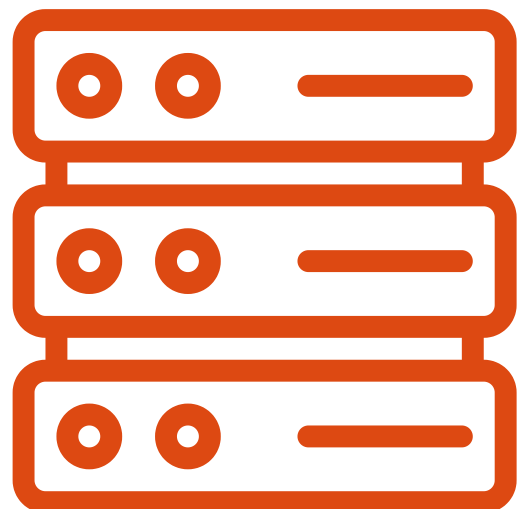


# Análisis Forense y Endpoint Security Cloud

Equipo 5



# Análisis Forense Digital



## Introducción

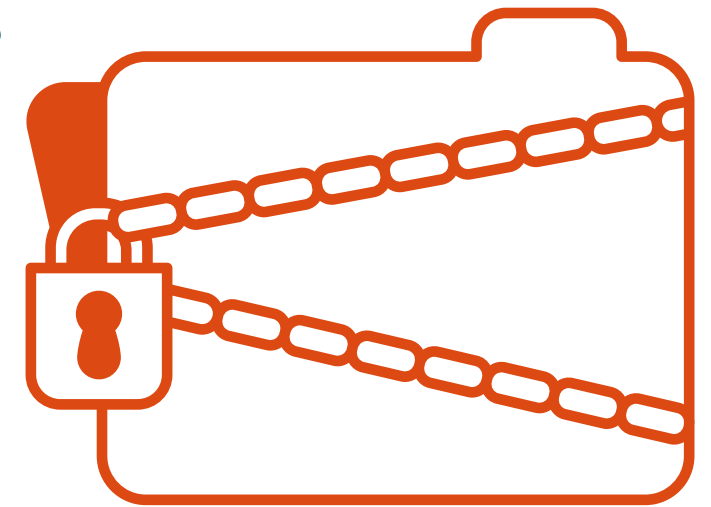
- Este año se han registrado 80,000 millones de intentos de ciberataques
- Se estima que para el año 2025 los ciberataques costarán un total de 10.5 billones de dólares
- Se divide nuestro reto en dos partes:
  - Pt. 1: USB
  - Pt. 2: Kaspersky

# Reto Pt.1

Una persona actúa maliciosamente, sobre-escribe la información y borra los archivos contenidos de una USB de una empresa Alemana.

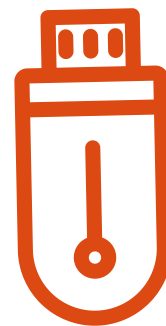
Objetivo:

- Recuperar los archivos eliminados, es específico uno que contiene información confidencial y de relevancia para la empresa
- Procedimiento de identificación de archivos sospechosos
- Uso de la versión doméstica de la herramienta Recuva



# Copia de seguridad

- No es un paso necesario, pero brinda mayor seguridad
- Para generar esta imagen
  - Terminal Ubuntu
  - Comando **lsblk**
    - discos conectados
    - particiones
  - Mount point
    - USB montada como sdb
  - Se creó un directorio en tmp
  - Comando **dd**
    - imagen del disco completo
  - No fue necesario restaurar la USB



```
Activities Terminal Oct 12 4:51 PM en ferre0x1a@yup: ~
lsblk
loop0 7:0 0 4K 1 loop /snap/bare/5
loop1 7:1 0 110.7M 1 loop /snap/core/12821
loop2 7:2 0 55.5M 1 loop /snap/core18/2253
loop3 7:3 0 55.5M 1 loop /snap/core18/2344
loop4 7:4 0 65.2M 1 loop /snap/gtk-common-themes/1519
loop5 7:5 0 61.9M 1 loop /snap/core20/1270
loop6 7:6 0 219M 1 loop /snap/gnome-3-34-1804/77
loop7 7:7 0 51M 1 loop /snap/snap-store/547
loop8 7:8 0 68.3M 1 loop /snap/cherrytree/40
loop9 7:9 0 219M 1 loop /snap/gnome-3-34-1804/72
loop10 7:10 0 43.6M 1 loop /snap/snapd/15177
loop11 7:11 0 247.9M 1 loop /snap/gnome-3-38-2004/87
loop12 7:12 0 140K 1 loop /snap/gtk2-common-themes/13
loop13 7:13 0 65.1M 1 loop /snap/gtk-common-themes/1515
loop14 7:14 0 61.9M 1 loop /snap/core20/1405
loop15 7:15 0 248.8M 1 loop /snap/gnome-3-38-2004/99
loop16 7:16 0 54.2M 1 loop /snap/snap-store/558
sda 8:0 0 931.5G 0 disk
├─sda1 8:1 0 16M 0 part
├─sda2 8:2 0 931.5G 0 part
├─sdb 8:16 1 28.8G 0 disk
├─sdb1 8:17 1 28.8G 0 part /media/ferre0x1a/KINGSTON
nvme0n1 259:0 0 232.9G 0 disk
├─nvme0n1p1 259:1 0 100M 0 part /boot/efi
├─nvme0n1p2 259:2 0 16M 0 part
├─nvme0n1p3 259:3 0 179.6G 0 part
├─nvme0n1p4 259:4 0 499M 0 part
└─nvme0n1p5 259:5 0 52.7G 0 part /
ferre0x1a@yup:~$ ls -l /dev/sdb
brw-rw---- 1 root disk 8, 16 Oct 12 16:37 /dev/sdb
ferre0x1a@yup:~$ mkdir /tmp/clone
ferre0x1a@yup:~$ sudo dd if=/dev/sdb of=/tmp/clone/clone_sdb status=progress
[sudo] password for ferre0x1a:
30902912512 bytes (31 GB, 29 GiB) copied, 380 s, 81.3 MB/s
60437492+0 records in
60437492+0 records out
30943995904 bytes (31 GB, 29 GiB) copied, 380.492 s, 81.3 MB/s
ferre0x1a@yup:~$
```

## Recuva

- Uso de la herramienta
  - Recuva de CCleaner
- Aplicación para recuperar archivos dañados o recientemente formateados
  - Capaz de restaurar cualquier tipo de archivo que se desee y de cualquier tipo de disco de almacenamiento
- Dentro del software
  - Escaneos simples, profundos, y muy específicos
- Función de borrado seguro
  - Técnicas de sobre-escritura con estándares militares

## Recuperación de archivos



# Procedimiento

## 1. Instalación de Recuva

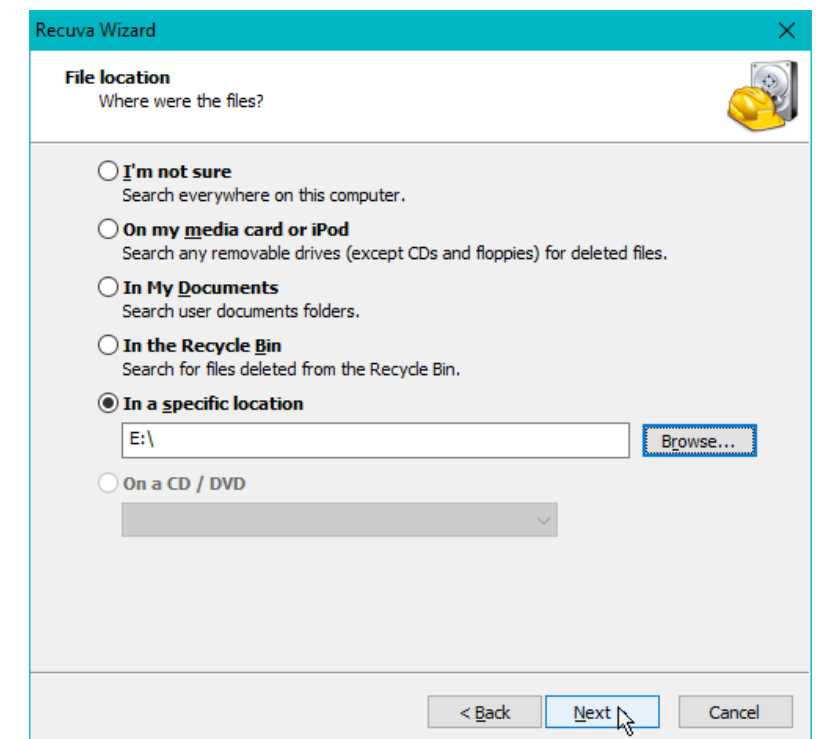
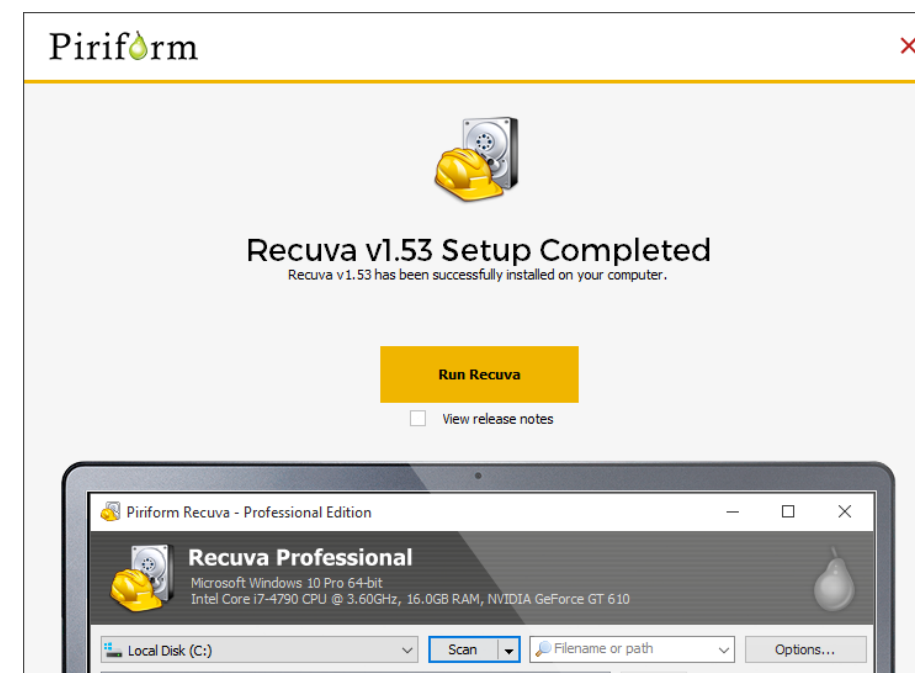
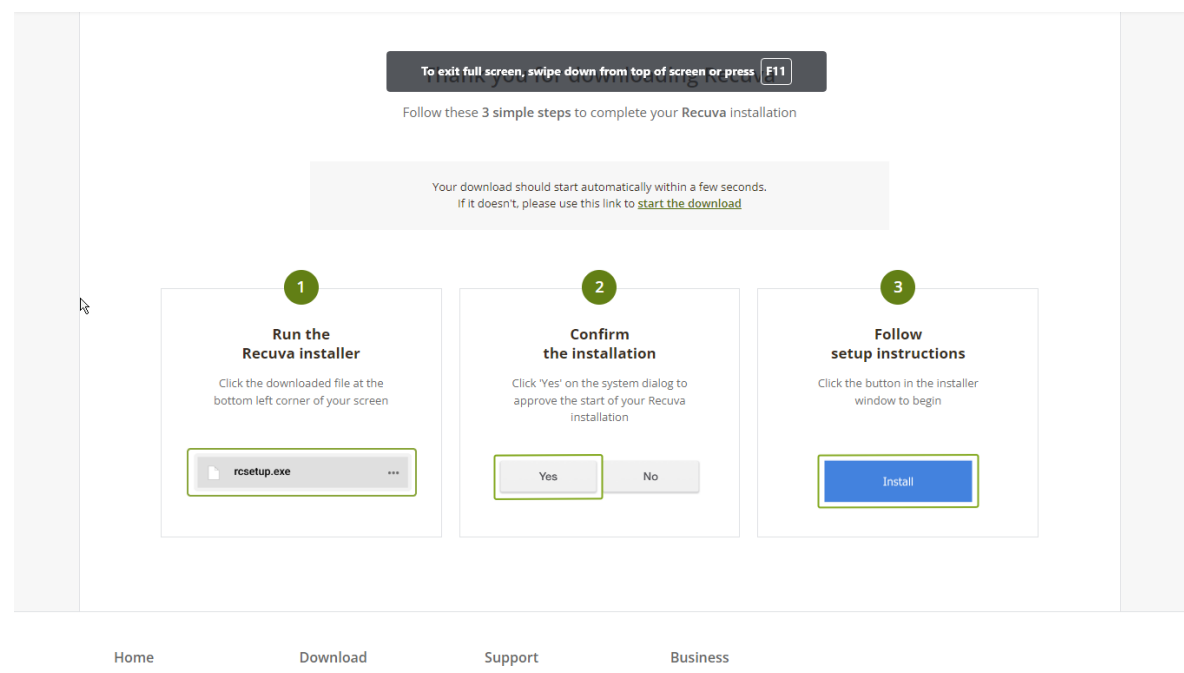
a. Página : <https://www.ccleaner.com/recuva/download/standard>

## 2. Escaneo del disco

a. Se abre una ventana y se da clic en **Run Recuva**

b. Se sigue la guía del wizard

c. Se elige la USB como la ubicación de los archivos



# Identificación de archivos



- Enfoque entre las diferencias del primer archivo y todos los demás.
- Todos los archivos se encuentran en la carpeta de **Wichtig**
- La mayoría se encuentra dentro de **Microsoft, Windows, Internet Explorer, Edge, Lenovo**
  - Archivos comunes de estas aplicaciones como PAK, de diferentes idiomas para Edge, logos, archivos de configuración, etc.
- Archivo encontrado
  - Imagen de 17 kb
  - Nombre: "Coasa que son muy impostantes y muy confidenciales que deben de ser muy secretas.jpg"
  - Las faltas de ortografía probablemente tienen que ver con que ya había sido borrada
- No se encontraron meta-datos, pero es evidente que ese es el archivo confidencial borrado



# Archivos que serán recuperados

**Recuva** v1.53.2083 (64-bit)  
Windows 10 64-bit  
Intel Core i5-8265U CPU @ 1.60GHz, 8.0GB RAM, Intel UHD Graphics 620

Select the files you want to Recover by ticking the boxes and then pressing Recover.  
For the best results, restore the files to a different drive.

Switch to advanced mode

<input type="checkbox"/>	Filename	Path	Last Modified	Size	State	Comment
<input type="checkbox"/>	Coasa que son muy importante...	E:\Wichtig\	09/25/2022 19:46	17 KB	Excellent	No overwritten clusters detected.
<input type="checkbox"/>	_fsvc.exe	E:\Wichtig\Windows\	10/16/2021 08:32	79 KB	Excellent	No overwritten clusters detected.
<input type="checkbox"/>	DirectX.log	E:\Wichtig\Windows\	10/14/2021 14:27	200 bytes	Excellent	No overwritten clusters detected.
<input type="checkbox"/>	_PINST.LOG	E:\Wichtig\Windows\	05/08/2022 13:10	10 KB	Excellent	No overwritten clusters detected.
<input type="checkbox"/>	DtcInstall.log	E:\Wichtig\Windows\	08/30/2021 16:37	2 KB	Excellent	No overwritten clusters detected.
<input type="checkbox"/>	_xplorer.exe	E:\Wichtig\Windows\	09/20/2022 07:31	5,021 KB	Excellent	No overwritten clusters detected.
<input type="checkbox"/>	HelpPane.exe	E:\Wichtig\Windows\	08/29/2021 12:01	1,050 KB	Excellent	No overwritten clusters detected.
<input type="checkbox"/>	_h.exe	E:\Wichtig\Windows\	12/07/2019 04:09	18 KB	Excellent	No overwritten clusters detected.
<input type="checkbox"/>	_sasetup.log	E:\Wichtig\Windows\	08/30/2021 16:36	1 KB	Excellent	No overwritten clusters detected.
<input type="checkbox"/>	_ib.bin	E:\Wichtig\Windows\	12/07/2019 04:09	42 KB	Excellent	No overwritten clusters detected.
<input type="checkbox"/>	_otepad.exe	E:\Wichtig\Windows\	08/02/2022 18:42	196 KB	Excellent	No overwritten clusters detected.
<input type="checkbox"/>	_FRO.log	E:\Wichtig\Windows\	09/20/2022 07:35	234 KB	Excellent	No overwritten clusters detected.
<input type="checkbox"/>	_egedit.exe	E:\Wichtig\Windows\	04/29/2021 11:57	361 KB	Excellent	No overwritten clusters detected.
<input type="checkbox"/>	RtlExUpd.dll	E:\Wichtig\Windows\	05/17/2021 09:50	2,809 KB	Excellent	No overwritten clusters detected.
<input type="checkbox"/>	_etupact.log	E:\Wichtig\Windows\	09/25/2022 18:55	4 KB	Excellent	No overwritten clusters detected.
<input type="checkbox"/>	_plwow64.exe	E:\Wichtig\Windows\	09/20/2022 07:31	160 KB	Excellent	No overwritten clusters detected.
<input type="checkbox"/>	Synaptics.log	E:\Wichtig\Windows\	05/25/2022 11:16	606 bytes	Excellent	No overwritten clusters detected.
<input type="checkbox"/>	Synaptics.PD.log	E:\Wichtig\Windows\	05/25/2022 11:16	2 KB	Excellent	No overwritten clusters detected.
<input type="checkbox"/>	_ystem.ini	E:\Wichtig\Windows\	08/30/2021 17:28	219 bytes	Excellent	No overwritten clusters detected.
<input type="checkbox"/>	_wain_32.dll	E:\Wichtig\Windows\	12/07/2019 04:10	63 KB	Excellent	No overwritten clusters detected.
<input type="checkbox"/>	_nsu.log	E:\Wichtig\Windows\	08/28/2022 19:39	5 KB	Excellent	No overwritten clusters detected.
<input type="checkbox"/>	_in.ini	E:\Wichtig\Windows\	08/30/2021 17:28	92 bytes	Excellent	No overwritten clusters detected.
<input type="checkbox"/>	WindowsShell.Manifest	E:\Wichtig\Windows\	12/07/2019 04:09	670 bytes	Excellent	No overwritten clusters detected.
<input type="checkbox"/>	WindowsUpdate.log	E:\Wichtig\Windows\	09/25/2022 19:58	276 bytes	Excellent	No overwritten clusters detected.
<input type="checkbox"/>	_inhlp32.exe	E:\Wichtig\Windows\	12/07/2019 04:10	11 KB	Excellent	No overwritten clusters detected.
<input type="checkbox"/>	WMSysPr9.prx	E:\Wichtig\Windows\	12/07/2019 10:05	309 KB	Excellent	No overwritten clusters detected.
<input type="checkbox"/>	_rite.exe	E:\Wichtig\Windows\	12/06/2019 16:29	11 KB	Excellent	No overwritten clusters detected.
<input type="checkbox"/>	appxblockmap.xml	E:\Wichtig\Windows\ImmersiveControlPanel\	08/29/2021 12:01	319 bytes	Unrecoverable	This file is overwritten with "E:\Videos\Der spezielle und streng vertraulich...
<input type="checkbox"/>	...	...	...	...	...	...

[E:] FAT32, 28.8 GB. Cluster size: 16384. Found 762 file(s) in 0.44 second.

Recover...

Online Help

Check for updates...



# Resultados

- 762 archivos borrados
- Estado de los archivos representados por círculos verdes, amarillos y rojos
- Formatos de archivos encontrados
  - ejecutables, imágenes, PAK, .dll, .xml, .log, .ini, .prx, etc.
- Archivos en distintos idiomas incluyendo el alemán
- Archivo objetivo con mensaje oculto
  - **"Coasa que son muy importantes y muy confidenciales que deben de ser muy secretas.jpg"**

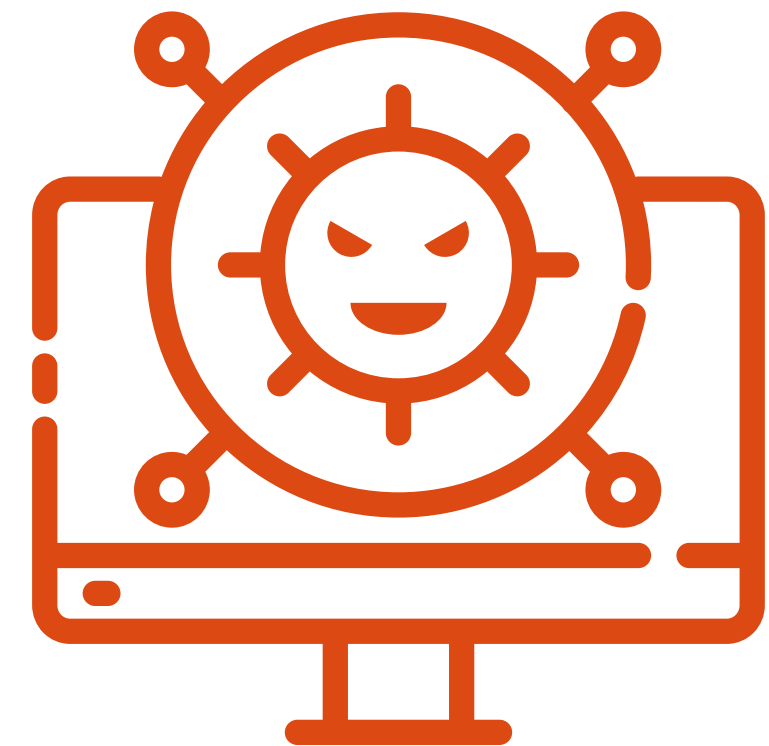


## Reto Pt.2

Aplicación de la herramienta Kaspersky Endpoint Security para Windows

Objetivo:

- Detección de malware y amenazas
- Uso de máquina virtual con virus previamente cargado



# Kaspersky Endpoint Security para Windows



- Aplicación de seguridad más probada y premiada para proteger todos los endpoints de Windows y los datos que contienen.
- Endpoints
  - Representan los puntos de entrada vulnerables clave para los ciber-criminales
  - Ejemplos:
    - Computadoras de escritorio
    - Servidores
    - Laptops
    - Tablets
    - Celulares

## Máquinas virtuales

- Máquina virtual con Windows 10
- Preparación del ambiente
  - Se desactiva Windows Defender
    - Asegurar que no se active de forma autónoma ni al reiniciarla

## Instalación del antivirus

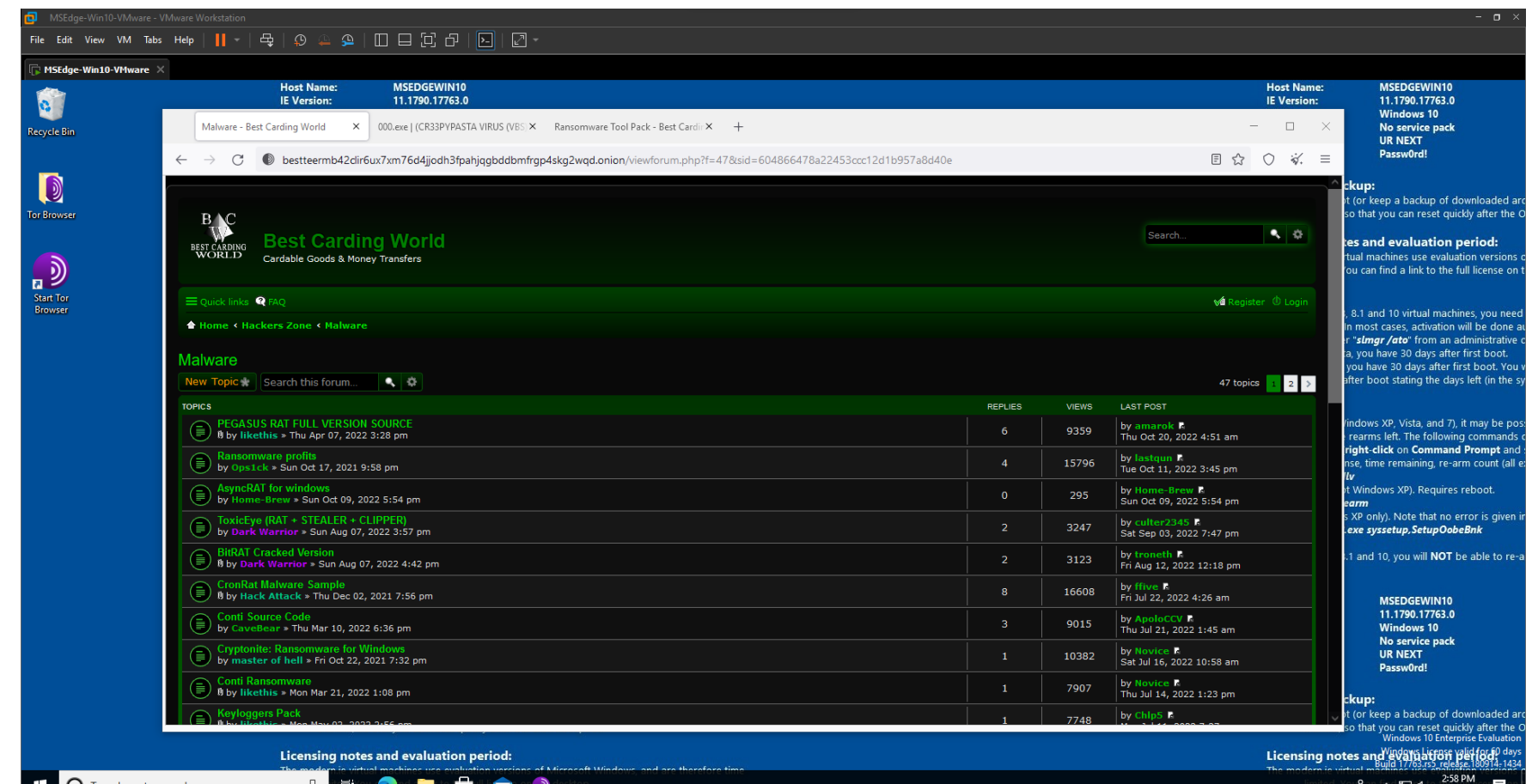
- Manual proporcionado por IPC Services
  - Enlace de descarga
    - Kaspersky dentro de la máquina virtual
    - Virus



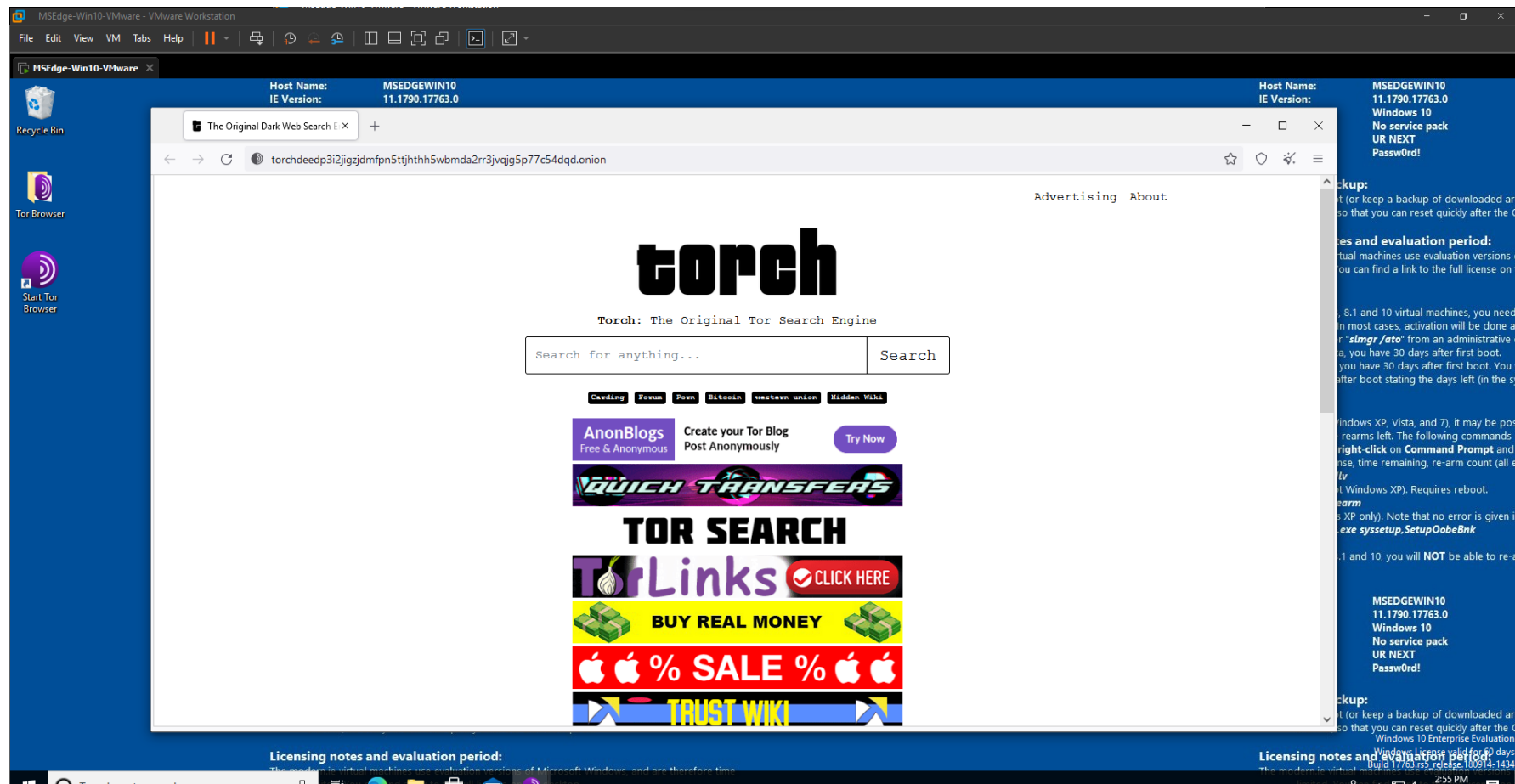
## Malware Traffic Analysis (clearnet)

- Malware llamado
  - "ICEDID (BOKBOT) INFECTION WITH COBALT STRIKE"
- Descarga de archivo
  - disco .ISO que se montó y se ejecutó
- Gráficamente no ocurrió nada
- Detectado por Kasperky posteriormente

## Descarga de malware



# Descarga de malware



## Best Carding World (darknet)

- Motor de búsqueda
  - Torch
- Muestra resultados sin filtros
- Búsqueda
  - "windus virus exe"

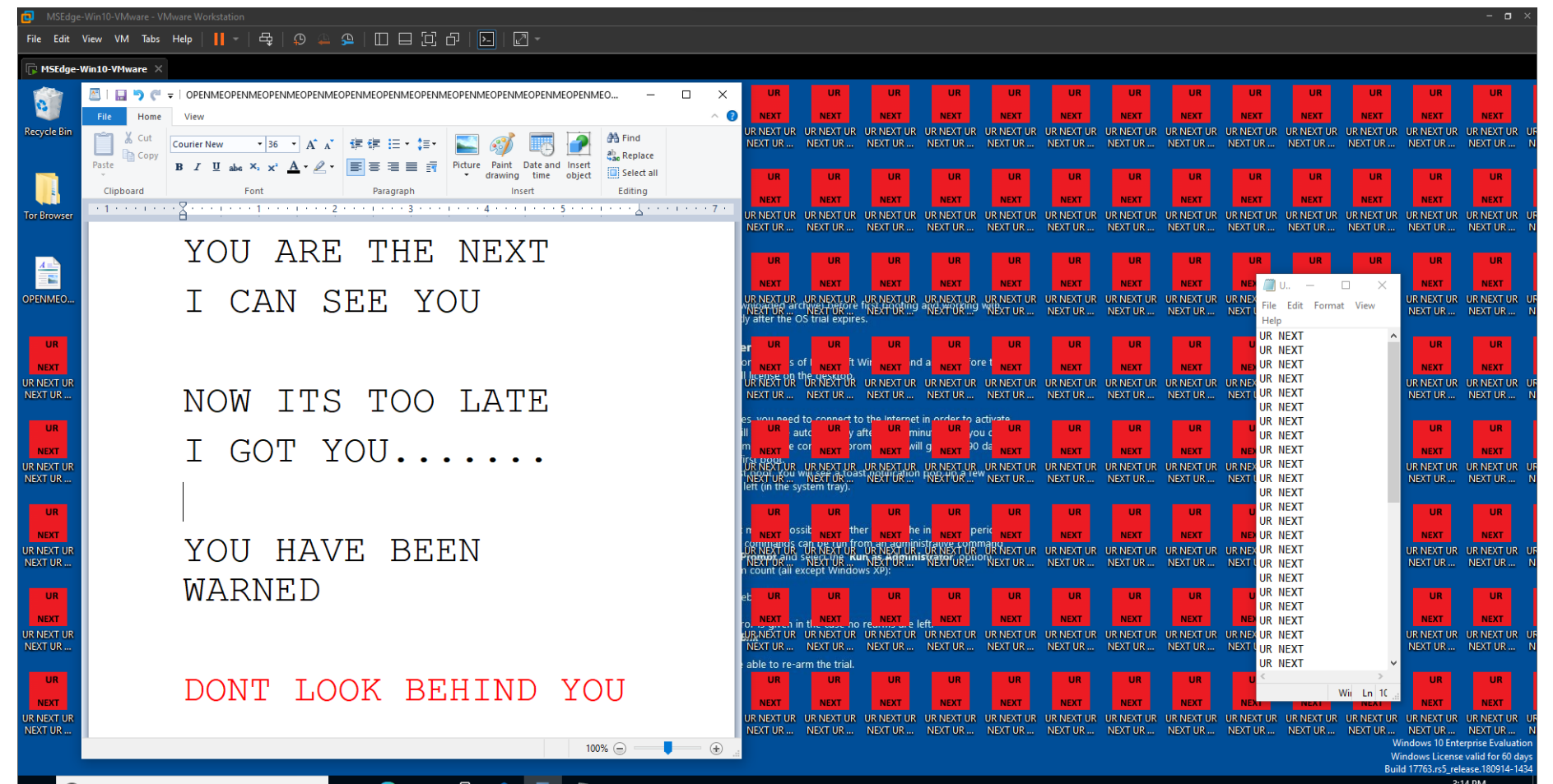
- Sección Malware
  - Archivo 1: **000.exe**
  - ZIP: ransomware **wannacry.exe**
- Se apagó Kaspersky y se dejó vulnerable a la máquina



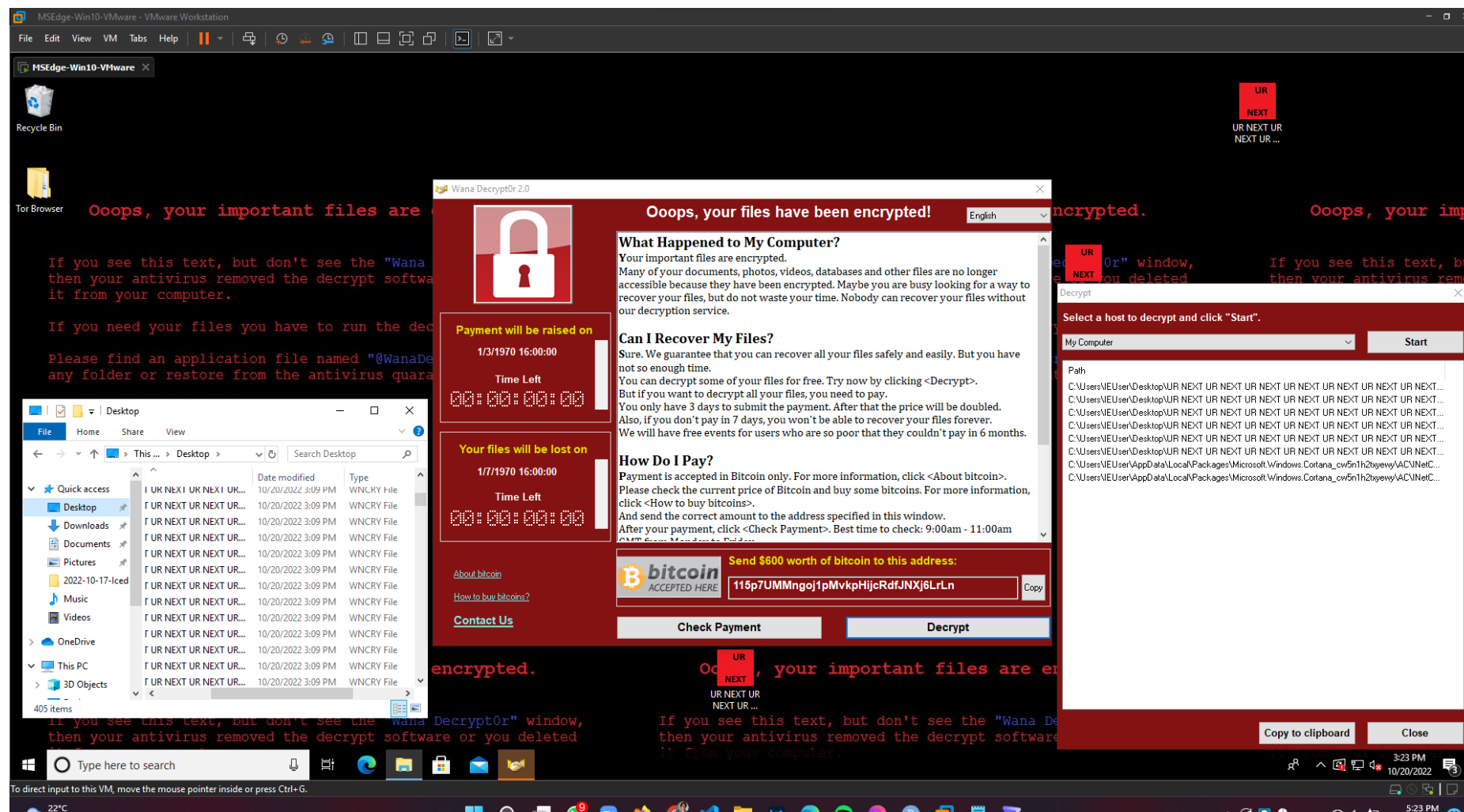
## 000.exe

- Pantalla en blanco
- Carretera y árboles
  - parpadeando y con distintos filtros
- Reinicio de la máquina virtual
  - nombre de usuario cambió
    - UR NEXT
  - escritorio lleno de imágenes con fondo rojo
  - administrador de tareas no se podía ejecutar
  - algunos permisos se cambiaron automáticamente

## Lo que sucedió a nivel gráfico



# Lo que sucedió a nivel gráfico



wannacry.exe

- Se refrescó la pantalla
- Se cifraron todos los archivos
- Cambio de fondo de pantalla
  - instrucciones para recuperar los archivos y el .exe
- Dirección de bitcoin
  - depósito de \$600 USD

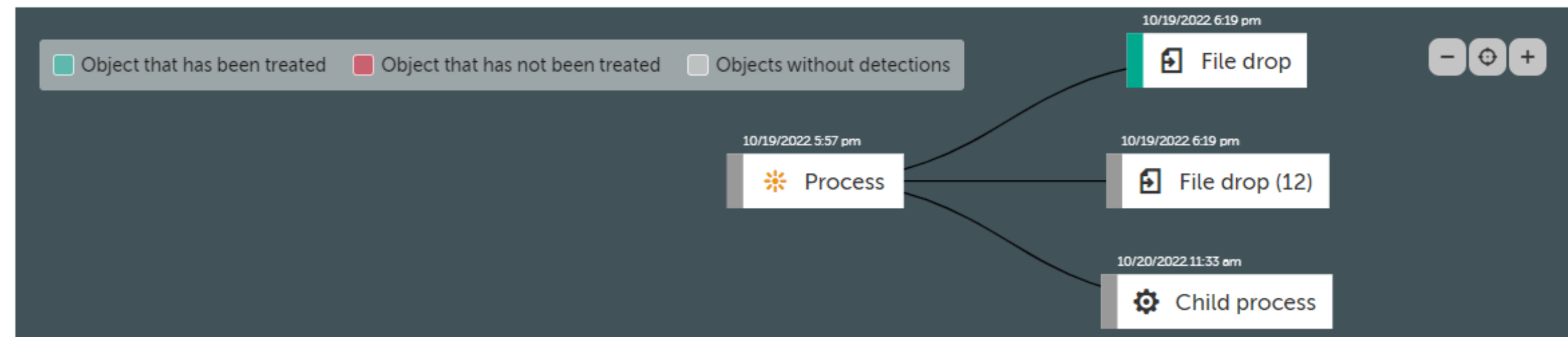
- Configuración de dos perfiles de protección
  - Con todas las herramientas recomendadas activadas
  - Con todas desactivadas
- El antivirus con el perfil recomendado analizaba todas las descargas y en la mayoría de los casos borraba los archivos antes de que estos pudieran ser ejecutados

#### Threat development chain graph

[How to read a threat development chain graph?](#)

✔ Treated: The object has been deleted

Detected on: 10/20/2022    Device owner: [daniel](#)    Device name: [MSEEDGEWIN10](#)    Security profile: [Default](#)    ...

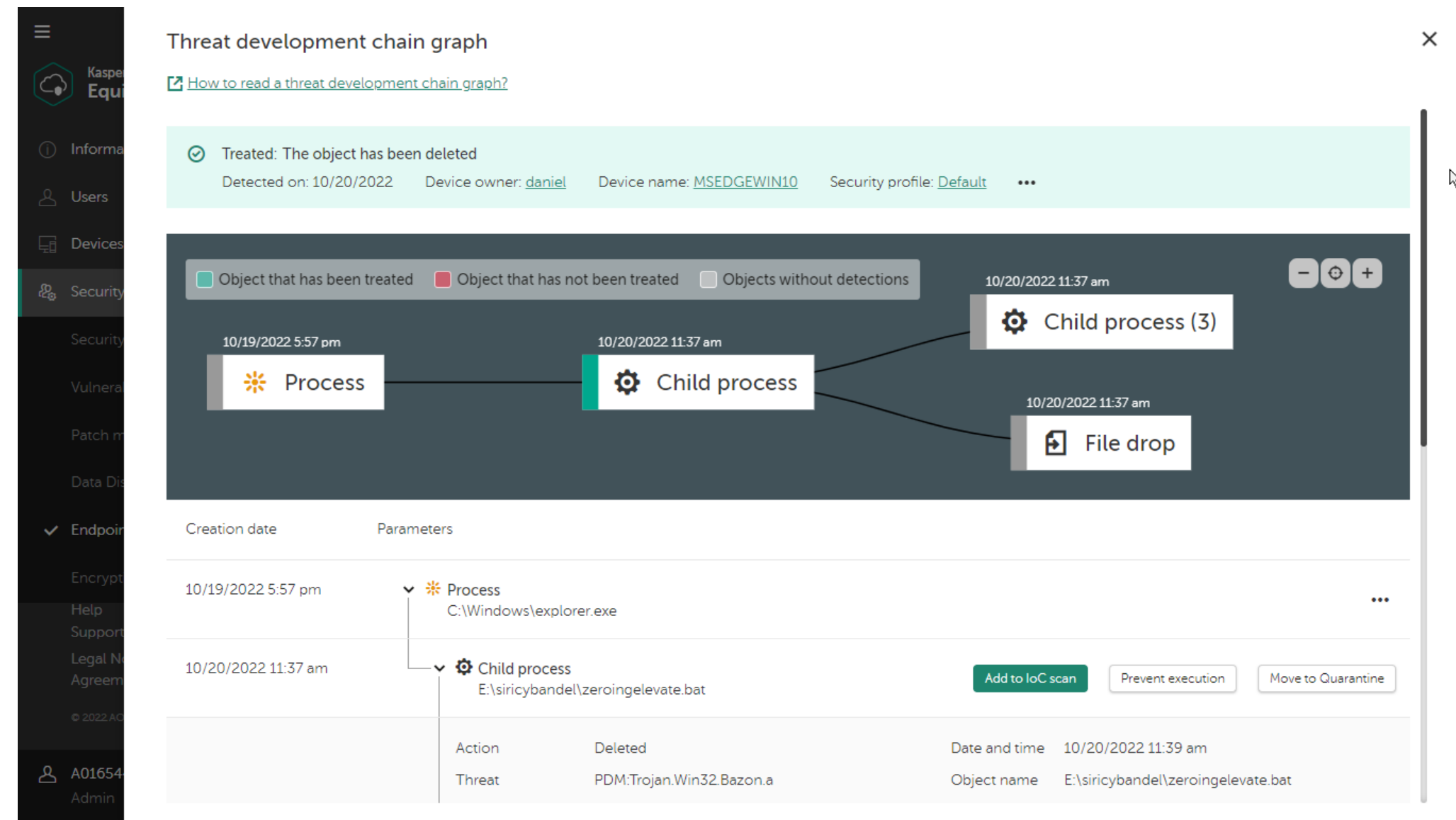


# Monitoreo, detección y respuesta

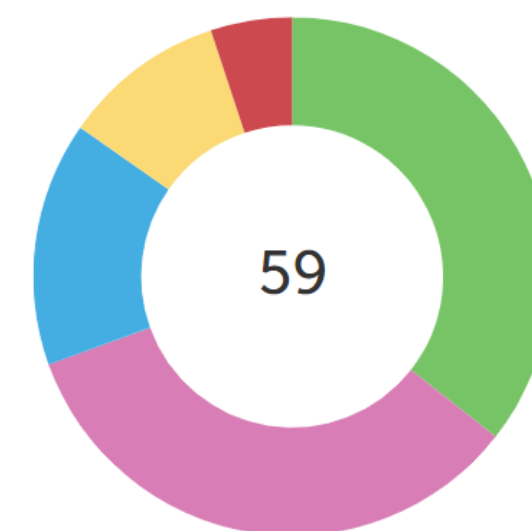


# Resultados

- Utilizando el perfil inseguro
  - descargar y correr un troyano
    - varios procesos antes de ser detectado y eliminado
- En los logs
  - detectado mediante análisis de comportamiento
  - se eliminó junto con los procesos que había iniciado
    - xcopy
    - rundll32
    - conhost
- Cambio al perfil recomendado
  - Eliminación de 59 archivos maliciosos



## Threats detected during last 7 days



- 21 UDS:DangerousObject.Multi....
- 20 HEUR:Trojan.Win32.Generic
- 9 Virus.Win32.PolyRansom.k
- 6 HEUR:Trojan.WinLNK.Agent.g...
- 3 Trojan.Win32.Diztakun.arpg

# Conclusiones

## Reto Pt. 1

- Recuva permite recuperar archivos eliminados
- Se encontró una vasta cantidad de archivos, incluyendo el archivo confidencial de la empresa alemana
  - "Coasa que son muy importantes y muy confidenciales que deben de ser muy secretas.jpg"

## Reto Pt. 2

- Estudiar el comportamiento de distintos tipos de malware en un ambiente seguro con la aplicación de Kaspersky.
- El antivirus es muy eficiente
  - amenazas:
    - hashes, análisis de actividad, aprendizaje automático y control de accesos.





# Referencias

CCleaner. (s.f.). Recuva: Recover your deleted files quickly and easily. <https://www.ccleaner.com/es-es/recuva>

Cyberpedia. (2022). What is an Endpoint? <https://www.paloaltonetworks.com/cyberpedia/what-is-an-endpoint>

Interpol. (s.f.). Análisis forense digital. <https://www.interpol.int/es/Como-trabajamos/Innovacion/Analisis-forense-digital>

Lab, A. K. (2022). Endpoint Security para Windows — Kaspersky. <https://latam.kaspersky.com/small-to-medium-business-security/endpoint-windows>

Prakash, B., Rani, K., Prasad, S., & Sudha, T. (2022). Techniques in Computer Forensics: A Recovery perspective. <https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.301.4008&rep=rep1&type=pdf>

Pro, I. (2019). Data recovery: Why is it so important? <https://www.itpro.co.uk/data-loss-prevention/28864/data-recovery-why-is-it-so-important#:~:text=In%5C%20technical%5C%20terms%5C%2C%5C%20data%5C%20recovery,applications%5C%20or%5C%20system%5C%20booting%5C%20failures15>