

# Manual Instalació | Kontor Tek Inc

# Index

<b>1. Antes de instalar.....</b>	<b>2</b>
1.1. Obtener Token.....	2
1.2. ChatID.....	3
<b>2. Instalación.....</b>	<b>4</b>
2.1. Paquete de instalación.....	4
2.2. Instalación del paquete.....	5
<b>3. Malware-Detector.....</b>	<b>6</b>
3.1. Comandos en terminal.....	6
<b>4. Backup.....</b>	<b>10</b>
4.1. informaciones basicos sobre Malware Detector backup.....	10
4.2. Crear Backup (.back).....	11
4.3 Restaurar desde .back.....	11
<b>5. Desinstalacion.....</b>	<b>12</b>

# 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.

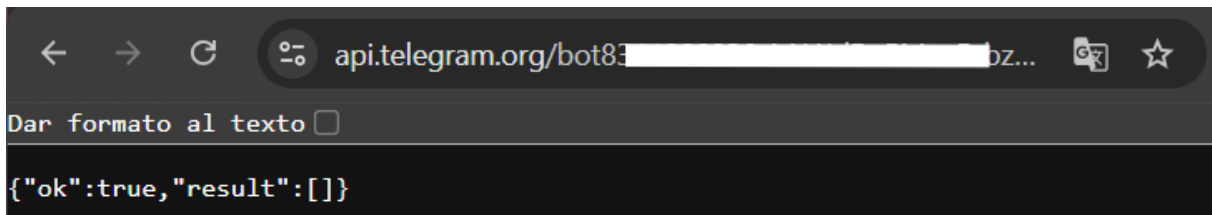
## 1.2. ChatID

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:

```
admin1@admin1-VirtualBox:~/Escritorio/Instalacion$ sudo bash install.sh
[sudo] contraseña para admin1:
  INICIANDO INSTALACIÓN DE MALWARE DETECTOR Y HERRAMIENTA DE BACKUP
=====

[+] Instalando dependencias del sistema...
Obj:1 http://es.archive.ubuntu.com/ubuntu noble InRelease
```

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.)

```
0.16.0 httcore-1.0.9 httpx-0.28.1 idna-3.13 python-telegram-bot-22.7 requests-2.33
.1 scapy-2.7.0 typing_extensions-4.15.0 urllib3-2.6.3

===== CONFIGURACIÓN TELEGRAM BOT =====
Introduce el TELEGRAM BOT TOKEN: 8[redacted]:[redacted]oo
Introduce tu TELEGRAM CHAT ID: 8[redacted]5
Interfaz de red a monitorizar [enp0s3]: enp0s8
```

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

```
INSTALACIÓN UNIFICADA COMPLETADA CON ÉXITO
-----
El Malware Detector y el Bot de Telegram están funcionando en segundo plano.
- Estado del Detector:      systemctl status malware-detector
- Estado del Bot:          systemctl status telegram-bot
- Logs del Detector:       /var/log/malware_detector/detector.log
- Configuración:           /etc/malware_detector/env
La herramienta de Backup está disponible en el menú de aplicaciones como 'Malware
Detector Backup'.
Para desinstalar el sistema en el futuro, ejecuta: sudo malware-uninstall
admin1@admin1-VirtualBox:~/Escritorio/Instalacion$
```

## 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
<b>sudo md-blocklist</b>	Muestra la lista de IPs actualmente bloqueadas
<b>sudo md-block &lt;ip&gt;</b>	Bloquea la IP especificada
<b>sudo md-unblock &lt;ip&gt;</b>	Desbloquea la IP especificada
<b>sudo md-whitelist</b>	Muestra la lista de IPs autorizadas (whitelist)
<b>sudo md-whitelist-add</b>	Agrega IP específica a whitelist(borra del blacklist si esta esa IP)
<b>sudo md-whitelist-del</b>	Elimina IP específica a whitelist

## Ejemplos:

### Ejemplo de 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”

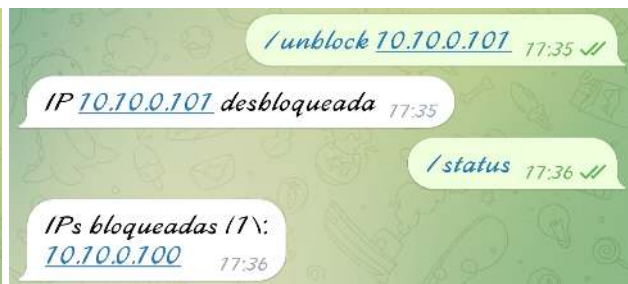
Comando	Descripción
<code>/start</code>	Inicia el servicio y te muestra botones para gestionar el sistema
<code>/status</code>	Ver los IPs bloqueados
<code>/block &lt;ip&gt;</code>	Bloquear IP específica
<code>/unblock &lt;ip&gt;</code>	Desbloquear IP específica
<code>/whitelist_add</code>	Agrega IP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

## Ejemplos:

### Ejemplo de inicio “/start”:



### Ejemplo de bloqueo y desbloqueo:

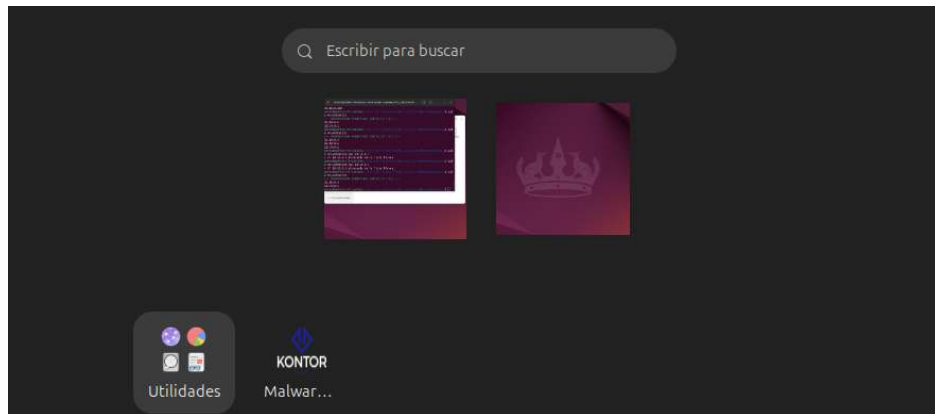


### Ejemplo de agregar y eliminar del Whitelist:



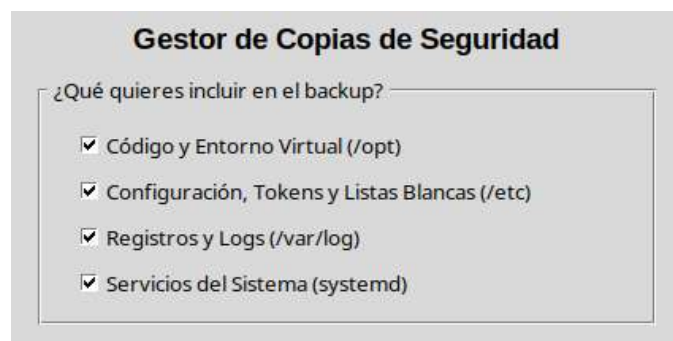
## 4. Backup

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.



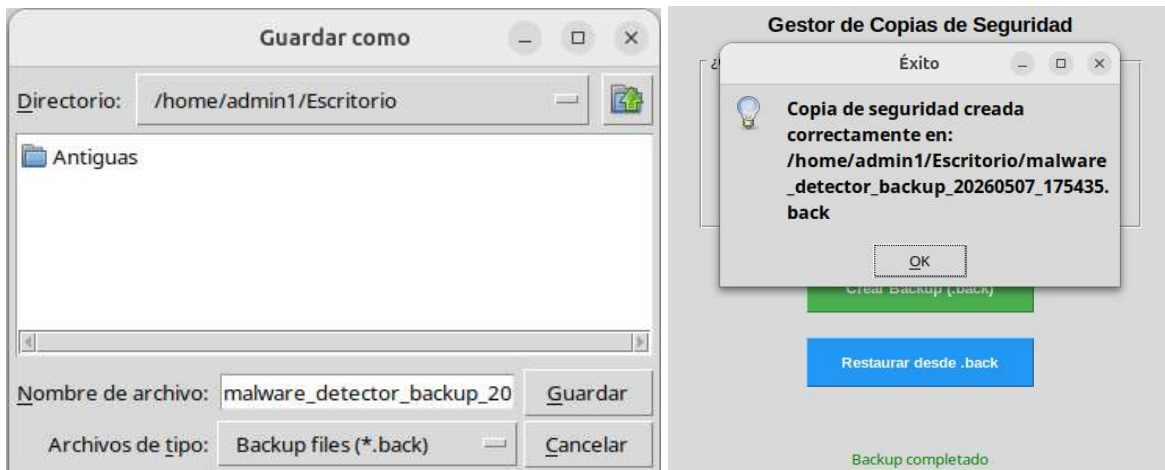
Y abajo de las opciones, encontrarás las opciones para **Crear** o **Restaurar** respaldos.



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

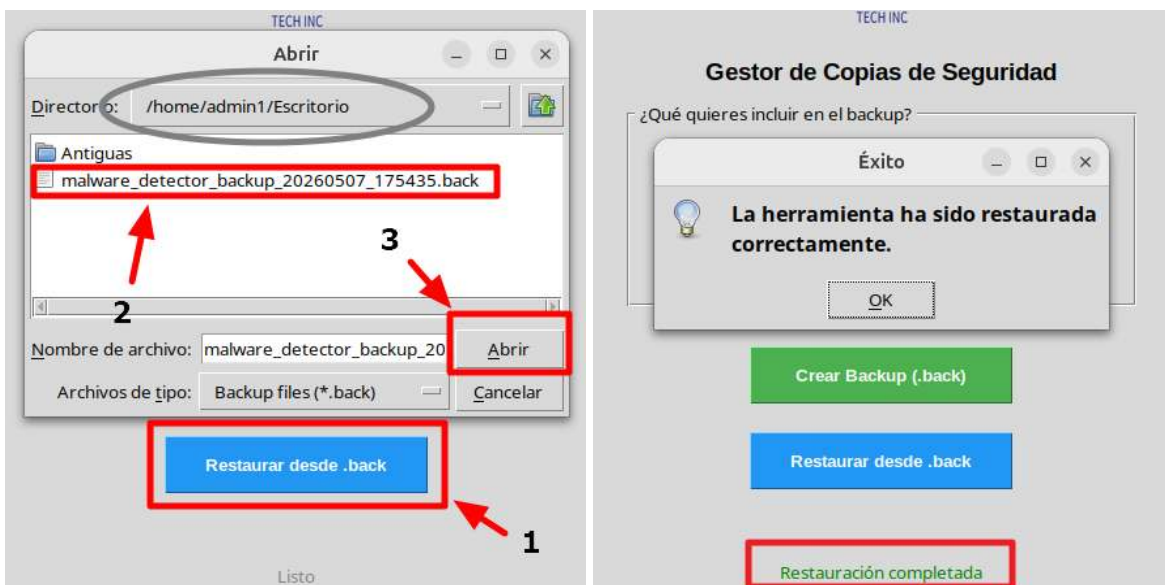
## 4.2. Crear Backup (.back)

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:

```
admini@admin1-VirtualBox:~$ sudo malware-uninstall
[sudo] contraseña para admini:
DESINSTALADOR COMPLETO
=====

[ATENCIÓN] Esto eliminara los componentes seleccionados

Componentes a desinstalar:
 1. Malware Detector (servicios, reglas, archivos)
 2. Backup Tool (aplicacion, acceso directo, scripts)
 3. Dependencias Python (opcional)
 4. Reglas nftables (opcional)

--- SELECCION DE COMPONENTES ---
Eliminar MALWARE DETECTOR completo? [y/n]: █
```

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.