



REPORTE RETO

Alberto Gómez
Arath Mendivil
Joaquin Sainz
Maximiliano García
Joana Barreto

¿EN QUÉ CONSISTE?

- Instalar máquina virtual
- Propagación y análisis 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?

Kaspersky Next

Equipo05

Panel de información

Usuarios

Dispositivos

Administración de la seguridad

Perfiles de seguridad

Diagnóstico de vulnerabilidades y

Alertas de Endpoint Detection and Response (89)

Las últimas alertas en los dispositivos de los usuarios.
[Ver en Ayuda en línea el artículo acerca de las alertas](#)

Detectado el

Cualquiera

Estado

Cualquiera

Tecnología

Cualquiera

Analisis de IoC

Configuración de las respuestas

Exportar alertas

DETECTADO EL	Estado	Amenaza	Dispositivo y usuario	Perfil de seguridad	Tecnología	Detalles
00:11 05/09/2024	Tratado	HEUR:Backdoor.Java...	VIRTUALMAC-6A34 Sin propietario	Predeterminado	EPP	Examinar
00:02 05/09/2024	Tratado	UDS:Hoax.OSX.Defm...	VIRTUALMAC-6A34 Sin propietario	Predeterminado	EPP	Examinar

Kaspe

Equi

Panel de

Usuario

Disposit

Adminis

Perfiles

Diagnós

Adminis

Data Di

✓ Endpoi

Cifrado

Ayuda

Soporte

Aviso le

Contrat

Gráfico de la cadena de desarrollo de la amenaza

[¿Cómo leer un gráfico de cadena de desarrollo de amenazas?](#)

Tratado: Se eliminó el objeto

Detectado el: 05/09/2024

Propietario del dispositivo: Sin propietario

Nombre del dispositivo: [VIRTUALMAC-6A34](#)

Perfil de seguridad: [Predeterminado](#)

...

Detect

Objeto que se trató

Objeto que no se trató

Objetos sin detecciones

Fecha de creación

Parámetros

23/03/2022 05:10

Detect

Agregar a Análisis de IOC

Impedir ejecución

Enviar a Cuarentena

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

Kaspe

Equ

Panel de

Usuarios

Dispositivos

Administración

Cuarentena

Paquetes

Configuración

Ayuda

Soporte

Aviso legal

Contratos

© 2024 AC

charlie

Admin

Gráfico de la cadena de desarrollo de la amenaza

¿Cómo leer un gráfico de cadena de desarrollo de amenazas?

Tratada

Detectado el: 05/09/2024

Propietario del dispositivo: Sin propietario

Nombre del dispositivo: [VIRTUALMAC-6A34](#)

Perfil de seguridad: [Predeterminado](#)

...

Detect

Objeto que se trató

Objeto que no se trató

Objetos sin detecciones

Fecha de creación

Parámetros

23/03/2022 05:10

Detect

Agregar a Análisis de IOC

Impedir ejecución

Enviar a Cuarentena

Kaspe

Equ

Panel de

Usuarios

Dispositivos

Administración

Cuarentena

Paquetes

Configuración

Ayuda

Soporte

Aviso legal

Contratos

© 2024 AC

charlie

Admin

Gráfico de la cadena de desarrollo de la amenaza

¿Cómo leer un gráfico de cadena de desarrollo de amenazas?

Tratada

Detectado el: 05/09/2024

Propietario del dispositivo: Sin propietario

Nombre del dispositivo: [VIRTUALMAC-6A34](#)

Perfil de seguridad: [Predeterminado](#)

...

Detect

Objeto que se trató

Objeto que no se trató

Objetos sin detecciones

Fecha de creación

Parámetros

23/03/2022 05:10

Detect

Agregar a Análisis de IOC

Impedir ejecución

Enviar a Cuarentena

Análisis de IoC

Nombre de la amenaza

[Threat Graph] HEUR:Trojan-PSW.OSX.Amos.w

Indicadores de vulneración (IoC)

Criterios de detección:

Coincidencia con CUALQUIERA de los siguientes elementos

Nuevos IoC (1)

MD5

112736f18669c0b52a9591aa19fbec8a

IoC previamente agregados (2)

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

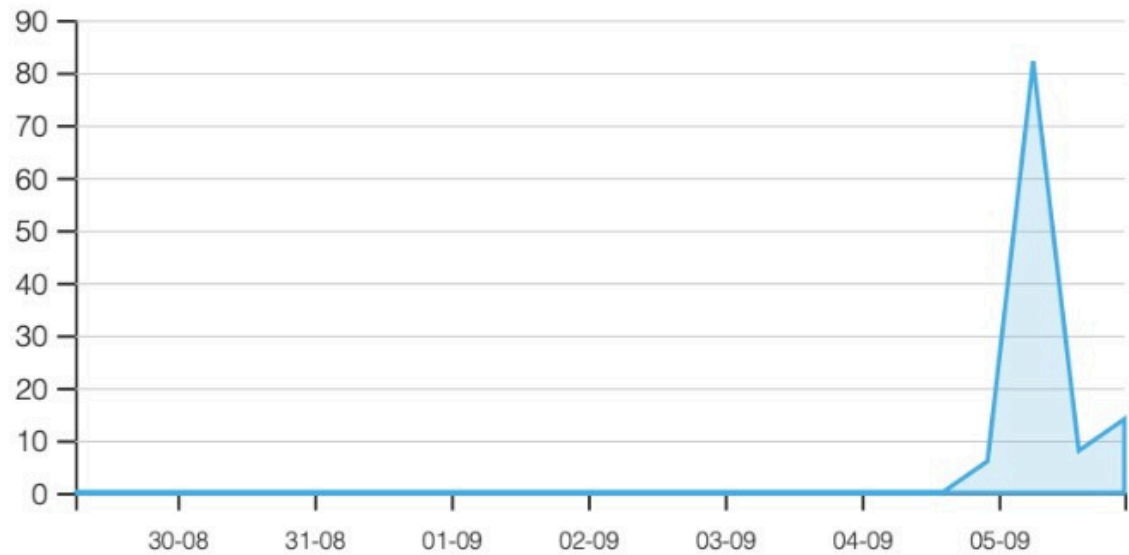
[Ir a la lista de alertas](#)

##	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



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