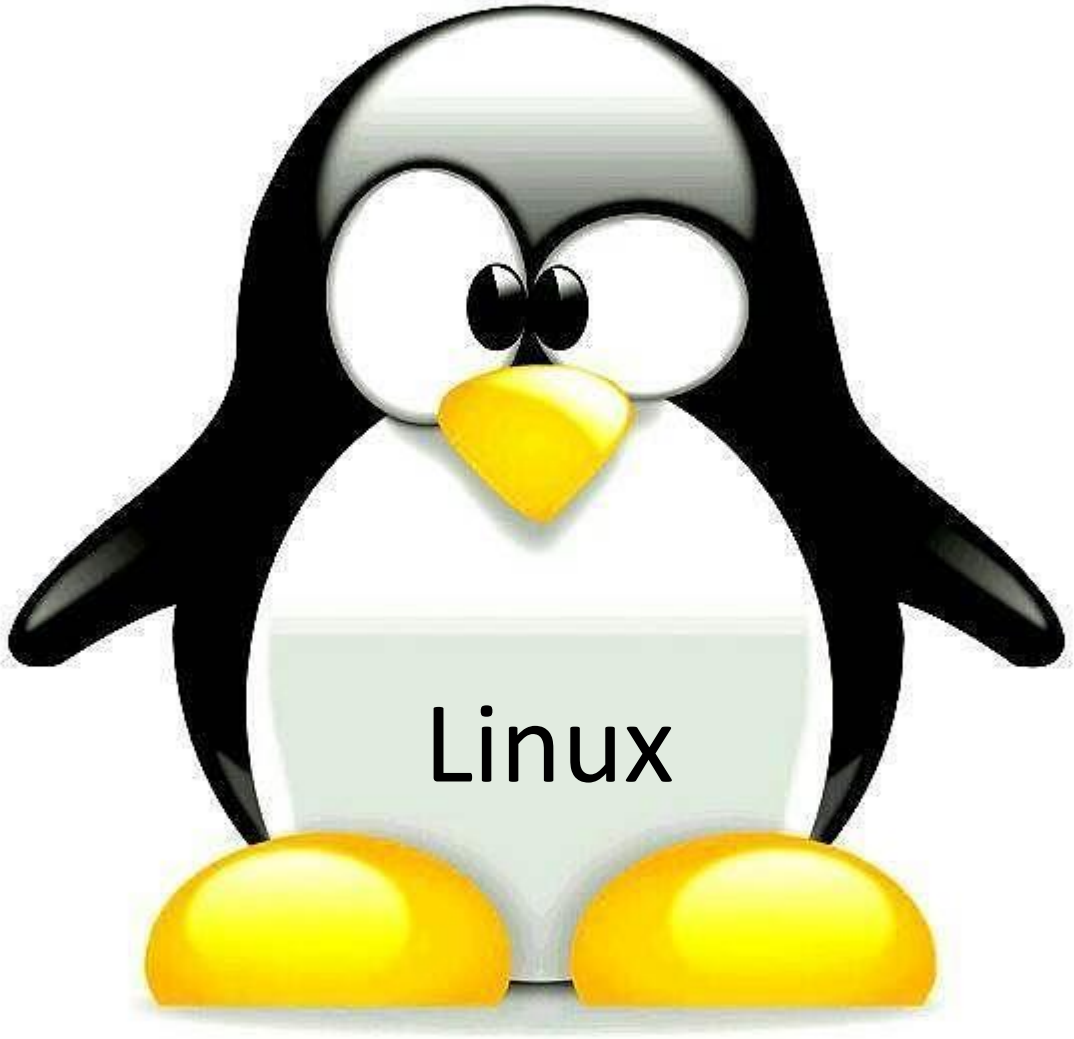
digital
escola
profissional

AntiVirus



Virus

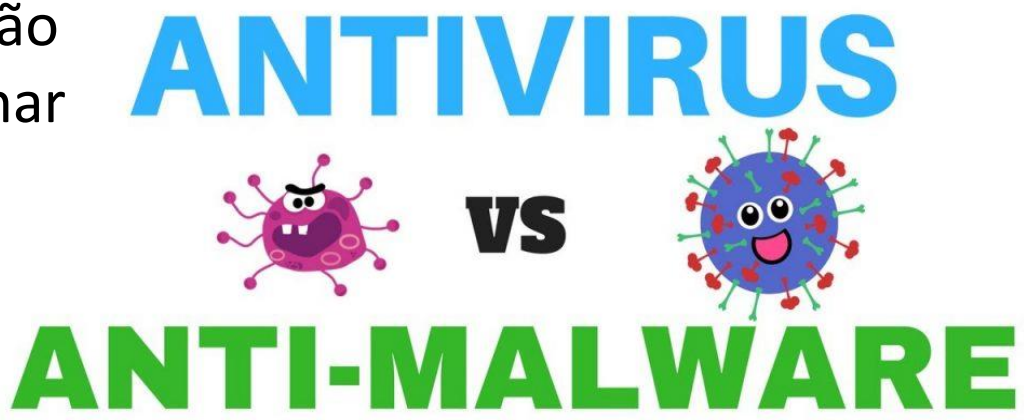
Virus informático é um programa que de alguma forma foi instalado no computador sem vontade expressa do utilizador.
Existem várias formas de propagação, mas normalmente está associado a uma má utilização por parte do utilizador, porque corre riscos ou porque não foi cuidadoso.

Malware

Malware é um termo mais genérico e agrega não só os vírus como todas as formas de criar situações indesejáveis pelo operador do computador.

Está associado a situações de destruição ou ocultação de informação ou só tornar o sistema inoperacional.

Exitem casos em que é pedido resgate para permitir a devolução da informação, normalmente em bitcoins.



Ransomware

Este é o tipo de ataque mais usado ultimamente.
Após infectado, o computador cifra a informação dos utilizadores.
Ao tentar aceder é apresentada informação que para conseguir a chave para descifrar os dados, terá que fazer um pagamento em bitcoins (ou outra moeda vulgar na internet).
Torna-se importante não pagar, raramente é possível a recuperação pela entrega da chave e estamos a alimentar uma actividade ilegal.

Se for vítima, não pague, veja se a plataforma nomoreransom tem ajuda.
https://www.nomoreransom.org/pt/index.html
https://www.nomoreransom.org/pt/decryption-tools.html

Métodos de propagação

Existem muitos métodos de propagação. Alguns mais derivados de brechas de segurança que uma aplicação tenha, ou ainda por causa imediata do utilizador que recebe um conteúdo e como o considera seguro, segue as instruções e executa o mesmo.

São exemplos prácticos a recepção de uma email com algo que propõe um benefício ou a pesquisa de algo legalmente mais questionável que leva o utilizador a sites pouco seguros.

LMD

Existem vários packages, aqui iremos usar um que é de utilização livre, o Linux Malware Detect (LMD) que é um malware scanner para Linux segundo a GNU GPLv2 license.

https://www.rfxn.com/projects/linux-malware-detect/

Utiliza o ClamAV como motor de anti-vírus para Linux.

Extra Packages for Enterprise Linux

Vamos começar por instalar um package que nos permite avançar, incluindo utilitários

```
[root@centos7 ~]# yum install epel-release
Loaded plugins: fastestmirror, langpacks
Loading mirror speeds from cached hostfile
 * base: mirrors.pt
...
================================================================
 Package            Arch          Version       Repository      Size
================================================================
Installing:
 epel-release       noarch        7-11          extras          15 k
...
Running transaction
  Installing : epel-release-7-11.noarch                          1/1
  Verifying  : epel-release-7-11.noarch                          1/1

Installed:
  epel-release.noarch 0:7-11

Complete!
```

Mailx

Como uma das formas como desejamos ser avisados é por email visto ser uma forma confortável para receber informação de várias máquinas, é importante ter instalado o mailx

```
[root@centos7 ~]# yum install mailx
Loaded plugins: fastestmirror, langpacks
Loading mirror speeds from cached hostfile
epel/x86_64/metalink                                    |  29 kB  00:00:00
 * base: mirrors.pt
 * epel: mirrors.ptisp.pt
 * extras: mirror.librelabucm.org
 * updates: mirrors.pt
epel                                                    | 4.7 kB  00:00:00
(1/3): epel/x86_64/group_gz                             |  95 kB  00:00:00
(2/3): epel/x86_64/updateinfo                           | 1.0 MB  00:00:00
(3/3): epel/x86_64/primary_db                           | 6.8 MB  00:00:01
Package mailx-12.5-19.el7.x86_64 already installed and latest version
Nothing to do
```

LMD

Vamos então fazer o download e descompactação do package para a directoria de temporários

```
[root@centos7 ~]# cd /tmp
[root@centos7 tmp]# wget http://www.rfxn.com/downloads/maldetect-current.tar.gz
--2020-05-29 14:43:30--  http://www.rfxn.com/downloads/maldetect-current.tar.gz
Resolving www.rfxn.com (www.rfxn.com)... 104.31.92.133, 104.31.93.133, 172.67.192.218, ...
Connecting to www.rfxn.com (www.rfxn.com)|104.31.92.133|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1549126 (1.5M) [application/x-gzip]
Saving to: ‘maldetect-current.tar.gz’

100%[======================================>] 1,549,126   2.89MB/s   in 0.5s

2020-05-29 14:43:37 (2.89 MB/s) - ‘maldetect-current.tar.gz’ saved [1549126/1549126]

[root@centos7 tmp]# tar -xzf maldetect-current.tar.gz
```

Instalação LMD

E proceder à sua instalação

```
[root@centos7 tmp]# cd maldetect-1.6.4/
[root@centos7 maldetect-1.6.4]# ./install.sh
Created symlink from /etc/systemd/system/multi-user.target.wants/maldet.servisse
To /usr/lib/systemd/system/maldet.service.
...
installation completed to /usr/local/maldetect
config file: /usr/local/maldetect/conf.maldet
exec file: /usr/local/maldetect/maldet
exec link: /usr/local/sbin/maldet
exec link: /usr/local/sbin/lmd
cron.daily: /etc/cron.daily/maldet
maldet(55851): {sigup} performing signature update check...
maldet(55851): {sigup} local signature set is version 201907043616
maldet(55851): {sigup} new signature set 2020052828325 available
maldet(55851): {sigup} 17030 signatures (14210 MD5 | 2035 HEX | 785 YARA | 0 USER)
...
[root@centos7 maldetect-1.6.4]# ln -s /usr/local/maldetect/maldet /bin/maldet
[root@centos7 maldetect-1.6.4]# hash -r
```

Configuração do LMD

Editar o ficheiro /usr/local/maldetect/conf.maldet e alterar os seguintes parâmetros:

email_alert="0” –> “1” para que os alertas possam ser enviados por email

email_addr="you@domain.com" para um endereço válido para envio de alertas

scan_clamscan="0” –> “1” para usar o scan do ClamAV

quarantine_hits="0” –> ”1” activar a quarentena

quarantine_clean="0” –> “1” remover os ficheiros em quarentena

ClamAV - instalação

Instalamos também o ClamAV que nos mostra muita informação mas aqui foi omitida.

```
[root@centos7 maldetect-1.6.4]# yum install clamav clamav-devel
Loaded plugins: fastestmirror, langpacks
Loading mirror speeds from cached hostfile
 * base: mirrors.pt
 * epel: mirrors.ptisp.pt
..
Installing:
 clamav              x86_64      0.102.2-4.el7      epel      399 k
 clamav-devel        x86_64      0.102.2-4.el7      epel       45 k
...
Total size: 7.2 M
Total download size: 4.0 M
Is this ok [y/d/N]: y
Downloading packages:
...
Complete!
```

ClamAV - actualizar

A instalação do produto não garante a sua actualidade e muito menos permite manter actualizado. Para isso teremos que usar o freshclam que actualiza com as novas políticas ...

```
[root@centos64 ~]# freshclam
ClamAV update process started at Tue Oct  6 13:15:06 2020
daily database available for update (local version: 25925, remote version: 25948)
Current database is 23 versions behind.
Downloading database patch # 25926...
Time: 1.2s, ETA: 0.0s [=============================>] 229.94KiB/229.94KiB
Downloading database patch # 25927...
Time: 0.4s, ETA: 0.0s [=============================>] 104.28KiB/104.28KiB
...
Testing database: '/var/lib/clamav/tmp.9cd16/clamav-02ba0b0019ff4b02b1daf7da3eb8d1c0.tmp-daily.cld' ...
Database test passed.
daily.cld updated (version: 25948, sigs: 4327670, f-level: 63, builder: raynman)
main.cvd database is up to date (version: 59, sigs: 4564902, f-level: 60, builder: sigmgr)
bytecode.cvd database is up to date (version: 331, sigs: 94, f-level: 63, builder: anvilleg)
```

Testar

Para testar iremos correr o maldet indicando que deve validar a home directory dos utilizadores, naturalmente o local mais provável de encontrar este tipo de ficheiros

```
[root@centos7 ~]# maldet -a /home
Linux Malware Detect v1.6.4
        (C) 2002-2019, R-fx Networks <proj@rfxn.com>
        (C) 2019, Ryan MacDonald <ryan@rfxn.com>
This program may be freely redistributed under the terms of the GNU GPL v2

maldet(7953): {scan} signatures loaded: 17030 (14210 MD5 | 2035 HEX | 785 YARA | 0 USER)
maldet(7953): {scan} building file list for /home, this might take awhile...
maldet(7953): {scan} setting nice scheduler priorities for all operations: cpunice 19 , ionice 6
maldet(7953): {scan} file list completed in 0s, found 958 files...
maldet(7953): {scan} found clamav binary at /bin/clamscan, using clamav scanner engine...
maldet(7953): {scan} scan of /home (958 files) in progress...

maldet(7953): {scan} scan completed on /home: files 958, malware hits 0, cleaned hits 0, time 15s
maldet(7953): {scan} scan report saved, to view run: maldet --report 200529-1603.7953
```

Relatório

E realizando o comando indicado:

maldet --report 200529-1603.7953

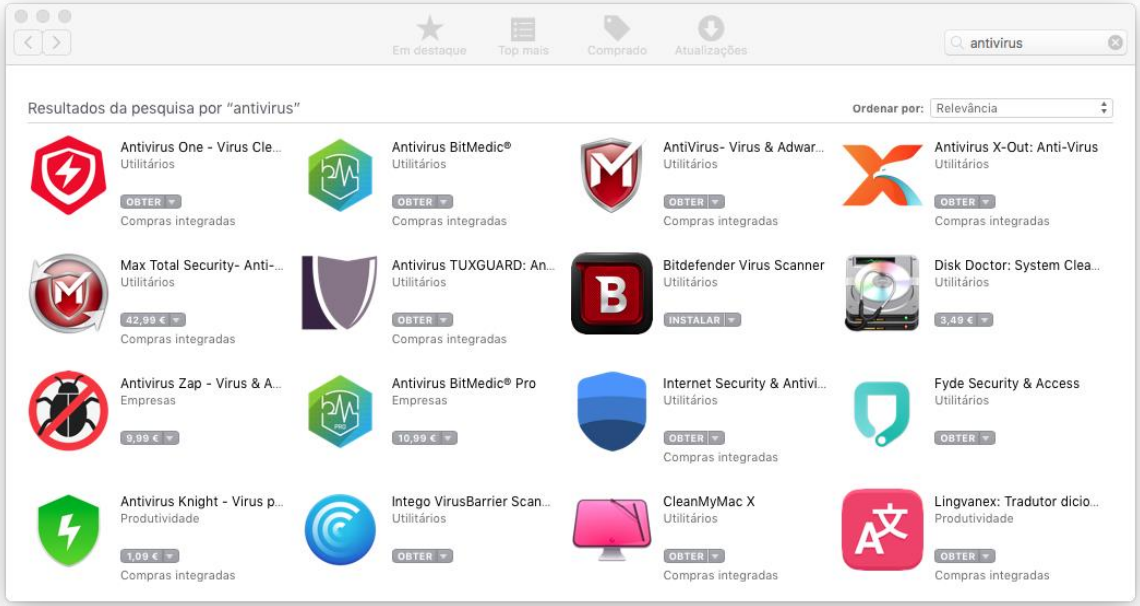
Iremos obter o relatório da execução


```
HOST:       centos7.myhome
SCAN ID:    200529-1603.7953
STARTED:    May 29 2020 16:04:01 +0100
COMPLETED: May 29 2020 16:04:16 +0100
ELAPSED:    15s [find: 0s]

PATH:       /home
TOTAL FILES:   958
TOTAL HITS:    0
TOTAL CLEANED: 0

==========================================
Linux Malware Detect v1.6.4 < proj@rfxn.com >
```

Outros Sistemas Operativos

Para cada sistema operativo existem vários packages de anti malware/antivirus e diferentes formas de instalação.

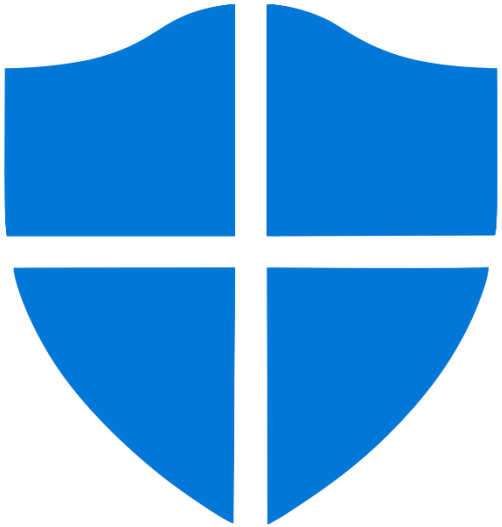
As lojas de aplicações têm normalmente vários, alguns sem custos, outros com custos inerentes ou ainda noutros casos free com certas limitações.



MS Windows

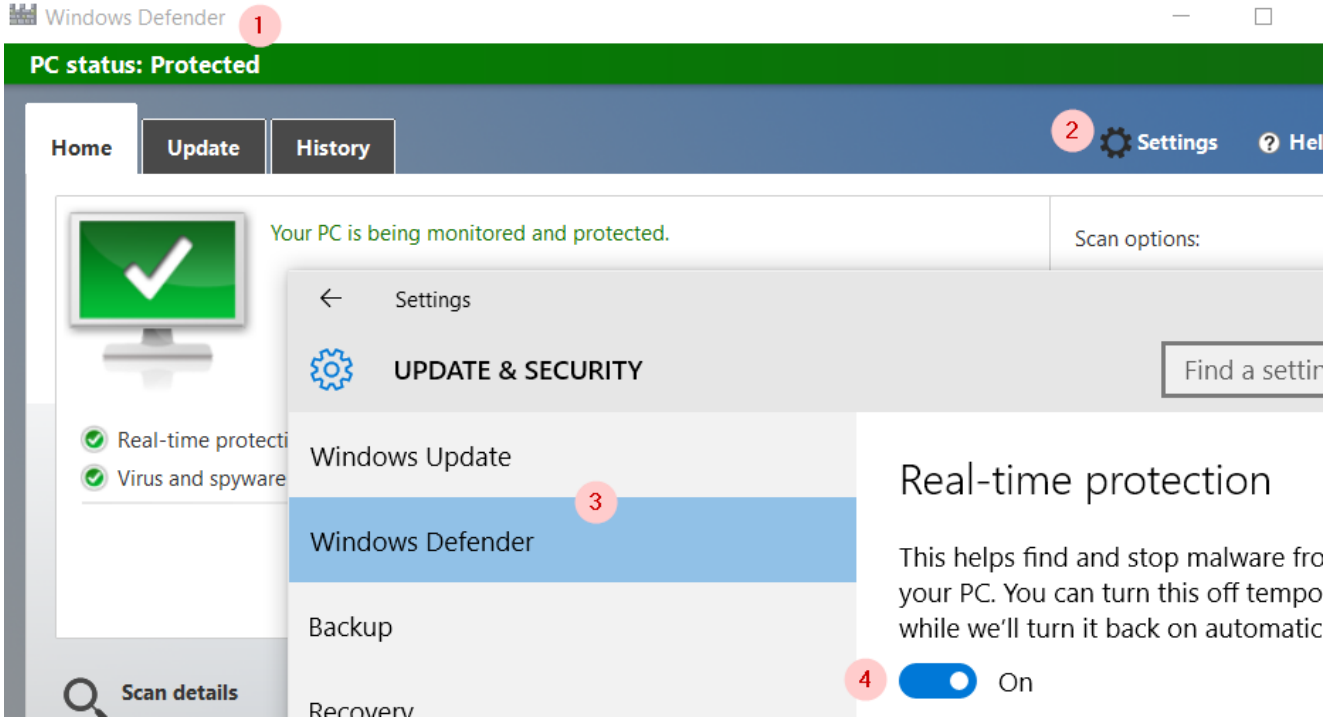
O Windows é uma sistema muito utilizado, logo particularmente apetecível para o desenvolvimento de ataques.
Com esse conhecimento, a Microsoft adicionou ao sistema operativo um sistema de anti-malware de base.

Windows Defender



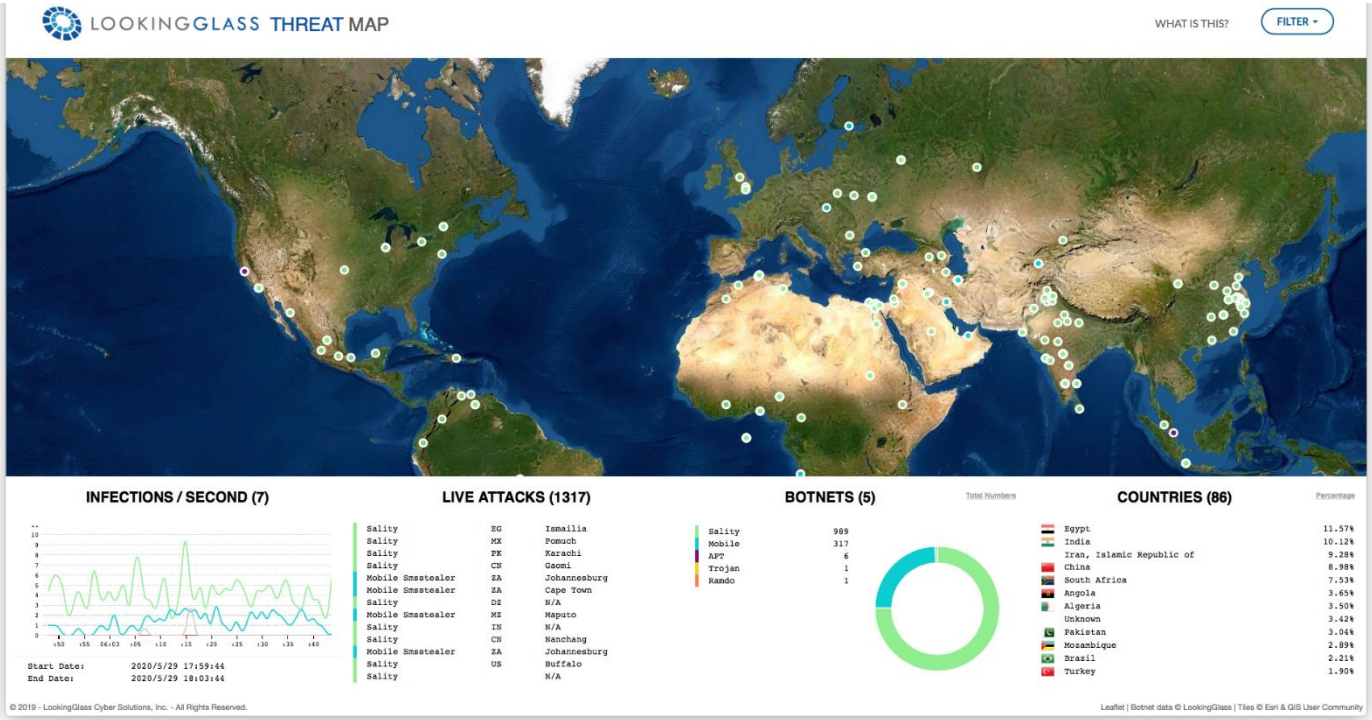
Windows Defender

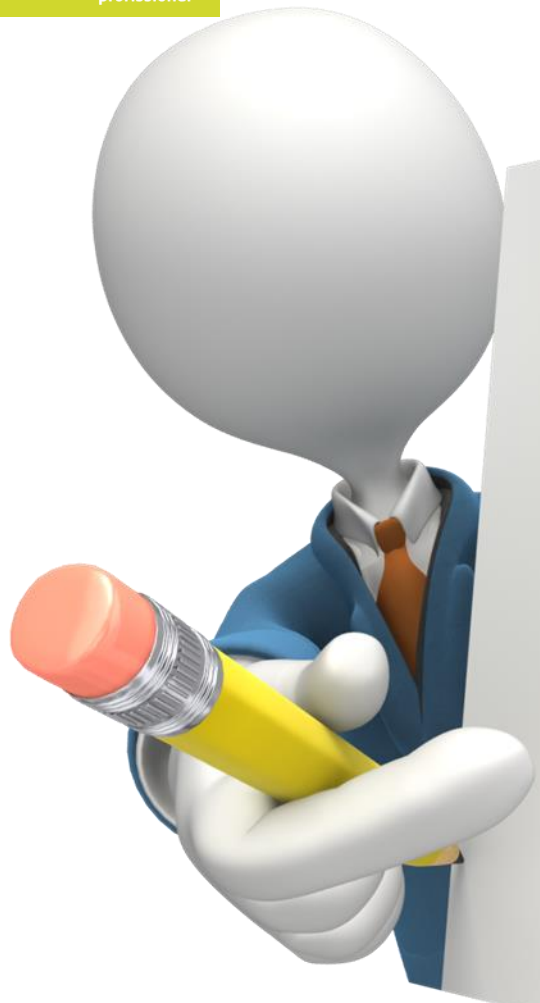
Nunca esquecer que a melhor garantia e está facilmente nas nossas mãos é manter as ferramentas actualizadas.



Visão global online

Uma visão global dos ataques que estão a acontecer pode ser vista em vários sites, por exemplo em https://map.lookingglasscyber.com





Perguntas

1. Qual a diferença entre malware e virus?
2. Quais os métodos de propagação que conhece?
3. Qual é normalmente o objectivo ?
4. Qual o package que normalmente usa? Porquê?
5. Todos os sistemas devem estar protegidos com package de anti-malware! Comente!