

DETECCIÓN Y MITIGACIÓN DE AMENAZAS

Valeria I Sada Chapa - A00837046

Carolina Treviño - A00835598

Paula M De Alba Barrera - A01722262

Antonio Noemi - A01026100

Gabriel Villanueva - A01781585



INTRODUCCIÓN

Objetivo

Tenemos como objetivo analizar la instalación y el comportamiento de distintos malwares en un entorno controlado utilizando la herramienta Kaspersky Endpoint Security Cloud, evaluando las amenazas identificadas y proponiendo estrategias de mitigación.

Contexto

El malware, en todas sus formas, representa un riesgo significativo para la ciberseguridad. Estos programas maliciosos pueden alterar sistemas, robar información o interrumpir servicios esenciales. El análisis de malware permite entender sus mecanismos y mitigar posibles daños.

Importancia

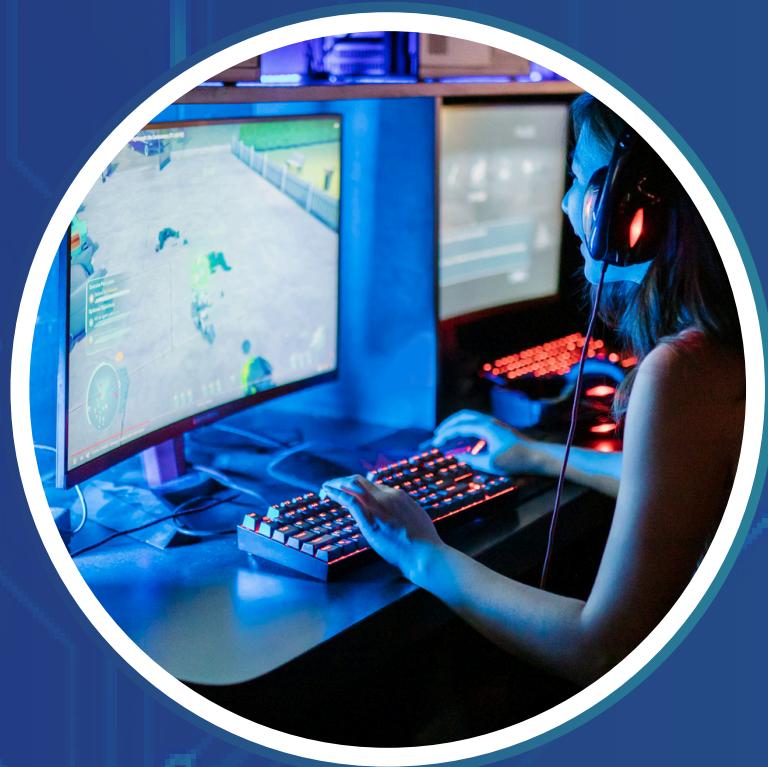
Estudiar los efectos del malware es fundamental para proteger tanto a usuarios individuales como a grandes organizaciones, ya que una infección puede tener consecuencias devastadoras para los datos y la continuidad del negocio.



kaspersky



¿QUE ES KASPERSKY ?



Kaspersky es una empresa global de ciberseguridad. Se especializa en el desarrollo de software de seguridad, soluciones de protección de información y servicios de ciberseguridad, principalmente para proteger a los usuarios de amenazas como malware, virus, spyware, phishing y otras formas de ciberataques

Antivirus y seguridad para consumidores

Seguridad empresarial y en la nube

Servicios de inteligencia de amenazas y ciberseguridad



Troyano Downloader

RAT (herramientas de acceso remoto)

Script malicioso

Escaneo de puertos

MALWARES



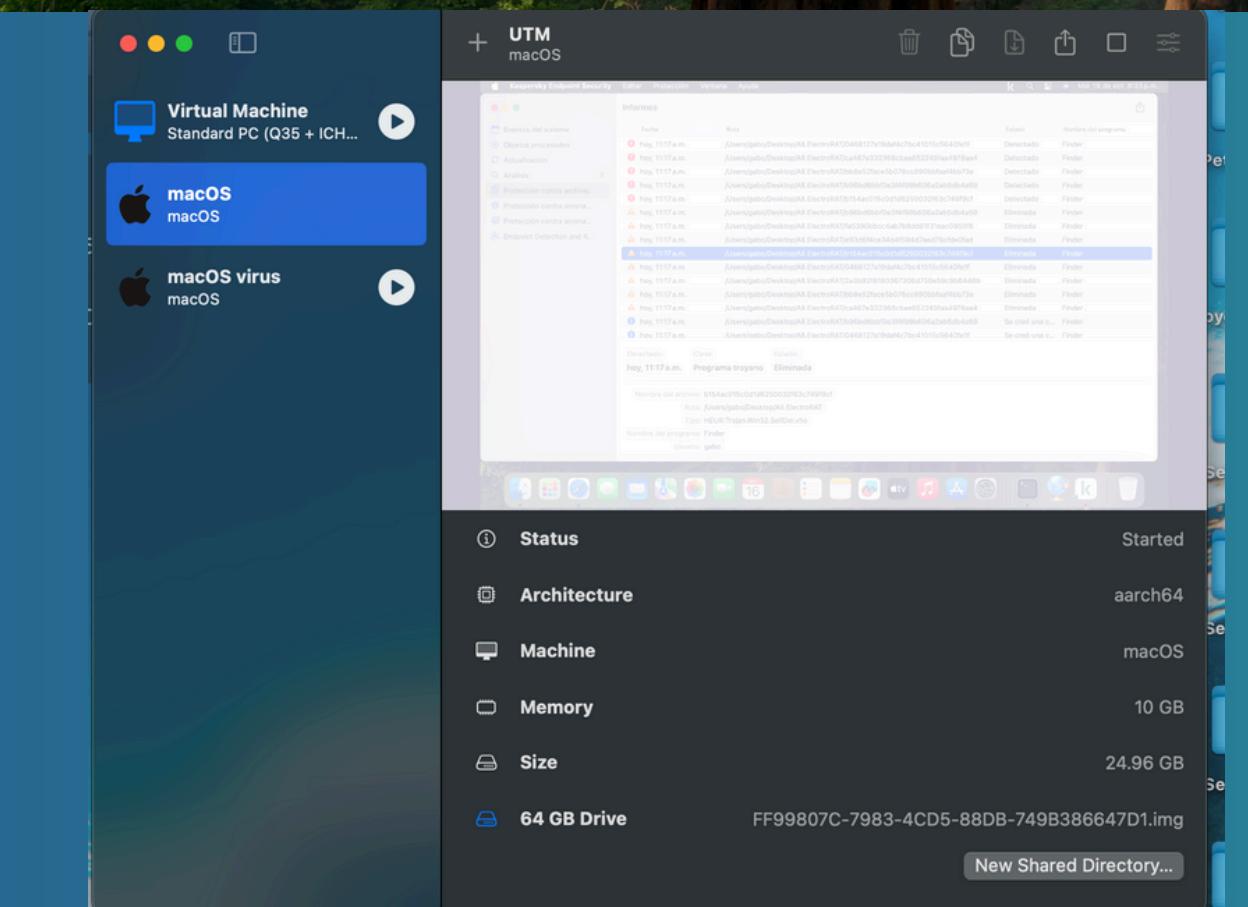
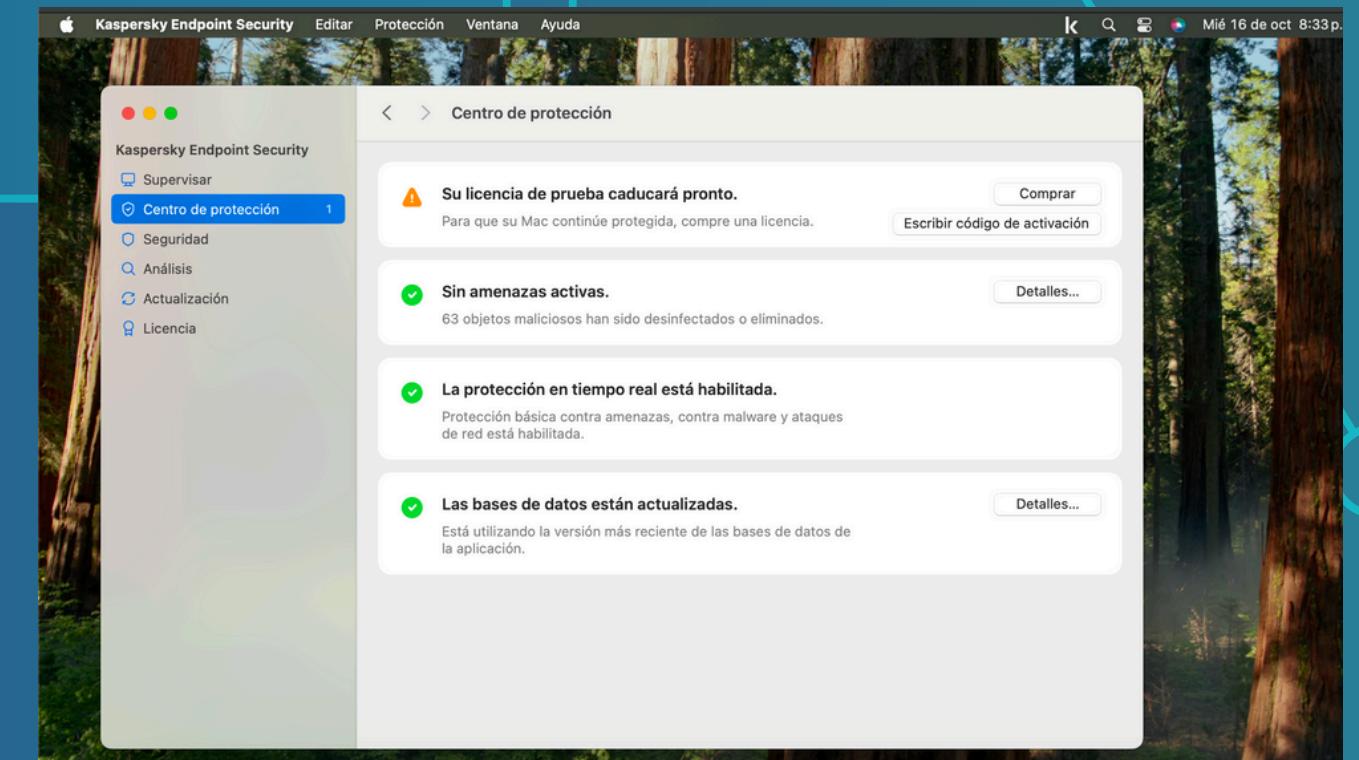
ANTECEDENTES

03/15

Descarga de Virtual Machines

Descarga de Kaspersky

MalwareBazaar y TheZoo repository

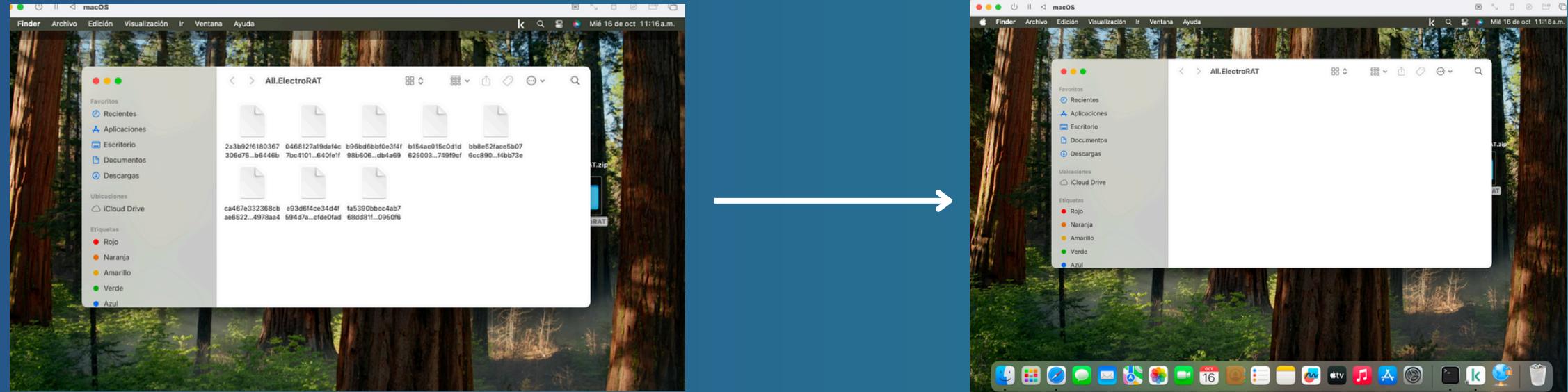


RESULTADOS

05/15

All.ElectroRAT

- Los RATs permiten a los atacantes obtener control remoto total sobre un sistema infectado.
- ElectroRAT fue descubierto en 2021 y se utilizó principalmente para atacar a usuarios de criptomonedas, robando claves privadas, credenciales y fondos.
- Este malware se disfrazaba como aplicaciones legítimas, incluyendo carteras de criptomonedas y herramientas de trading, engañando a los usuarios para que lo instalaran.



Fecha	Ruta	Estado	Nombre del programa
! hoy, 11:17 a.m.	/Users/gabo/Desktop/All.ElectroRAT/2a3b92f6180367306d750e59c9b6446b	Detectedo	Finder
! hoy, 11:17 a.m.	/Users/gabo/Desktop/All.ElectroRAT/fa5390bbcc4ab768dd81f31eac0950f6	Detectedo	Finder
! hoy, 11:17 a.m.	/Users/gabo/Desktop/All.ElectroRAT/e93d6f4ce34d4f594d7aed76cfde0fad	Detectedo	Finder
! hoy, 11:17 a.m.	/Users/gabo/Desktop/All.ElectroRAT/0468127a19daf4c7bc41015c5640fe1f	Detectedo	Finder
! hoy, 11:17 a.m.	/Users/gabo/Desktop/All.ElectroRAT/ca467e332368cbae652245faa4978aa4	Detectedo	Finder
! hoy, 11:17 a.m.	/Users/gabo/Desktop/All.ElectroRAT/bb8e52face5b076cc890bbfaaf4bb73e	Detectedo	Finder
! hoy, 11:17 a.m.	/Users/gabo/Desktop/All.ElectroRAT/b96bd6bbf0e3f4f98b606a2ab5db4a69	Detectedo	Finder
! hoy, 11:17 a.m.	/Users/gabo/Desktop/All.ElectroRAT/b154ac015c0d1d6250032f63c749f9cf	Detectedo	Finder
⚠ hoy, 11:17 a.m.	/Users/gabo/Desktop/All.ElectroRAT/b96bd6bbf0e3f4f98b606a2ab5db4a69	Eliminada	Finder
⚠ hoy, 11:17 a.m.	/Users/gabo/Desktop/All.ElectroRAT/fa5390bbcc4ab768dd81f31eac0950f6	Eliminada	Finder
⚠ hoy, 11:17 a.m.	/Users/gabo/Desktop/All.ElectroRAT/e93d6f4ce34d4f594d7aed76cfde0fad	Eliminada	Finder
⚠ hoy, 11:17 a.m.	/Users/gabo/Desktop/All.ElectroRAT/b154ac015c0d1d6250032f63c749f9cf	Eliminada	Finder
⚠ hoy, 11:17 a.m.	/Users/gabo/Desktop/All.ElectroRAT/0468127a19daf4c7bc41015c5640fe1f	Eliminada	Finder
⚠ hoy, 11:17 a.m.	/Users/gabo/Desktop/All.ElectroRAT/2a3b92f6180367306d750e59c9b6446b	Eliminada	Finder
⚠ hoy, 11:17 a.m.	/Users/gabo/Desktop/All.ElectroRAT/bb8e52face5b076cc890bbfaaf4bb73e	Eliminada	Finder



RESULTADOS

06/15

Trojan Downloader

Amenaza:
HEUR.Win32.Deyma.gen

Trojan-Downloader: Este malware intenta descargar más archivos maliciosos una vez que se instala.

El archivo malicioso estaba localizado en la carpeta All.ElectroRAT dentro del escritorio del usuario. ElectroRAT podría haber intentado descargar este troyano como parte de sus operaciones.

The screenshot shows a security software interface with a dark theme. At the top, there are three status indicators: 'treated' (green), 'Object that has not been treated' (red), and 'Objects without detections' (grey). Below this is a date and time stamp: '03/23/2022 5:10 am'. A large green button labeled 'Detect' is prominently displayed. To the right of the button are three small icons: a minus sign, a plus sign, and a square. The main area is titled 'Parameters' and contains a single row of information: 'Action Deleted' (with a yellow star icon), 'Threat HEUR:Trojan-Downloader.Win32.Deyma.gen', 'Date and time 10/16/2024 11:17 am', and 'Object name /Users/gabo/Desktop/All.ElectroRAT/2a3b92f6180367306d750e59c9b6446b'. At the bottom of this section are three buttons: 'Add to IoC scan' (green), 'Prevent execution' (grey), and 'Move to Quarantine' (grey).

Hash MD5: 2a3b92f6180367306d750e59c9b6446b
SHA256:
18fd6b193be1d5416a3188f5d9e4047cca719fa067d7d0169cf2df5c7fed54c0



RESULTADOS

07/15

Trojan Downloader - Amaday

Hash MD5: 2a3b92f6180367306d750e59c9b6446b

SHA256:

18fd6b193be1d5416a3188f5d9e4047cca719fa067d7d0169cf2df5c7fed54c0

¿Qué hace este Trojan Downloader?

- Descarga malware adicional y ejecuta instrucciones desde servidores remotos.
- Capaz de establecer comunicación con servidores externos para recibir datos y enviar solicitudes. Así los atacantes pueden enviar instrucciones en tiempo real
- Utiliza técnicas de evasión para evitar ser detectado en entornos de análisis como sandbox.

Es capaz de cambiar los registros y ocultar sus archivos para evitar ser eliminado

- Ejecuta su código malicioso a intervalos regulares con tareas programadas sin que la víctima lo note.

Capabilities	— Anti-Behavioral Analysis	OB0001
— Host-Interaction		
Get user security identifier	Debugger Detection	B0001
Create process on Windows	Process Environment Block	B0001.019
Create process suspended		
Allocate or change RWX memory		
Resume thread		
Suspend thread		
Create thread		
Get file attributes		
Get session user name		
Write file on Windows		
Use process replacement		
Get common file path		
Get hostname		
Create mutex		
Terminate process		
Check mutex and exit		
Check if file exists		
Read file on Windows		
Create directory		
Get system information on Windows		
Check OS version		
Delete file		
— Communication		
Create HTTP request		
Connect to URL		
Read data from Internet		
Receive data		
Download and write a file		
Receive and write data from server to client		
Connect to HTTP server		
Send HTTP request		
Send data		



RESULTADOS

08/15

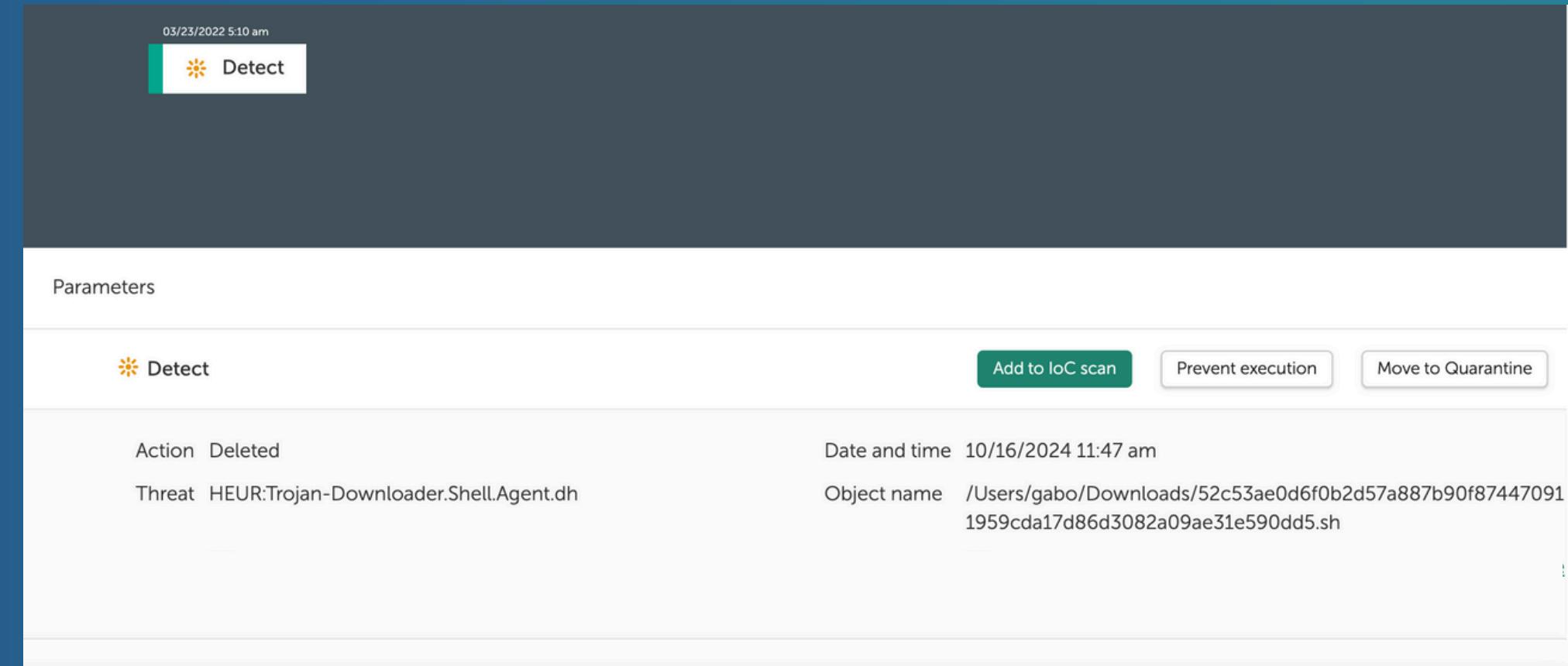
Hash MD5: 83b52b0f54758f58e53ac3ca4befd5a5

SHA256:

152c53ae0d6f0b2d57a887b90f874470911959cda17d86d3082a09ae31e590dd5

Amenaza:
HEUR.Shell.Agent.dh
Este es un troyano downloader

Shell.Agent: Indica que puede ser un script de shell malicioso, diseñado para ejecutarse desde la terminal del sistema.



The screenshot shows a threat detection interface. At the top, there is a timestamp '03/23/2022 5:10 am' and a 'Detect' button. Below this is a 'Parameters' section with a 'Detect' button. In the center, it displays 'Action Deleted' and 'Threat HEUR:Trojan-Downloader.Shell.Agent.dh'. On the right side, there are buttons for 'Add to IoC scan', 'Prevent execution', and 'Move to Quarantine'. At the bottom right, it shows 'Date and time 10/16/2024 11:47 am' and 'Object name /Users/gabo/Downloads/52c53ae0d6f0b2d57a887b90f874470911959cda17d86d3082a09ae31e590dd5.sh'.

Este tipo de malware es especialmente peligroso porque puede descargar otros archivos y ejecutar comandos en el sistema sin que el usuario lo note.



RESULTADOS

09/15

Trojan Shell

Hash MD5: 83b52b0f54758f58e53ac3ca4befd5a5

SHA256:

152c53ae0d6f0b2d57a887b90f874470911959cda17d86d3082a09ae31e590dd5

¿Qué hace este Trojan Downloader – Shell?

- Ejecuta shellcode directamente en el sistema infectado, lo que permite al atacante ejecutar comandos a nivel del sistema.

Establece conexiones con servidores remotos para recibir órdenes adicionales

- Modifica procesos del sistema para obtener permisos elevados.

- Utiliza tareas programadas (crontab) y procesos de iniciación del sistema (systemd) para mantenerse activo incluso después de reinicios del sistema.

— Execution TA0002	
 Scheduled Task/Job T1053	Executes the "crontab" command typically for achieving persistence
— Scripting T1064	
Found strings indicative of a multi-platform dropper	
Found strings indicative of a multi-platform dropper	
Found strings indicative of a multi-platform dropper	
Executes commands using a shell command-line interpreter	
— Persistence TA0003	
 Scheduled Task/Job T1053	Executes the "crontab" command typically for achieving persistence
 Create or Modify System Process T1543	
 Systemd Service T1543.002	Executes the "systemctl" command used for controlling the systemd system and service manager
— Privilege Escalation TA0004	
 Scheduled Task/Job T1053	Executes the "crontab" command typically for achieving persistence
 Create or Modify System Process T1543	
 Systemd Service T1543.002	Executes the "systemctl" command used for controlling the systemd system and service manager



RESULTADOS

Kaspersky Next

Network attacks

This report displays network attacks on managed devices over the last 7 days.

Total attacks: 3. Attacking IP addresses: 1. Devices attacked: 1. First detection: 10/10/2024 6:19 pm. Last detection: 10/14/2024 3:15 pm.

Details

Report generated on 10/16/2024 at 9:17 am

Time of device operating system is displayed

Device	Attack	Attack time	Attack IP address	Protocol	Port	Attacked interface address
mac con kaspersky	Scan.Generic.PortScan.UDP	10/10/2024 6:21 pm	74.125.250.129	17	51620	
mac con kaspersky	Scan.Generic.PortScan.UDP	10/10/2024 6:19 pm	74.125.250.129	17	59066	
mac con kaspersky	Scan.Generic.PortScan.UDP	10/14/2024 3:15 pm	74.125.250.129	17	55392	

Cloud Discovery: Blocked attempts to access cloud services | PDF | CSV |

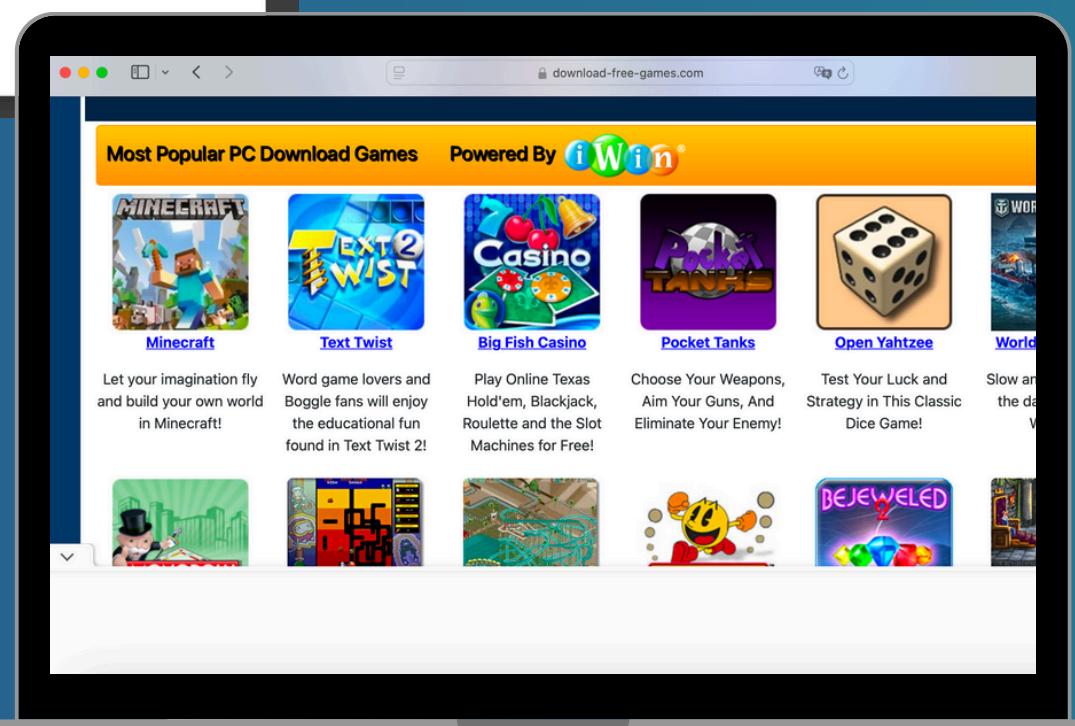
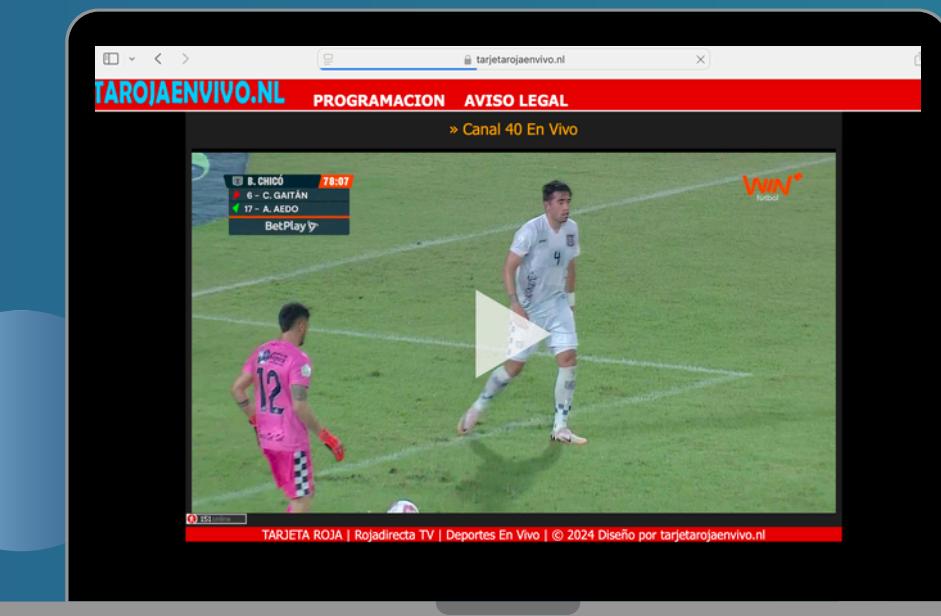
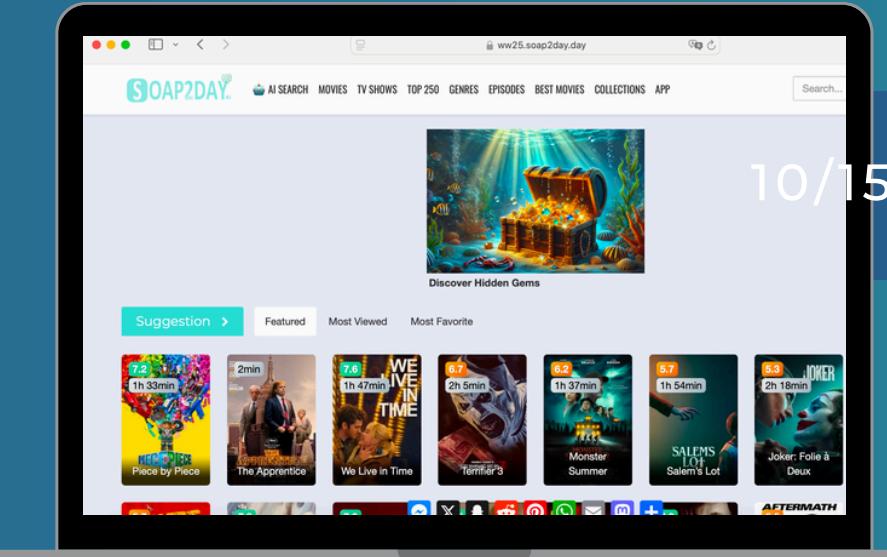
Detalles del Ataque:

Tipo: Scan.Generic.PortScan.UDP

Protocolo: UDP (17)

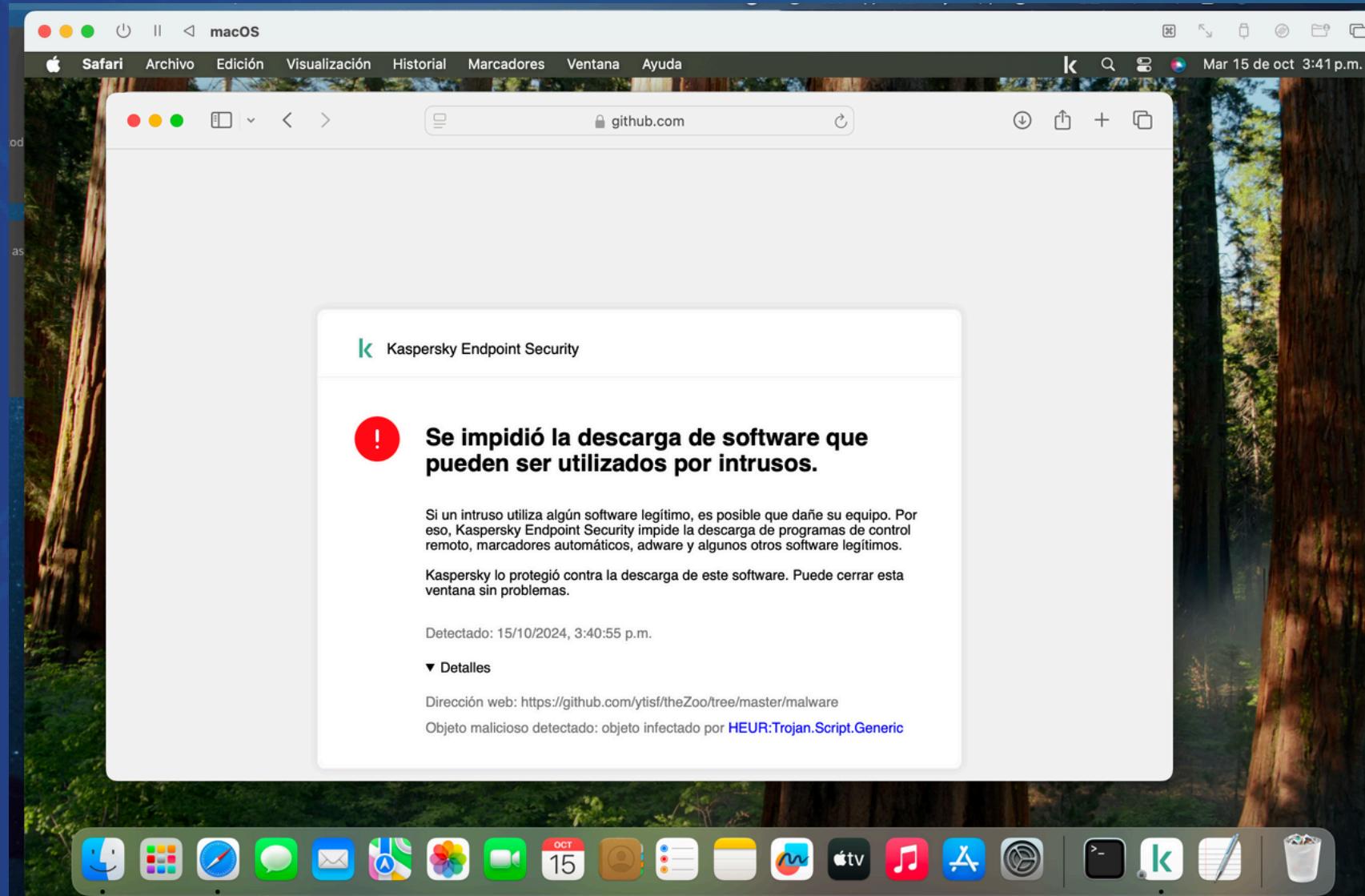
Puertos escaneados: **51620, 59066, 55392**

Objetivo: El escaneo de puertos es una técnica utilizada por atacantes para descubrir qué puertos y servicios están abiertos en un dispositivo, con el fin de encontrar vulnerabilidades explotables.



RESULTADOS

11/15



Motivo del Bloqueo:

La protección de Kaspersky Endpoint Security ha identificado que la descarga contenía un objeto malicioso clasificado como:
HEUR.Script.Generic

HEUR: Indica que la detección fue heurística, es decir, basada en comportamientos sospechosos en lugar de una firma específica.

Trojan.Script.Generic: Hace referencia a un troyano que se disfraza como un script o código que podría ejecutar acciones maliciosas.

CONCLUSIONES

12/15

01

ElectroRAT

RATs sigue siendo una de las amenazas más peligrosas debido a su capacidad para controlar el sistema infectado. Esto muestra la importancia de contar con sistemas de seguridad fuertes, especialmente para usuarios que manejan activos digitales.

02

Troyanos

El análisis de los Troyanos muestra que este tipo de malware no solo afecta el sistema directamente, sino que actúa como un punto de entrada para otros archivos maliciosos. Esto resalta la necesidad de una detección temprana antes de tener mayores daños.

03

Kaspersky

La protección de Kaspersky fue efectiva al identificar y bloquear amenazas mediante la observación de cómo actúan los programas (heurística). Esto permitió detectar amenazas que no fueron reconocidas antes.

Con base a los resultados, notamos lo importante que es implementar un enfoque de seguridad múltiple que incluya no solo detección basada en firmas, sino también análisis de comportamiento, monitoreo continuo de la red y actualizaciones regulares de software.



GRACIAS

