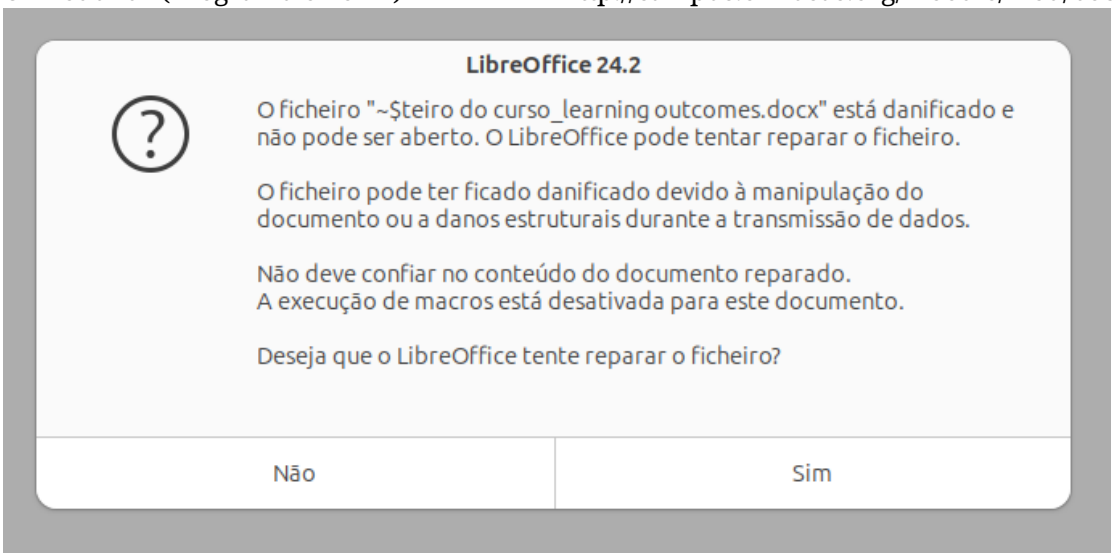
Sempre que se tenta remover a *pen* do sistema Windows, esta acusa um erro, apesar de se ter seguido o método seguro para remoção da *pen*.

Independentemente das preocupações do utilizador, este pode realizar uma inspecção mais aprofundada ao seu dispositivo, mas receberá sempre a mesma mensagem:
"*O seu computador foi analisado 7 vezes e não encontrou nenhuma ameaça.*"!



"O antivírus do Microsoft Defender não encontrou ameaças desde o último resumo."

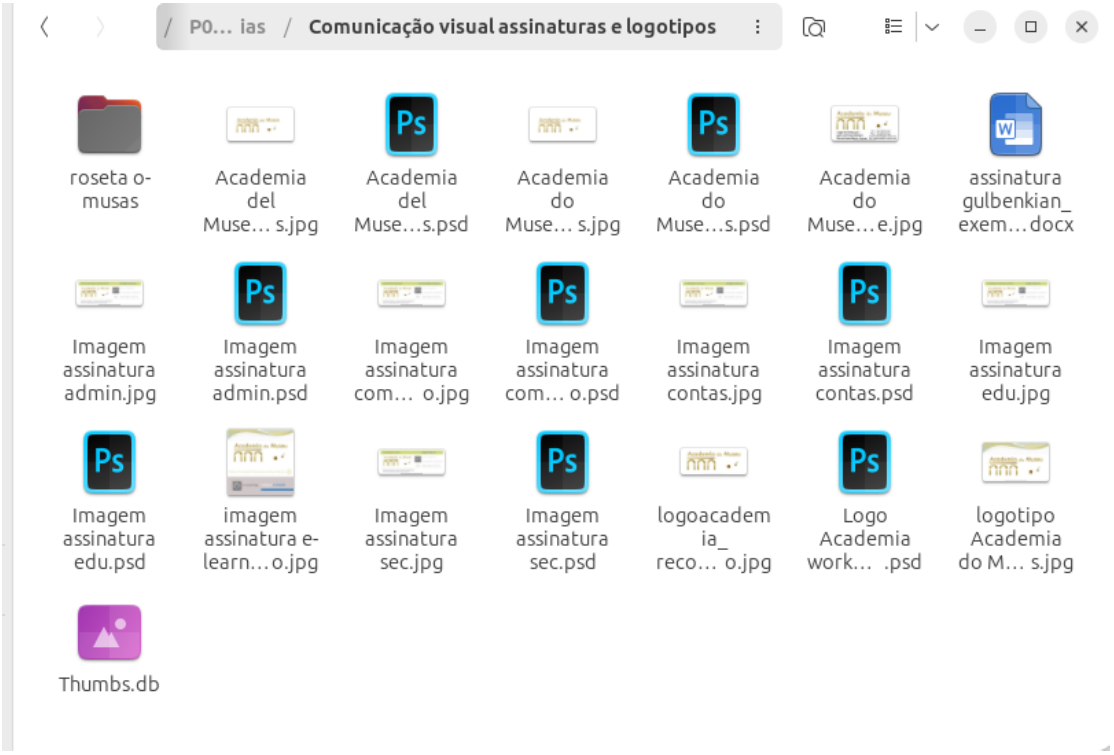
- *O seu computador está a funcionar lindamente!* Não tem nenhuma ameaça. -



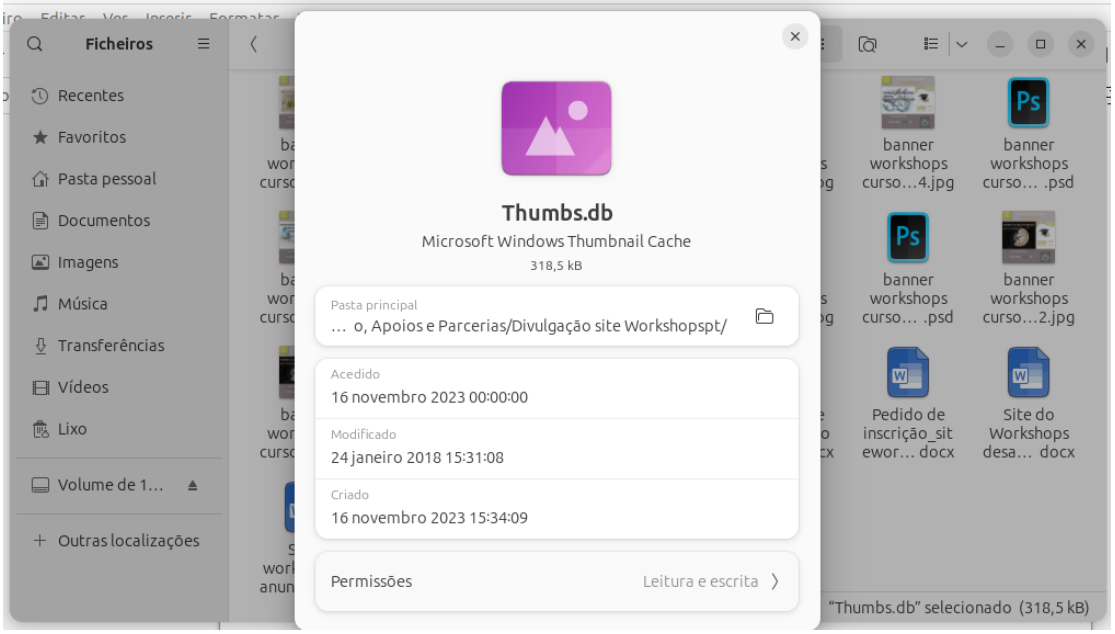
De facto, muitos ficheiros da *pen* começam, de repente, a aparecer danificados... são dezenas de ficheiros. Isto acontece porque, por um lado, o dispositivo nunca se desliga em absoluto quando é retirado (tem o processo AI pendente e ligado aos documentos), mas também porque existe uma intenção propositada para que os mesmos fiquem danificados.

(ficheiros obliterados - imagens)

Também poderá ser de todo o interesse do utilizador inspeccionar as suas drives (*pen*; disco externo) e procurar pela existência de ficheiros do tipo "thumbs.db".



Em todas as pastas começam a aparecer estes ficheiros Thumbs.db



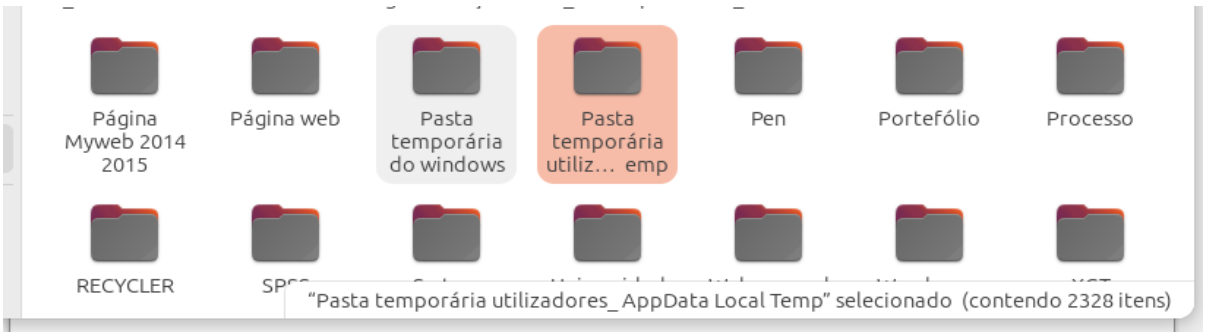
Importa tentar perceber qual o conteúdo exacto destes ficheiros .db (*data base format*).

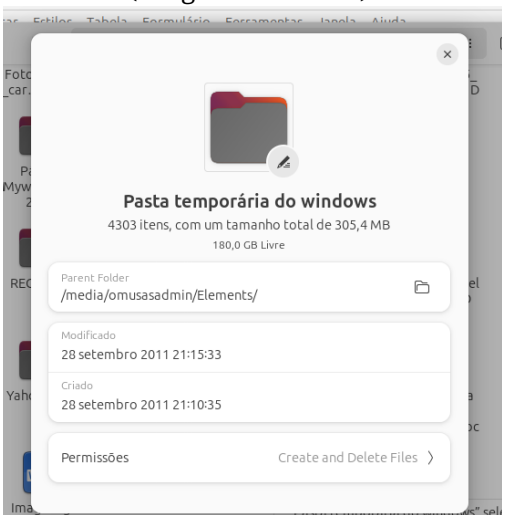
- **Backdoor** [num disco externo]

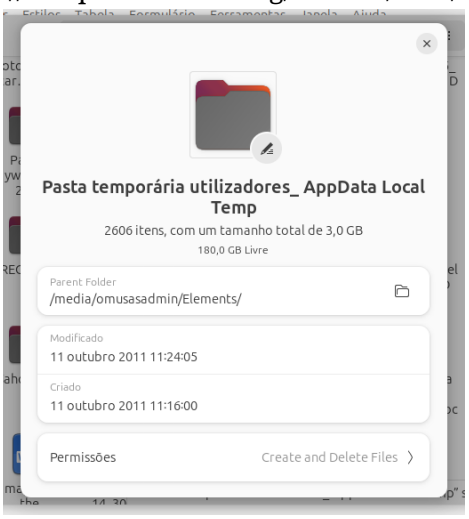
```
- “Backdoor” (do Inglês): Programa(s) implementado secretamente num computador, o qual po
de ter vários objectivos, tais como, obter informações e dados armazenados.
```

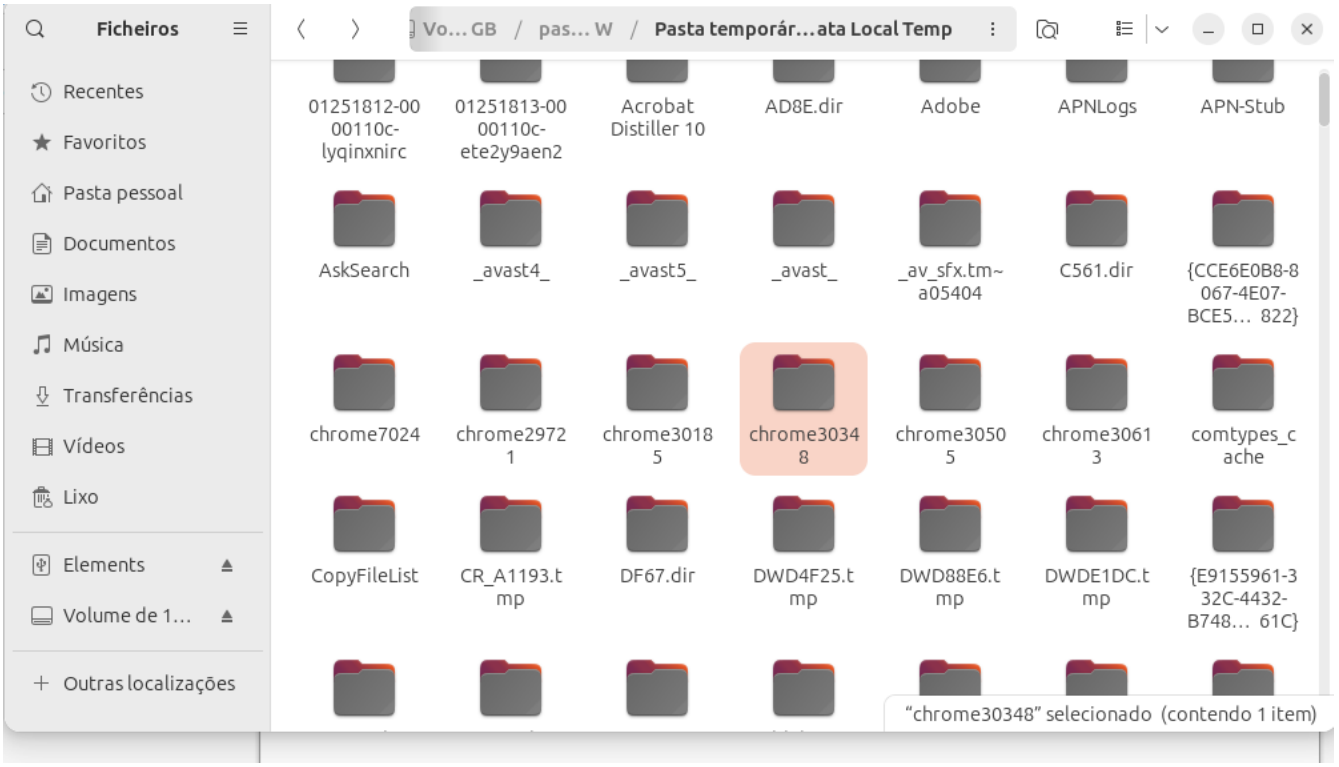
Se o utilizador não sabe o que são as pastas temporárias do Windows, não é nada disto que vai ver a seguir.
As antigas pastas temporárias do Windows ficavam localizadas num directório um pouco escondido, mas ainda assim acessível, em \AppData Local temp. Esta pasta acumulava ficheiros temporários não necessários, com extensão .tmp, e era preciso apagar alguns deste ficheiros de forma manual (isto porque o disco rígido ficava cheio - sem espaço disponível para gravação - sem se perceber bem porquê... Com o computador sempre no "red line" nem memória virtual há para se poder fazer uma transferência ftp).

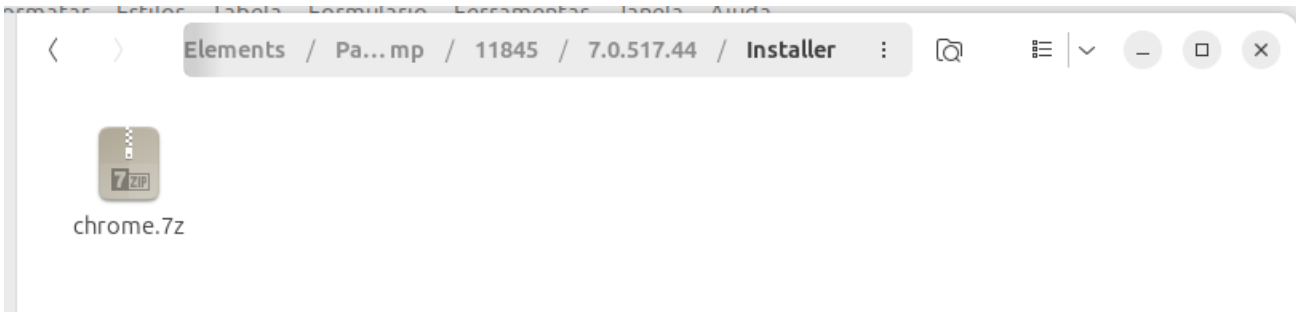
As novas pastas temporárias do Windows estão ainda mais escusas (ocultas) e acumulam outras funções, agora na forma de Backdoor [instaladas num disco externo]. E têm este aspecto:




Pasta temporária do windows
4303 itens, com um tamanho total de 305,4 MB
180,0 GB Livre
Parent Folder
/media/omusasadmin/Elements/
Modificado
28 setembro 2011 21:15:33
Criado
28 setembro 2011 21:10:35
Permissões
Create and Delete Files


Pasta temporária utilizadores_ AppData Local Temp
2606 itens, com um tamanho total de 3,0 GB
180,0 GB Livre
Parent Folder
/media/omusasadmin/Elements/
Modificado
11 outubro 2011 11:24:05
Criado
11 outubro 2011 11:16:00
Permissões
Create and Delete Files


Ficheiros
Recentes
Favoritos
Pasta pessoal
Documentos
Imagens
Música
Transferências
Vídeos
Lixo
Elements
Volume de 1...
Outras localizações
Vo... GB / pas... W / Pasta temporár...ata Local Temp
01251812-00 00110c-lyqinxnirc
01251813-00 00110c-ete2y9aen2
Acrobat Distiller 10
AD8E.dir
Adobe
APNLogs
APN-Stub
AskSearch
avast4
avast5
avast
_av_sfx.tm~ a05404
C561.dir
{CCE6E0B8-8 067-4E07-BCE5... 822}
chrome7024
chrome2972 1
chrome3018 5
chrome3034 8
chrome3050 5
chrome3061 3
comtypes_c ache
CopyFileList
CR_A1193.t mp
DF67.dir
DWD4F25.t mp
DWD88E6.t mp
DWDE1DC.t mp
{E9155961-3 32C-4432-B748... 61C}
"chrome30348" selecionado (contendo 1 item)

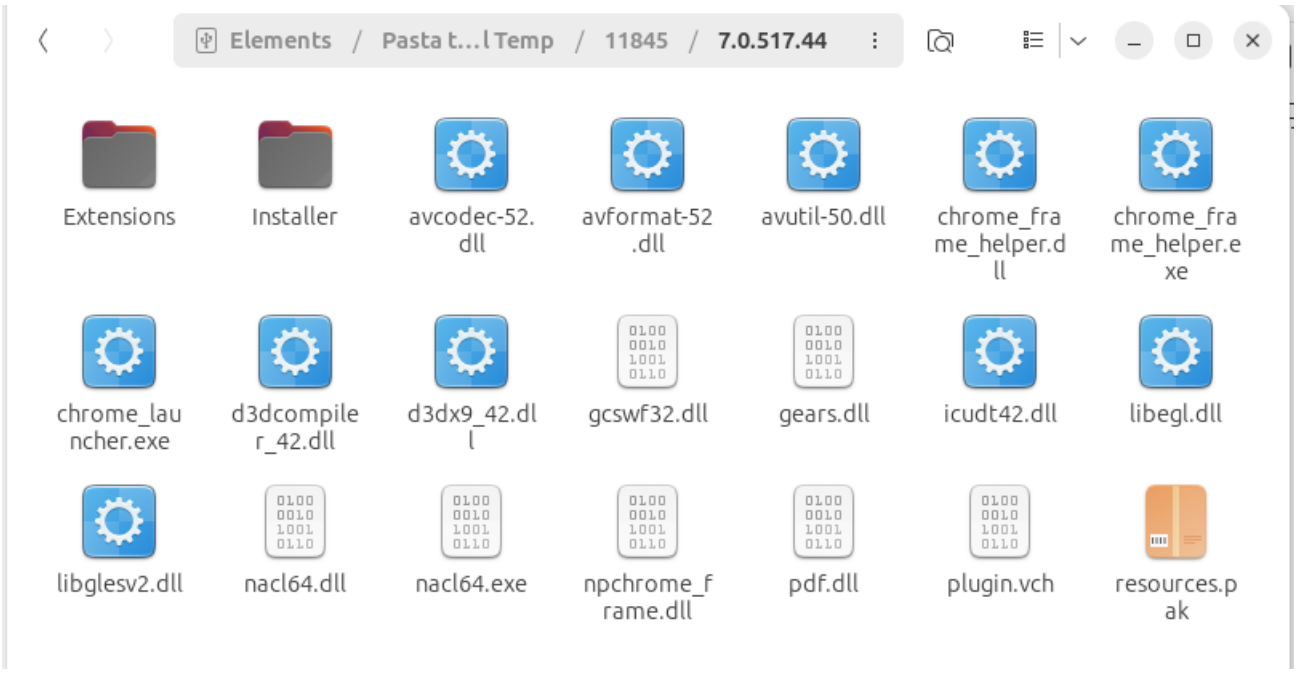

Elements / Pa... mp / 11845 / 7.0.517.44 / Installer
chrome.7z


Elements / Pasta tempor... ta Local Temp / 11842
chrome.dll

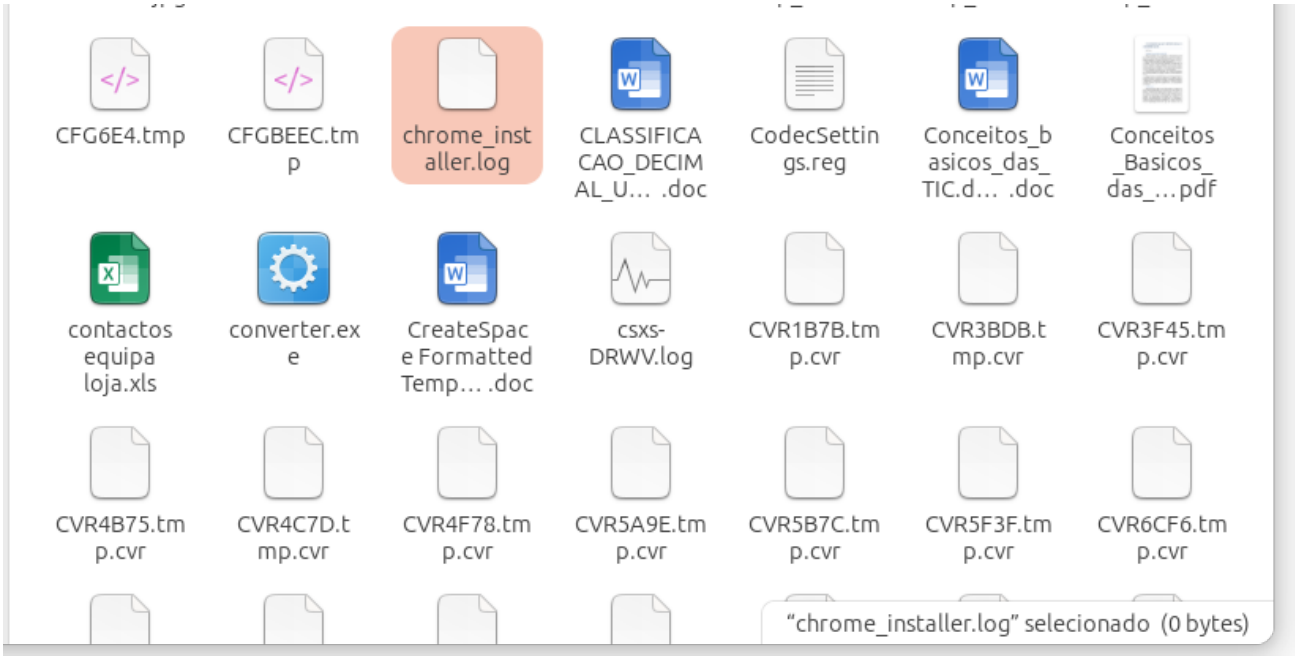
- Asksearch – motor de busca
- Chrome – browser de navegação da Google (chrome 7 zip, chrome dll)

Pasta intitulada "CopyFileList"

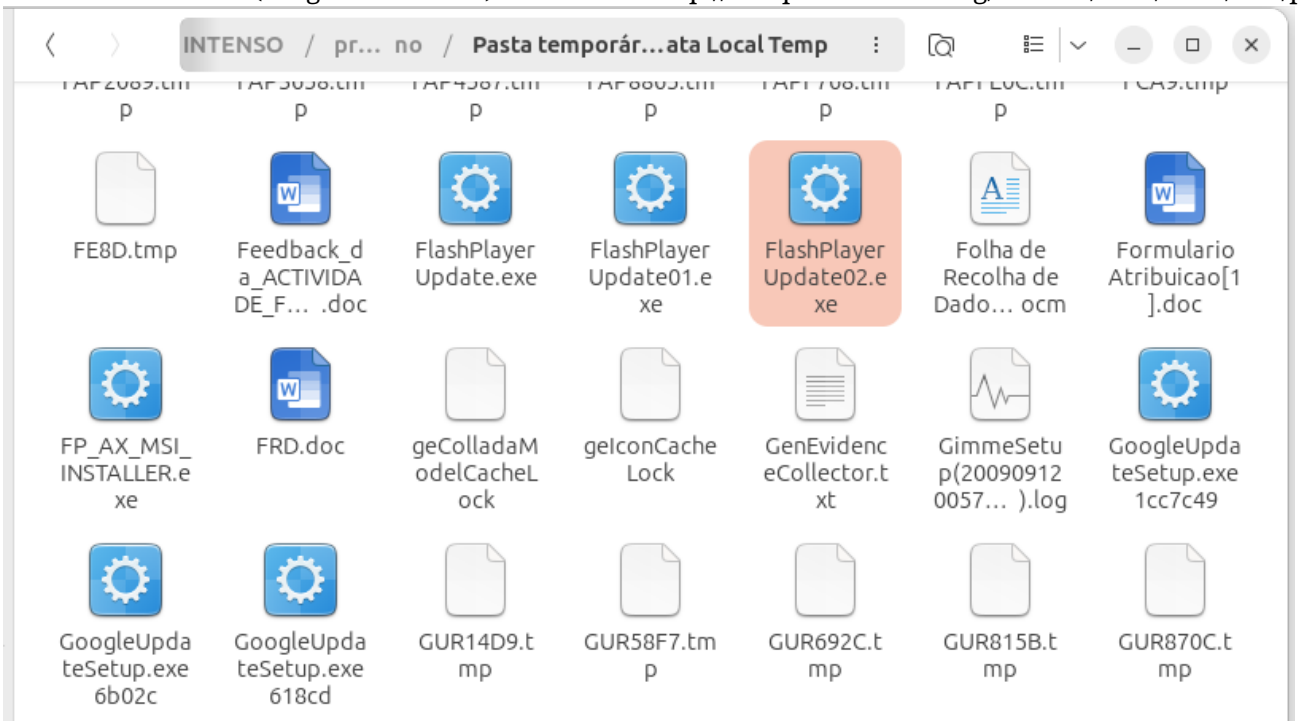
Chrome_launcher.exe e Avast dll



converter.exe



flash player exe



extensões externas json (semelhante à compilação de dados em XML - legível por máquina e por humanos)

(....)

- **Descrição iconográfica e leitura iconológica de um "print screen"**

Para analisar este tópico vamos pedir alguma ajuda ao campo da Arte.

◙ Serviço de Firewall do Windows no modo No Network FireWall!

Continuamos interessados em saber o que é que se passa com o nosso computador.

Questionamos a um funcionário de uma loja de informática se sabe o que é que são aqueles "processos AI pendurados" nos nossos documentos do Word, Powerpoint, etc. A resposta do funcionário é a seguinte:
- *«São coisas que o Windows **precisa para funcionar**.»* ... - muito esclarecedor.

Questionamos a outra pessoa, agora formada em informática e professor de informática, se sabe o que é que significa o processo LocalServiceNoNetworkFirewall. A resposta que obtivemos é a seguinte:
- *«O serviço mpssvc (localservicenonetworkfirewall) é um serviço utilizado pela firewall do windows defender. **Estar em execução é bom sinal.**»*

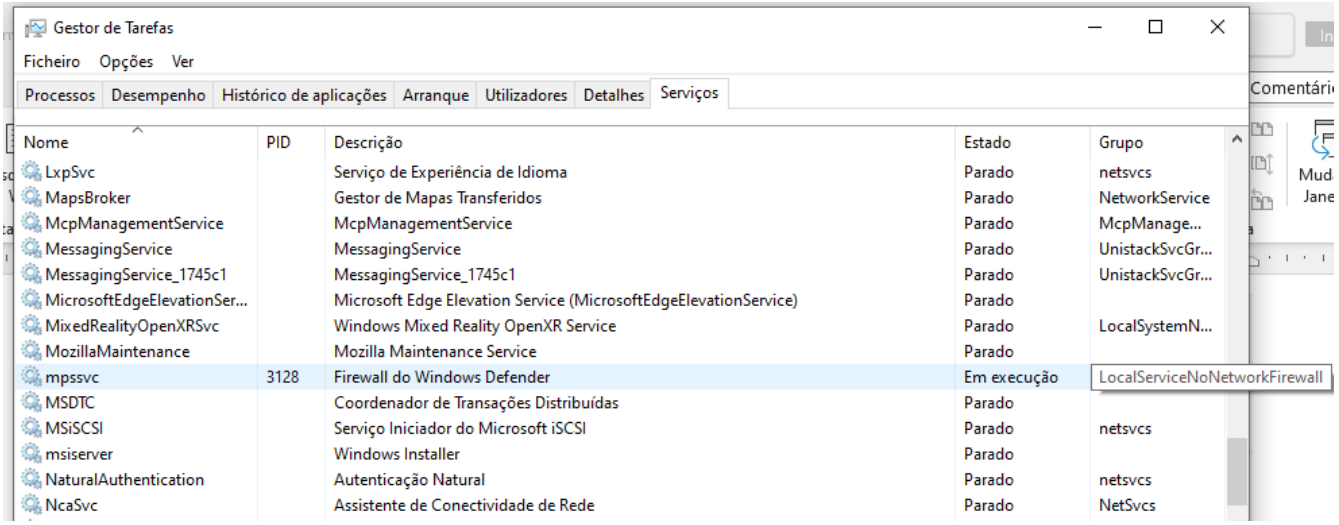
Agora, questionamos uma terceira pessoa, que pouco ou nada percebe de informática, se sabe o que é que significa No Network Firewall e que observe o printscreen que abaixo apresentamos.

Na ausência de referenciais de conhecimento do campo da Informática, esta pessoa irá focar-se no significado literal da palavra/s.
- *"No Network Firewall" significa que* ***a internet está desprovida (não tem) Firewall activa!***

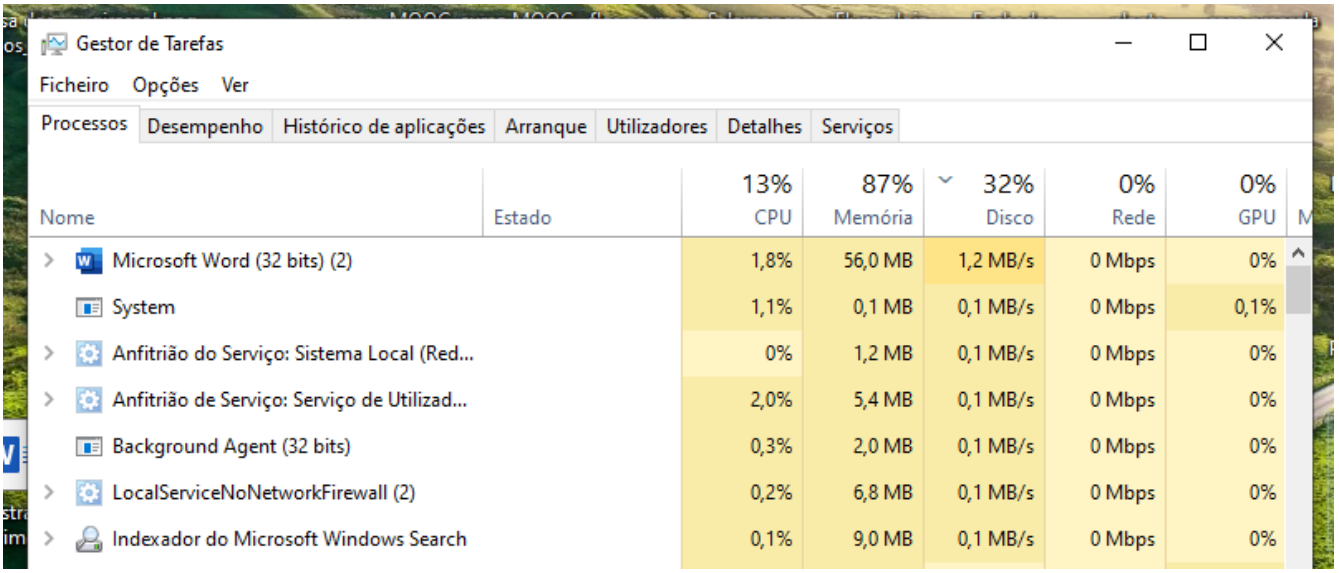
(...)

Os primeiros dois casos correspondem a uma leitura iconológica; e o terceiro corresponde a uma descrição iconográfica daquilo que é observado.

(...)

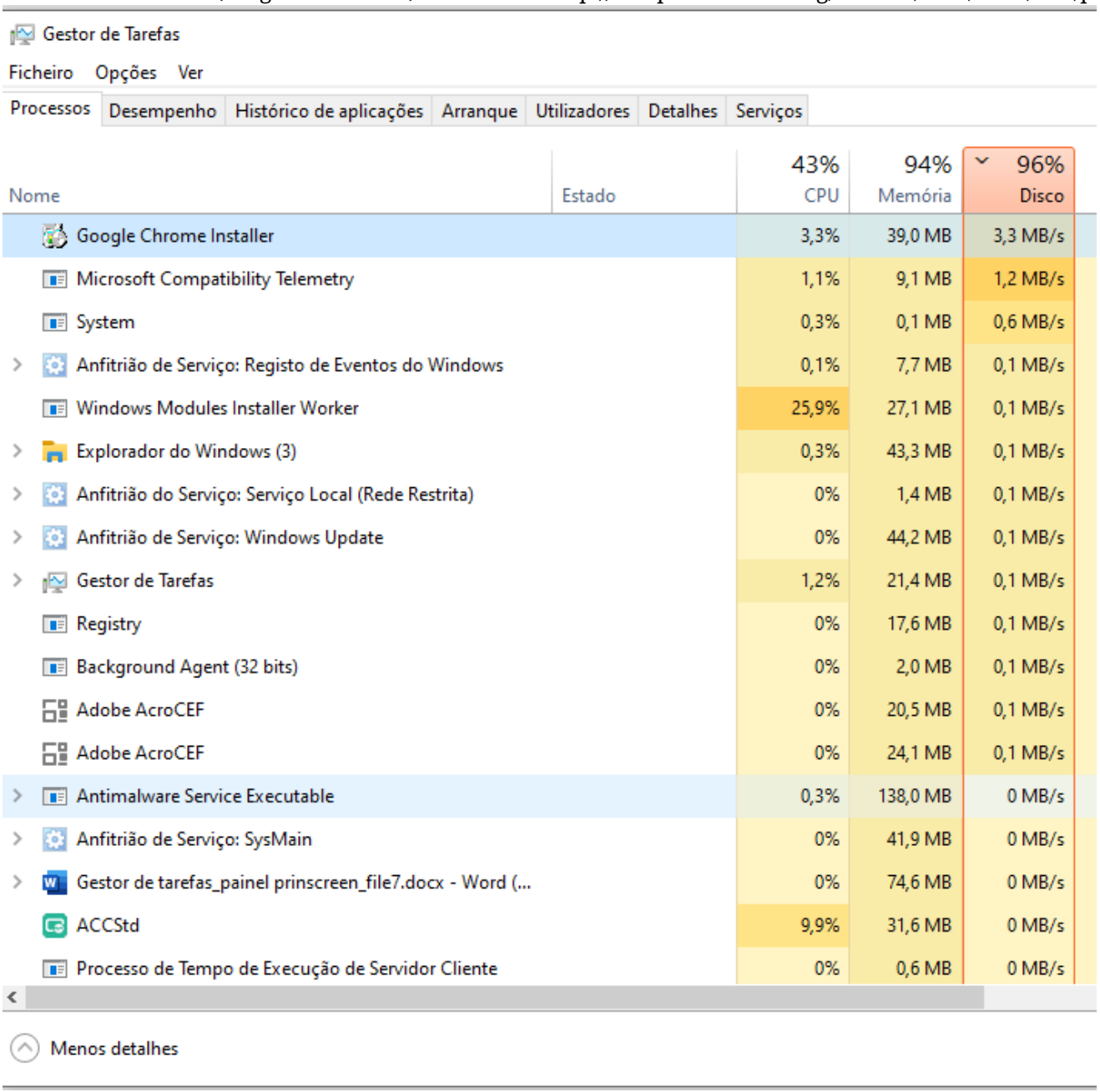


No Network Firewall:



- **Alienação de Software**

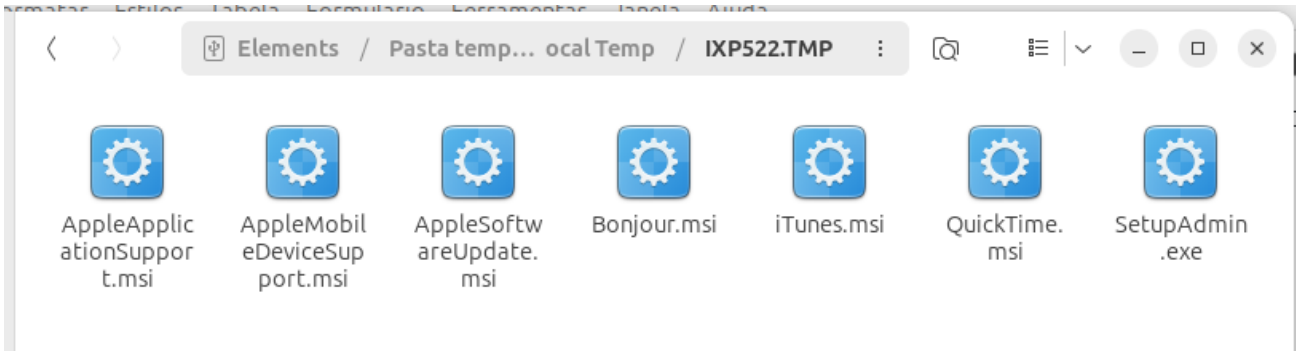
O Windows corre a instalação, por iniciativa própria, do instalador do Google Chrome:



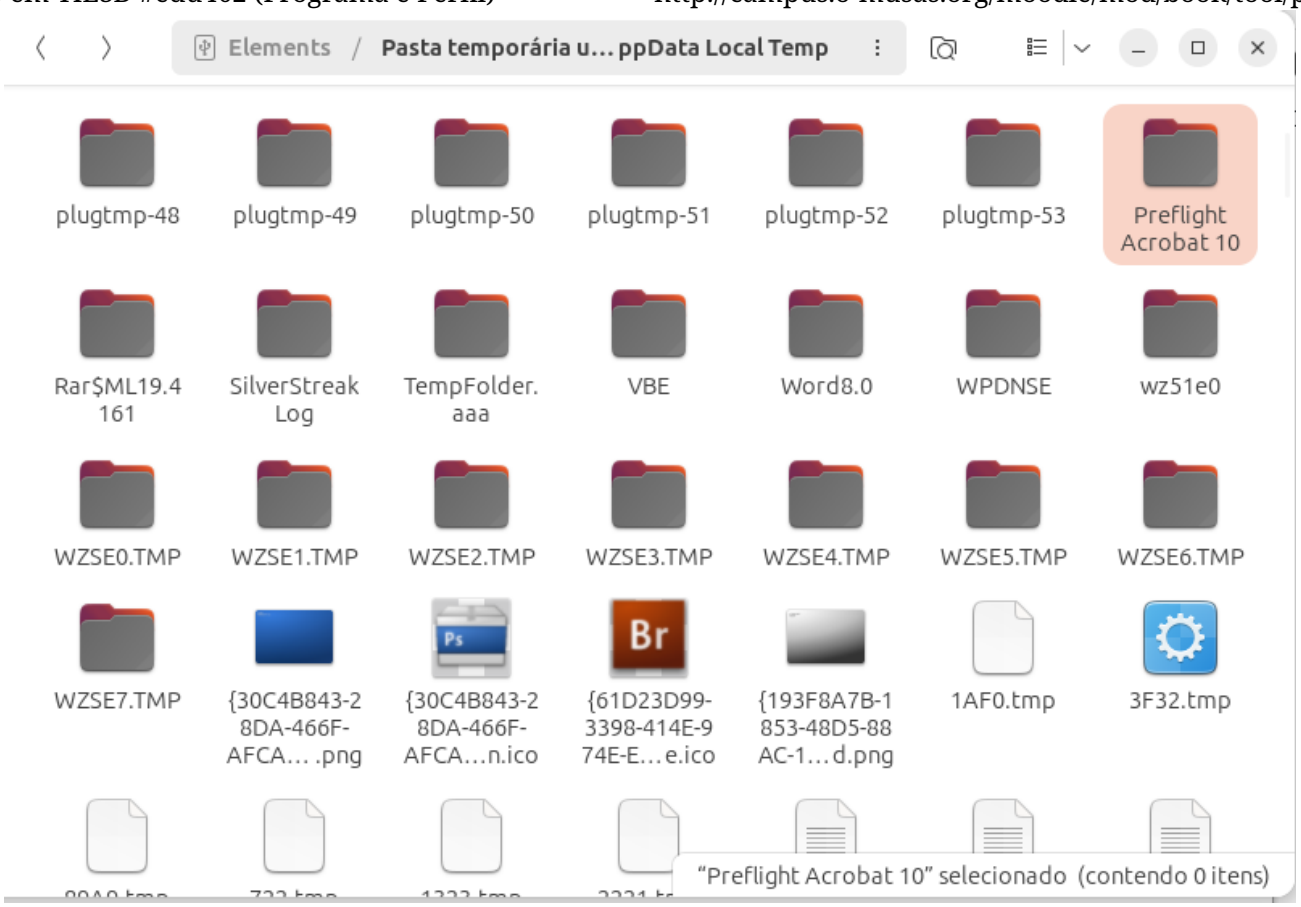
Utilização/apropriação de software de outras entidades, para além da Google há a Apple:
(Apple software; iTunes; Quicktime; Bonjour; Apple Mobile)

[Recordamos que todos este programas de execução estão instalados em pastas num disco externo.]

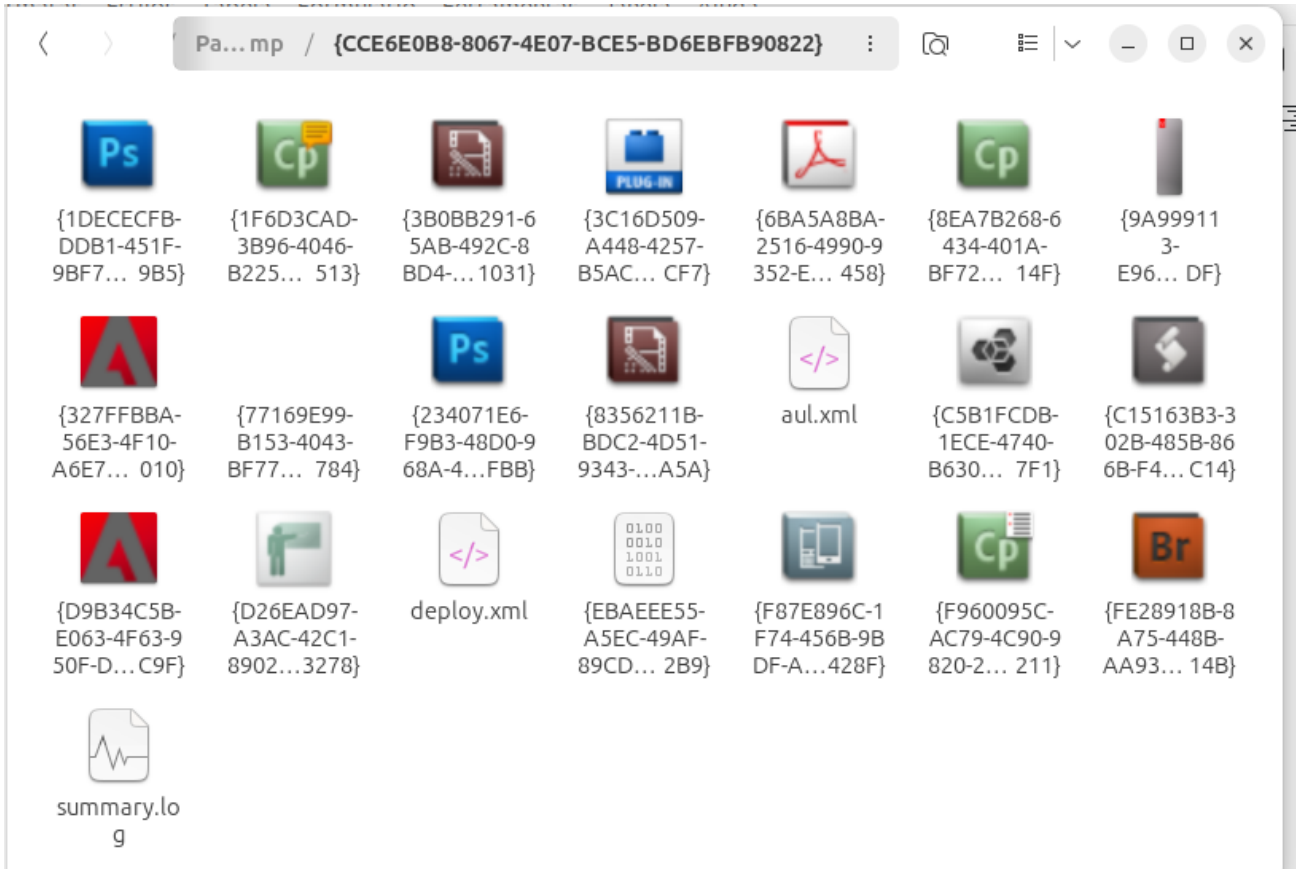
Desde logo não pode haver programas de execução e/ou de actualizações, ao nível da aplicação, instalados sem a autorização do utilizador (muito menos num disco externo... em "pastas temporárias" inacessíveis do Windows. Ver-se-á que todos estes programas destinam-se a diversos fins.)



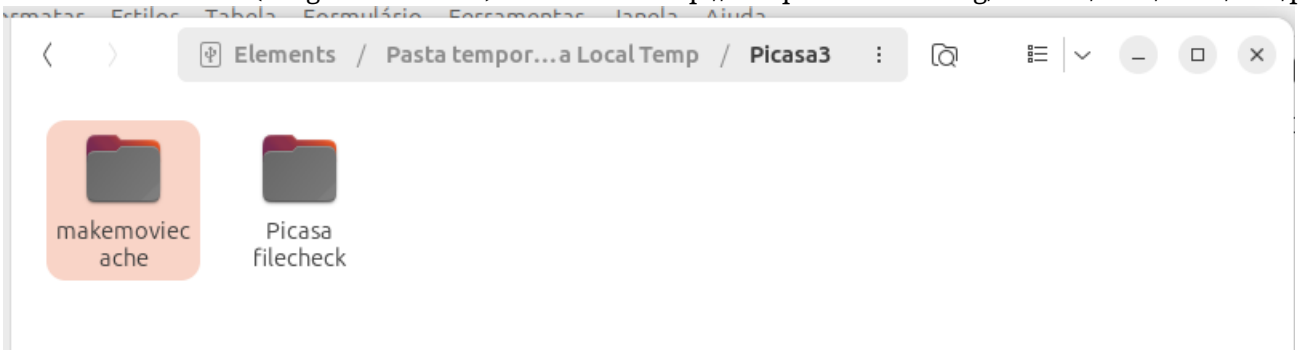
Acrobat



linhas de código para Photoshop; Movie maker, etc.

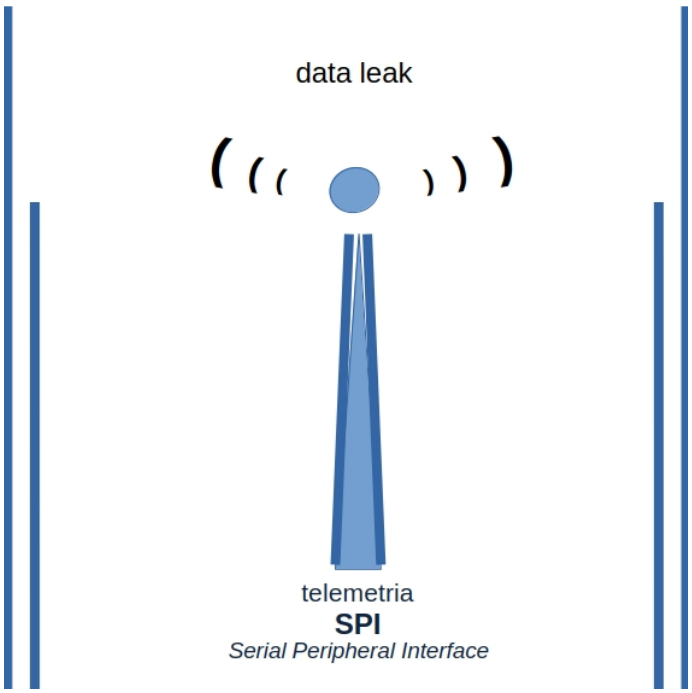


Picasa file check; Make movie cache:

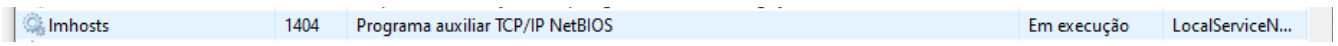


- **Conflitos de interesses**

Uma empresa não pode querer fornecer e vender informação (motor de busca Bing e tecnologia IA com chat GPT – que actualmente já é preciso pagar se quisermos uma resposta mais desenvolvida), e, simultaneamente, garantir a segurança, salvaguarda, sigilo e integridade da informação dos computadores dos utilizadores.
É óbvio que há, desde logo, um conflito de interesses subjacente.



- Protocolo de chamada SPI (antena) -
SPI - Serial Peripheral Interface - *de facto* standard para comunicações síncronas (protocolo não oficial – não regulamentado).

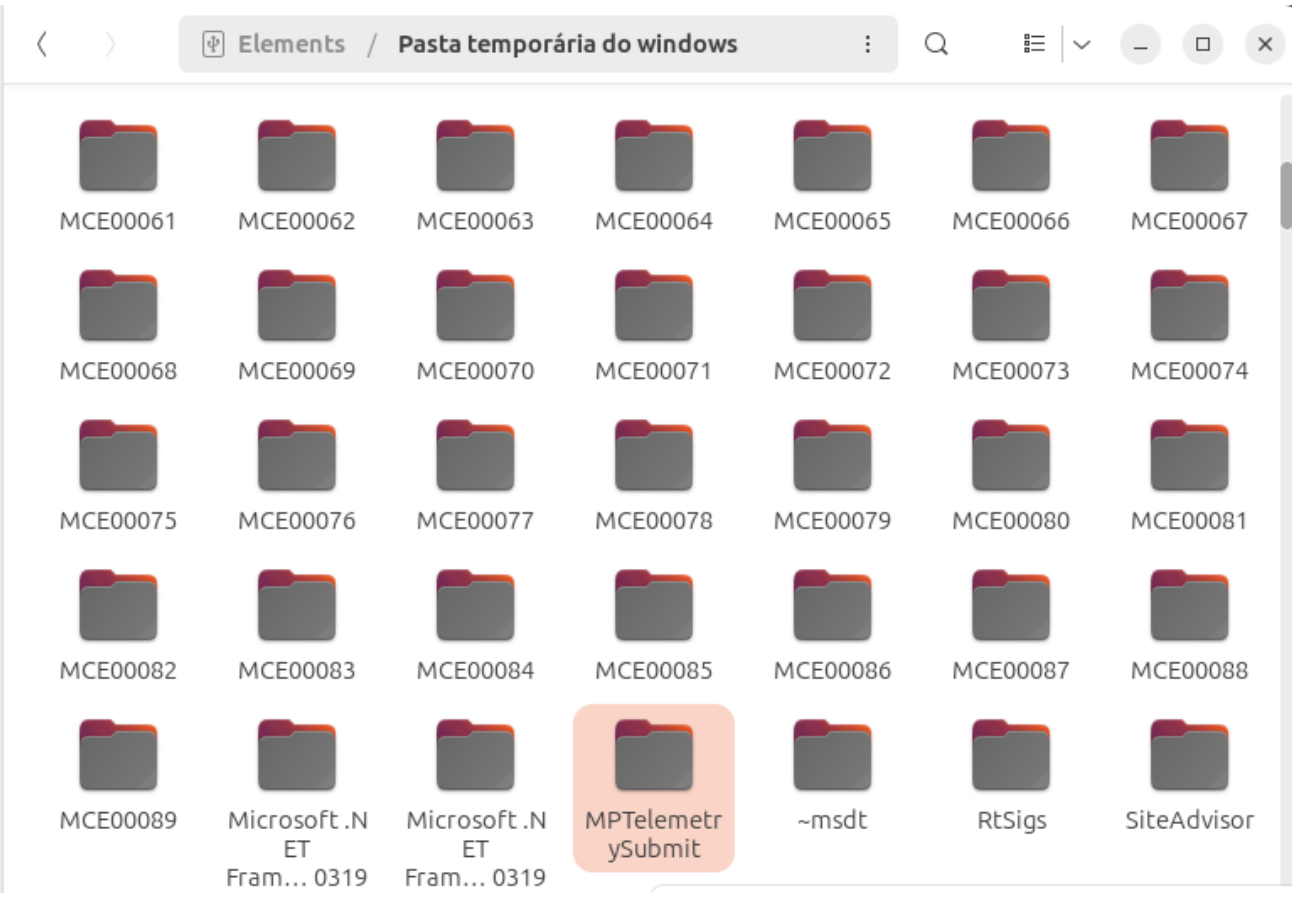


Rede Net BIOS

Um canal de comunicação (SPI) que, em teoria, deveria servir apenas para "efectuar chamadas de emergência" de forma remota é utilizado em contínuo para saída de dados a "conta-gotas" (telemetria está sempre ligada no computador do utilizador. O som que este sinal produz é algo semelhante a um sinal de fax, e é omnipresente. Pode ser ouvido em qualquer zona do território. Os dados que saem por esta via não são passíveis de serem conhecidos nem determinados, uma vez que não deixam "pegada electrónica".).

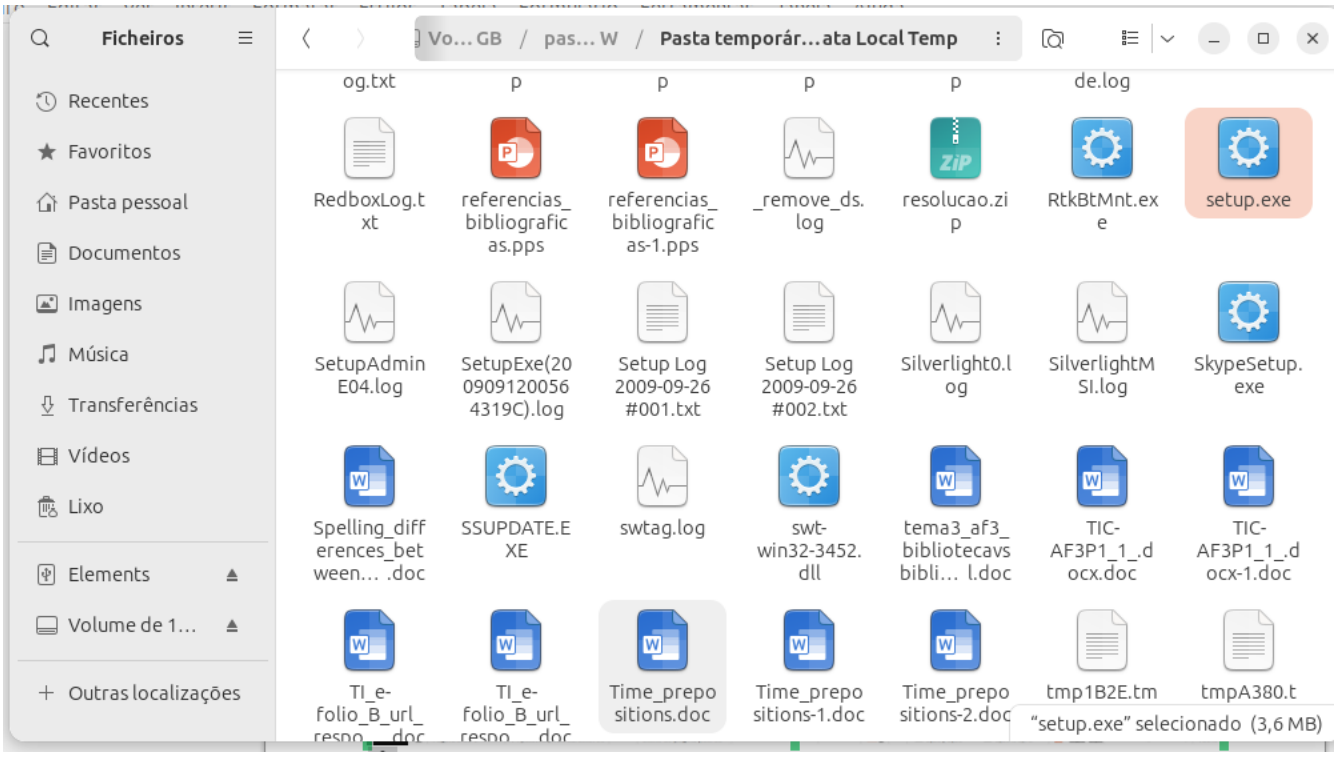
MP Telemetry submit

Criação de diversas pastas para alojamento de ficheiros pessoais do utilizador, que posteriormente serão 'tratados' para saída de dados.

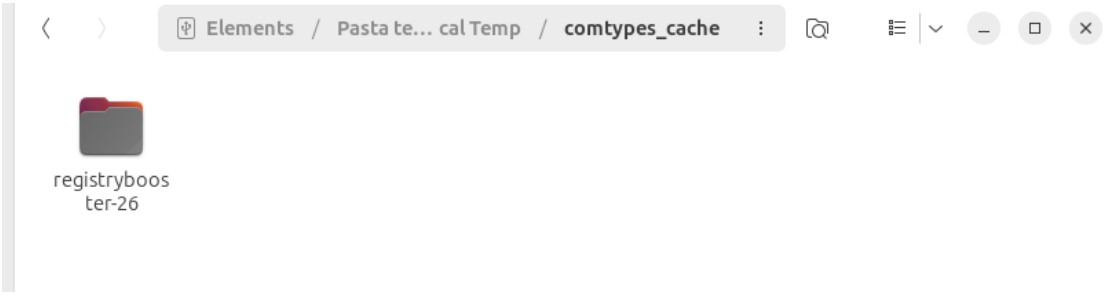


Win32 dll (pseudo sistema operativo do Windows na versão partilhada - instalado no disco externo)

Mais um complemento de gestão do Windows. O seu computador já tem, pelo menos, **dois sistemas operativos instalados**! E, um deles, num disco externo: uma verdadeira acrobacia digital...

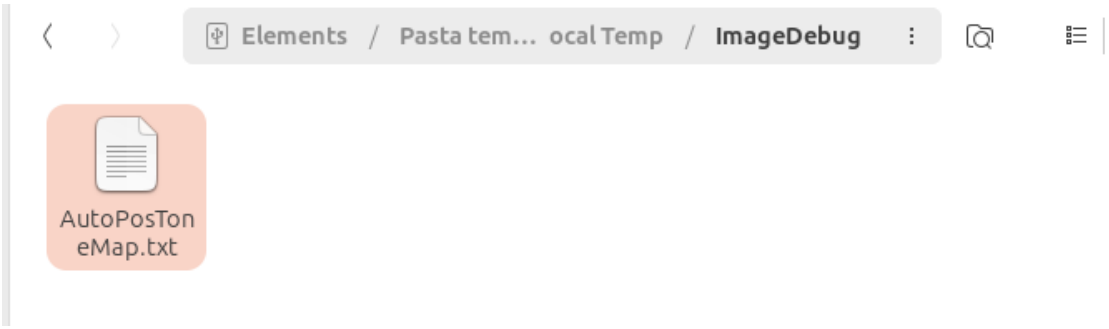


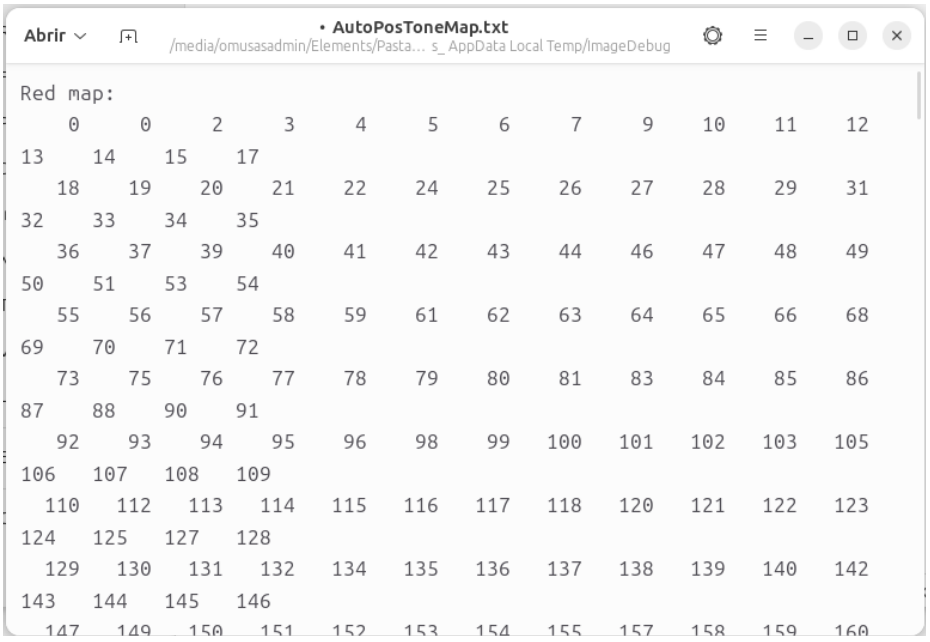
pasta Registry Booster alojada no disco externo para arrancar com os diversos programas de execução:



[Nota: este disco externo arranca e liga-se 'sozinho' quando o computador está desligado - isto mantendo o cabo USB ligado ao computador]

Grelha de coordenadas de cor que indicia um modelo de saída de dados ponto-por-ponto (telemetria):



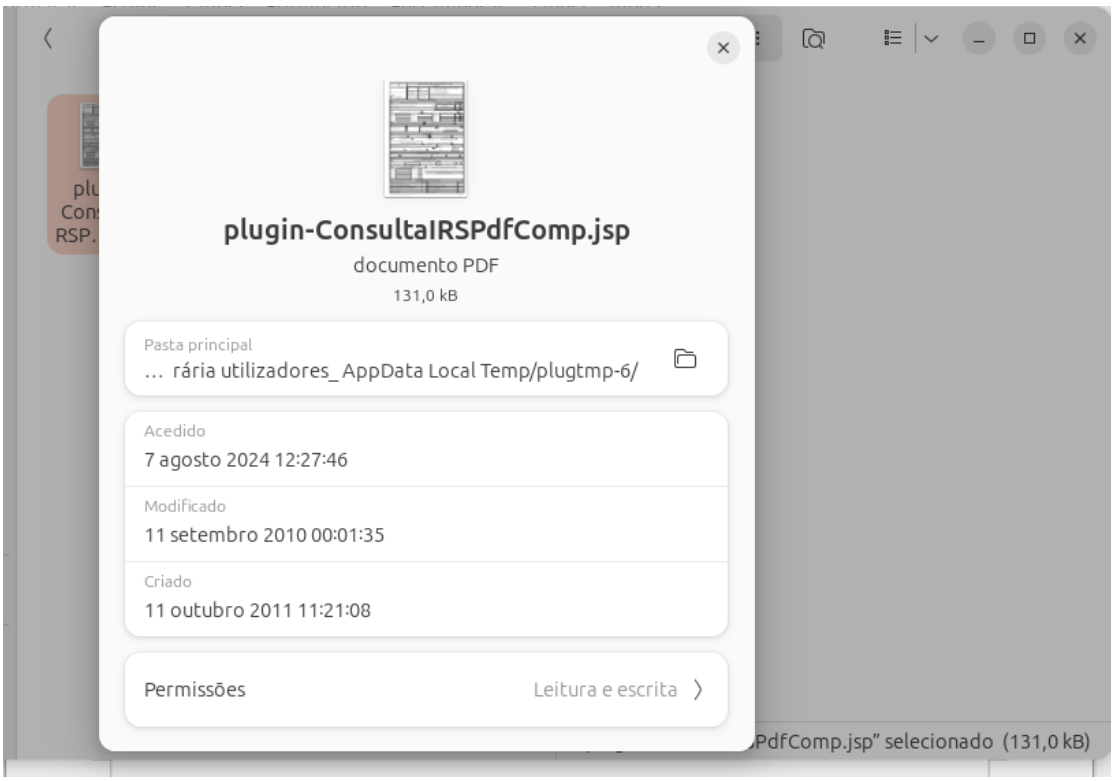


- **Um modelo de análise**

Consulta directa de um documento de IRS no computador do utilizador:

plugin .jsp (uma combinação de Java script com HTML)

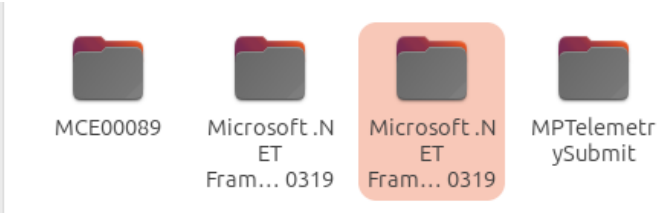

Elements / Pasta temp... Local Temp / plugtmp-1
plugin-ConsultaIRSP... .jsp
"plugin-ConsultaIRSPdfComp.jsp" selecionado (2,0 MB)


plugin-ConsultaIRSPdfComp.jsp
documento PDF
131,0 kB
Pasta principal
... rária utilizadores_ AppData Local Temp/plugtmp-6/
Acedido
7 agosto 2024 12:27:46
Modificado
11 setembro 2010 00:01:35
Criado
11 outubro 2011 11:21:08
Permissões
Leitura e escrita
PdfComp.jsp" selecionado (131,0 kB)

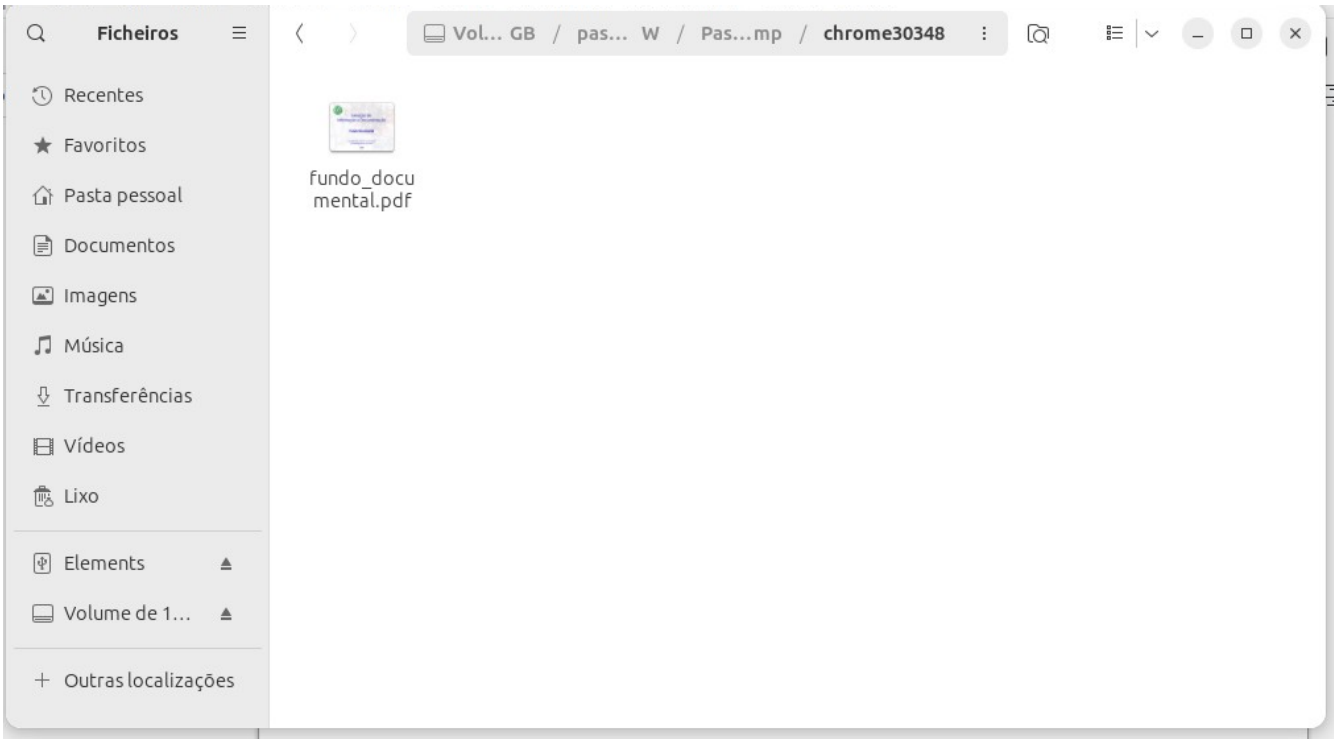

Elements / Pasta tem... cal Temp / DWD4F25.tmp
Explorer.EXE.hu.kdmp
Explorer.EXE.xml

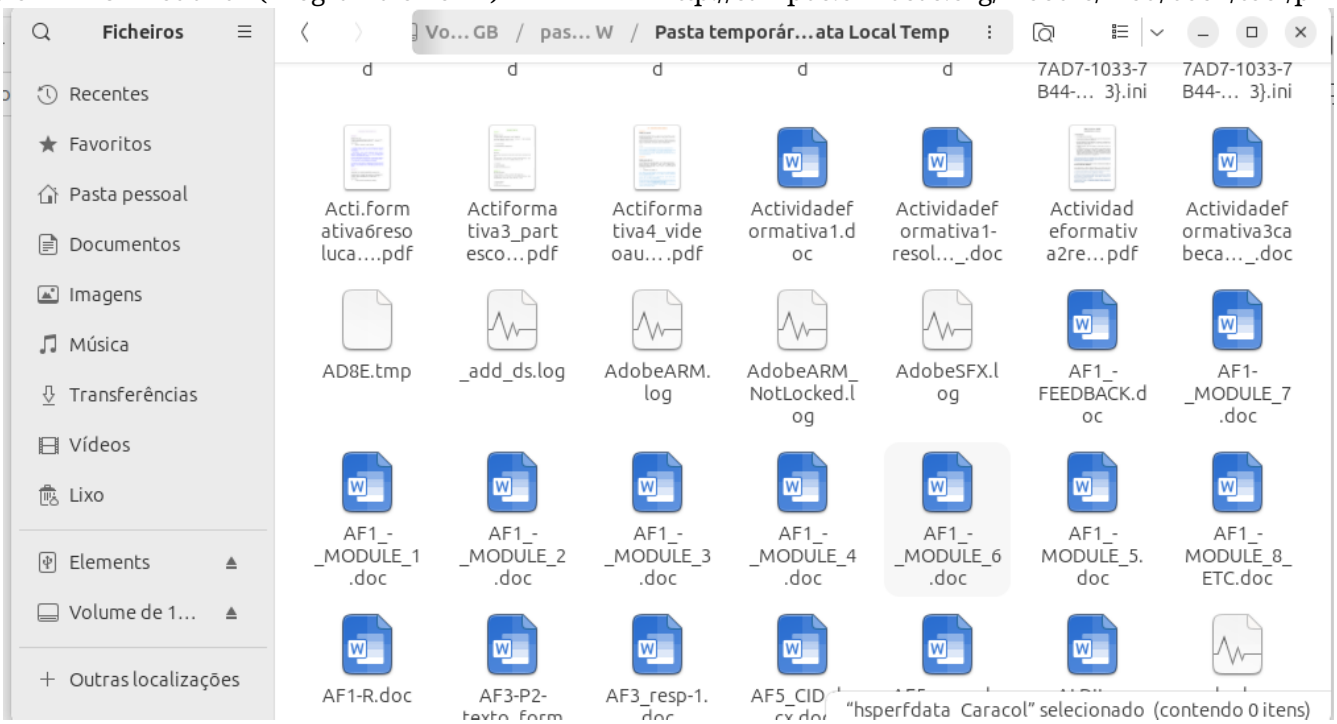
É difícil fazer-se um exposição sintética das técnicas invasivas da Microsoft, porque não existe uma técnica, existe uma multiplicidade de técnicas.
(e, algumas delas são experimentais - para ver o que é que funciona melhor...)

Microsoft.Net FrameWork - permite criar uma janela [Frame] virtual para a internet:



Do conjunto de documentos do utilizador reunidos nestas "pastas temporárias do Windows", pode-se verificar que a maioria são documentos Word e pdf's inteiros do tipo:
- resumos, resoluções e recursos de aulas;
- actividades formativas e exames;
- materiais pedagógicos;
- ficheiros de sistemas de classificação e tratamento documental (ISBD, CDU, etc.)





O principal interesse neste tipo de informação é óbvio: proporcionar fontes de informação de qualidade para ensinar um modelo de inteligência artificial.

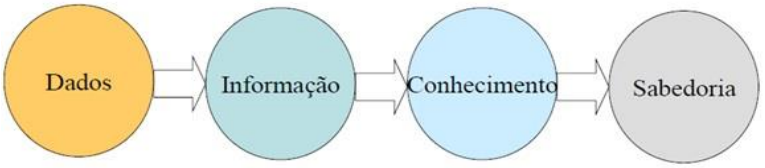
Ensinar um modelo de inteligência artificial é, basicamente, oferecer muitos exemplos para que a máquina possa identificar padrões [*data mining*] e, seguidamente, aprender a gerar previsões e/ou criar respostas com base nesse mesmo modelo(s) de aprendizagem.

Neste processo de AI haverá sempre dados recolhidos para fornecer um armazém de dados.

INPUT serão as fontes de dados e o OUTPUT será um Sistema de Informação.

Daqui realça-se o potencial da informação:

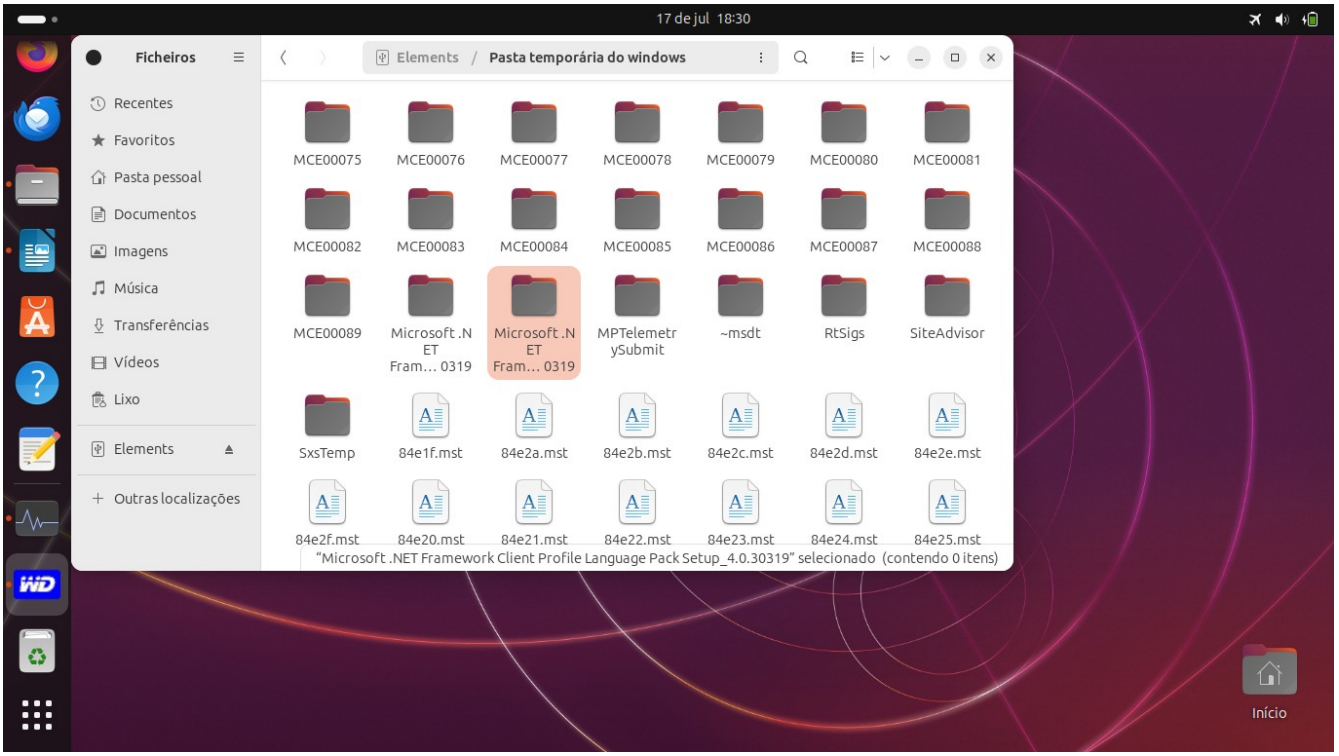
A informação pode ser crítica e importante; pode ser essencial e útil, ou pode ser mínima; ou, ainda, servir para... nada (informação lixo).



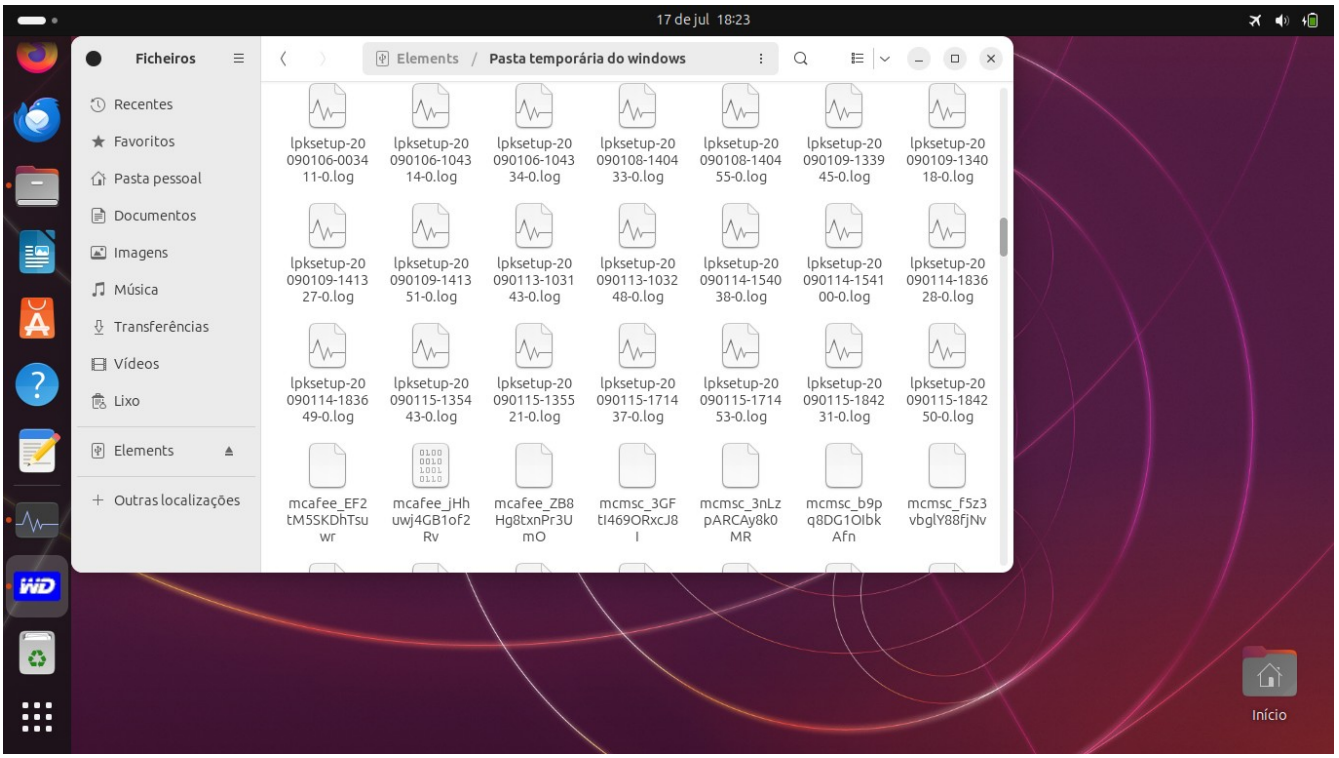
A relevância que a informação adquiriu no mundo actual, passando a ter um valor económico crescente, proporciona a que as fontes de informação tenham cada vez mais importância e valor.
As fontes de informação mais ricas serão sempre aquelas que resultam directamente do trabalho intelectual produzido pelo indivíduo no decurso da sua vida activa, independentemente dos avanços tecnológicos que se venham a verificar em termos de Inteligência Artificial.
É por este motivo que o trabalho resultante da produção humana será sempre um bem de maior valor e insubstituível.

De certa forma, é lógico que estas "ferramentas especiais do Windows" estejam alojadas num disco externo. Isto porque, é num disco externo que o utilizador guarda os seus activos digitais de maior valor.

Todavia, muitos dos ficheiros contidos nestas "pastas temporárias suspeitas do Windows" são, simplesmente, uma incógnita. E somente um especialista é que poderá tentar perceber ao certo qual o seu propósito.



- ficheiros .mst (arquivos de configurações de software) -



- ficheiros .log (arquivos de registos) -

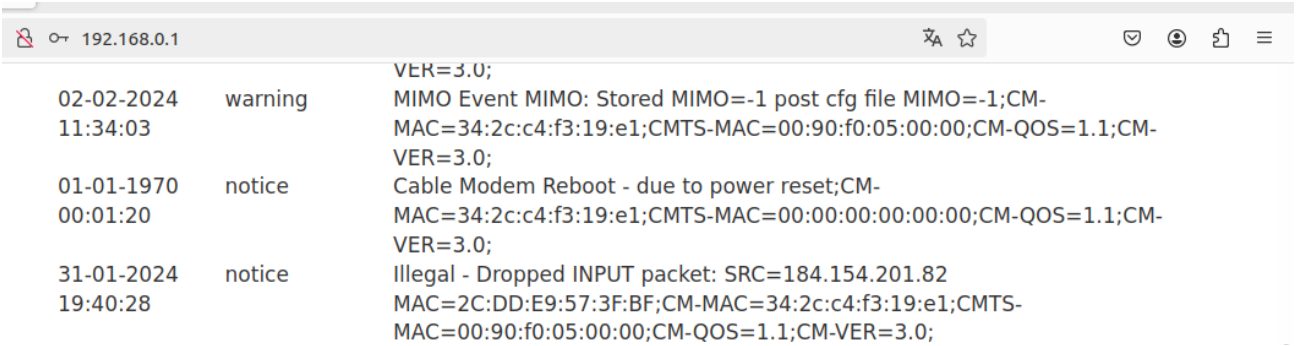
Parte II - Comunicações em risco

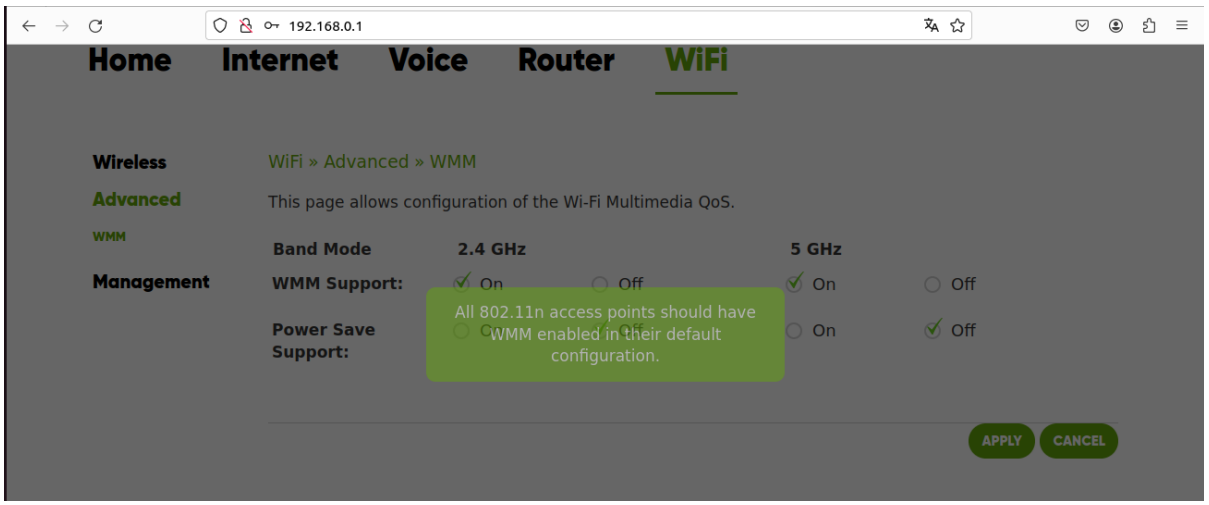
- **Comunicações paralelas de rede por Wi-Fi Multimedia no gateway:** Warning - MIMO event illegal packet - 802.11n Win [UDP?] [VMX?]

Tecnologia MIMO
- Multiple Inputs Multiple Outputs -

Configuração ilegal no Gateway de rede de internet:
--> Permite que o computador do utilizador esteja ligado a duas redes em simultâneo: a rede do operador de serviços e outro link de rede wi-fi para a configuração MIMO (rede do mafioso).

! Alerta: Esta configuração no gateway é absolutamente ilegal

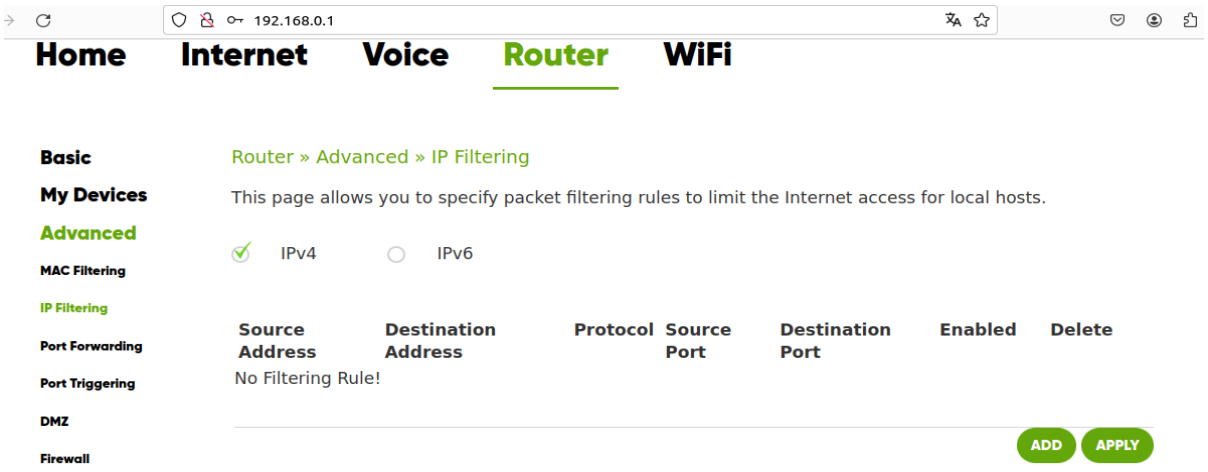




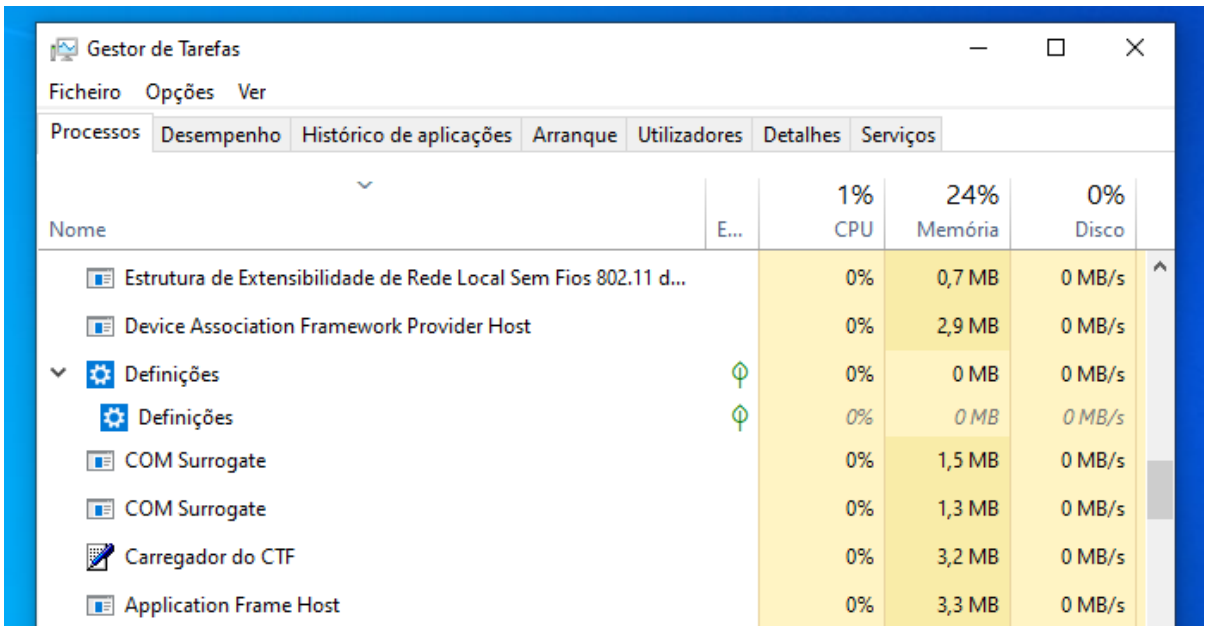
Identificação de máquinas recolhidas que carregam o ficheiro MIMO para o gateway, são sempre as mesmas (interpretação nossa):

MAC=2C:DD:E9:57:3F:BF;
MAC=2C:DD:E9:57:3D:77;
MAC=C8:5B:76:FC:0D:1A.

- No Filtering Rule!

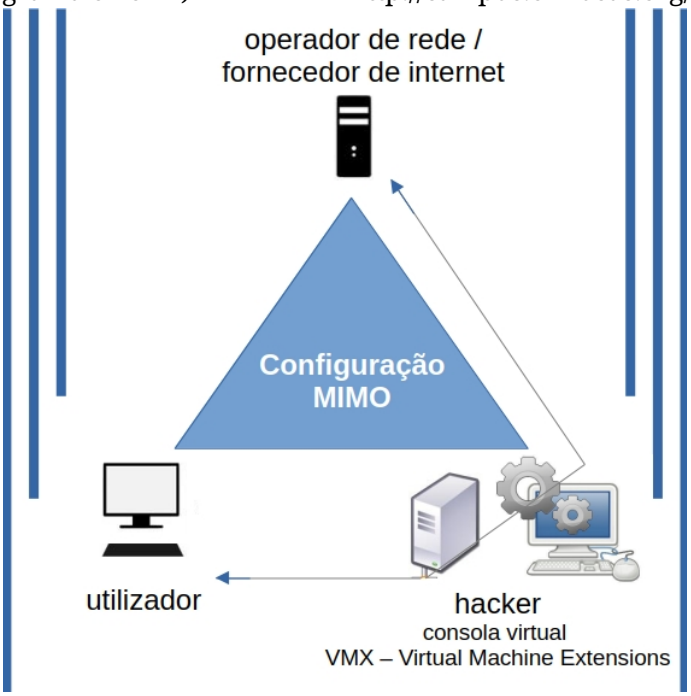


Estrutura de Extensibilidade de rede sem fios (wi-fi) 802.11 do Windows - *print screen* que atesta o momento em que o Windows realiza a configuração ilegal MIMO:



| um verdadeiro ex-libris deste acervo digital |

O "Triângulo das Bermudas" da Microsoft: configuração ilegal MIMO:



- Rede triangular MIMO -

- Net TCP port sharing do Windows: serviço de partilha de porta Net.Tcp! (permite partilhar conexões TCP entre aplicações) -

A configuração MIMO é semelhante aos zoombie cookies que a Microsoft anteriormente utilizava (mas também a Apple), só que agora surgem na versão *Transformer* - muito mais perigoso.

Tal como acontecia com os ficheiros zoombie-cookies, também a configuração triangular MIMO não é passível de ser eliminada.

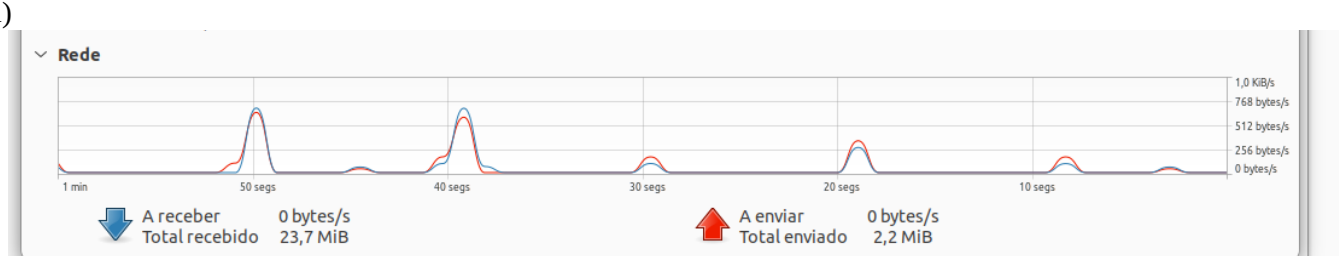
O utilizador pode formatar o seu computador; pode fazer um *reset* à rede no gateway para as configurações iniciais; pode inclusive mudar de sistema operativo, mas a configuração paralela de rede MIMO mantém-se sempre activa.

Escusado será dizer que o utilizador não tem conhecimento desta configuração nem tão-pouco tem acesso à mesma; e é perigosa por dois motivos:
1) Porque permite espiar as comunicações do browser;
2) Porque permite inverter o modelo Cliente/Servidor para Servidor/Cliente.

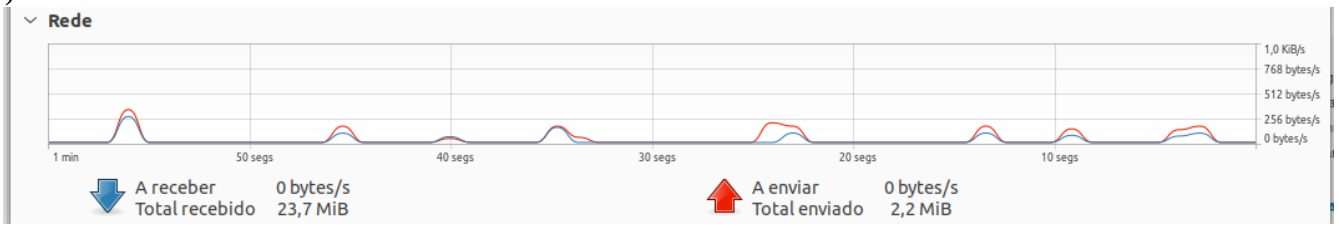
Abaixo ilustra-se graficamente os efeitos e consequências da existência desta rede WIFI paralela, a qual permite que os dados que entram na rede sejam sempre idênticos aos dados que saem (*upstream* = *downstream*), de onde se demonstra que as intenções desta configuração virtual de rede MIMO são maliciosas e permitem que as comunicações do browser do utilizador sejam espiadas!

Sinal de rede de entrada e de saída de dados com ondas sempre acopladas (sobrepostas):

i)

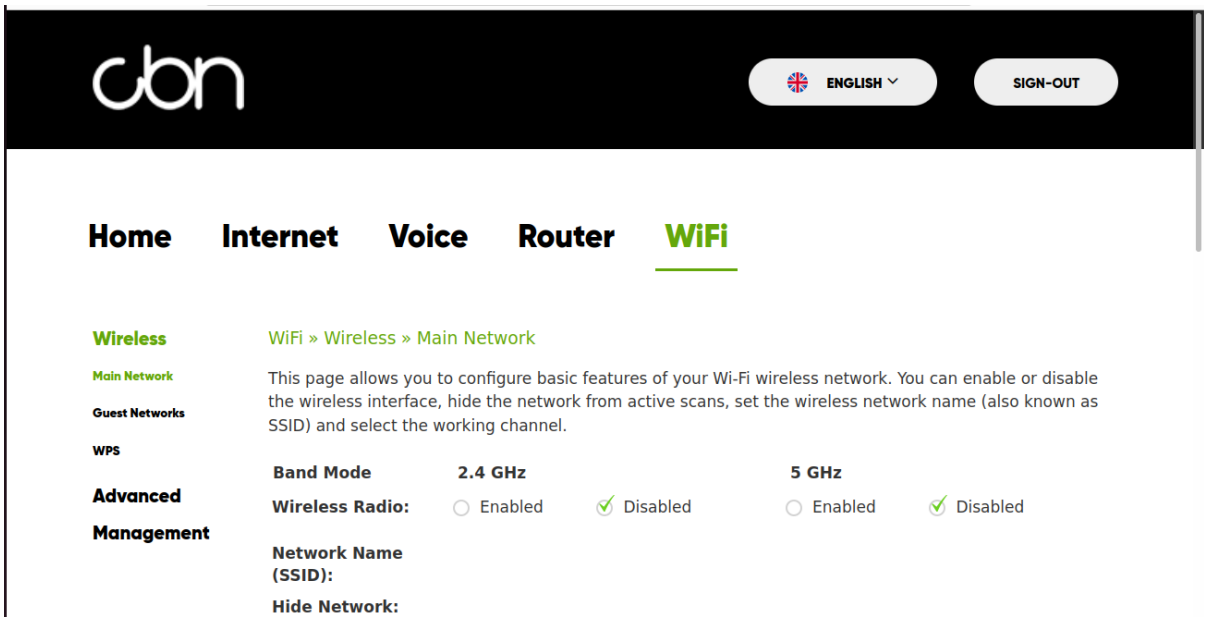


ii)



Preferências do utilizador não são consideradas:

O computador do utilizador é suposto estar ligado por ethernet - porque é essa a preferência do utilizador. No painel do gateway CBN verifica-se que o Wi-Fi está desactivado. Contudo, há uma rede avançada ligada e a funcionar que é a configuração paralela da rede MIMO (wi-fi).



(...)

Com o avanço das tecnologias, os novos processadores permitem configurações no código da máquina que são extensões virtuais (VMX – Virtual Machine Extensions).

Sobre a Tecnologia MIMO, esta permite acelerar a entrada e saída de dados (multiplica a capacidade de transmissão), usando como recurso o uso de múltiplas antenas em simultâneo, sobretudo, do exterior (não só torres de micro-ondas próximas, mas todas as disponíveis: um telemóvel próximo, por exemplo, de um familiar seu, pode ser utilizado para saída de dados). Foi inventada com boas intenções com o objectivo de estabilizar as comunicações remotas por WI-FI.

- **Configurações ilegais em telemóveis smartphone via bluetooth**

Este é o telefone fixo que o utilizador não tem (o utilizador tem, sim, e apenas, um número de telefone fixo que lhe foi consignado pelo operador de internet quando contratou o serviço).

O que o utilizador não sabe é que existem chamadas recebidas neste telefone fixo que o utilizador não tem.
Parece confuso?! Assim é.
Importa recordar que em ambiente digital não existe uma realidade objectiva que obedeça à nossa lógica de causalidade. Tudo o que existe é uma realidade programada.

"Trim trim" toca o telefone. Ou melhor dizendo, o telefone não toca, nem faz som.
Há, sim, um sinal digital bluetooth que viaja pelo espaço e intercepta o seu router/modem na forma de chamada falsa.

Esta chamada telefónica, que nem chamada é (é uma chamada vazia, simulada), passa em tudo pelos operadores de comunicações telefónicas como sendo uma chamada real.
E com algo tão simples quanto isto é possível entrar na rede telefónica com códigos maliciosos, e, consequentemente, interceptar a rede de internet.

O acesso à rede é, ainda, facilitado pelo facto de que as senhas de acesso ao gateway são, de um modo geral, de conhecimento público.

Cada operador de serviço de internet (MEO, NÓS, NOWO...) tem o seu próprio fornecedor de rede/gateway.

A informação de acesso ao Gateway é um endereço URL em formato IP que consta na base do router/modem.
Exemplos de endereços e respectivas passwords de acesso:

MEO gateway: http://192.168.1.254

utilizador: **meo**
password: **meo**

NOWO gateway: http://192.168.0.1

utilizador: **admin**
password: **admin**

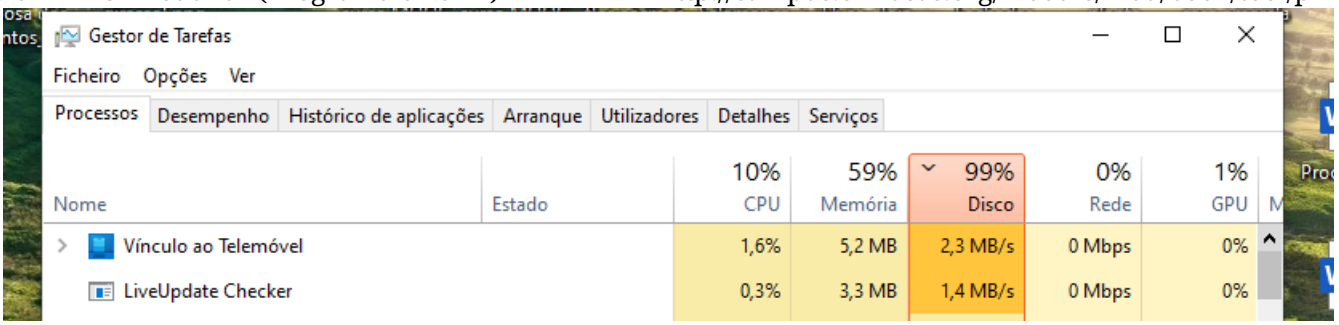
Portanto, o 'cofre' de informação que segura o nosso 'ouro' não tem senha, é só puxar o 'trinco'.
Aconselha-se a todos os utilizadores que mudem a password do gateway de rede.

Configurações ilegais em telemóveis estão na ordem do dia [Vínculo ao Telemóvel]. Esses equipamentos *smartphone*, tão inocentes que parecem, devem ser o alvo preferido desta entidade.

As configurações ilegais podem servir diversos motivos, nomeadamente, 'colar' um código para *tracking* no telemóvel do utilizador, o que consubstancia um crime de geolocalização abusiva; ou podem servir para outros intuitos, como por exemplo, espionagem de comunicações ou recrutamento do dispositivo para fins de *hacking* (emissão de sinais e frequências não-autorizadas).

Notas:
1. Utilizaremos o conceito de sinal quando está associada uma transmissão remota com informação digital codificada.

2. Utilizaremos o conceito de frequência quando se está na presença de emissão de radiação electromagnética sem sinal modulado associado.

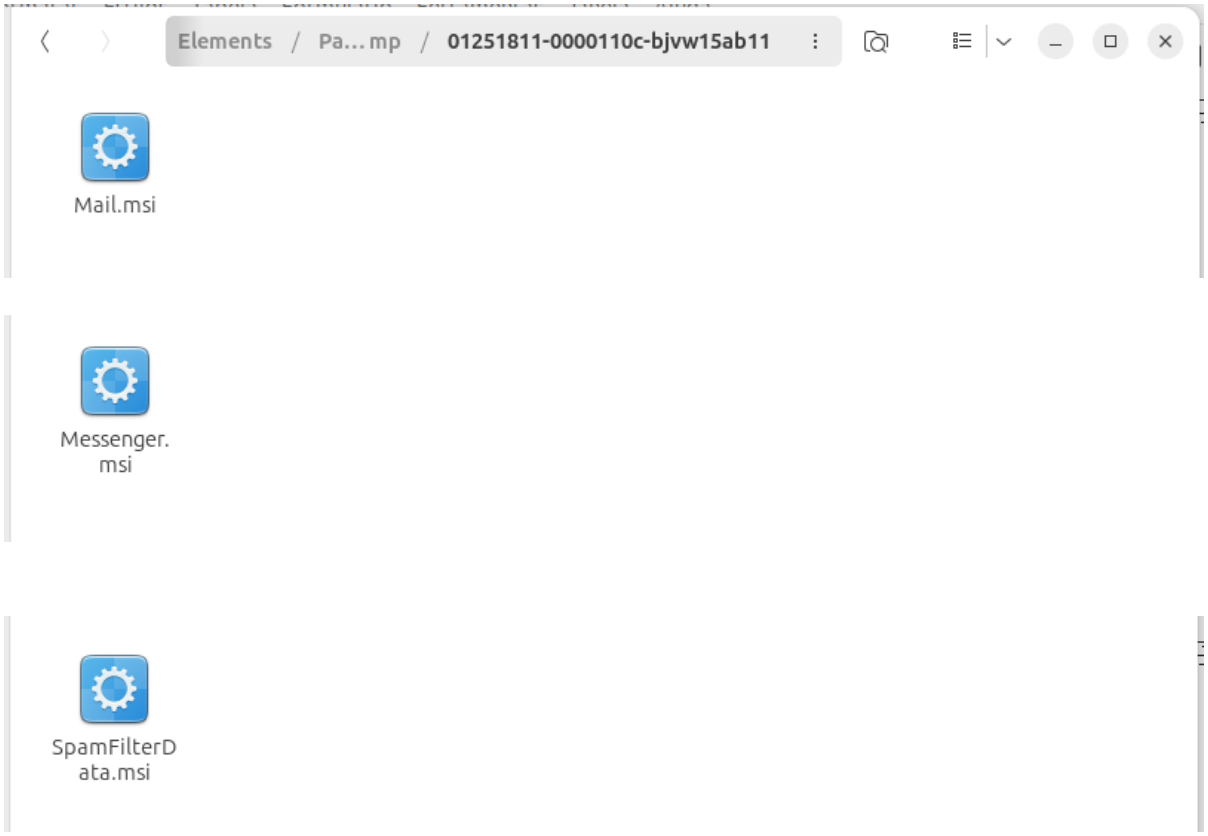


E como é que se processa tudo isto?
Não é suposto ser óbvio... o criminoso não quer ser identificado nem quer deixar rasto...

Se o seu telemóvel canta tanto que mais parece um papagaio, desconfie das mensagens e e-mails que recebe. Pode acontecer que o seu telemóvel tenha sido recrutado para *hacking*.

O contexto de origem:

O utilizador recebe no seu telefone uma notificação: pode ser uma recepção de mensagem com informação meteorológica, por exemplo; pode ser a recepção de um e-mail de spam chato no Gmail. Aparentemente, nada de especial.
O utilizador nem precisa de abrir a mensagem. Assim que ouve a recepção da notificação no seu telemóvel - o som "plim" ou "dong" - inicia-se o processo automático de activação: o envio do sinal bluetooth.



Este sinal de bluetooth atinge o router, intercepta a linha telefónica e invade a rede.

Sendo um sinal de bluetooth, não passa pelas redes de comunicações móveis, logo, é muito mais difícil de se rastrear.

Parte III - Novas armas do séc. XXI

- **O Wi-Fi como arma: formas de se ultrapassar potências de transmissão** (há a forma directa e a indirecta)

Casos práticos - ataque da pen:

Quando o seu equipamento (*pen*) é atingido por um feixe de Wi-Fi em potência, podem acontecer duas hipóteses:

Ou o seu Sistema consegue defender-se, ou não.

(img)
...

- **Frequências clandestinas não-autorizadas** [radiação electromagnética pura]
  --> Frequências da gama rádio potencialmente perigosas pelos efeitos que geram no meio-ambiente e nos equipamentos, como por exemplo, frequências de ressonância magnética (frequências que alteram o estado do *spin* electrónico de um átomo).

Mas, não são 'só' frequências de ressonância que utilizam. Na verdade, dispõem de um "arsenal de frequências". O conhecimento desenvolvido nesta matéria por esta empresa chega a ser assustador. Importa aqui realçar que esta entidade dispõe de conhecimentos que ainda mais ninguém tem. O que também nos leva a questionar, qual será o verdadeiro objectivo desta entidade?
Recordo-me, de repente, dos trabalhos desenvolvidos por Tesla, que considerava que era possível mapear os impulsos eléctricos do cérebro; ou seja: captar ondas cerebrais para saber o que é que a pessoa está a pensar.

- E que «frequências estranhas» são estas que a Microsoft utiliza e que põe a gerar nos equipamentos (computadores, routers e telemóveis)?

Isso é mais difícil de saber ao certo o que são.
É quase um pouco como termos de adivinhar qual é a frequência que os nossos homónimos do espaço interestelar [outros seres inteligentes] estarão a transmitir.
Neste sentido, talvez pudéssemos pedir alguma ajuda ao SETI - *Search for ExtraTerrestrial Intelligence* para nos ajudar com esta tarefa.
Mas para se dedicarem a este novo projecto deveriam, primeiramente, mudar o acrónimo de SETI para SATI - *Search for Abnormal Terrestrial Intelligence*.

- E pergunta o utilizador, como é que o utilizador sabe isso? E respondemos:
O utilizador não sabe.
Ninguém sabe.
Só o Sistema Operativo é que sabe.
Uma grande pista pode ser dada neste sentido, visto que, mesmo num dia de apagão total, como foi aquele que ocorreu recentemente no final de Abril de 2025 - em que não havia internet, nem havia routers ligados, pois não há energia eléctrica - o seu telemóvel é uma fonte de rádio a transmitir continuamente!

Para o utilizador saber isto tem de ter iniciativa própria. Ou seja, tem de monitorizar a actividade electromagnética do(s) seu(s) equipamento(s).

Actividade paranormal

Pode ainda acontecer, em conversa de corredor, o utilizador falar com o seu vizinho do andar de baixo e este comentar-lhe que só se liga à rede por ethernet, que não utiliza Wi-Fi [*pensa ele que está ligado por ethernet...]*.

No andar directamente acima do utilizador, é um andar vago, não vive lá ninguém. Ao lado do andar do utilizador vive uma velhota com mais de 80 anos que nem internet tem nem utiliza smartphone. Contudo, há sempre um chinfrim de frequências estridentes que se ouve no ar [se o utilizador tapar os ouvidos ou utilizar uns tampões consegue abafar os sons exteriores e ouvir melhor os *sons interiores*].
Então, de onde vêm estas frequências ruidosas que circulam no ar? Serão alienígenas?!
Não, não são alienígenas: são as frequências de hacking da Microsoft.
Outra característica que identifica estas frequências não-autorizadas é que são particularmente ruidosas.

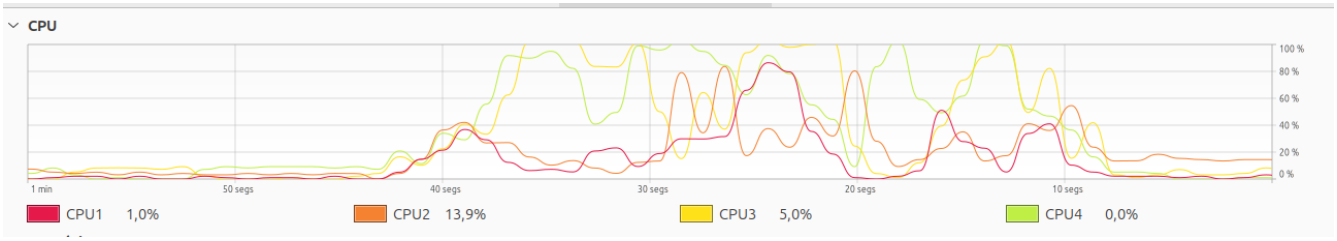
- **Armas integradas em computadores:** pulsos ou pulsares electromagnéticos

No campo da informática sabe-se que a Microsoft é líder de mercado. Muito possivelmente, 80% das pessoas com computadores utiliza Windows – a Microsoft tem domínio sobre o Universo Digital.
Contudo, a Microsoft não é só uma empresa de software. Esta empresa também fornece algum hardware para computadores (muito conveniente...).

Chegámos ao ponto em que já existem armas integradas num computador! No entanto, para funcionar em pleno esta arma "espingarda electromagnética" precisa de algumas configurações eléctricas externas. [Nos nós da rede ou caixa de derivação?]
O pulsar electromagnético é uma arma, no verdadeiro sentido do termo: faz parte do conjunto das armas ofensivas. Funciona na forma de "disparos" que ocorrem numa cadência regular, tal como um pulsar estelar. O efeito que esta arma produz 'depende da dose', em todo o caso, o objectivo é imobilizar os equipamentos tecnológicos, e verifica-se que pode imobilizar um rato.
Para um utilizador que seja apanhado juntamente com este pulsar, esse tem a sensação de estar a passar uma onda electromagnética gravitacional e de se estar a afundar na curvatura do espaço-tempo, com a iminente sensação de que o coração pode parar a qualquer momento.
Julgamos que, para um utilizador que tivesse um pacemaker, esse aparelho, certamente, não voltaria a arrancar...

- **Outros:** Pressões magnéticas; Ultrassons; Armas de Electrões (impulsos eléctricos), etc.

Ilustração gráfica que apresenta um computador atingido por impulsos eléctricos e consequente afectação dos processos:



- O gráfico acima representa picos de energia que afectaram a integridade do computador causado por impulsos eléctricos. -
[O acontecimento gráfico acima representa um ataque de um sistema Windows a um sistema Linux.]

```
Impulsos eléctricos

Impulsos eléctricos são cargas libertadas (electrões) que criam campos eléctricos desgove
rnados e que atingem os equipamentos.

Este conceito “impulsos eléctricos” é diferente de “pulsos ou pulsares electromagnético
s”.
```

- **Sinais clandestinos criminosos** [sinal modulado]
  O bluetooth como técnica utilizada para invadir sistemas informáticos (computadores e routers/ modems) corrompendo a sua segurança: há formas de maximizar o impulso, alcance e orientação de um sinal de bluetooth.
  Hardware integrado para *hacking* remoto (componentes): o recurso ao electroíman e a outros "engenhos" que exploram princípios de Física.

Parte IV - Conclusões

Balança - símbolo da justiça

(imagem muito apropriada; é o meu signo)

Isto significa que o crime não pode passar impune.

- **Convite ao crime**

Uma pequena história para introdução:

Se eu contactar as autoridades e disser que está um carro estacionado em frente à minha garagem; eu quero sair e não consigo...
As autoridades deslocam-se ao local, verificam que o carro está efectivamente estacionado em frente à minha garagem, e, se não se conseguir contactar o proprietário, o carro corre o risco de ser rebocado.
Tudo certo até aqui. Agora:

- Se eu contactar as autoridades e disser que alguém dispara contra o meu computador pulsos electromagnéticos (e, consecutivamente, contra mim, pois que estou sentada em frente ao computador) as autoridades não têm como verificar se isto está ou não está a acontecer; além de que, parte-se do pressuposto: como não se conseguirá chegar ao autor do crime, 'o caso é arquivado'!
- Qual é a interpretação que se tira desta história?
R: - O crime compensa. (?!)
Mas o crime não pode passar impune...

No âmbito digital há muitas situações que comportam uma dificuldade acrescida pelo facto de trazerem "assinaturas anónimas".
- Então, como ultrapassar isto?
1º
2º
3º

(...)

- **O crime ideal**

Modelo OSI - estrutura conceptual de um computador e da internet: a camada física

Open System

Interconnection

7 - Aplicação
6 - Apresentação
5 - Sessão
4 - Transporte
3 - Rede
2 - Lógica
1 - Física

Na camada física define-se as propriedades do sinal eléctrico; o nível e filtros de ruído; o meio físico através do qual são transmitidos os dados, bem como, os sistemas eléctricos e mecânicos de ligação do computador à rede são definidos neste nível.

[Transístor...

(...)

Excerto de texto de um contrato de serviços de internet:

«*A regra geral aplicável é a da inexistência de um dever geral de vigilância, seja quando se presta serviços de envio de sinais ou quando se presta serviços de alojamento [de websites no servidor], e consequente irresponsabilidade em relação a qualquer eventual ilegalidade dos serviços suportados.*»

Neste sentido, a operadora de internet só actua de forma reactiva, ou seja, tem de ser o utilizador a apresentar uma denúncia e a apresentar algum tipo de "registo" que comprove, com um grau de probabilidade razoável, a existência dessa ilegalidade ou infracção.

Se o utilizador se der ao trabalho de ler e reler o excerto de texto anterior com alguma atenção, isto significa que ninguém controla comunicações digitais!!
Ninguém monitoriza que sinais é que efectivamente saem dos seus equipamentos; e, também, ninguém controla que tráfego digital é que circula no espaço exterior - isso seria algo demasiado utópico para os dias de hoje. Ninguém impede que os seus sinais possam ser interceptados quando em trânsito. Na verdade, esta tarefa não está, oficialmente, a cargo de ninguém, pois não existem "fiscais de internet" nem "brigadistas digitais".

(...)

- **Um mundo de invasões**

Espera-se que o utilizador seja uma pessoa altamente instruída em literacia digital e que esteja a par das últimas tendências de hacking. - imagens de *printscreen*: Logs de erros do servidor:

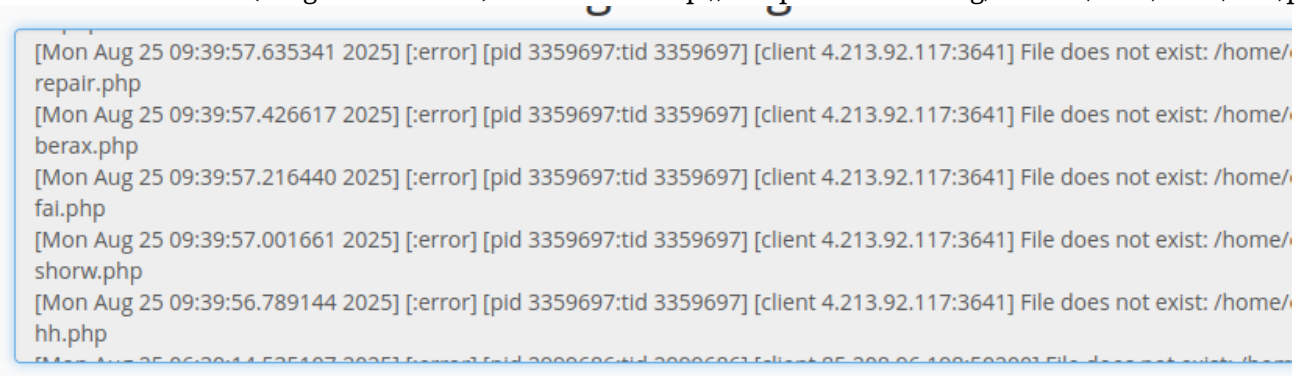
Latest web server error log messages:

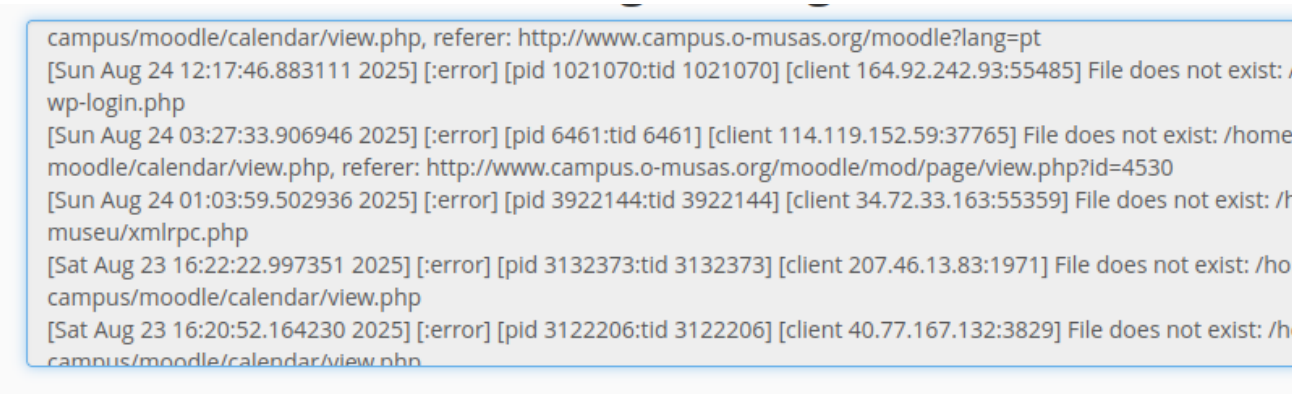
[Mon Aug 25 09:39:57.635341 2025] [:error] [pid 3359697:tid 3359697] [client 4.213.92.117:3641] File does not exist: /home/
repair.php
[Mon Aug 25 09:39:57.426617 2025] [:error] [pid 3359697:tid 3359697] [client 4.213.92.117:3641] File does not exist: /home/
berax.php
[Mon Aug 25 09:39:57.216440 2025] [:error] [pid 3359697:tid 3359697] [client 4.213.92.117:3641] File does not exist: /home/
fai.php
[Mon Aug 25 09:39:57.001661 2025] [:error] [pid 3359697:tid 3359697] [client 4.213.92.117:3641] File does not exist: /home/
shorw.php
[Mon Aug 25 09:39:56.789144 2025] [:error] [pid 3359697:tid 3359697] [client 4.213.92.117:3641] File does not exist: /home/
hh.php

campus/moodle/calendar/view.php
[Mon Aug 25 10:20:49.293214 2025] [:error] [pid 3473306:tid 3473306] [client 216.244.66.230:44960] File does not exist: /ho
campus/moodle/calendar/view.php
[Mon Aug 25 09:39:59.102439 2025] [:error] [pid 3359697:tid 3359697] [client 4.213.92.117:3641] File does not exist: /home/
feed-atom.php
[Mon Aug 25 09:39:58.892025 2025] [:error] [pid 3359697:tid 3359697] [client 4.213.92.117:3641] File does not exist: /home/
public_html/24.php
[Mon Aug 25 09:39:58.682694 2025] [:error] [pid 3359697:tid 3359697] [client 4.213.92.117:3641] File does not exist: /home/
sallu.php
[Mon Aug 25 09:39:58.473171 2025] [:error] [pid 3359697:tid 3359697] [client 4.213.92.117:3641] File does not exist: /home/

public_html/24.php
[Mon Aug 25 09:39:58.682694 2025] [:error] [pid 3359697:tid 3359697] [client 4.213.92.117:3641] File does not exist: /home/
sallu.php
[Mon Aug 25 09:39:58.473171 2025] [:error] [pid 3359697:tid 3359697] [client 4.213.92.117:3641] File does not exist: /home/
x7.php
[Mon Aug 25 09:39:58.264439 2025] [:error] [pid 3359697:tid 3359697] [client 4.213.92.117:3641] File does not exist: /home/
uwu2.php
[Mon Aug 25 09:39:58.054514 2025] [:error] [pid 3359697:tid 3359697] [client 4.213.92.117:3641] File does not exist: /home/
yu123.php
[Mon Aug 25 09:39:57.844726 2025] [:error] [pid 3359697:tid 3359697] [client 4.213.92.117:3641] File does not exist: /home/

uwu2.php
[Mon Aug 25 09:39:58.054514 2025] [:error] [pid 3359697:tid 3359697] [client 4.213.92.117:3641] File does not exist: /home/
yu123.php
[Mon Aug 25 09:39:57.844726 2025] [:error] [pid 3359697:tid 3359697] [client 4.213.92.117:3641] File does not exist: /home/
ot.php
[Mon Aug 25 09:39:57.635341 2025] [:error] [pid 3359697:tid 3359697] [client 4.213.92.117:3641] File does not exist: /home/
repair.php
[Mon Aug 25 09:39:57.426617 2025] [:error] [pid 3359697:tid 3359697] [client 4.213.92.117:3641] File does not exist: /home/
berax.php
[Mon Aug 25 09:39:57.216440 2025] [:error] [pid 3359697:tid 3359697] [client 4.213.92.117:3641] File does not exist: /home/


[Mon Aug 25 09:39:57.635341 2025] [:error] [pid 3359697:tid 3359697] [client 4.213.92.117:3641] File does not exist: /home/
repair.php
[Mon Aug 25 09:39:57.426617 2025] [:error] [pid 3359697:tid 3359697] [client 4.213.92.117:3641] File does not exist: /home/
berax.php
[Mon Aug 25 09:39:57.216440 2025] [:error] [pid 3359697:tid 3359697] [client 4.213.92.117:3641] File does not exist: /home/
fai.php
[Mon Aug 25 09:39:57.001661 2025] [:error] [pid 3359697:tid 3359697] [client 4.213.92.117:3641] File does not exist: /home/
shorw.php
[Mon Aug 25 09:39:56.789144 2025] [:error] [pid 3359697:tid 3359697] [client 4.213.92.117:3641] File does not exist: /home/
hh.php


campus/moodle/calendar/view.php, referer: http://www.campus.o-musas.org/moodle?lang=pt
[Sun Aug 24 12:17:46.883111 2025] [:error] [pid 1021070:tid 1021070] [client 164.92.242.93:55485] File does not exist:
wp-login.php
[Sun Aug 24 03:27:33.906946 2025] [:error] [pid 6461:tid 6461] [client 114.119.152.59:37765] File does not exist: /home
moodle/calendar/view.php, referer: http://www.campus.o-musas.org/moodle/mod/page/view.php?id=4530
[Sun Aug 24 01:03:59.502936 2025] [:error] [pid 3922144:tid 3922144] [client 34.72.33.163:55359] File does not exist: /h
museu/xmlrpc.php
[Sat Aug 23 16:22:22.997351 2025] [:error] [pid 3132373:tid 3132373] [client 207.46.13.83:1971] File does not exist: /ho
campus/moodle/calendar/view.php
[Sat Aug 23 16:20:52.164230 2025] [:error] [pid 3122206:tid 3122206] [client 40.77.167.132:3829] File does not exist: /h


campus/moodle/calendar/view.php
[Fri Aug 22 23:41:08.215860 2025] [:error] [pid 1422837:tid 1422837] [client 48.218.63.161:1591] File does not exist: /home/
livraria/fm.php
[Fri Aug 22 23:41:08.070867 2025] [:error] [pid 1422837:tid 1422837] [client 48.218.63.161:1591] File does not exist: /home/
livraria/2x.php
[Fri Aug 22 23:41:07.926586 2025] [:error] [pid 1422837:tid 1422837] [client 48.218.63.161:1591] File does not exist: /home/
livraria/size.php
[Fri Aug 22 23:41:07.781753 2025] [:error] [pid 1422837:tid 1422837] [client 48.218.63.161:1591] File does not exist: /home/
livraria/class20.php
[Fri Aug 22 23:41:07.636785 2025] [:error] [pid 1422837:tid 1422837] [client 48.218.63.161:1591] File does not exist: /home/


livraria/size.php
[Fri Aug 22 23:41:07.781753 2025] [:error] [pid 1422837:tid 1422837] [client 48.218.63.161:1591] File does not exist: /home/
livraria/class20.php
[Fri Aug 22 23:41:07.636785 2025] [:error] [pid 1422837:tid 1422837] [client 48.218.63.161:1591] File does not exist: /home/
livraria/chosen.php
[Fri Aug 22 23:41:07.489386 2025] [:error] [pid 1422837:tid 1422837] [client 48.218.63.161:1591] File does not exist: /home/
livraria/build.php
[Fri Aug 22 23:41:07.343378 2025] [:error] [pid 1422837:tid 1422837] [client 48.218.63.161:1591] File does not exist: /home/
livraria/wp-gr.php
[Fri Aug 22 23:41:07.200155 2025] [:error] [pid 1422837:tid 1422837] [client 48.218.63.161:1591] File does not exist: /home/

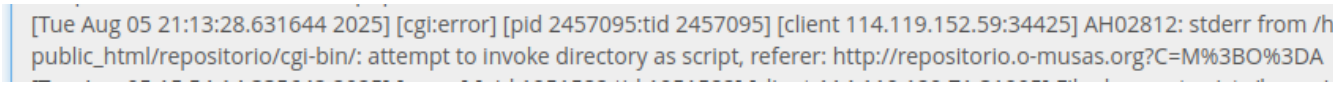
As tentativas de invasão que se apresentam neste servidor de alojamento ocorrem de forma constante. Nalguns casos, verifica-se uma frequência a cada segundo!
Se estas acções estivessem ao abrigo de fiscalização e fossem alvo de investigação e punição (tal como se aplica uma infracção por mau estacionamento), o Estado já estaria milionário!

Para evitar este rol de tentativas de acesso - ainda que mal sucedidas - era suficiente que houvesse algum elemento dissuasor... Mas não há, por enquanto, nenhuma "polícia digital".

Observações: O potencial intruso, muito insistentemente, pretende deitar abaixo a página-web desta livraria:

https://www.livraria.o-musas.org/index.html

Idem, para a página-web deste repositório:

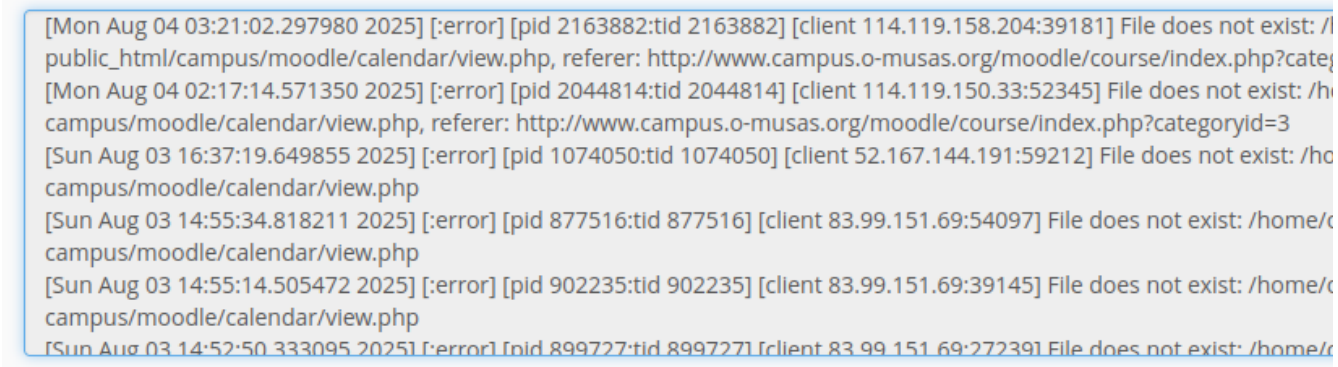


https://www.repositorio.o-musas.org/index.html

Para um acesso não-autorizado a esta plataforma de aprendizagem virtual MOODLE, o hacker explora uma possível vulnerabilidade no 'script' do calendário.

http://campus.o-musas.org/moodle/

As tentativas de acesso ilegítimo por esta via são incontáveis (centenas!):



- **Canal de denúncias**

Páginas web viciadas

(...)

- **O que é interceptar uma rede?**

Ainda que a tecnologia de comunicações digitais seja uma tecnologia extremamente complexa, o conceito de interceptar uma rede pode ser exemplificado da seguinte forma:

- Pense naqueles Walkie-talkies infantis que os pais dão às crianças, mas que serve para os pais disporem de uma forma de comunicação imediata com os filhos sempre que se deslocam para um espaço exterior ao ar livre (imagine um acampamento em família e que o filho foi andar de bicicleta). O pai pode contactar com o filho via walkie-talkie para saber se está tudo bem. Para este propósito, tanto o pai como o filho têm de estar sintonizados para a mesma frequência para poderem comunicar. Mas se por acaso a criança decidir "brincar" com o botão das frequências pode acontecer ouvir comunicações de outras pessoas/outras famílias - isso é interceptar uma comunicação.

Da mesma forma, na frota marítima, existem canais de comunicação (frequências rádio) pré-estabelecidos para efectuar determinado tipo de comunicações. Por exemplo: canais para pedir socorro; canais para pedir permissão para atracar; canais para poder falar livremente com outras embarcações. Neste último caso pode acontecer que uma frequência já esteja a ser utilizada para comunicação entre duas embarcações. E se você utilizar essa mesma frequência pode acontecer ouvir a conversa dessas pessoas - isto é interceptar uma comunicação.

Para interceptar uma comunicação você precisa de ter um receptor (antena), um sintonizador, e saber qual é a frequência da comunicação.

Em contexto informático podem ocorrer as seguintes situações:

O utilizador pode estar online a trabalhar numa plataforma de aprendizagem virtual moodle e, de repente, o sistema abre uma janela de diálogo que lhe apresenta a seguinte informação:

"Esta mensagem vai ser enviada para terceiros". Isto significa que a rede foi interceptada.

Ou, então, o utilizador pode estar tranquilamente a trabalhar no seu computador e olha para o seu painel de registos de segurança e depara-se com a seguinte informação:

"Attempted to reach computer with bluetooth". Isto pode indicar, por exemplo, que o Sistema Operativo do seu vizinho abaixo (Windows) opera de forma criminosa para invadir computadores alheios (Linux).

- **Segurança da informação**

Conforme se tem vindo a demonstrar ao longo deste artigo, há um conjunto de operações ilegais que o sistema operativo realiza, desde:
- os computadores permanecem ligados, quando deveriam estar desligados da internet;
- os computadores 'ligam-se' por wi-fi, quando é suposto estarem ligados por ethernet;
- os computadores têm configurações ilegais associadas aos gateways;
- os computadores têm configurações de risco: No NetWorkFirewall/ No filtering rule/ Net TCP port sharing;
- os computadores pessoais funcionam com Telemetria sempre activa;
- a indexação de metadados é feita via protocolos de comunicação (A indexação da informação não pode deixar o dispositivo do utilizador. Tem de funcionar sob um programa fechado.);
- pode-se ainda vir a verificar que o computador do utilizador já esteja ligado à internet sem intermediário de um operador de serviços (NÓS, MEO, NOWO, etc.), com uma configuração do tipo MicrosoftWiFi Direct Virtual configurada sem conhecimento ou autorização do utilizador (esta configuração fica visível na interface

gráfica, e pode ser 'útil' para computadores mais antigos, com processador Pentium, por exemplo), etc.
isto apenas para referir aquilo que se destaca logo à primeira vista.
E ninguém se apercebe de nada disto. Como é que é possível?

Com tudo isto a funcionar num computador não pode haver garantias de Segurança da informação.

A avaliar pela data do backdoor existente no disco externo: 2009 [data aproximada com base nos ficheiros com extensão .log (ainda que 2009 seja, provavelmente, a data de aquisição do computador, e, 2010 ou 2011 a data de aquisição do disco externo)], estas práticas ilícitas de acesso indevido à informação, entre outros aspectos, têm, pelo menos, 15 anos.
A extensão temporal de tudo isto é imensa. E não soa nenhum alarme... tudo passa despercebido. Como é que é possível?!

E aqui é que reside o verdadeiro **paradoxo**:

- Até onde é que falha a segurança da informação?
- Porquê que falha a segurança da informação?

Quando a fraude está no sistema designa-se de corrupção. Há a corrupção política; há a corrupção bancária; e agora é a *onda* da corrupção informática.

(...)

- **O "chuveiro de radiação" da Microsoft**

À falta de um modelo teórico que nos possamos basear - uma vez que todo este conhecimento é novo - propõe-se o seguinte:

Frequências "a.i." (frequências agressivas e invasivas), são compostas por 3 ou 4 categorias:

[frequências agressivas para os equipamentos; frequências invasivas para as pessoas]

FREQUÊNCIAS ELECTROMAGNÉTICAS DE CONTACTO	**Ondas Rádio**
Frequências de ressonância: altera o estado do *spin* do electrão	Exemplo:
Frequências de alinhamentos: determinadas frequências promovem, de forma significativa, o alinhamento dos domínios magnéticos	Exemplo:
Frequências de interferência: se a natureza da luz é misturar-se sem interferir, então, só há interferência quando se utiliza uma frequência idêntica ao processo que se pretende perturbar	Exemplo:

Frequências embebidas*	Exemplo:
há transferência de uma espécie de magnetismo para a própria frequência	

---

*tem o 'apoio' do electroíman.

- (O electroíman é um dispositivo que gera magnetismo recorrendo à corrente eléctrica. Todavia, sabe-se que o magnetismo é uma força de muito curto alcance - pense num íman que quer colocar num frigorífico, a força de atracção só se sente quando este está muito próximo do frigorífico. Porém, se se considerar que Wi-Fi ou frequências de radiação geradas em cima de um electroíman permite que haja transferência de uma certa proporção desta grandeza - magnetismo -, então, o alcance deste magnetismo passa a ser muito superior. Julgamos que este magnetismo residual introduzido no ambiente facilite a permeabilidade magnética do meio, e, consecutivamente, potencie um maior alcance dos sinais de bluetooth.)

Existem ainda outras frequências que podem ser consideradas potencialmente perigosas pelo facto de causarem determinados efeitos no ambiente (como por exemplo: frequências que promovem energias cinéticas de rotação, mais perto do Infra-Vermelho; ou frequências que procuram perturbar o momento angular intrínseco de um átomo/ electrão, etc.) [a ideia de introduzir estas frequências talvez tenham o propósito de funcionar, de certa forma, como um "parafuso de Arquimedes"]; mas são frequências que estão sempre a testar a capacidade de resistência das forças internas atómicas das pessoas.
Todavia, considera-se que as que estão expostas no quadro acima são as mais agressivas e invasivas, pois podem ser usadas como armas: as novas armas do século XXI.
No entanto, mesmo estas frequências de '2º grau' não deixam de ser, como diria um esteta, "horrorosas", pois acentuam condições inflamatórias; promovem perturbações de equilíbrio, etc.
Estas frequências estão relacionadas com números quânticos de um átomo.

Em resumo: a exposição a estas frequências de radiação "a.i." promove efeitos físico-químicos sobre os materiais; e interacções biofísicas sobre as pessoas.

Fazemos agora uma pequena pausa para perguntar ao leitor o que é que ele consideraria ser uma "arma ideal"?
Com alguma reflexão o leitor talvez dissesse:
- Uma arma que não se pudesse ver, ouvir ou sentir.
E responderíamos que a resposta está certa mas não está completa.

Uma arma ideal é uma arma que passa totalmente despercebida - conforme referimos acima; mas, também, é uma arma em que não tenhamos de fazer qualquer investimento para sua aquisição; ou seja, não é preciso comprar armamento porque "pode-se usar aquilo que é dos outros": software e hardware (e ainda dá muito jeito para despiste do crime...).
E tudo isto faz parte do **conceito** do crime:

- 1 - O conceito do invisível.
- 2 - A alienação de recursos.

- 3 - Um outro aspecto que diz respeito ao conceito, é o conceito de *efeito*.

O que torna as técnicas de hacking remoto da Microsoft tão eficientes, não é o envio de sinais; é o facto de conseguirem manipular o ambiente.

As técnicas de invasão por via remota podem ser um efeito (amplificado e/ou combinado), e, por isso, difíceis de ver, de perceber, de comprovar...

Contudo, o mais macabro de todo este cenário, é que quem transporta estas armas são as pessoas: nos seus computadores; nos seus telemóveis; no router que têm em casa; por vezes, também se recrutam televisores domésticos.

Há muito tempo que esta entidade já ultrapassou os limites daquilo que é ético, e agora transformou-se numa entidade criminosa. E quanto mais avançam mais difícil é de se provar aquilo que fazem...

Uma agressão electromagnética é uma agressão, quer a pessoa esteja consciente da sua presença ou não.

Agressões electromagnéticas são crimes contra as pessoas. Fazem parte do Direito Penal.
Estas agressões podem ser algo tão *clássico* como, por exemplo, *estudar* energias de ionização; *estudar* transições de valência e buracos de valência para poder gerar pequenas formas de electricidade pelo ar.
Neste caso não há electrões livres a "flutuar" pelo ar. Ou melhor dizendo, os electrões estão livres por um curtíssimo momento no tempo e procuram o buraco de valência (lacuna electrónica) do átomo mais próximo que encontrarem. É um pouco como aquele jogo das cadeiras, onde se procura a cadeira livre para se sentar.
Esta electrificação não pode ser designada de corrente eléctrica, porque não tem um sentido; não é orientada, é aleatória. Mas é uma forma de manter o ambiente "electrificado". Ainda que esta forma de electricidade seja mínima, efémera, e a maioria das pessoas poderá até não ser sensível a ela; manter pessoas 24 horas debaixo deste ambiente, porque se geram frequências que promovem este tipo de reacção no ar, é uma forma de agressão que roça a tortura lenta: um pouco como aquela "gota de água" que cai sempre na testa.

Como é do conhecimento comum, as pessoas sabem que não podem viver debaixo de ambientes electrificados. Obrigar pessoas e viverem debaixo de ambientes electrificados é uma forma de agressão física.

O que as pessoas talvez não saibam é que também não se pode viver debaixo de ambientes permeados de magnetismo (este conceito Magnetismo é diferente de Campo Magnético).

(...)

- **Efeitos adversos na saúde do utilizador devido à exposição continuada (24h/dia) às frequências de hacking da Microsoft**

Sabe-se que toda a exposição à radiação tem sempre um efeito cumulativo. É comum dizer-se que "toda a luz degrada". Um princípio existente na Física é o princípio da equivalência.
Tendo como exemplo a luz branca (luz visível): 50 lux durante 100 horas causam o mesmo efeito de 500 lux em 10 horas ou 5000 lux durante 1 hora. Esta relação representa uma lei de reciprocidade ou de equivalência.

Para além da exposição às frequências não-autorizadas propriamente ditas, há ainda que considerar os efeitos bioeléctricos e biomagnéticos que outros "engenhos" utilizados pela Microsoft produzem.

Quando não têm o electroíman a funcionar à potência máxima, com o computador em *overclocking*, que mais parece que se ouve uma máquina em esforço, sempre a trabalhar às 6.000 rotações e que até faz disparar o quadro eléctrico da habitação... e do prédio! (data do evento: 5 Nov. 2024, 14h)
[Debaixo deste ambiente, o utilizador, em menos de 1 minuto, pode começar a ver caleidoscópios, o que já não é bom sinal... (sintoma de escotoma - cuja causa, neste caso, está fortemente associada ao excesso de poluição electromagnética)]

Há que manter as pessoas debaixo de um "banho-maria" de um electromagnetismo ambiente permanente. Este electromagnetismo não dá para levitar contentores, mas é suficiente para alterar propriedades do meio.

- E qual a necessidade de tudo isto?

Conforme já se referiu neste artigo, a principal forma de invasão é feita por sinais de bluetooth, que, em teoria, é um sinal de curto alcance.

Para garantir a eficácia do impacto e maximizar o alcance destes sinais é preciso "criar ambiente".

Conforme se pretende elucidar neste texto, há um uso indevido de equipamentos para fins de hacking remoto, com a particularidade de que esta prática constitui uma forma de hacking remoto agressivo.

O esquema de hacking da Microsoft não funciona sem agressões electromagnéticas.

[- *Programar agressões electromagnéticas...*
Acho que nem o Diabo se lembraria de tal coisa.]

Tudo está programado para ser feito (*hacking*):

1. As tentativas de intrusão via linha telefónica (chamadas falsas) para fins de acesso à rede - que ocorrem várias vezes ao dia;
2. As tentativas de invasão no servidor de alojamento web: ocorrem de dia, de noite e de madrugada;
3. O 'portefólio' de frequências a.i. geradas em *loop* (rotina/ciclo) em telemóveis 24h (não necessitam, necessariamente, de estar ligadas a nenhuma rede. É enviar frequências para o espaço).

É só programar e deixar ficar...

(...)

Este mau ambiente que se introduz nas habitações domésticas é algo semelhante ao Síndrome do Edifício Doente. Não será surpreendente, portanto, se se vier a verificar um aumento da taxa de incidência de doenças como Alzheimer ou Parkinson, na ordem dos 20%. Doenças que por si só já são uma enfermidade... Há pessoas que contribuem para que você venha a desenvolver estas patologias muito rapidamente.

O *background* catalisador envolve mexer nas constantes mais fundamentais da Física: constantes de permissividade eléctrica e de permeabilidade magnética do meio, e isso perturba toda a estabilidade do sistema (porque permite alterar permanentemente as propriedades do meio - isto, enquanto o mecanismo indutor estiver activo: o electroíman ou outro "engenho").

Estas pessoas não são teóricos. Não sabem o que é que estão a fazer: são experimentalistas.

Para esta entidade, as constantes da Física não devem ter o valor que têm; a matéria não deve ser electricamente neutra; e os átomos não podem estar no seu estado fundamental.

Observe-se que, para que a matéria não possa ser electricamente neutra, simplesmente introduz-se, paulatinamente, electrões no meio-ambiente do utilizador e do equipamento que se pretende *hackear*. Isto permite criar um diferencial eléctrico no meio e alterar substancialmente a permissividade eléctrica. (debaixo deste ambiente alterado pode acontecer que dentro do seu micro-ondas em funcionamento comece a haver "faíscas" com frequência)

Em resumo:

Esta entidade, não só invade os seus arquivos, dados e ficheiros; como também tem conhecimentos e meios tecnológicos suficientes para invadir e espiar as suas comunicações, quer seja de internet ou de telemóveis; e, agora, dedicam-se a invadir o seu ambiente e a sua saúde.

Nova poluição electromagnética:

Note-se que a poluição electromagnética já não vem somente na forma de campo magnético (esta está mais ou menos controlada - excepto quando a Microsoft decide aumentar brutalmente os campos magnéticos dos equipamentos); a sua principal manifestação reside, agora, na forma de frequências não-autorizadas e magnetismo.

E se o utilizador não está familiarizado com o termo 'frequência de ressonância'; digamos que: uma frequência de ressonância magnética significa que esta entidade pode, por exemplo, de forma totalmente remota, tocar nos átomos do seu cérebro e pô-los a "dançar" como se fossem marionetas. A "dançar" ou a fazer o "pino". Depende daquilo que se entende por alterar o sentido de rotação de um electrão...

Alguns destes conhecimentos não são propriamente novos. Fazem parte da Física Médica e da Mecânica Quântica.
Mas que exista uma entidade que explore estes conhecimentos para fins de hacking anónimo e outros interesses, é, simplesmente, abominável e hediondo.

Neste campo, o que esta entidade faz - ou procura fazer - é um pouco nesta linha: encontrar outras formas alternativas de interagir com a matéria (elementos químicos) para além das formas convencionais.

(...)

- **O crime digital é um crime complexo**

Dada a complexidade inerente a este tipo de crime, temos até de o dividir em três partes/ ou três fases:

1) A percepção do crime;
2) A demonstração da existência de crime para poder apresentar e fundamentar uma queixa nas Autoridades (a autoridade competente nesta matéria é a Polícia Judiciária);
3) A prova do crime que permita chegar ao culpado.

(...)

Há uma lógica-base nisto tudo que deve ser compreendida: o denominador comum. A maioria das ocorrências ilícitas apresentadas implica o controlo de hardware (ex.: controlo de antenas). E a única entidade que pode ter controlo de hardware é o próprio sistema operativo. Os vírus não comandam máquinas; as aplicações não comandam máquinas. Não pode haver controlo da máquina sem que o sistema operativo se aperceba disso...

Por isso, na análise desta tipologia de crime importa analisar a lógica, pois, se atendermos apenas à busca das provas isso pode revelar-se altamente improvável de se adquirir.

Vejamos o exemplo apresentado sobre a configuração MIMO ilustrada anteriormente. Para se obter o *print screen* que revela que é a própria Microsoft/Windows que realiza o processo da configuração ilegal MIMO que aparece depois no Gateway, quase que é preciso prever o crime, porque a prova é recolhida antes do crime ocorrer.
Uma vez feita a configuração MIMO, não há mais evidências dela no computador do utilizador (não aparece na interface gráfica. Esta configuração é feita via VMX – Virtual Machine Extensions –, directamente no código da máquina).

- **A parte psicológica**

Nesta secção vamos falar sobre a parte psicológica.

(A parte psicológica, mas não é do perfil do criminoso. Isso, como já vimos, só há duas hipóteses: ou estas pessoas são genuinamente loucas ou ignorantes.
Há alguém que se dedica a percorrer o espectro todo da gama rádio à procura de frequências que gerem efeitos agressivos sobre a matéria. E, neste campo, têm uma infinidade de possibilidades...
Ou porque são frequências que causam perturbações do momento angular; ou porque geram energias cinéticas de rotação; ou porque alteram o estado do *spin* electrónico; ou porque interferem com energias de ligação; ou porque promovem energias de activação; ou porque são frequências que provocam alinhamento dos domínios magnéticos e obrigam o material a exibir magnetismo; e ainda acrescentam a tudo isto, se necessário, a introdução de electrões no ambiente; o electromagnetismo do electroíman; e outras coisas mais fantásticas que se pode aplicar quando se controla um conjunto de antenas e se faz disto um "brinquedo *extra fun*": é possível fazer gerar uma força que praticamente não existe à superfície da Terra, porque vivemos debaixo de um campo magnético sensivelmente uniforme e essa força apresenta-se praticamente como nula: a força de gradiente de pressão magnética: uma espécie de um vento ou redemoinho magnético; ainda conseguem pôr a gerar aquilo

que se supõe que possa ser os monopólos magnéticos - uma partícula que existe, porque foi teoricamente demonstrada, mas ainda não foi observada [talvez sim, talvez não. Talvez também possa ser outra coisa: a acção de um campo sobre a luz, por exemplo]; e outras coisas mais misteriosas como aquilo que se designa de "tensões magnéticas" [não sabemos se constitui uma grandeza própria, como por exemplo a ddp, ou se é resultado da acção de uma frequência que causa este tipo de *stress* atómico] e "armações eléctricas" [tem-se como analogia o arco eléctrico, mas esta armação eléctrica que referimos apresenta-se na versão oculta e mais lenta na sua passagem]. Para além disto, ainda se pode enriquecer o cardápio elevando campos magnéticos; ou utilizando pressões magnéticas [i. e., mantendo o equipamento desligado mas em *stand-by* - ligado na ficha. A energia de baixa tensão eléctrica está ligada ao emissor e/ou receptor e aumenta-se a ddp - diferença de potencial.]; ou, ainda, recorrendo a compressões por ultrassons; ou trabalhando picos de frequência - se vários equipamentos estiverem a transmitir na mesma frequência, é só esperar que se aproximem para que haja um pico de frequência. Idem para campos magnético e eléctrico - com a particularidade de que campos eléctricos mais depressa se sobrepõem porque atraem-se mutuamente.
Tudo isto opera no "espectro" do invisível.
Seguidamente, é só programar isto nos equipamentos tecnológicos das pessoas, por exemplo, no seu telemóvel, e deixar a gerar 24 horas por dia. E 24 horas é: a cada minuto que passa, de dia e de noite a atingir a cabeça das pessoas e a causar estímulos no seu organismo.
etc., etc., etc.)

Nota: O atrás exposto serviu para apresentar o potencial que estes equipamentos têm para funcionarem de forma maliciosa e agressiva, inclusive, poderem ser utilizados como armas.
Não são armas nucleares; não são armas químicas nem biológicas, nem radiológicas; mas podem ser classificadas como: armas físico-químicas.
● Definição de arma: algo que permite tirar a vida a uma pessoa, ou a várias de uma só vez.

[*Manter pessoas debaixo de agressões electromagnéticas de forma permanente.*
Eu conheço formas de tortura mais "suaves"...]

As pessoas não sabem que são alvo de agressões electromagnéticas.

Teoricamente possível. Sim, é.
Não é difícil de se pôr em prática. Mas é extraordinariamente difícil de se provar...

Enquanto que a sociedade, em geral, ainda nem sequer se apercebeu do potencial que tudo isto pode ter; há alguém que já percebeu muito bem o potencial que pode haver - quando se tem em mãos um conjunto de dispositivos com antenas transmissoras; quando se possui um determinado conjunto de conhecimentos; quando se consegue pôr a gerar as frequências que bem se entende - e já aplica estes conhecimentos na prática.

A parte psicológica que iremos abordar é a parte psicológica de todo nós. Porquê que ninguém vê nada disto?

Dimensão imagética

O caso "Colgate com Flúor", para introdução.
- Deve-se utilizar pasta de dentes com flúor ou sem flúor?

(...)

Boa *gestalt*

(...)

- **Operação Frankenstein**

No laboratório de investigação secreto da Microsoft há espaço para mais coisas. Afinal, 15 anos de investigação para fins ilícitos permite desenvolver muita coisa.

Cocktail mix!

Efeitos combinados

Têm mais técnica do que um incendiário. Se não há fonte; não há foco:

- Algumas das "frequências especiais" que a Microsoft desenvolve parecem não ter outro propósito, a não ser, atingir pessoas:

--> Frequências orientadas para a molécula do sangue (Ferro?);
--> Frequências orientadas para a estrutura óssea / medula (Cálcio?).

Portanto, as armas que esta entidade desenvolve não se destinam somente a atingir equipamentos tecnológicos.

A título de exemplo, a *Prisão da Microsoft* consiste em pôr a gerar estas frequências, uma vez mais recorrendo aos equipamentos tecnológicos pessoais das pessoas (telemóveis smartphone), e programá-las para serem emitidas durante a noite (enquanto o utilizador dorme).
Consideremos a frequência emitida para atingir a estrutura óssea: para maximizar, e também para dissimular a fonte de emissão desta radiação, vários telemóveis de um edifício habitacional são recrutados e programados para funcionarem em uníssono. E assim obrigam as pessoas que lá habitam a passarem a noite debaixo desta 'nuvem' de radiação.
No dia seguinte, o utilizador ao acordar pode sentir que tem muitas dores nos ossos, nas pernas, em especial nas canelas.

Múltiplas causas:

1. Após uma exposição a uma "sova" de radiação wi-fi; ou a elevados campos magnéticos, por exemplo, a pessoa e/ou utilizador pode vir a sentir dores de cabeça...
2. Uma exposição a um ambiente permeado com magnetismo induzido no ar, a pessoa irá começar a sentir que o ambiente está abafado; depois irá ficar maldisposta, sintomaticamente enojada... se o magnetismo ambiente aumentar ficará com náuseas e vómitos...
3. A exposição a outras frequências particularmente agressivas poderão deixar o utilizador com a sensação de uma baixa/quebra de tensão...

Conforme é sabido, todos estes sintomas podem ter múltiplas causas, e daqui a dificuldade que surge em se poder fazer prova, de forma *objectiva*, da existência de uma relação causa-efeito.

O que torna estas frequências especialmente danosas, perniciosas e penetrantes, é o facto de nunca virem sozinhas. São quase sempre geradas em cima de magnetismo e "ruído" eléctrico. [A energia pode ser transformada e transferida de múltiplas formas.]
E é com isto que esta entidade mantém as pessoas debaixo da sua "cerca eléctrica".

Tudo indica que esta entidade tem os equipamentos manipulados, não só ao nível de software, como também de hardware (componentes).

O "chuveiro de radiação da Microsoft" pode ser facilmente identificado pelo som que emite. É algo semelhante a um chuveiro sempre ligado a correr água, combinado com o som de cerca eléctrica. No extremo, os sons destas frequências ruidosas podem lembrar o som paranormal da Twilight Zone. Por vezes, também poderá se assemelhar a uma espécie de música electrónica (de má qualidade...).
(Nenhuma frequência dita "normal" emite tanto ruído. É claro que o som é relativo. São sons baixos mas audíveis.).

E se lhe parecer que este som de "frequências zoombie" já está por todo o lado (interior e exterior), então, deve-se considerar a hipótese de que as frequências de hacking da Microsoft já estão mesmo por todo o lado.

Voltando ao caso da frequência orientada para a a estrutura óssea: outra pessoa habitando a mesma casa, no dia seguinte à exposição nocturna da passagem desta radiação, queixa-se exactamente do mesmo. Sem que tenha sido questionada ou confrontada com nenhuma pergunta directa, comenta de forma espontânea:
- *Hoje acordei com imensas dores nos ossos, em especial nas pernas.*
E acrescenta:
- *Mas isto é da idade...*

As pessoas não sabem, nem suspeitam, que são alvo de agressões electromagéticas de diversa ordem, e, por este motivo, também não tomam qualquer tipo de precaução para se protegerem. E, neste caso em particular, a pessoa julga que os sintomas que tem são inerentes à sua condição de idade avançada, ou eventualmente, a pessoa poderá vir a pensar que tem algum problema de saúde.
Mas a pessoa não nenhum problema de saúde. Existe, sim, uma entidade que promove de forma deliberada a degeneração da saúde das pessoas.

Outros detalhes que dizem respeito a esta forma de radiação:
Como o cabelo também levanta um pouco no ar com a passagem desta nova frequência, significa que há potencial eléctrico ou electricidade estática no ambiente.

Ainda que estas observações possam não ser suficientemente *objectivas*, é evidente que nada disto é suposto ser óbvio. Tudo está feito para passar despercebido...

Ultrassons e frequências sonoras

Outras formas de agressão que passam totalmente despercebidas: ultassons e frequências particularmente agudas e frequências muito graves de tom.

Estas "frequências especiais" que a Microsoft utiliza poderiam também ser designadas - para além de "frequências zoombie" ou "frequências de hacking" - de "Frequências de desgaste rápido 24/7"...

[- *Só pelo barulho que fazem já mereciam ser processados.*]

O **cocktail mix** é como uma receita de culinária:

Primeiro faz-se um refogado com uma frequência AI escolhida do vasto portefólio (por exemplo, uma frequência que permita induzir o alinhamento magnético do cobre - principal componente dos fios condutores e de cabos coaxiais de rede);
depois junta-se uma pitada de magnetismo induzido no ambiente para aumentar a permeabilidade magnética;
de seguida cobre-se tudo com um pouco de campo;
e, por fim, adiciona-se o ingrediente especial (por exemplo, um pouco de ultrassons).
No final não pode faltar a colher de pau para envolver tudo e puxar/ou empurrar tudo com Força.

Depois, é só enfiar tudo isto na cabeça e nos ouvidos da pessoa e ver se funciona!

De facto, alguns destes cocktails que a Microsoft utiliza parecem desestabilizar os equipamentos tecnológicos: pode acontecer que o router, de repente, acenda todas as luzes em simultâneo como que se fosse reiniciar...

Nota: Um dos momentos de maior vulnerabilidade dos equipamentos informáticos é quando estão a iniciar.

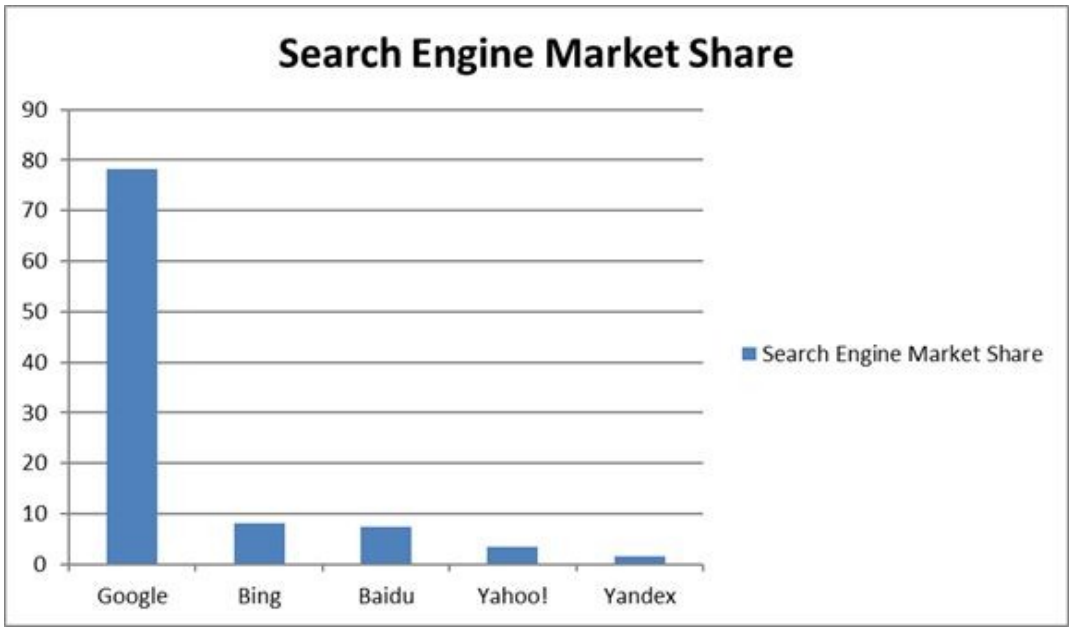
(...)

(...)

- **Considerações finais**

- Porquê que tudo isto acontece?!
Conforme diz o ditado popular "Porque é fácil, é barato e dá milhões".

E iremos agora tentar sintetizar o que é que é "fácil", o que é que é "barato" e o que é que dá "milhões":



- Ranking dos principais motores de busca -
(ano de 2014, salvo erro)

Antes de mais, importa pôr alguns pontos em perspectiva:

1. - Os computadores chegam à casa das pessoas e nunca mais são inspeccionados.
2. - No código da máquina - aquela *'garagem fechada'* - ninguém entra.
3. - Os computadores são alvo de múltiplas actualizações: de software (controla aplicações) e de firmware (controla hardware).
4. - A memória da BIOS é uma memória do tipo EEPROM (*Electric Erasable Programable Read Only Memory*) e pode ser totalmente reescrita (já não é uma memória ROM fixa). Com todas estas operações na máquina permite-se que o computador possa ser totalmente transformado.
5. - O "Estado Digital" está sob 'comando' da Microsoft. Não há independência de poderes. Se necessário, eles são o Software (Office); o Antivírus (Windows Defender); a Rede (Avast), etc.
6. - Identificam-se conflitos de interesses nas diversas actividades e serviços que prestam. E, evidentemente, que qualquer que seja a actividade exercida, esta não pode estar sujeita a conflitos de interesses.
7. - Mais de 25 anos passados de internet e nunca ninguém se lembrou de fazer um teste para validar a segurança da informação - tirar a "prova dos 9". A Segurança da Informação passa somente pelo pressuposto da Confiança.

[ainda que existam anti-vírus independentes (Norton, Kasper, etc.), estes não têm acesso a tudo o que o computador anda a fazer... não chegam a todos os processos, sobretudo, àqueles que operam na linguagem de baixo nível - código da máquina - que controla hardware]

Importa também observar os acontecimentos nesta perspectiva. Pode-se:

- a) Roubar ficheiros que não desaparecem (recursos digitais);
- b) Usar armas que ninguém vê para atingir computadores (ex.: wi-fi em potência);
- c) Cometer agressões sobre pessoas sem que estas se queixem (insensibilidade às frequências de radiação; e a outras formas de agressão de âmbito eléctrico e magnético, até determinado nível de intensidade; entre

outros).

Comecemos, então, pelo que é que **é fácil**:

É fácil retirar do utilizador as funções de administrador do seu próprio computador. O utilizador - dono do computador - tem, apenas, uma 'sessão' no seu computador; e só se apercebe deste facto quando pretende desinstalar programas e não consegue porque "não tem permissões de administrador".

Com isto em mãos, podem ser instalados quaisquer programas na vista de administrador, sem que o utilizador se aperceba de nada.

(...)

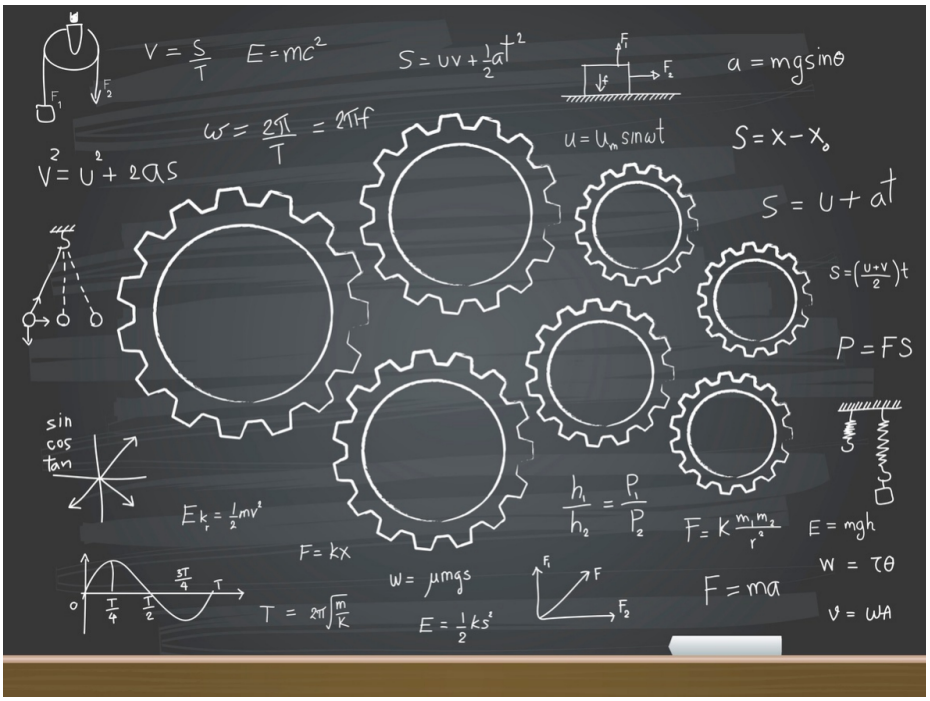
É preciso observar nestes sistemas informáticos: como é que se tem acesso à informação; quem tem acesso à informação; por onde é que pode haver fugas de informação; como é que é tratada a informação.

(...)

Uma sociedade ilusoriamente embalada por um provedor de serviços informáticos corrupto, completamente desvirtuado das suas funções, onde um povo inocente ou ignorante (ignorante no bom sentido: porque ignoram tudo o que acontece; porque confiam no sistema), subsidia a malvadez pela utilização contínua dos seus serviços.

Uma entidade insana que segue e soma como se nada fosse, porque, no Estado Digital mandam eles.

◊◊◊
final de artigo
data de publicação 2025



Cenário da sala de aula - o professor de TIC e o aluno:

PROFESSOR - Se o seu router aquece tanto que mais parece uma torradeira, isso pode indicar energia dissipada por efeito de Joule. Ou seja, corrente eléctrica a mais a passar no seu equipamento.
Isso pode ser feito ajustando resistências; ou manipulando tensões de entrada, etc.

ALUNO - E porquê que haveria de haver corrente eléctrica a mais a passar no router?
R: O facto do router aumentar de temperatura amplifica o campo magnético inerente ao equipamento, pois o campo é susceptível a influências de variáveis externas, como sendo, a temperatura.

- E porquê que haviam de fazer isso?
R: Porque isso denuncia o equipamento e facilita a sua localização.

- E o que é que é isso?
R: É uma forma de hackear redes de computadores de forma remota.

- E como é que fazem isso?
R: Com "frequências sentinela" que detectam campos magnéticos com precisam cirúrgica.

- Verdade?!
R: Sim. O suficiente para poderem detectar o campo magnético da máquina de lavar roupa e da chaleira eléctrica de uma casa.

- Não sabia que isso era possível!
R: É a espionagem moderna. Já não é só para pessoas VIP. A internet funciona em piloto automático e dedicam-se a controlar pessoas.

- E quem são eles?
R: Eles são o Sistema.

- Como é que fazem isso?
R: Basta um pouco de tecnologia.

- Só isso?
R: Bem, também têm "livre acesso" a todo um conjunto de software e hardware e utilizam tudo isso para benefício pessoal.

- Mas não se pode fazer isso!
R: Pois é... não se pode mas fazem.

- Mas, então, essas pessoas são criminosas, professor?!
R: Excelente dedução. Já passou na disciplina.

DEFINIÇÕES - GLOSSÁRIO

Firewall

É o conjunto de software e hardware (computador, servidor + router) destinados à restrição do acesso e protecção de uma rede de um computador individual ou conjunto de computadores em rede.

A sua função básica é de garantir a segurança de uma rede e proteger a rede interna (intranet/rede local) de ataques externos (internet). Funciona como uma barreira “alfandegária” de controlo de acesso entre estas duas redes. Permite definir o tipo de tráfego – entrada e saída; aplicar filtragem de pacotes de dados; estabelecer sistemas de autenticação; evitar acesso não-autorizado de pessoas na rede, etc.

Quer seja instalada em servidores ou no próprio sistema operativo do computador deve ser cuidadosamente configurada para o nível máximo de protecção.

Esta barreira “corta-fogo” é eficaz contra ataques externos, mas internamente não. Por exemplo, se um utilizador interno se ligar à rede externa, e tendo intenções maliciosas, criará uma porta de acesso à rede sem passar pelo firewall.

Modelo Cliente/Servidor

Computadores e equipamentos informatizados podem comunicar uns com os outros através de standards estabelecidos que ditam como cada participante na *conversa* se deve comportar. O padrão utilizado na internet, e na maioria dos sistemas actuais, é o chamado “Cliente/Servidor”.

A comunicação num modelo cliente/servidor é composta de dois módulos básicos:
- um módulo que faz requisições de serviços, designado de *cliente*;
- um módulo que recebe estes pedidos para executar as tarefas solicitadas, designado de *servidor*.

Por exemplo, quando se faz uma ligação à internet, o browser é o programa cliente que faz um pedido a uma programa servidor instalado num computador-servidor onde está hospedada uma página web. O servidor reconhece o pedido e retorna a página pretendida para acesso via http://. O mesmo acontece quando se abre um programa de e-mail (o utilizador pode aceder ao email e ter acesso ao seu conteúdo).

No nosso computador os programas-clientes só podem fazer pedidos e receber respostas, como por exemplo, aceder a um ficheiro e poder descarregá-lo. Teoricamente, isto é o que deve acontecer.
Contudo, há programas que podem inverter este papel, fazendo com que os nossos computadores se tornem servidores. Isto é, aplicam o modelo Servidor/Cliente. Com este modelo instalado o computador passa a responder a pedidos de ligação externos para acesso e transferência de ficheiros, por exemplo.

Permeabilidade Magnética μ

A permeabilidade magnética de um meio (*mu*) corresponde ao grau de magnetização de um material em resposta à exposição a um campo magnético externo.

Permissividade Eléctrica ε

A permissividade eléctrica de um meio (*épsilon*) é uma medida que permite obter o grau de polarização de um material em consequência à exposição de um campo eléctrico externo.

Participação Cidadã

EXPERIÊNCIA

Este teste tem como intuito comprovar (ou, pelos menos, levantar a suspeita) de que existem frequências artificiais geradas (por exemplo, por telemóveis) não-autorizadas que circulam no ambiente (ambiente doméstico e espaço público). Frequências estas, que não estão identificadas e não são nem do conhecimento público nem do conhecimento da comunidade científica.

Participe!

Colaboração: o Teste do Leite = Iogurte

Para saber se o seu ambiente está exposto às frequências de radiação da Microsoft, propomos-lhe que faça um teste verdadeiramente caseiro.

Atenção: este teste não é suficientemente objectivo, porque não exclui outras possibilidades. Não obstante, pode ser um bom indicador.

Obs.: Os resultados obtidos podem ter outras causas associadas a condições óptimas de pressão ambiente e temperatura que estimulam a função bacteriana e outros factores.

PROCEDIMENTOS:

1º passo:
Este teste é muito simples de se realizar. Só precisa de ter/adquirir uma chávena de cerâmica e um pacote de leite convencional (ex.: marca Agros ou Modelo-Continente. Não precisa de ser leite fresco.)

Observações:
A chávena pode ser uma caneca de loiça comum.

2º passo:
Sirva-se de uma chávena de leite (isto é: encha a chávena com leite. O leite deve estar bom, com validade.)

Observações:
O leite pode estar ao natural ou frio (tirado do frigorífico), é indiferente. Mas não ferva o leite.

3º passo:
Leve a chávena de leite para o ambiente onde normalmente trabalha no computador (ex.: escritório ou quarto).

4º passo:
Cubra/tape/esconda a chávena de leite para protegê-la da luz solar (a chávena deve estar na escuridão).

Observações:
Não utilize chávenas de vidro nem chávenas de plástico.
Não utilize tampas de rosca. Deixe que o leite fique arejado a 'absorver a energia ambiente'.

5º passo:
Aguarde, pelo menos, 14 horas.
(Faz de conta que levou a chávena de leite ao final da tarde e que se esqueceu de beber. Deixe-o passar assim a noite.)

Observações:
Desligue o seu computador ao final da tarde ou ao final do dia (supostamente, também ficará desligado da internet. O wi-fi deve estar desligado).
Pode deixar o seu telemóvel smartphone no mesmo quarto do computador (o telemóvel pode estar ligado ou desligado, é indiferente - estes dispositivos nunca estão verdadeiramente 'desligados'...)

Se estiver exposto às frequências de radiação da Microsoft, haverá uma energia constante a ser introduzida no seu ambiente.

6º passo:
Realize este teste pelo menos 10 vezes e aponte os resultados.

Hipóteses:

Acontecimento A (normal):
--> O leite tem tendência a estragar-se; talha; azeda; fica com mau gosto.

Acontecimento B (outro):
--> O leite transforma-se em iogurte. Apresenta-se com alguma densidade, aparência homogénea e bem formado; bom de gosto.

Observações:
Depois de realizada a experiência deite o leite fora e lave normalmente com sabão da loiça.

(mesmo que o leite/iogurte esteja bom de gosto não aconselhamos que o consuma, uma vez que não se sabe, exactamente, que propriedades é que adquiriu)

ANÁLISE DOS RESULTADOS:

(...)

ENVIO DOS RESULTADOS PARA O SEGUINTE E-MAIL:

forumsocial@o-musas.org

EXERCÍCIO DE FÍSICA PARA QUÍMICOS

Considere a experiência acima descrita.

- Que energia de activação (E) é necessária para que a molécula do leite comece a desencadear a reacção do iogurte?

Relação de Planck:

$E = h.f$

$E = (E_f - E_i)$

h = constante de Planck

f = frequência de radiação = ?

EXERCÍCIO DE FÍSICA PARA MATEMÁTICOS

Tema: pressões magnéticas

Considere o seguinte evento: