Manual Instalació | Kontor Tek Inc

Index

1. Antes de instalar

Antes de instalar el paquete **malware-detector**, es importante tener creado un “bot” de **Telegram** usando **Botfather**.

Nota: Actualmente, esta aplicación solo funciona en sistemas operativos Linux. Si deseas usarla en Windows, por favor espera futuras versiones.

1.1. Obtener Token

Una vez creado tu bot, utiliza el siguiente procedimiento para obtener el Token:

1. Abre Telegram y busca **@BotFather**.
2. Envía el comando **/mybots**.
3. Selecciona tu bot (ej. @ejemplo_bot).
4. Haz clic en API Token para verlo.

Guarda este Token en un lugar seguro, ya que lo necesitarás más adelante para obtener el ChatID y durante la instalación.

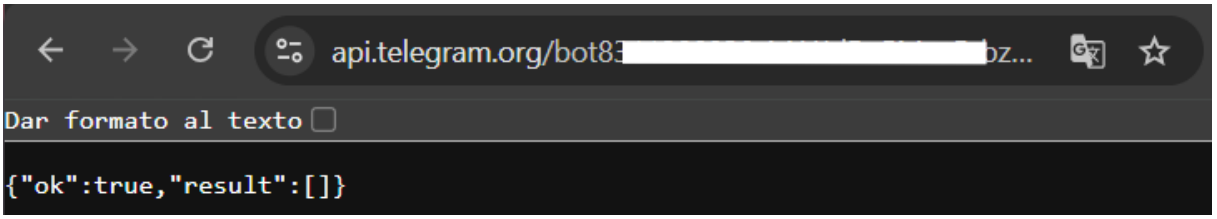
1.2. ChatID

Para obtener el ChatID, sigue estos pasos:

1. Abre un navegador web y usa el siguiente enlace (reemplaza <TU TOKEN> con el Token que guardaste):

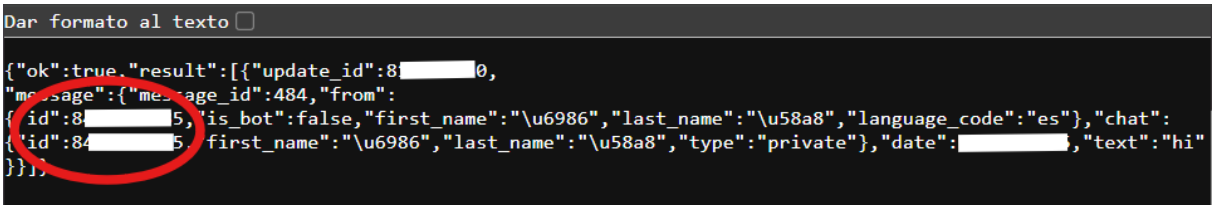
https://api.telegram.org/bot<TU TOKEN>/getUpdates

foto ejemplo que muestra el link:



2. Envía cualquier mensaje desde tu cuenta de Telegram al bot que creaste.

3. Vuelve a cargar la página del navegador. Ahora deberías ver una respuesta que incluye el ChatID.



Advertencia: No compartas tu Token ni tu ChatID con nadie. Si son expuestos, terceros podrían tomar el control de tu bot o de tu cuenta.

2. Instalación

Para obtener el paquete de instalación, primero debes crear una cuenta en el sitio web de Kontor Tek Inc.

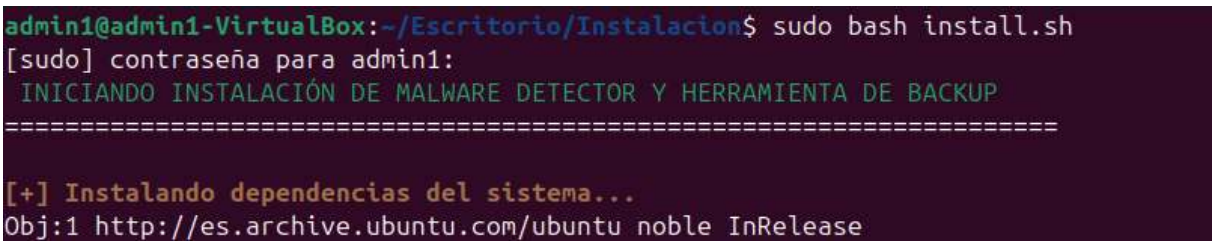
2.1. Paquete de instalación

Una vez descargado el archivo “instalacion.zip”, descomprímelo.

Obtendrás los siguientes archivos dentro de la carpeta instalacion:

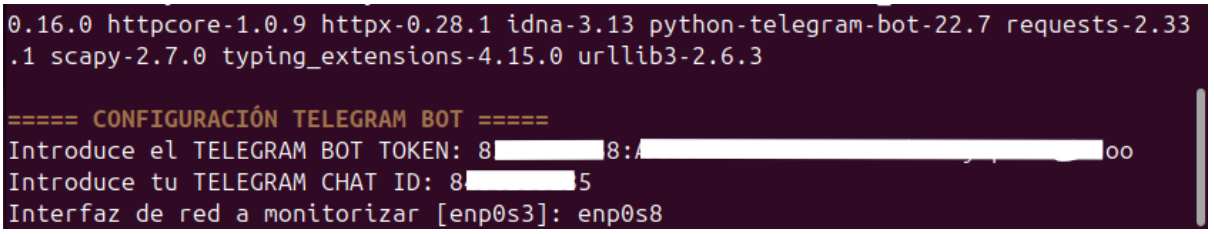
2.2. Instalación del paquete

Abre una terminal y accede a la ruta donde desempaquetaste los archivos. Luego, ejecuta el siguiente comando:

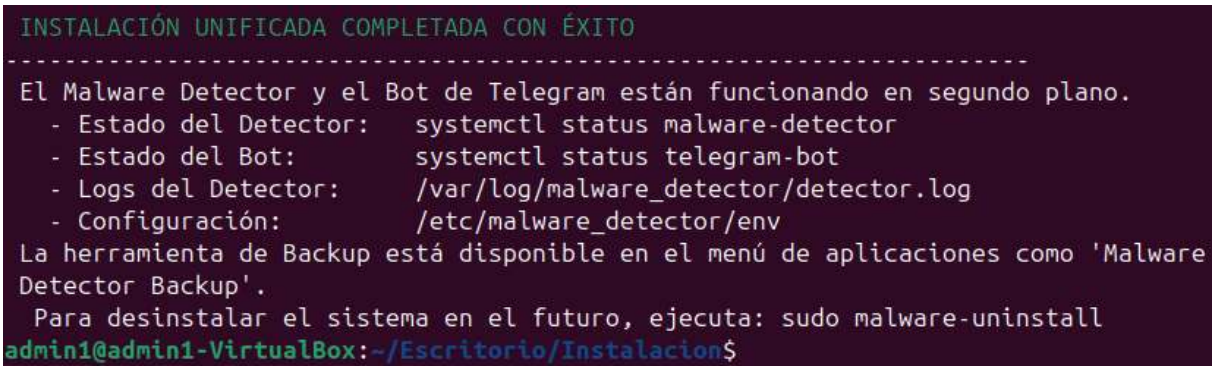


Durante la instalación, el script descargará automáticamente todas las dependencias necesarias. Los únicos datos que deberás proporcionar son:

- Token del bot de Telegram (obtenido en el paso 1.1)
- ChatID (obtenido en el paso 1.2)
- Interfaz de red a proteger (ej. enp0s3, enp0s8, etc.)



Una vez completada la configuración, verás un mensaje como el siguiente:



3. Malware-Detector

Esta herramienta protege tu red bloqueando los dispositivos no autorizados. Los dispositivos permitidos deben agregarse a la lista blanca (whitelist).

- Archivo de whitelist: /etc/malware_detector/whitelist.txt. Agrega aquí las direcciones IP que deseas autorizar para que no sean bloqueadas por error o por comando.

3.1. Comandos en terminal

comando	Descripción
sudo md-blocklist	Muestra la lista de IPs actualmente bloqueadas
sudo md-block <ip>	Bloquea la IP especificada
sudo md-unblock <ip>	Desbloquea la IP especificada
sudo md-whitelist	Muestra la lista de IPs autorizadas (whitelist)
sudo md-whitelist-add	Agrega IP específica a whitelist(borra del blacklist si esta esa IP)
sudo md-whitelist-del	Elimina IP especifica a whitelist

Ejemplos:

Ejemplo de la la lista de ip bloqueadas:

```
admin1@admin1-VirtualBox:~$ sudo md-blocklist
--- LISTA DE IPS BLOQUEADAS EN NFTABLES ---
Chain INPUT (policy ACCEPT)
num   target     prot opt source               destination
1     DROP       0    --  142.154.166.110      0.0.0.0/0
2     DROP       0    --  142.251.142.138      0.0.0.0/0
3     DROP       0    --  142.251.173.95       0.0.0.0/0
4     DROP       0    --  192.168.111.111      0.0.0.0/0

--- CONTENIDO DE BLACKLIST.TXT ---
192.168.111.111
142.154.166.110
142.251.173.95
142.251.142.138
admin1@admin1-VirtualBox:~$
```

Ejemplo de bloqueo:

```
admin1@admin1-VirtualBox:~$ sudo md-block 192.168.111.111
✓ IP 192.168.111.111 bloqueada en nftables.
✓ IP 192.168.111.111 guardada en /etc/malware_detector/blacklist.txt.
admin1@admin1-VirtualBox:~$
```

Ejemplo de desbloqueo:

```
admin1@admin1-VirtualBox:~$ sudo md-unblock 192.168.111.111
✓ IP 192.168.111.111 desbloqueada en nftables.
✓ IP 192.168.111.111 eliminada de /etc/malware_detector/blacklist.txt.
admin1@admin1-VirtualBox:~$
```

Ejemplo de verificación de whitelist:

```
admin1@admin1-VirtualBox:~$ sudo md-whitelist
--- DISPOSITIVOS PERMITIDOS (WHITELIST.TXT) ---
10.10.0.5
127.0.0.1
10.10.0.66
10.10.0.77
10.10.0.88
admin1@admin1-VirtualBox:~$
```

Ejemplo de verificación de Agregar/Eliminar IP whitelist:

```
admin1@admin1-VirtualBox:~$ sudo md-whitelist-add 10.10.0.66
✓ IP 10.10.0.66 desbloqueada en nftables.
✓ IP 10.10.0.66 eliminada de /etc/malware_detector/blacklist.txt.
✓ IP 10.10.0.66 añadida a la lista blanca.
admin1@admin1-VirtualBox:~$
```

```
admin1@admin1-VirtualBox:~$ sudo md-whitelist-del 10.10.0.66
✓ IP 10.10.0.66 eliminada de la lista blanca.
admin1@admin1-VirtualBox:~$
```

3.2. Comandos en el chat del “bot”

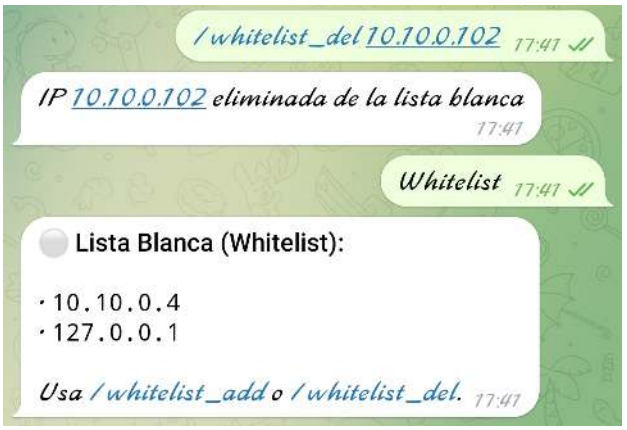
Comando	Descripción
/start	Inicia el servicio y te muestra botones para gestionar el sistema
/status	Ver los IPs bloqueados
/block <ip>	Bloquear IP específica
/unblock <ip>	Desbloquear IP específica
/whitelist_add	Agrega IP específica a Whitelist
/whitelist_del	Elimina IP específica del Whitelist

Ejemplos:

Ejemplo de inicio “/start”:

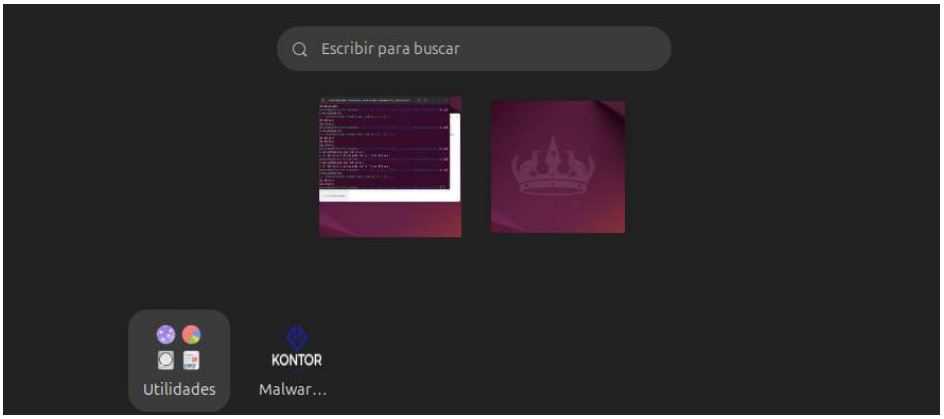
Ejemplo de bloqueo y desbloqueo:

Ejemplo de agregar y eliminar del Whitelist:



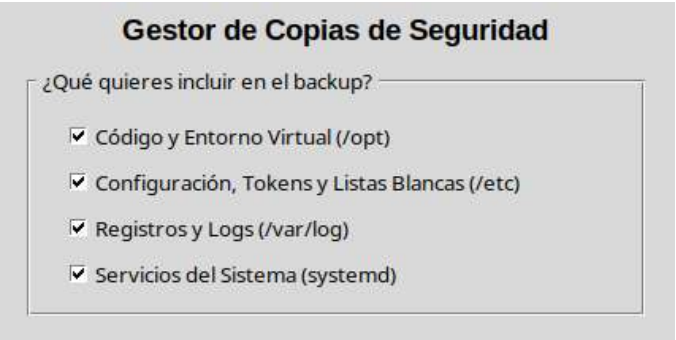
4. Backup

Siguiendo los anteriores pasos, en “mostrar aplicaciones” te saldrá un aplicación que se llama “Malware Detector Backup” y para poder usarla se necesita autenticación de root.



4.1. informaciones basicos sobre Malware Detector backup

En la ventana principal de Backup, puedes seleccionar qué elementos deseas incluir en el respaldo.

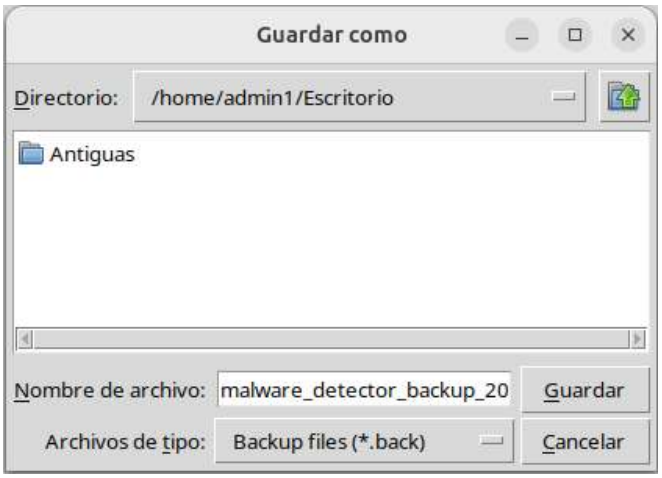


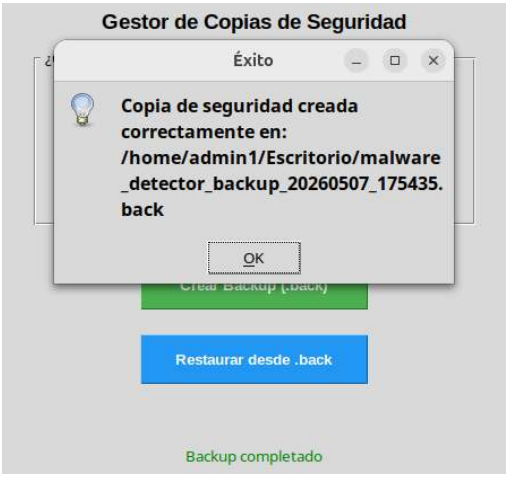
Y abajo de las opciones, encontrarás las opciones para **Crear** o **Restaurar** respaldos.

Nota: La opción "Restaurar desde .back" solo funcionará si ya has creado al menos un respaldo previamente.

4.2. Crear Backup (.back)

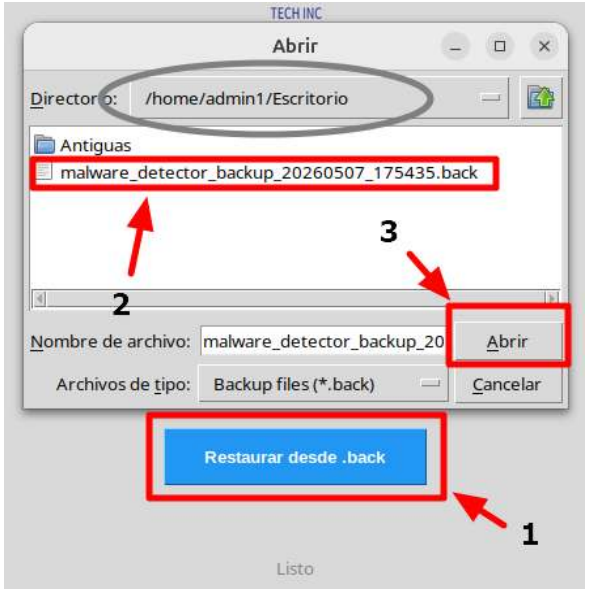
Una vez que hagas clic en "**Crear Backup (.back)**" después de seleccionar los elementos que deseas copiar, se te pedirá que elijas la ruta donde guardar el archivo .back. Después de hacer clic en **Guardar**, tendrás que esperar a que se complete la copia.

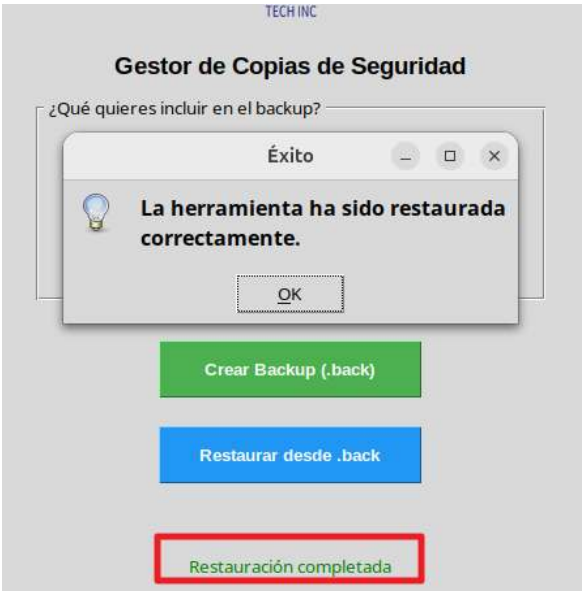




4.3 Restaurar desde .back

En caso de que hayas modificado algo y la herramienta ya no funcione correctamente, o hayas eliminado datos sin querer, puedes restaurar la versión de cuando hiciste la última copia .back.





5. Desinstalacion

Para desinstalar la aplicación, ejecuta el siguiente comando en la terminal:

Durante el proceso, se te preguntará qué datos deseas conservar y cuáles eliminar. Responde según tus necesidades.

Advertencia: Este proceso eliminará la mayoría de los archivos generados por la aplicación, a menos que indiques lo contrario.