REPORTE RETO

Alberto Gómez
Arath Mendivil
Joaquin Sainz
Maximiliano García
Joana Barreto

¿EN QUÉ CONSISTE?

- Instalar máquina virtual
- Propagación y analisis de los virus
- Desarrollar habilidades de seguridad informática

KASPERSKI

- Protección contra Malware
- Firewall personal
- Protección contra Phishing
- Protección en tiempo real
- Forensia Digital
- Uso de Inteligencia Artificial
- Etc.

OSX.DEFMA

- Malware dirigido a usuarios de Mac y pertenece a la familia de programas antivirus falsos (FAKEAV).

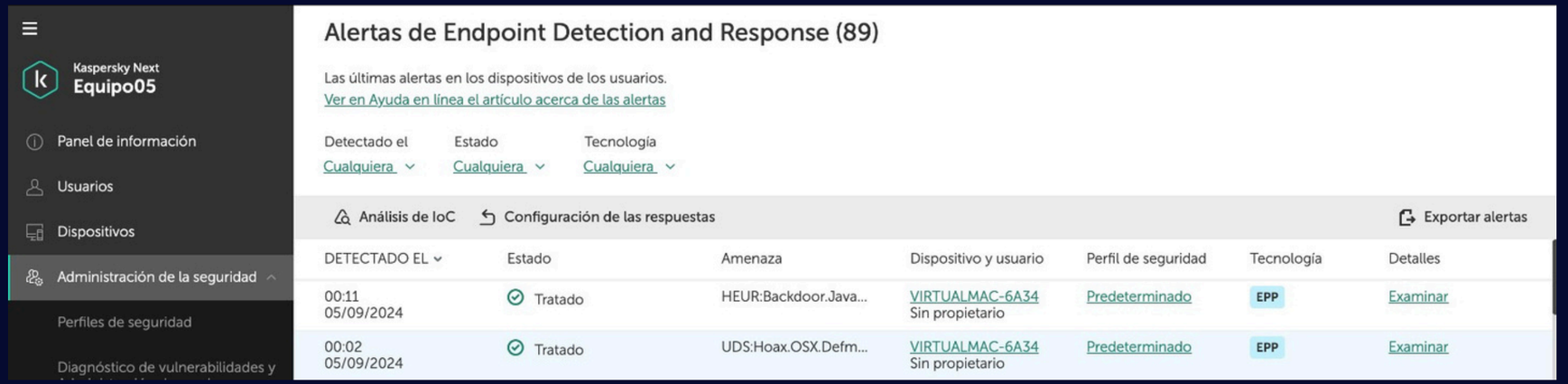
- Su objetivo es engañar a los usuarios haciéndoles creer que sus sistemas están infectados, para que compren software innecesario con la promesa de "limpiar" el sistema.

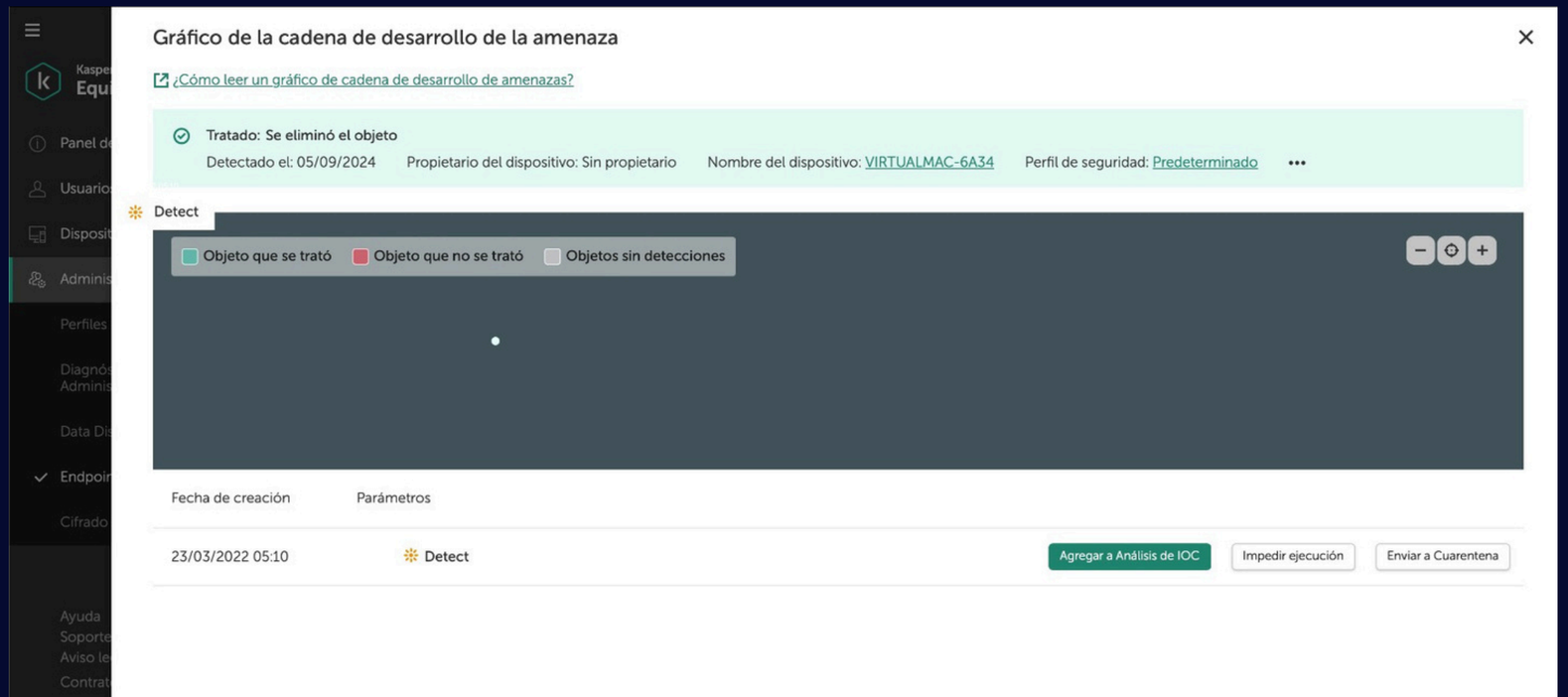
- Se propaga principalmente a través de tácticas de ingeniería social

PRINCIPALES FUNCIONES

- Engaño mediante falsas alertas de seguridad
- Extorsión financiera
- Descarga de malware adicional
- Acciones de ingeniería social

¿CÓMO SE TRATÓ?





CONSECUENCIAS

- Pérdida de confianza y credibilidad
- Robo de Información
- Interrupción de Operaciones
- Costos Adicionales por Respuestas a Incidentes
- Exposición a más amenazas

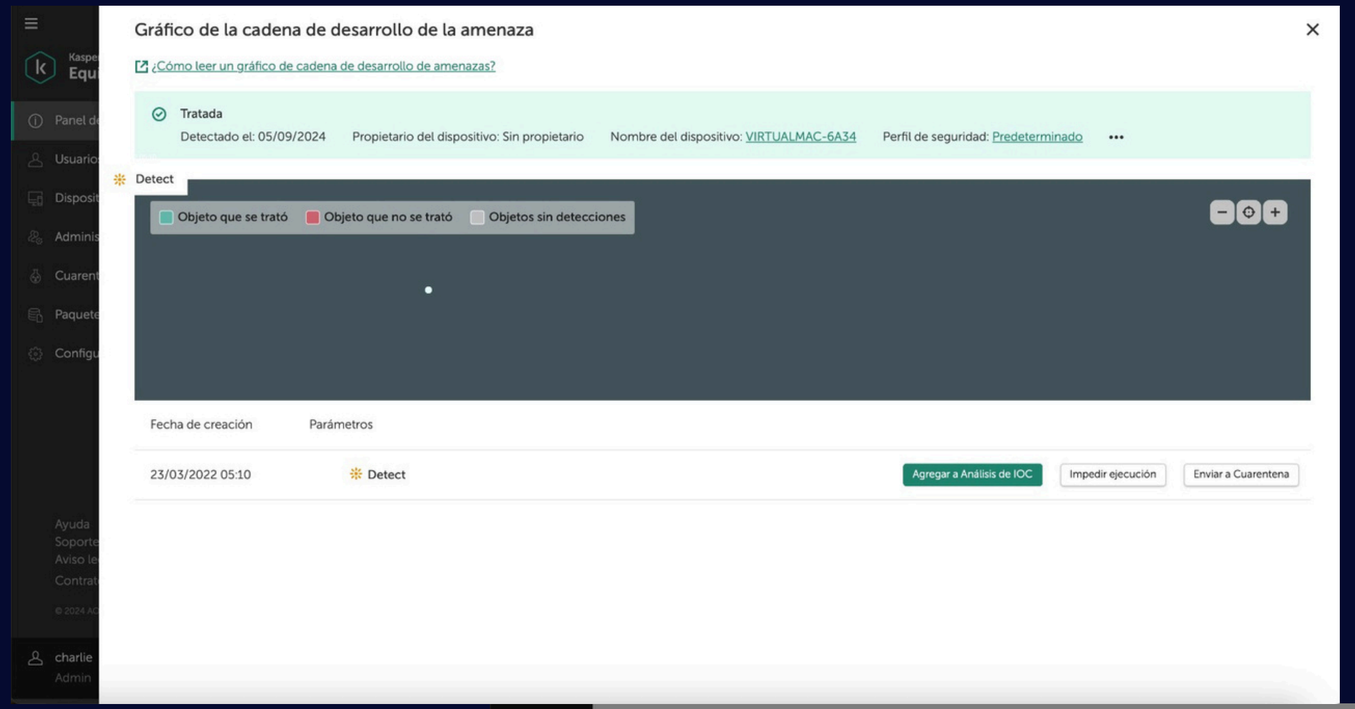
OSX.AMOS

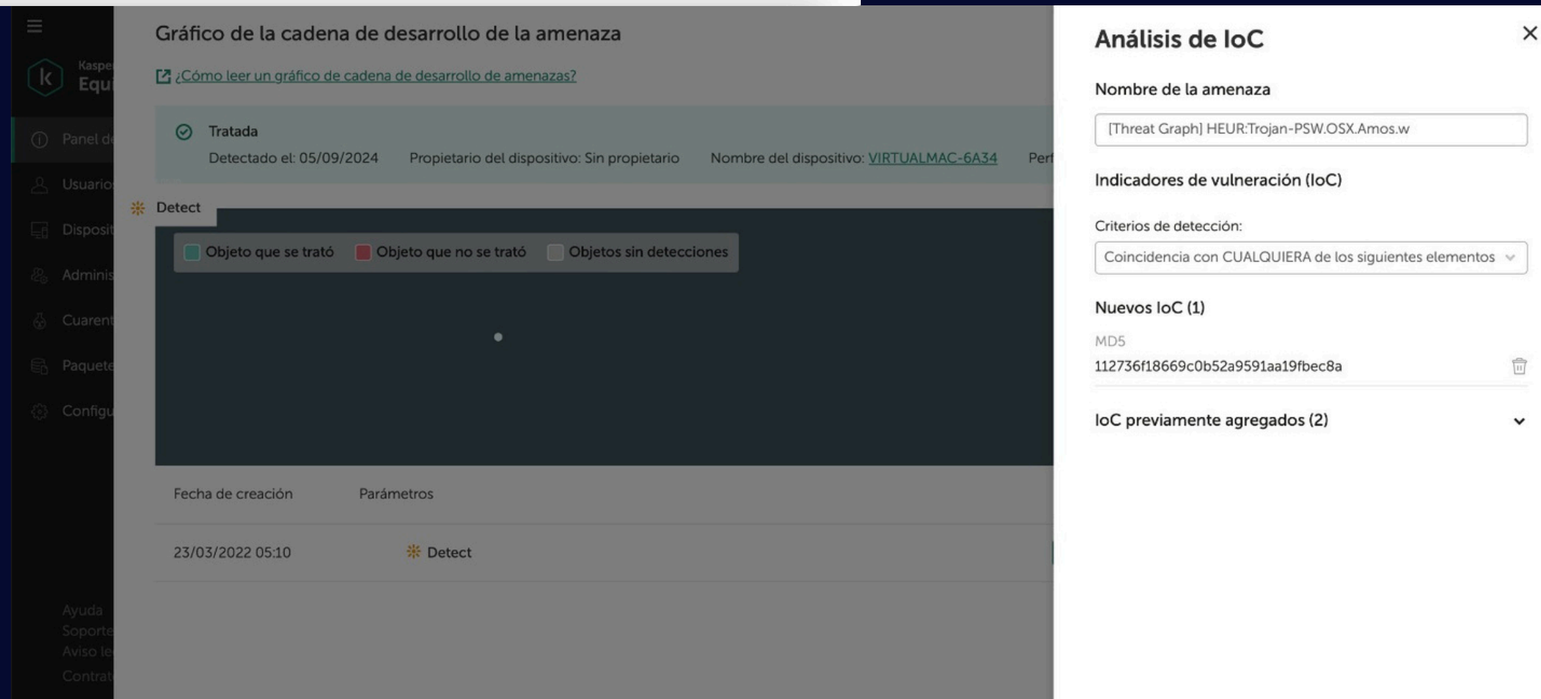
- Malware diseñado específicamente para robar información sensible de dispositivos Mac.
- Troyano
- Se distribuye a través de archivos maliciosos disfrazados de aplicaciones legítimas, como actualizaciones falsas de navegadores o software popular.

PRINCIPALES FUNCIONES

- Robo de información personal
- Filtración de datos
- Ingeniería social
- Ataques a navegadores y criptocarteras

CÓMO SE TRATÓ





CONSECUENCIAS

- Comprometer datos críticos
- Exposición de información financiera
- Robo de identidad
- Fraudes financieros

COMPARACIÓN

Característica	OSX.Defma	OSX.Amos (Atomic macOS Stealer)
Tipo de Malware	FakeAV	Troyano robador de información
Métodos de Distribución	Redes sociales, phishing, alertas falsas de antivirus	Anuncios maliciosos, sitios de descargas falsas, malvertising
Objetivo Principal	Extorsionar al usuario para que compre software falso	Robar información sensible como contraseñas y criptocarteras
Peligrosidad	Moderada, enfocado en fraude financiero	Alta, enfocado en robo de datos y pérdida financiera grave
Métodos de Detección	Detectado fácilmente por antivirus tradicionales	Difícil de detectar, usa técnicas avanzadas de evasión
Consecuencias	Pérdida de dinero, ralentización del sistema	Robo de identidad, acceso a cuentas financieras y criptográficas
Información Robada	Ninguna	Contraseñas, datos de navegadores, criptocarteras, archivos del sistema
Técnicas Utilizadas	Ingeniería social para engañar al usuario	Exfiltración de datos, evasión de sandbox, uso de AppleScript y Python

OTRAS PRUEBAS

- ZeroAccess
- Zeus
- AgentTesla

OTROS VIRUS

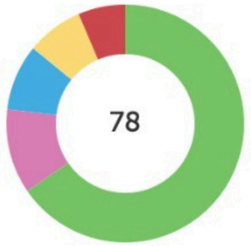
Alertas de Endpoint Detection and Response

Mostrar alertas: Todos: 10 | No examinadas: 9 | Examinadas: 1

LAS 10 ALERTAS PRINCIPALES — Ir a la lista de alertas

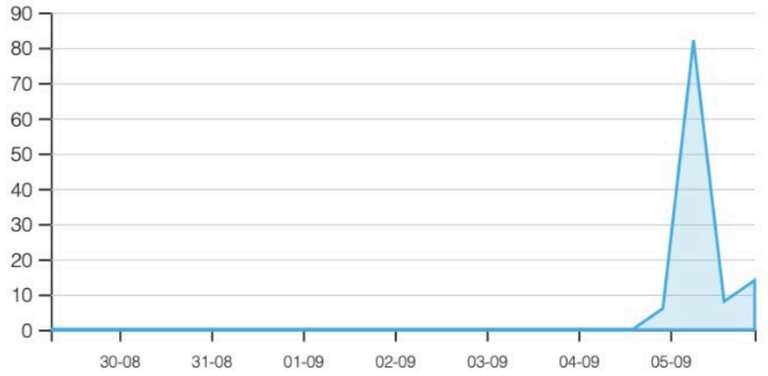
##	Detectado el	Estado	Amenaza	Nombre del dispositivo	Tecnología	Detalles
1	15:12 05/09/2024	Tratado	https://githu...	DESKTOP-UPD1...	EPP	Examinar
2	15:08 05/09/2024	Tratado	https://githu...	DESKTOP-UPD1...	EPP	Examinar
3	15:07 05/09/2024	Tratado	https://githu...	DESKTOP-UPD1...	EPP	Examinar
4	15:06 05/09/2024	Tratado	https://githu...	DESKTOP-UPD1...	EPP	Examinar
5	15:06 05/09/2024	Tratado	https://githu...	DESKTOP-UPD1...	EPP	Examinar
6	15:06 05/09/2024	Tratado	https://githu...	DESKTOP-UPD1...	EPP	Examinar
7	15:04 05/09/2024	Tratado	HEUR:Trojan-...	VIRTUALMAC-6A...	EPP	Examinar
8	14:43 05/09/2024	Tratado		VIRTUALMAC-6...	EPP	Examinar
9	14:37 05/09/2024	Tratado	https://githu...	DESKTOP-UPD1...	EPP	Examinar
10	14:37 05/09/2024	Tratado	https://githu...	DESKTOP-UPD1...	EPP	Examinar

Amenazas que se detectaron durante los últimos siete días



51
9 https://github.com/ytisf/theZoo
7 HEUR:Trojan.Script.Generic
6 HEUR:Trojan-PSW.OSX.Amos.w
5 HEUR:Trojan.Win32.Agent.gen

Detección de amenazas durante los últimos siete días



QUE HACER

- Preparación y protección
- Detección y análisis
- Aislamiento, erradicación y recuperación
- Post-mortem

CONCLUSIÓN

OSX.Amos > OSX.Defma

OSX.Defma es más sencillo, ya que ejecuta menos pasos al intentar engañar al usuario mediante tácticas de miedo. Por otro lado, OSX.Amos realiza múltiples pasos, desde la infección inicial hasta la exfiltración de una gran variedad de datos, lo que lo convierte en una amenaza más sofisticada y difícil de detectar.

CONCLUSIÓN

GRACIAS