

Nom i Cognoms	Data	QUALIFICACIÓ
Arnau Subirós Puigarnau	03-10-2018	

## ACTIVITAT PT1 001

### ● **MALWARE** : **Autorun.inf**

**Cerca informació sobre el malware *autorun.inf* i respon les següents qüestions:**

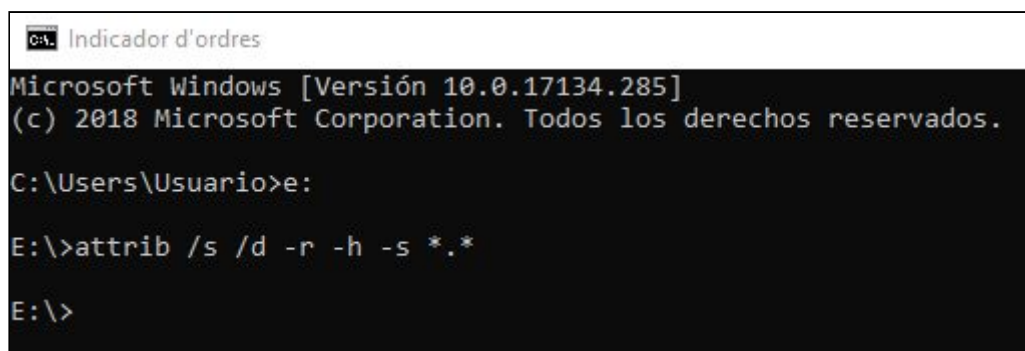
#### ❑ **Quin tipus de malware és *autorun.inf*?**

Autorun.INF és un **CUC** que es reproduïx creant còpies de si mateix, sense infectar altres arxius.

Es propaga i afecta a altres ordinadors. Es propaga , a través xarxa d'ordinadors, a través de recursos compartits de xarxa, mitjançant la infecció d'arxius que posteriorment són distribuïts.

**Important:** Els arxius autorun.inf tenen els atributs d'ocult, solament lectura i de sistema pel que en examinar la teva memòria flaix en l'explorador no els veuràs.

- Obrint la consola de windows escrivint CMD
- Un cop oberta escrit el següent comand : attrib /s /d -r -h -s \*.\*
- Et mostrarà els arxius ocults ( en cas que n'hi hagi)



```
Indicador d'ordres
Microsoft Windows [Versión 10.0.17134.285]
(c) 2018 Microsoft Corporation. Todos los derechos reservados.

C:\Users\Usuario>e:

E:\>attrib /s /d -r -h -s *.*

E:\>
```

Nom i Cognoms	Data	QUALIFICACIÓ
Arnau Subirós Puigarnau	03-10-2018	

Autorun.INF utilitza els següents mètodes de propagació:

- Explotació de vulnerabilitats amb intervenció de l'usuari: aprofita vulnerabilitats en formats d'arxiu o aplicacions. Per explotar-les amb èxit, necessita de la intervenció de l'usuari: obertura d'arxius, visita a pàgines web malicioses, lectura de missatges de correu, etc.
- Xarxes d'ordinadors (unitats mapeadas): crea còpies de si mateix en les unitats de xarxa mapeadas.
- Xarxes d'ordinadors (recursos compartits): crea còpies de si mateix en els recursos compartits de xarxa als quals aconsegueix accedir.
- Infecció d'arxius: infecta arxius de diferents tipus, que posteriorment són distribuïts a través de qualsevol de les vies habituals: disquets, missatges de correu electrònic amb arxius adjunts, descàrregues d'Internet, transferència d'arxius a través de FTP, canals de IRC i xarxes d'intercanvi d'arxius entre parells (P2P), etc.

### ❑ A quins sistemes afecta?

Els sistemes operatius afectats són :

- Windows 95
- Windows 98
- Windows XP
- Windows 2000
- Windows NT
- Windows ME
- Windows 2003

Nom i Cognoms	Data	QUALIFICACIÓ
Arnau Subirós Puigarnau	03-10-2018	

## ❑ Què és USB Vaccine?

- És una utilitat de seguretat (*gratuïta*) desenvolupada per Panda Security per evitar la forma d'infecció més comuna en els dispositius extraïbles com a discos durs, pendrives, mp3...

La seva forma de treballar és bastant senzilla i efectiva crea un fitxer autorun.inf en el dispositiu i ho protegeix perquè no es pugui modificar ni eliminar, d'aquesta forma, encara que es copii un virus en aquest dispositiu, no s'executarà de forma automàtica en connectar el dispositiu a un ordinador..



## ❑ Quines mesures de seguretat pots prendre?

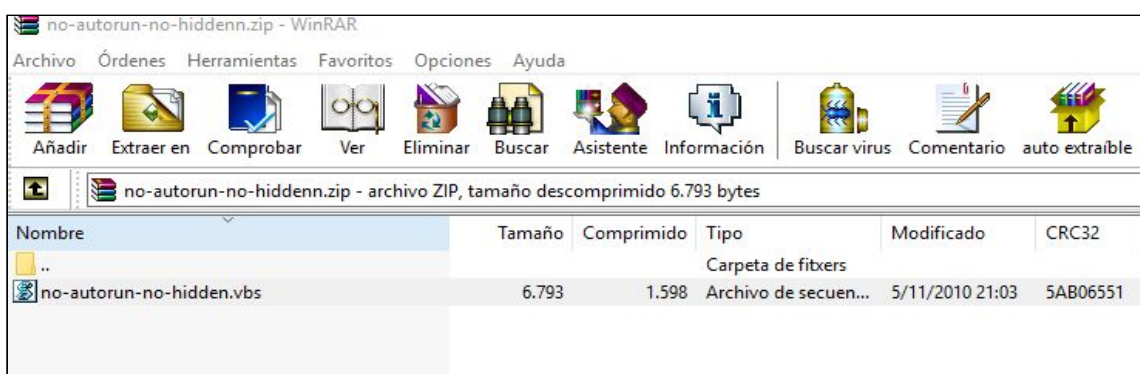
**Nota:** Per tenir més informació de com eliminar el virus autorun.inf podeu visitar el vídeo:  
[http://www.youtube.com/watch?v=8f4Fd1tPRw8&feature=player\\_embedded](http://www.youtube.com/watch?v=8f4Fd1tPRw8&feature=player_embedded)

Existeixen varies formes per eliminar el virus “**autorun.inf**” de qualsevol dispositiu USB :

- **Utilitzant un arxiu batch** ( és un arxiu de processament per lots. Es tracta d'arxius de text sense format, guardats amb l'extensió .BAT que contenen un conjunt d'instruccions MS-DOS.) .És un script d'arxius .bat
  - S'ha de tenir en compte que cap dels arxius batch s'han d'executar des d'una memòria USB o un altre dispositiu d'emmagatzematge. S'han d'executar directament des de carpetes que es trobin en el disc dur de la PC, per exemple L'Escriptori.

Nom i Cognoms	Data	QUALIFICACIÓ
Arnau Subirós Puigarnau	03-10-2018	

En el meu cas em baixaria l'arxiu d'internet (tot i que només hauria de ser de pàgines verificades )per eliminar de qualsevol arxiu que acabi amb l'extensió .inf, s'executa amb els atributs /A:R /A:H /A:S, que li indica a la consola de comandos eliminar l'arxiu encara que sigui de solament lectura, aquest ocult, i de sistema.



Nom i Cognoms	Data	QUALIFICACIÓ
Arnau Subirós Puigarnau	03-10-2018	

- **Eliminant els arxius “.autorun.inf” manualment utilitzant la consola CMD**
  - Obrint la consola de windows escrivint CMD
  - Un cop oberta escrit el següent comand : DEL \*.INF /F /Q /A:RHS
  - Enter i eliminar l'arxiu en cas que existeixi

```

Microsoft Windows [Versión 10.0.17134.285]
(c) 2018 Microsoft Corporation. Todos los derechos reservados.

C:\Users\Usuario>

E:\>DEL *.INF /F /Q /A:RHS
  
```

- **Evitar temporalment l'atac del virus “autorun.inf”** : Oprimint la tecla Shift en connectar la memòria en la PC i no deixar-la anar durant uns 6 a 8 segons, no obstant això si obres l'explorador i dónes dos clic en la icona de la memòria, es realitzarà l'acció predeterminada.
- **Utilitzant un Antivirus**
  - Per exemple, es pot utilitzar **Panda Antivirus\*** que és una eina gratuïta d'anàlisi online de Panda Security, que detectarà ràpidament tots els possibles virus i en cas de detectar “Autorun.Inf” automàticament es tindrà l'opció d'eliminar-lo.

En aquest exemple es mostra l'anàlisi de **Panda Dome**



Nom i Cognoms	Data	QUALIFICACIÓ
Arnau Subirós Puigarnau	03-10-2018	

## ❖ ANTIMALWARE : Malwarebytes

**Malwarebytes per Windows**, és una de les eines més utilitzades pel seu grau d'actualització de base de dades de malware i la seva eficàcia. La seva descàrrega i instal·lació és senzilla.

Podem obtenir una versió gratuïta a: <http://www.malwarebytes.org/>

Instal·leu l'eina en una màquina virtual amb el Windows XP i seguïu els passos dels següents apartats i, en primer lloc, feu-ne una actualització. A continuació podem fer un anàlisi complet del sistema des de la pestanya Escàner. Un cop fet l'escaneig podrem analitzar cada una de les entrades i eliminar les que desitgem.

Aquesta eina és molt útil per a rootkits que hagin modificat el registre de Windows i no permeti la seva edició o la execució de comandes mitjançant la consola.

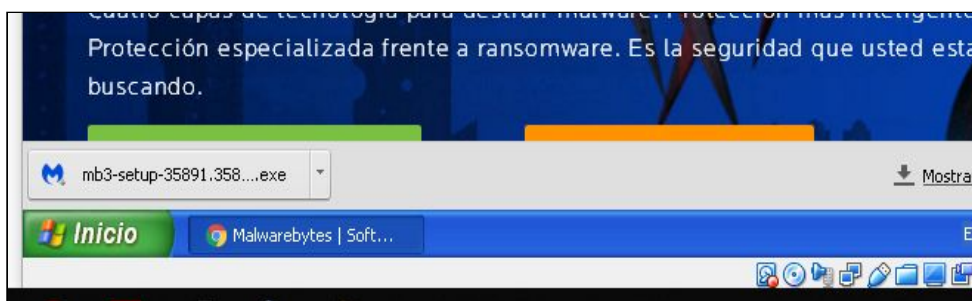
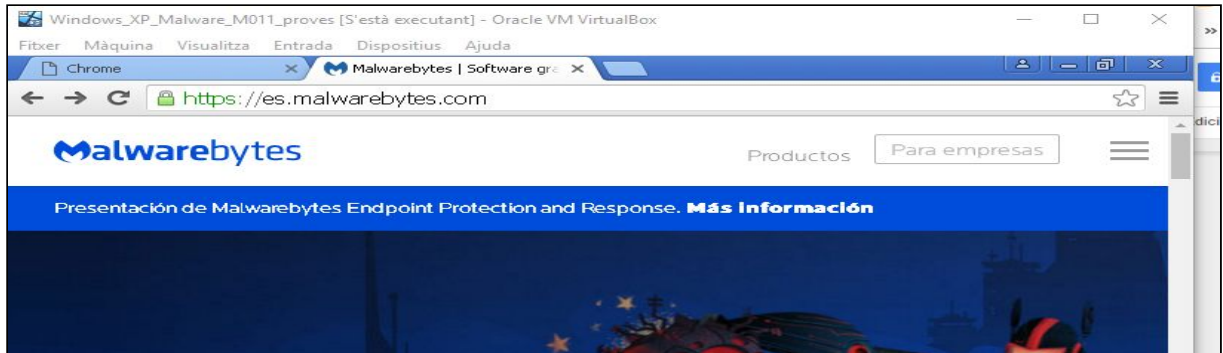
Eina capaç de detectar: codi malware (malware.trace), portes del darrera (backdoors), troians (trojan), etc..

Feu un anàlisi ràpid del sistema (captura la pantalla de l'anàlisi) i comenteu el resultat obtingut. Es demana unes captures de pantalla de com heu fet el procés (especifiqueu també si heu hagut de visualitzar algun vídeo o manual d'internet).

### ➤ Instal·lació Malwarebytes a la màquina virtual (Windows XP)

Un cop instal·lada la màquina virtual, m'he descarregat el navegador Chrome, ja que amb Internet Explorer em donava problemes. (tenint en compte que aquest sistema actualment és molt vulnerable a atacs ja que desde el 8 d'abril del 2014 ja no hi ha suport ni actualitzacions per aquest sistema operatiu).

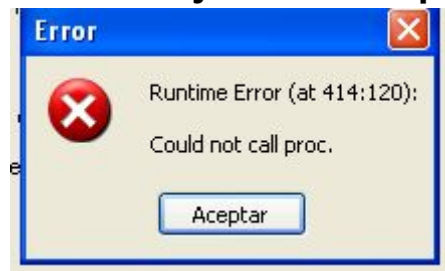
Nom i Cognoms	Data	QUALIFICACIÓ
Arnau Subirós Puigarnau	03-10-2018	



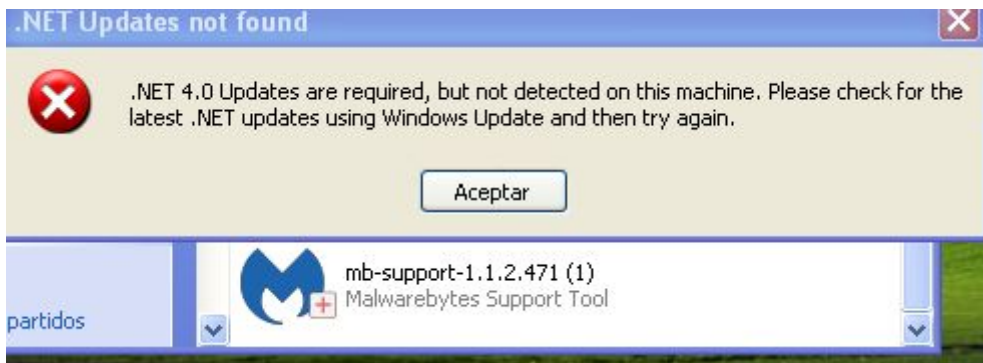


Nom i Cognoms	Data	QUALIFICACIÓ
Arnau Subirós Puigarnau	03-10-2018	

## ➤ Instal·lació Malwarebytes a la màquina virtual (Windows XP)



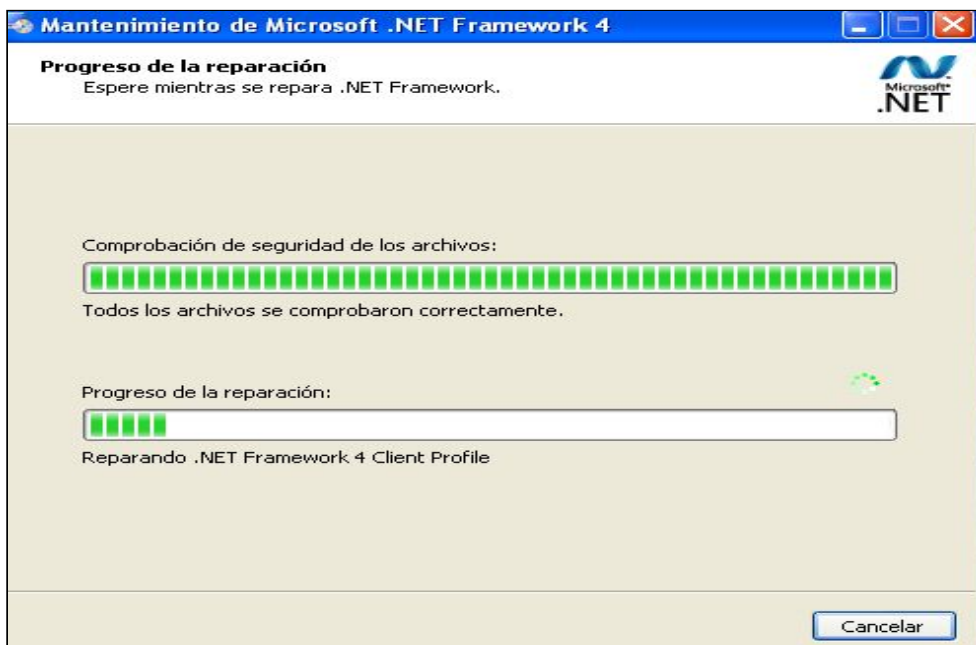
- Em dona error al intentar instal·lar i m'haig d'instal·lar una aplicació complementària:  
***mb-suport-1.2.2.471*** però també em dona error



- Em descarrego una actualització de ***.net 4.0*** ( tot i que Windows XP està obsolet)



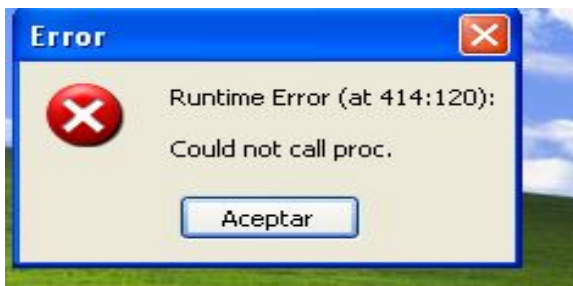
Nom i Cognoms	Data	QUALIFICACIÓ
Arnau Subirós Puigarnau	03-10-2018	



Nom i Cognoms	Data	QUALIFICACIÓ
Arnau Subirós Puigarnau	03-10-2018	

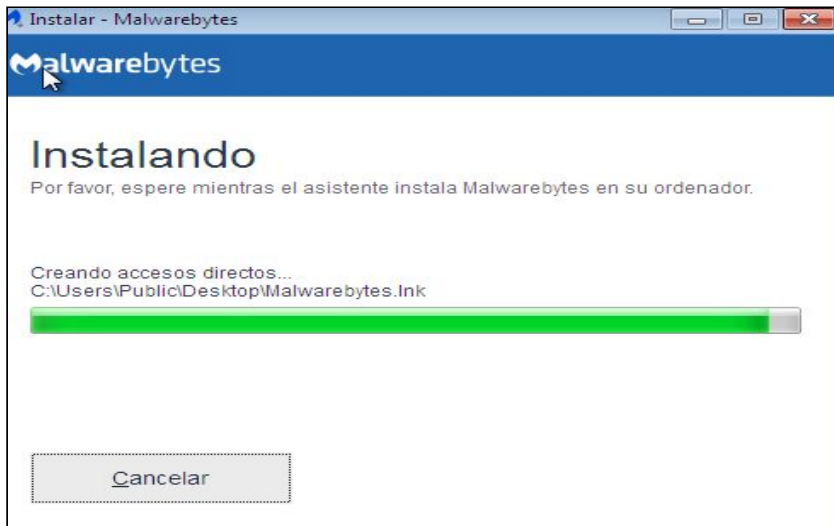


He intentat sense èxit, pero no puc instal·lar Malwarebytes al Windows XP , em torna a sortir el mateix error. Decideixo instal·lar Malwarebytes a una altra màquina virtual, amb un sistema superior, Windows 7.



Nom i Cognoms	Data	QUALIFICACIÓ
Arnau Subirós Puigarnau	03-10-2018	

## ➤ Instal·lació Malwarebytes a la màquina virtual (Windows 7)



Nom i Cognoms	Data	QUALIFICACIÓ
Arnau Subirós Puigarnau	03-10-2018	

Analizar

Programación de análisis

### Análisis de amenazas

✓

✓

↻

⌚

⌚

⌚

⌚

Buscar actualizaciones

Operaciones de pre-análisis

Analizar memoria

Analizar archivos de inicio

Analizar registro

Analizar sistema de archivos

Análisis heurístico

Analizando en este momento: Objetos en memoria

Elementos analizados: 291

Tiempo transcurrido: 00:00:04

Amenazas identificadas: 0

Ver amenazas identificadas


Pausa

Cancelar

Analizar

Programación de análisis

Cerrar ✕



**El Análisis terminado.**  
**No se han detectado amenazas.**

Hora de análisis:	27 s
Elementos analizados:	147.602
Amenazas detectadas:	0

Nom i Cognoms	Data	QUALIFICACIÓ
Arnau Subirós Puigarnau	03-10-2018	

### Detalles del registro

Resultados del análisis:

No se han detectado amenazas

Fecha del análisis:

2/10/18

Hora del análisis:

23:19

Archivo de registro:

d292d144-c688-11e8-9596-0800276bde2f.json

### Información del software

Versión:

3.6.1.2711

Versión del paquete de componentes:

1.0.463

Versión del paquete de actualización:

1.0.7143

Licencia:

Prueba

### Información del sistema

SO:

Windows 7 Service Pack 1

CPU:

x86

### Resumen del análisis


Tipo de análisis:

Amenaza

Análisis iniciado por:

Manual

Nom i Cognoms	Data	QUALIFICACIÓ
Arnau Subirós Puigarnau	03-10-2018	

 Malwarebytes

**Informe: Analizar**

Este informe proporciona detalles de su análisis. Haga clic en el botón Exportar para exportar el registro o copiarlo en el portapapeles.

Resumen

Avanzado

Tipo de sistema de archivos:  
NTFS

Usuario:  
M011-Security\Arnau

**Opciones de análisis**

Memoria:  
Activado

Inicio:  
Activado

Sistema de archivos:  
Activado

Archivos:  
Activado

Rootkits:  
Desactivado

Heurística:  
Desactivado

Resultado:  
Completado

Objetos analizados:  
147.602

Amenazas detectadas:  
0

Amenazas en cuarentena:  
0

Tiempo transcurrido:  
00:00:27

Exportar

Cerrar

Nom i Cognoms	Data	QUALIFICACIÓ
Arnau Subirós Puigarnau	03-10-2018	

## • **ANTIVIRUS**

### **1. Anomeneu 3 antivirus en línia, comentant les seves característiques (no feu un copia/enganxa de la pàgina web):**

Un Antivirus en línia és un programa antivirus que funciona a través del navegador web.

#### Avantatges generals

- Constants actualitzacions
- Alta disponibilitat
- Bona alternativa quan el antivirus offline no detecta o no pot eliminar un programa maliciós
- Pots escanejar amb múltiples antivirus online a la vegada
- Acostuma ser gratuït

#### Desavantatges generals

- Falta eficàcia i no són tan complets com els antivirus que s'instalen a l'ordinador
- Lògicament no tenen protecció permanent (acaba al tancar al navegador)
- Només escanejan l'ordinador en busca d'antivirus
  - No protegeixen les àrees crítiques del sistema
  - No tenen mòduls especials per control de tràfic d'e-mails, etc.

### **1. ESET Online Scanner**

[www.eset.com/es/hogar/online-scanner//](http://www.eset.com/es/hogar/online-scanner//)

#### Característiques:

- S'accedeix desde qualsevol navegador web (Chrome, Opera, Firefox, Internet Explorer y Edge)
- Analiza el teu sistema operatiu
- Analiza i elimina malware
  - també analiza els arxius comprimits



Nom i Cognoms	Data	QUALIFICACIÓ
Arnau Subirós Puigarnau	03-10-2018	

## 2. VirusTotal Free Online

<https://www.virustotal.com/es/>

### Característiques:

- Opció per analitzar arxius concrets del teu ordinador ( 128 Mb màxim)
- Opció per analitzar URL concretes
- Opció de búsqueda : hash, dominis, direccions IP

### Objectiu:

- Un cop seleccionat l'arxiu o URL analitza la detecció de tot tipus de malware.

## 3. Jotti's Malware

<https://virusscan.jotti.org/contact>

### Característiques:

- Opció per analitzar 5 arxius concrets del teu ordinador simultàneament ( 100 Mb màxim/per arxiu)

### Objectiu:

- Un cop seleccionat els arxius els analitza la detecció de malware amb el suport de els principals antivirus (Kaspersky, Avira, F-Secure, Ad-aware)

Nom i Cognoms	Data	QUALIFICACIÓ
Arnau Subirós Puigarnau	03-10-2018	

**2. Ompliu la següent taula indicant les característiques dels següents antivirus en les seves últimes versions:**

Característica	KASPERSKY TOTAL SECURITY 19	Security Essentials	Trend Micro Maxium Security (2018)	BitDefender Total Security 2019
Antivirus	SI	SI	SI	SI
Antispyware	SI	SI	SI	SI
Link Scanner	SI	-	SI	SI
Firewall	SI	SI	SI	SI
Antispam	SI	-	SI	SI
Sistemes x64	SI	-	SI	SI
Espanyol	SI	SI	SI	SI
Suport tècnic	SI	-	SI	SI
(Mac i Linux	No suporta sistemes Linux	No suporta sistemes Linux	No suporta sistemes Linux	SI
Consum de recursos (optimització)	SI	-	SI	SI
Gratuït o pagament	59,95€	Gratis	69.95€	69,98€

- Antivirus Kaspersky te 3 tipus de protecció ( bàsica, completa ,premium o prova de 30 días on varies les caracteísitiques i el preu),

[https://www.bitdefender.es/solutions/total-security.html#tsmd\\_features](https://www.bitdefender.es/solutions/total-security.html#tsmd_features)

**3. Què és la EICAR? I la CARO? Feu una recerca exhaustiva sobre els diferents tipus d'antivirus que s'han desenvolupat a Espanya i expliqueu els vostres resultats.**

- ☐ **EICAR**( European Institute for Computer Antivirus) és una organització formal( format per un conjunt de persones semblants a CARO)

Nom i Cognoms	Data	QUALIFICACIÓ
Arnau Subirós Puigarnau	03-10-2018	

❖ Té un enfocament diferent a CARO respecte a la seguretat jurídica

- ❑ **CARO** (Computer Antivirus Research Organization) : És una organització (grup tècnic) que estudia desde 1990 els virus informàtics . Anterior a EICAR

Tot i que avui dia els 2 grups treballen per separat, un projecte conjunt històric . Un projecte conjunt històric va ser EICAR- Test File (EICAR-AV-TEST) prova que va ser creada per membres CARO i publicat per EICAR.

- EICAR-AV-TEST no és un virus (només el simula) però no té codi maliciós i es pot executar sense cap problema.

## Antivirus Linux

Tots els sistemes operatius poden ser susceptibles a malwares i virus, incloent els sistemes Linux. Afortunadament són pocs els virus existents en aquests, i és per això que la gran majoria d'usuaris decideixen deixar el seu sistema desprotegit, sense fer ús de cap software antivirus. Es recomana especialment a aquells usuaris que utilitzen sistemes Linux i estan connectats a xarxes on tenen lloc transferències de fitxers. Alguns usuaris poden pensar que un antivirus requereix massa recursos del seu sistema, i tampoc és així, ja que existeixen low-footprint softwares per Linux. Per entendre millor el funcionament dels software antivirus és especialment important i beneficiós entendre en primer lloc el funcionament del malware per sí mateix.

En aquesta activitat se us demana que instal·leu i estudeu el funcionament de l'antivirus ClamAv i la seva versió gràfica Clamtk. Ho podeu fer seguint els següents passos de manera aproximada (és possible que hagueu de modificar alguna comanda):

### 1. Instal·lar l'antivirus ClamAv i la seva versió gràfica Clamtk:

```
> sudo aptitude install clamav  
> sudo aptitude install clamtk
```

Nom i Cognoms	Data	QUALIFICACIÓ
Arnau Subirós Puigarnau	03-10-2018	

```
arnsub@arnsub-m06: ~
Fitxer Edita Visualitza Cerca Terminal Ajuda
0%[[S'està treballant]^C
arnsub@arnsub-m06:~$ sudo aptitude install clamav
Els paquets nous següents s'instal·laran:
clamav clamav-base{a} clamav-freshclam{a} libclamav7{a} libcurl3{a} libjson-c3{a} libllvm3.8{a} libmspack0{a}
libtftml{a}
0 paquets actualitzats, 9 instal·lats, 0 a suprimir i 4 a no actualitzar.
Es necessita obtenir 12,0 MB d'arxius. Després del desempaquetat s'utilitzaran 46,5 MB.
Esteu segur de voler continuar? [Y/n/?] y
Obté: 1 http://security.debian.org/debian-security stretch/updates/main amd64 libmspack0 amd64 0.5-1+deb9u2 [46,1 kB]
Obté: 2 http://security.debian.org/debian-security stretch/updates/main amd64 libcurl3 amd64 7.52.1-5+deb9u7 [292 kB]
Obté: 3 http://ftp.fi.debian.org/debian stretch-updates/main amd64 clamav-base all 0.100.1+dfsg-0+deb9u1 [66,9 kB]
Obté: 4 http://ftp.fi.debian.org/debian stretch/main amd64 libjson-c3 amd64 0.12.1-1.1 [25,8 kB]
Obté: 5 http://ftp.fi.debian.org/debian stretch/main amd64 libllvm3.8 amd64 1:3.8.1-24 [10,4 MB]
Obté: 6 http://ftp.fi.debian.org/debian stretch/main amd64 libtftml amd64 0.13-4 [60,5 kB]
```

```
arnsub@arnsub-m06: ~
Fitxer Edita Visualitza Cerca Terminal Ajuda
arnsub@arnsub-m06:~$ sudo aptitude install clamtk
Els paquets nous següents s'instal·laran:
clamtk gnome-icon-theme{a} libcommon-sense-perl{a} libjson-perl{a} libjson-xs-perl{a} libtext-csv-perl{a}
libtext-csv-xs-perl{a} libtypes-serialiser-perl{a}
0 paquets actualitzats, 8 instal·lats, 0 a suprimir i 4 a no actualitzar.
Es necessita obtenir 10,5 MB d'arxius. Després del desempaquetat s'utilitzaran 17,5 MB.
Esteu segur de voler continuar? [Y/n/?] y
Obté: 1 http://ftp.fi.debian.org/debian stretch/main amd64 libtext-csv-perl all 1.33-2 [50,5 kB]
Obté: 2 http://ftp.fi.debian.org/debian stretch/main amd64 libjson-perl all 2.90-1 [86,0 kB]
Obté: 3 http://ftp.fi.debian.org/debian stretch/main amd64 gnome-icon-theme all 3.12.0-2 [9890 kB]
Obté: 4 http://ftp.fi.debian.org/debian stretch/main amd64 clamtk all 5.24-1 [193 kB]
```

Confirmo que s'ha instal·lat correctament utilitzant el comando search , si surt una “i” vol dir que està instal·lat

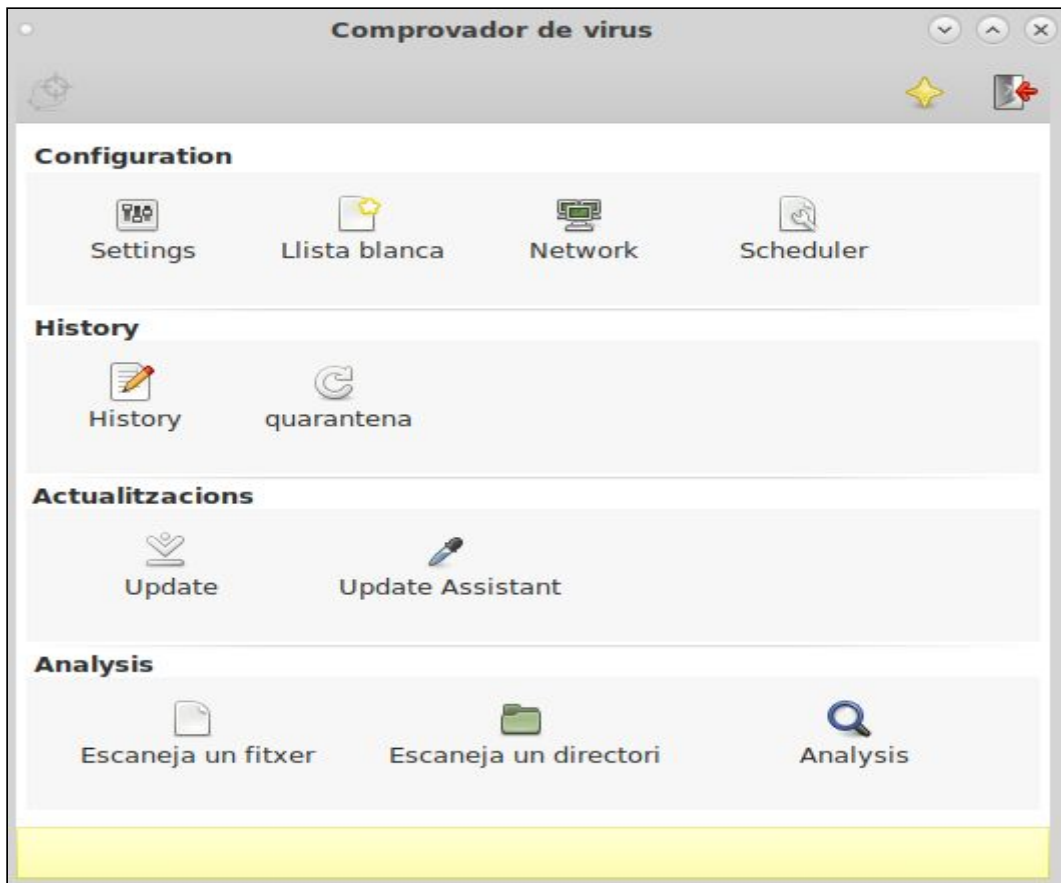
Nom i Cognoms	Data	QUALIFICACIÓ
Arnau Subirós Puigarnau	03-10-2018	

```
arnsub@arnsub-m06: ~
Fitxer Edita Visualitza Cerca Terminal Ajuda
arnsub@arnsub-m06:~$ sudo aptitude search clamav | grep clamav
i clamav - anti-virus utility for Unix - command-line interface
i A clamav-base - anti-virus utility for Unix - base package
p clamav-daemon - anti-virus utility for Unix - scanner daemon
v clamav-data -
p clamav-docs - anti-virus utility for Unix - documentation
i A clamav-freshclam - anti-virus utility for Unix - virus database update utility
p clamav-milter - anti-virus utility for Unix - sendmail integration
p clamav-testfiles - anti-virus utility for Unix - test files
p clamav-unofficial-sigs - update script for 3rd-party clamav signatures
p libc-icap-mod-clamav - transitional dummy package
p libclamav-client-perl - Perl client for the ClamAV virus scanner daemon
p libclamav-dev - anti-virus utility for Unix - development files
i A libclamav7 - anti-virus utility for Unix - library
p proftpd-mod-clamav - ProFTPD module mod_clamav
p python-pyclamav - Python bindings to ClamAV
arnsub@arnsub-m06:~$
```

```
arnsub@arnsub-m06: ~
Fitxer Edita Visualitza Cerca Terminal Ajuda
arnsub@arnsub-m06:~$ sudo aptitude search clamtk | grep clamtk
i clamtk - graphical front-end for ClamAV
p clamtk-gnome - GNOME (Nautilus) MenuProvider extension for ClamTk
p clamtk-nautilus - Nautilus MenuProvider extension for ClamTk
arnsub@arnsub-m06:~$
```

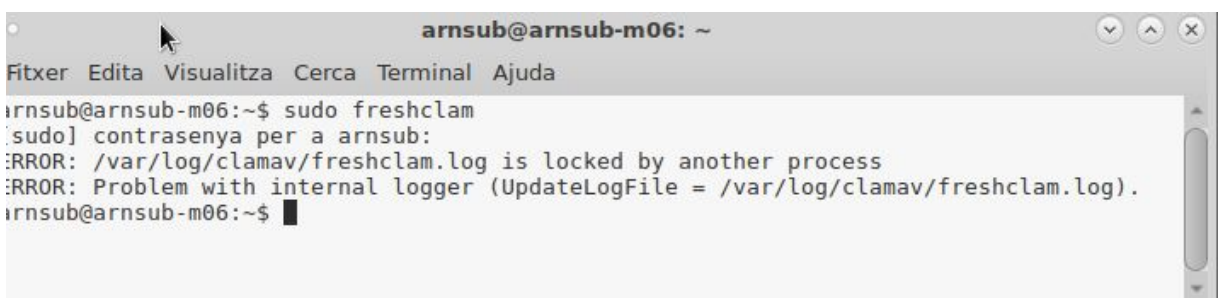


Nom i Cognoms	Data	QUALIFICACIÓ
Arnau Subirós Puigarnau	03-10-2018	



**2. Actualitzar la base de dades de virus de l'eina de forma online, mitjançant la comanda:**

```
> sudo freshclam
```





Nom i Cognoms	Data	QUALIFICACIÓ
Arnau Subirós Puigarnau	03-10-2018	

Em dona error, segurament l'actualització s'està executant de forma automàtica  
Utilitzaré aquest comando per detenir l'execució automàtica executant :

**sudo dpkg-reconfigure clamav-freshclam**

```
Configuració del paquet «clamav-freshclam»
Please choose the method for virus database updates.

daemon:  freshclam is running as a daemon all the time. You should choose
         this option if you have a permanent network connection;
ifup.d:  freshclam will be running as a daemon as long as your Internet
         connection is up. Choose this one if you use a dialup Internet
         connection and don't want freshclam to initiate new connections;
cron:    freshclam is started from cron. Choose this if you want full control
         of when the database is updated;
manual:  no automatic invocation of freshclam. This is not recommended,
         as ClamAV's database is constantly updated.

Virus database update method:

                                daemon
                                ifup.d
                                cron
                                manual

                                <D'acord>                                <Cancel·la>
```

```
Configuració del paquet «clamav-freshclam»
Please select the closest local mirror site.

Freshclam updates its database from a world wide network of mirror sites. Please select the closest mirror. If you
leave the default setting, an attempt will be made to guess a nearby mirror.

Local database mirror site:

db.local.clamav.net
db.ac.clamav.net (Ascension Island)
db.ad.clamav.net (Andorra)
db.ae.clamav.net (United Arab Emirates)
db.af.clamav.net (Afghanistan)
db.ag.clamav.net (Antigua and Barbuda)
db.ai.clamav.net (Anguilla)
db.al.clamav.net (Albania)
db.am.clamav.net (Armenia)
db.an.clamav.net (Netherlands Antilles)
db.ao.clamav.net (Angola)
db.aq.clamav.net (Antarctica)
db.ar.clamav.net (Argentina)
db.as.clamav.net (American Samoa)
db.at.clamav.net (Austria)
db.au.clamav.net (Australia)
db.aw.clamav.net (Aruba)
db.ax.clamav.net (Aland Islands)
db.az.clamav.net (Azerbaijan)
db.ba.clamav.net (Bosnia and Herzegovina)
db.bb.clamav.net (Barbados)
db.bd.clamav.net (Bangladesh)
db.be.clamav.net (Belgium)
db.bf.clamav.net (Burkina Faso)
db.bg.clamav.net (Bulgaria)
db.bh.clamav.net (Bahrain)
db.bi.clamav.net (Burundi)

                                <D'acord>                                <Cancel·la>
```



Nom i Cognoms	Data	QUALIFICACIÓ
Arnau Subirós Puigarnau	03-10-2018	

```

Please choose the method for virus database updates.

daemon: freshclam is running as a daemon all the time. You should choose
[Més] ^C
arnsub@arnsub-m06:~$ sudo dpkg-reconfigure clamav-freshclam
Replacing config file /etc/clamav/freshclam.conf with new version
Starting database update:
Wed Oct 3 00:03:27 2018 -> ClamAV update process started at Wed Oct 3 00:03:27 2018
Wed Oct 3 00:03:27 2018 -> main.cvd is up to date (version: 58, sigs: 4566249, f-level: 60, builder: sigmgr)
Wed Oct 3 00:03:27 2018 -> daily.cvd is up to date (version: 25001, sigs: 2107224, f-level: 63, builder: neo)
Wed Oct 3 00:03:27 2018 -> bytecode.cvd is up to date (version: 327, sigs: 91, f-level: 63, builder: neo)
arnsub@arnsub-m06:~$ █

```

Ara utilitzo novament el comando sudo freshclam

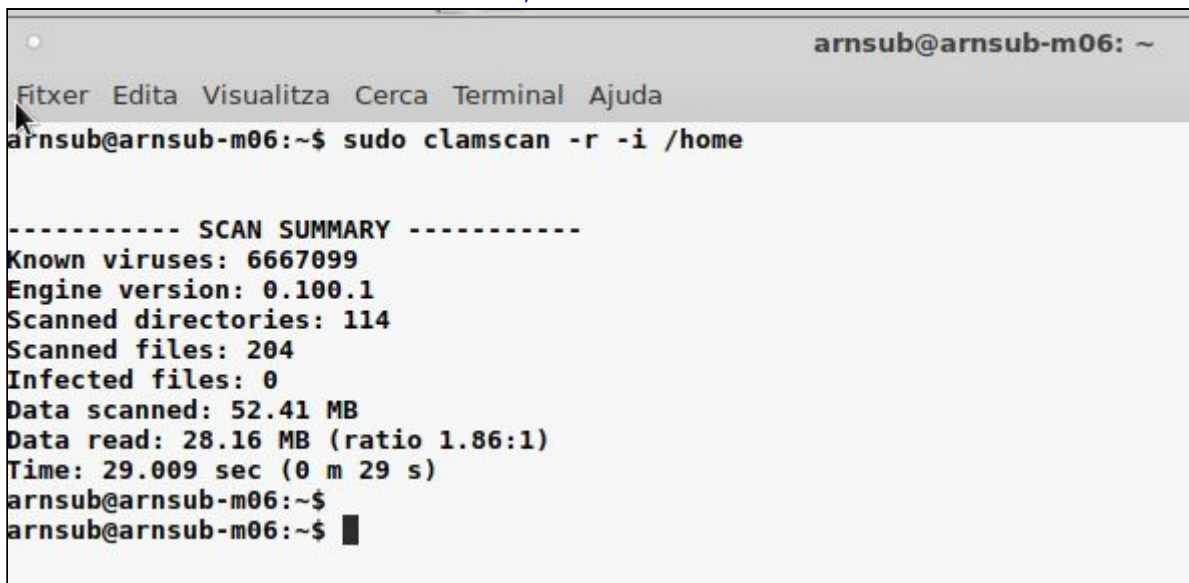
```

arnsub@arnsub-m06:~$ sudo freshclam
Wed Oct 3 00:04:30 2018 -> ClamAV update process started at Wed Oct 3 00:04:30 2018
Wed Oct 3 00:04:30 2018 -> main.cvd is up to date (version: 58, sigs: 4566249, f-level: 60, builder: sigmgr)
Wed Oct 3 00:04:30 2018 -> daily.cvd is up to date (version: 25001, sigs: 2107224, f-level: 63, builder: neo)
Wed Oct 3 00:04:30 2018 -> bytecode.cvd is up to date (version: 327, sigs: 91, f-level: 63, builder: neo)
arnsub@arnsub-m06:~$ █

```

### 3. Escannejar el directori (/home) de forma recursiva (opció -r) i que només ens mostri els arxius infectats (-i), per exemple:

```
> sudo clamscan -r -i /home
```



```

arnsub@arnsub-m06:~$ sudo clamscan -r -i /home

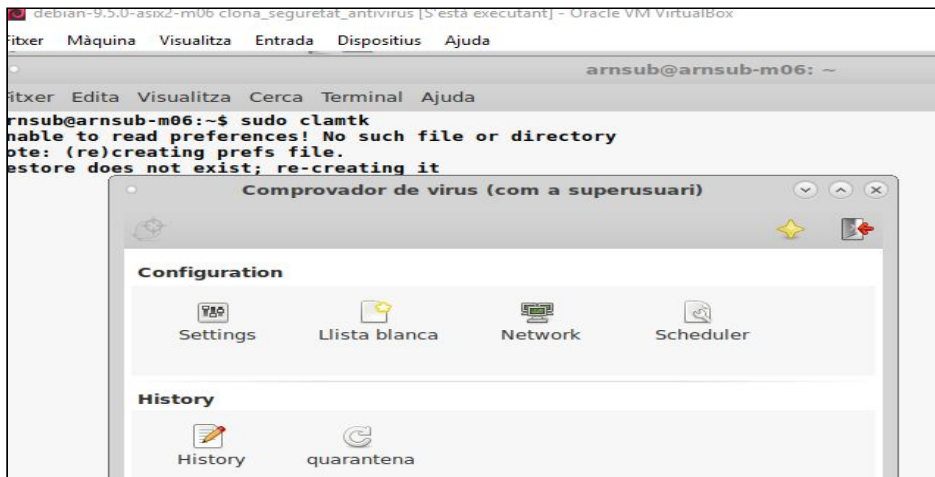
----- SCAN SUMMARY -----
Known viruses: 6667099
Engine version: 0.100.1
Scanned directories: 114
Scanned files: 204
Infected files: 0
Data scanned: 52.41 MB
Data read: 28.16 MB (ratio 1.86:1)
Time: 29.009 sec (0 m 29 s)
arnsub@arnsub-m06:~$
arnsub@arnsub-m06:~$ █

```

Nom i Cognoms	Data	QUALIFICACIÓ
Arnau Subirós Puigarnau	03-10-2018	

#### 4. Executar la versió gràfica mitjançant:

```
> sudo clamtk
```



**Es demana unes captures de pantalla de com heu fet el procés (especifiqueu també si heu hagut de visualitzar algun vídeo o manual d'internet).**

Per instal·lar ClamAv i la seva versió gràfica Clamtk no he tingut problema seguint les indicacions.

Tot i que he tingut problema al actualitzar el programa ja que freshclam es un daemon ( un servei que funciona en segon pla ) i he tingut que buscar per internet la manera per desactivarlo y actualitzar-lo manualment.

```
sudo dpkg-reconfigure clamav-freshclam
```