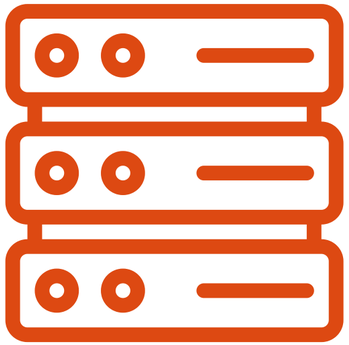
Análisis Forense y Endpoint Security Cloud

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 ciberatques costarán un total de 10.5 billones de dólares
- Se divide nuestro reto en dos partes:
  - Pt. 1: USB
  - Pt. 2: Kaspersky

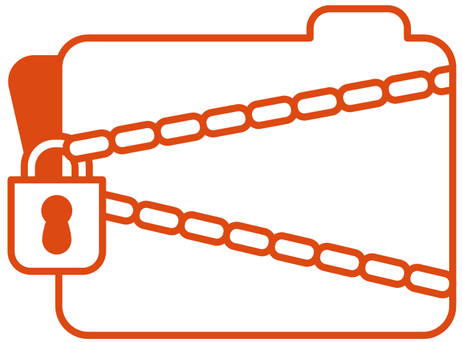


Reto Pt.1

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

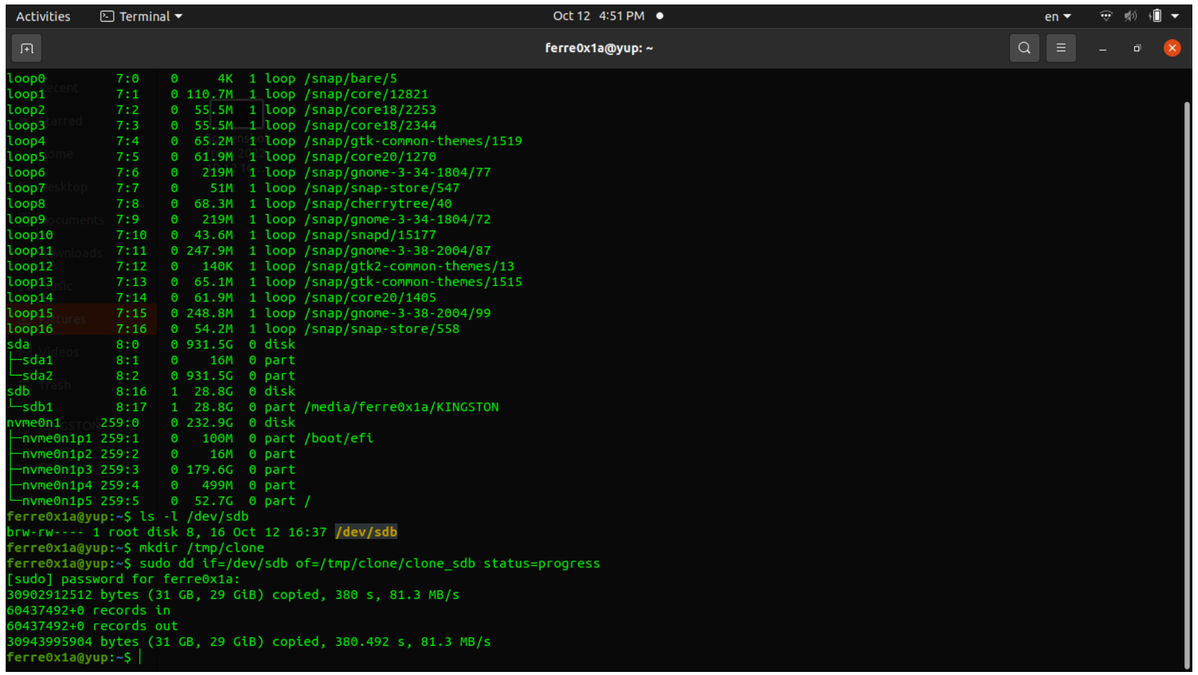
Objetivo:

- 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 imgen
  - 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



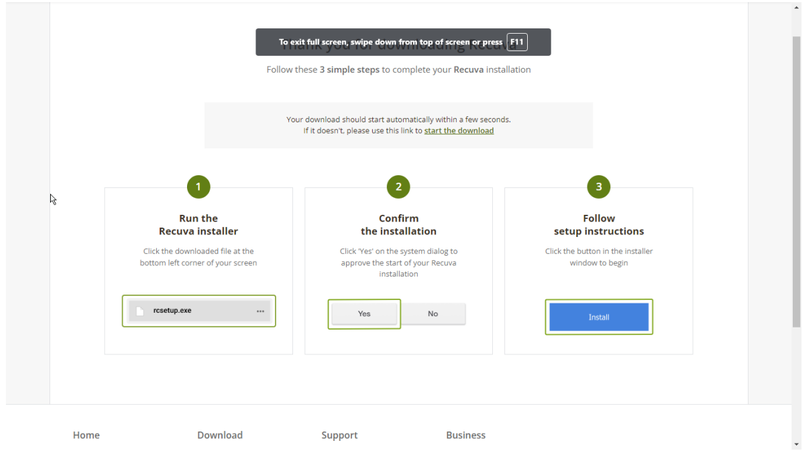
Recuperación de archivos

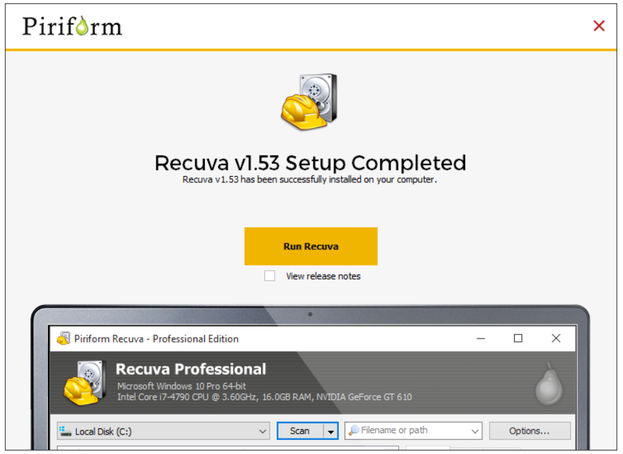
Recuva

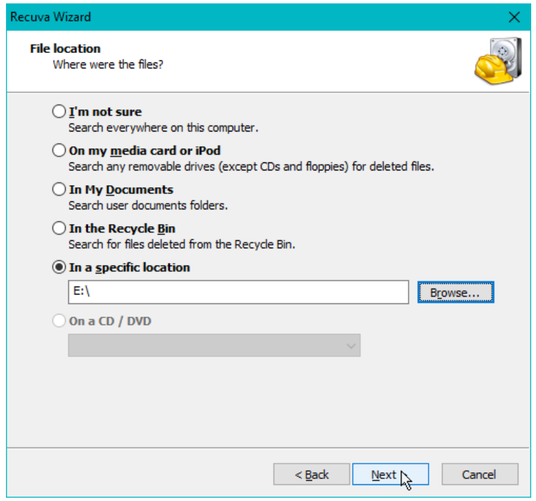
- Uso de la herramienta
  - Recuva de CCleaner
- Aplicación para recuperar archivos dañados o recientemente formateados
  - Capaz de restaurar cualquier tipo de archivo que se desee y de cualquier tipo de disco de almacenamiento
- Dentro del software
  - Escaneos simples, profundos, y muy específicos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

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

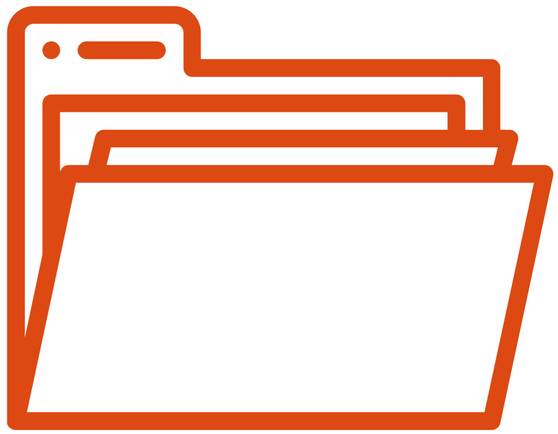




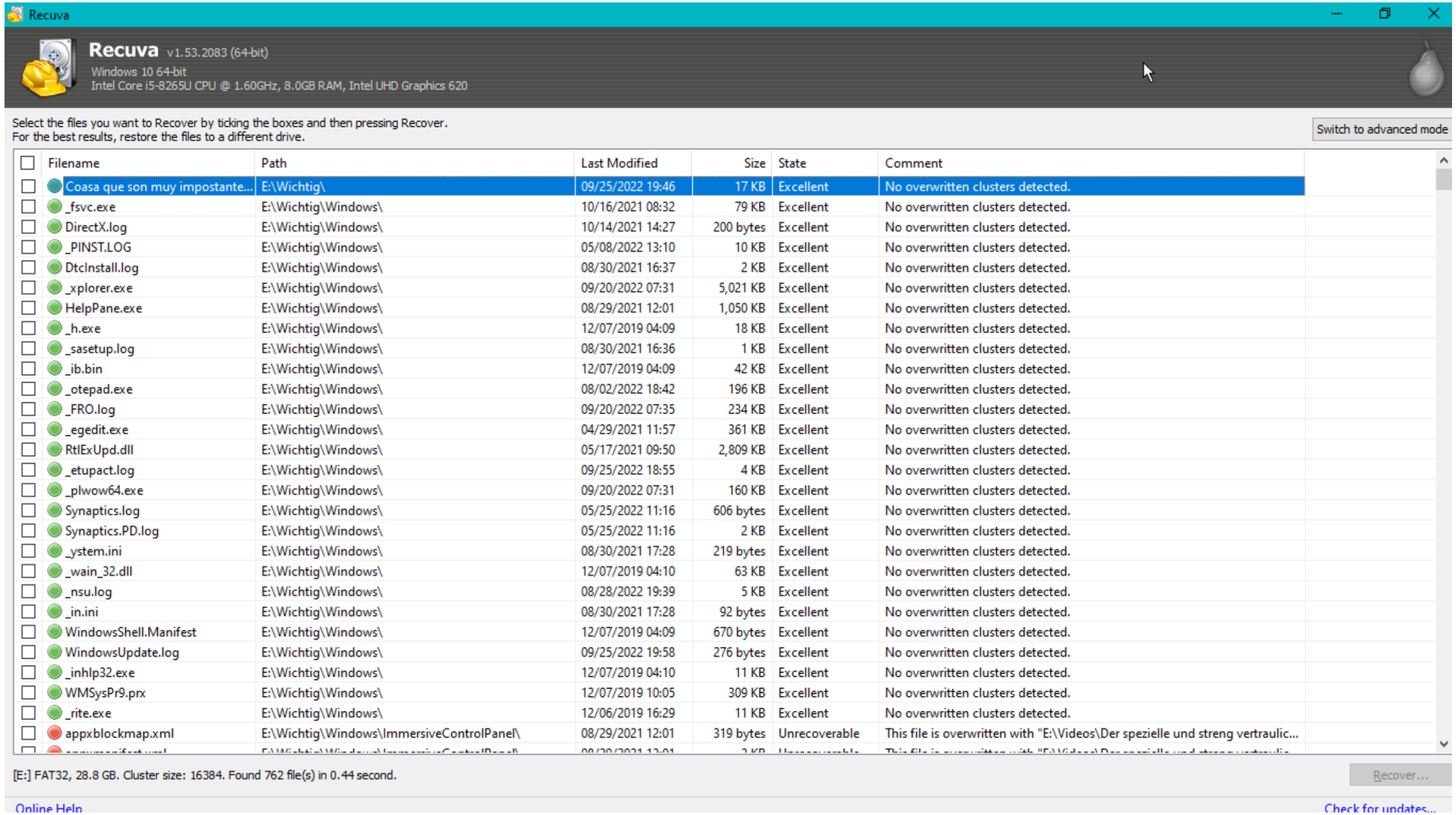


Identificación de archivos

- 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



Resultados

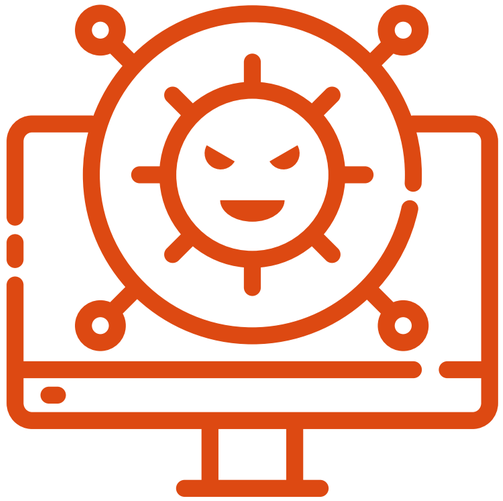
- 762 archivos borrados
- Estado de los archivos representados por círculos verdes, amarillos y rojos
- Formatos de archivos encontrados
  - ejecutables, imágenes, PAK, .dll, .xml, .log, .ini, .prx, etc.
- Archivos en distintos idiomas incluyendo el alemán
- Archivo objetivo con mensaje oculto
  - "**Coasa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

Procedimiento

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

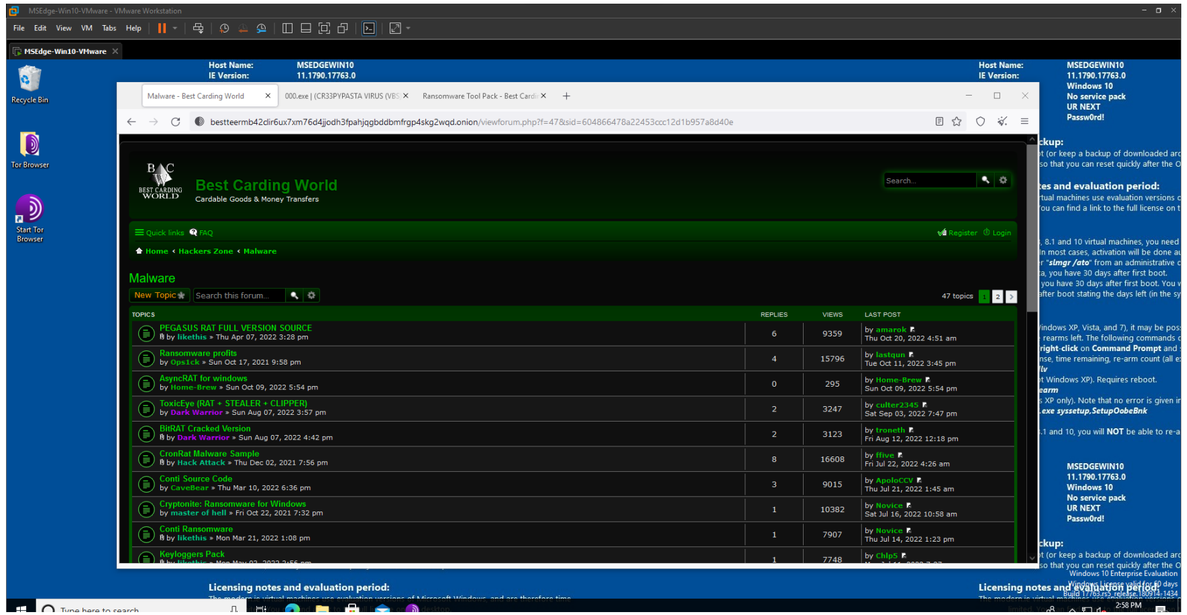
Instalación del antivirus

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

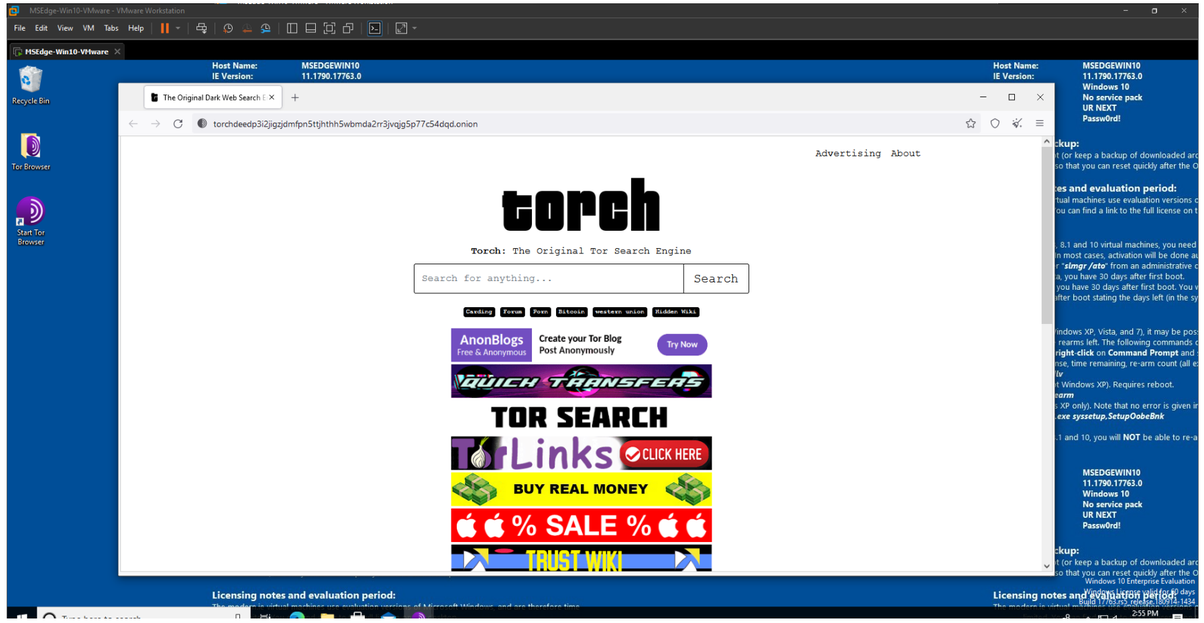
Malware Traffic Analysis (clearnet)

- Malware llamado
  - "ICEDID (BOKBOT) INFECTION WITH COBALT STRIKE"
- Descraga 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)

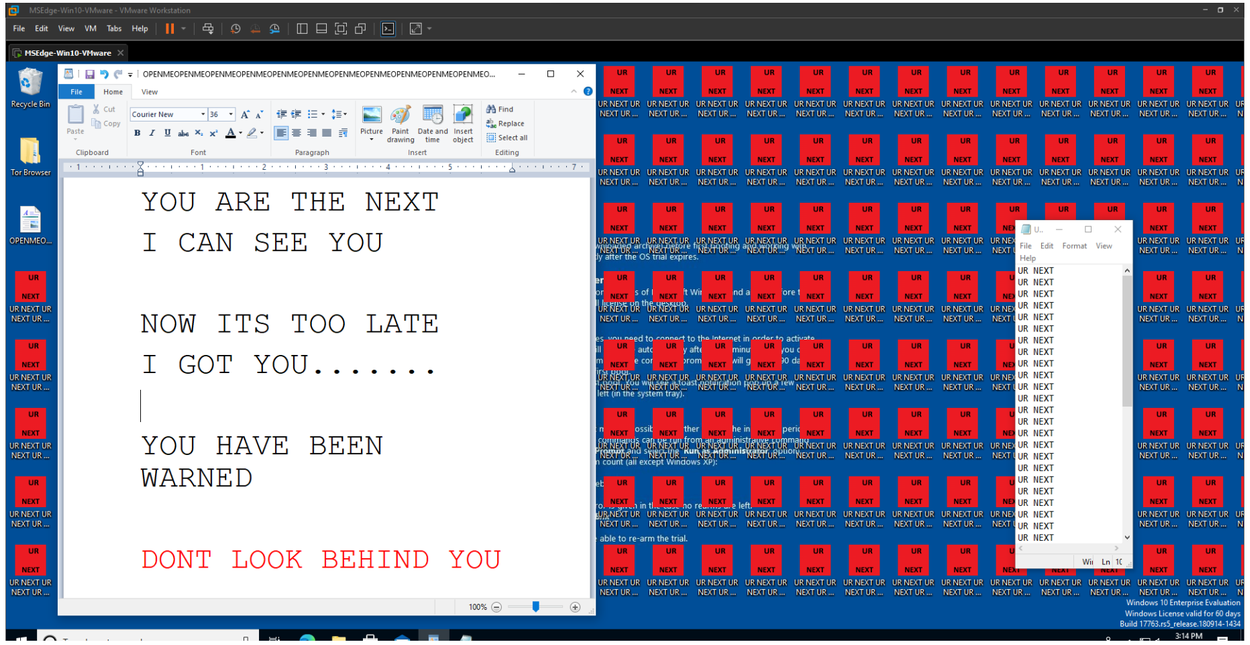
- Motor de búsqueda
  - Torch
- Muestra resultados sin filtros
- Búsqueda
  - "windus virus exe"

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

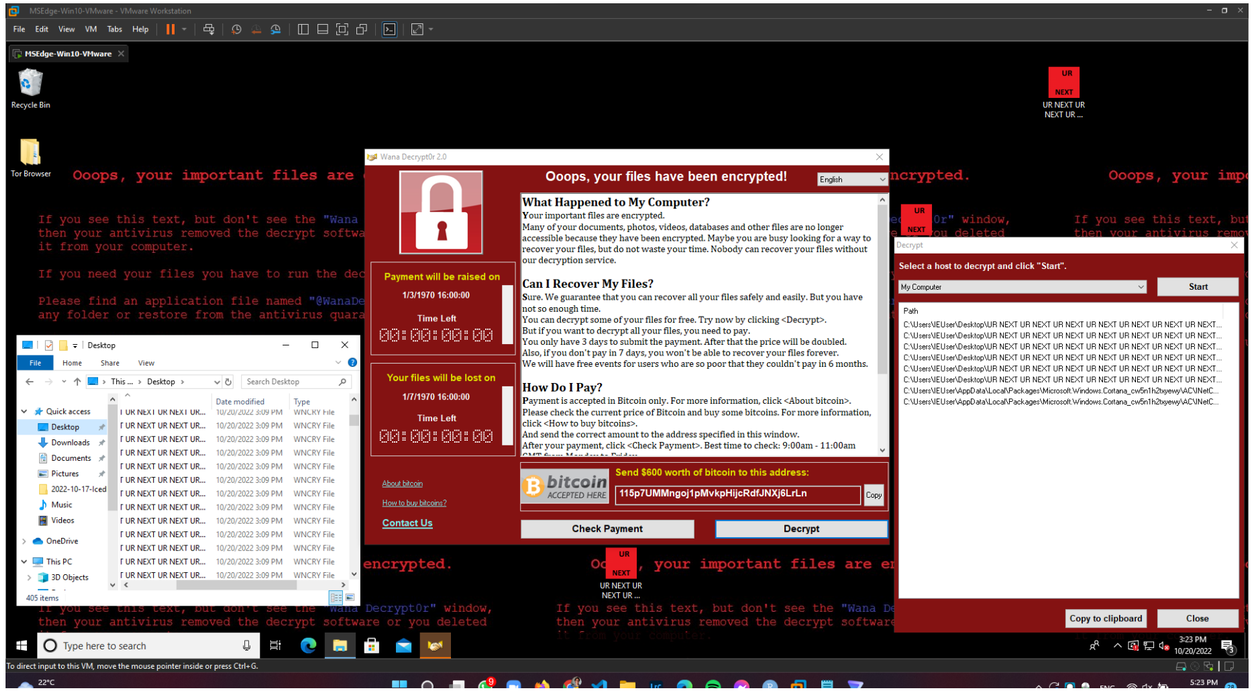
OOO.exe

- 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

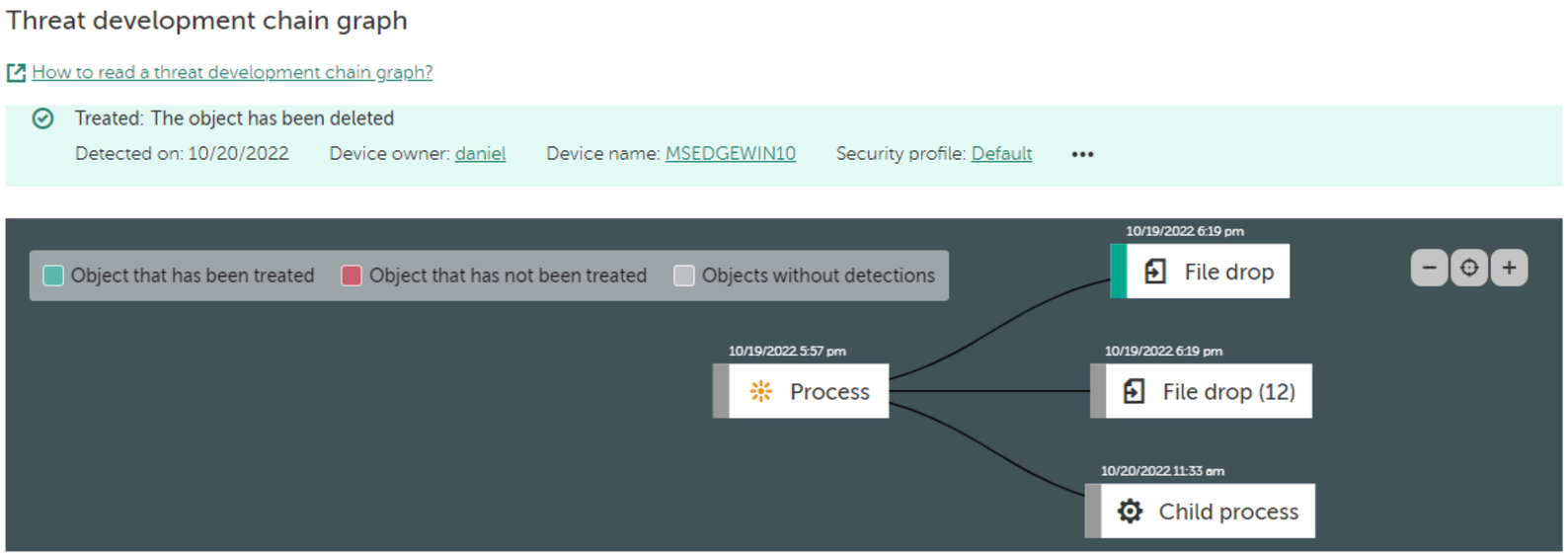


wannacry.exe

- 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

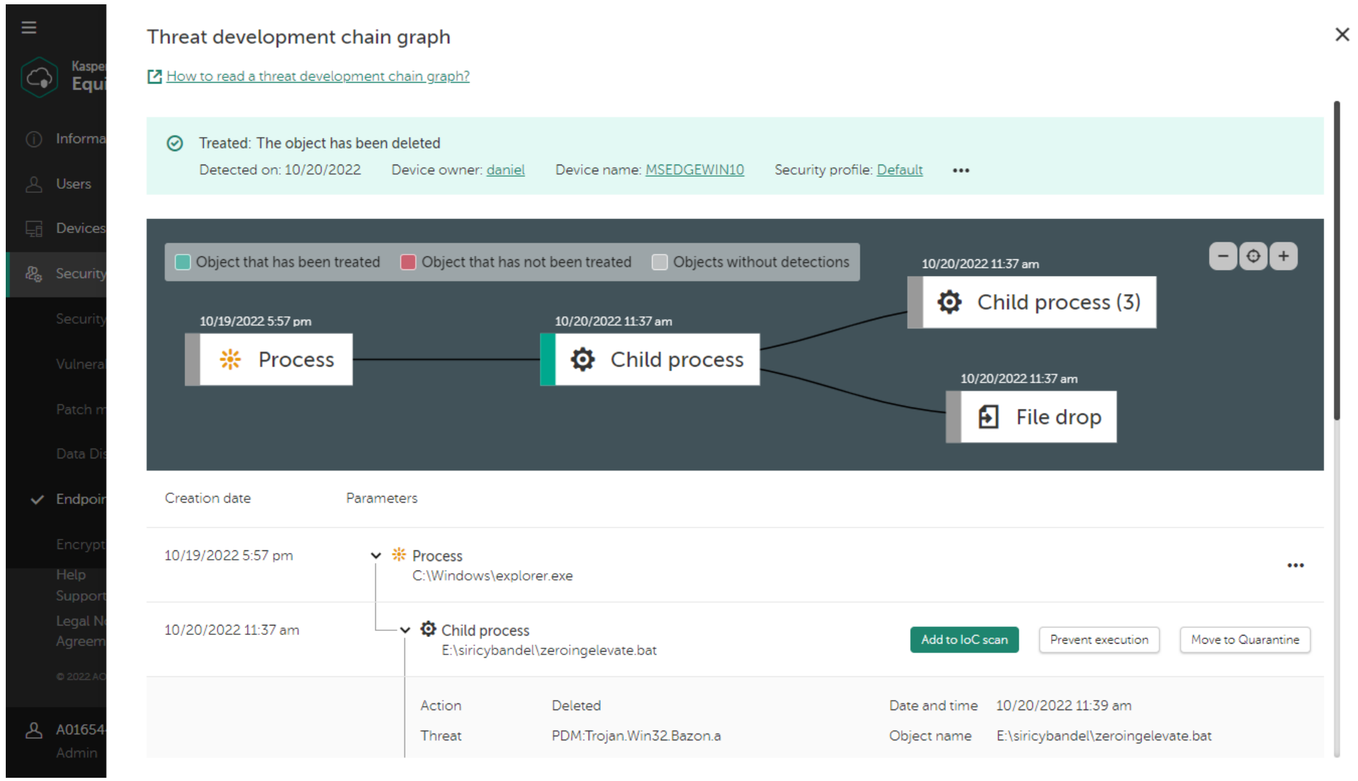
Monitoreo, detección y respuesta

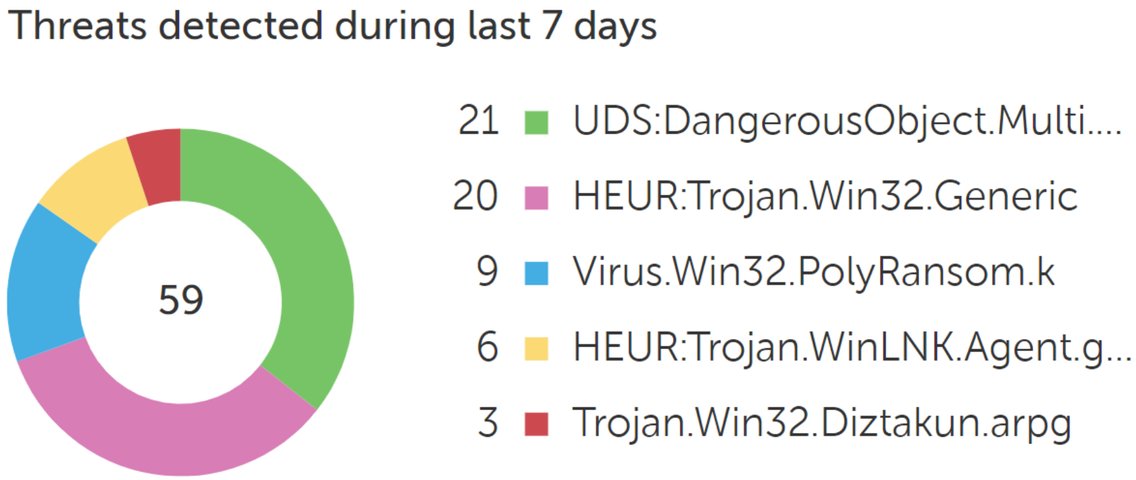
- Configuración de dos perfiles de protección
  - Con todas las herramientas recomendadas activadas
  - Con todas desactivadas
- El antivirus con el perfil recomendado analizaba todas las descargas y en la mayoría de los casos borraba los archivos antes de que estos pudieran ser ejecutados



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





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 impostantes 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.). An ́alisis 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: ARecovery 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