
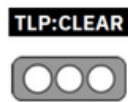


Nro. Alerta:	AL-2023-055	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR ALERTAS DE SEGURIDAD	 V 1.1
TLP:			
Fecha:	05-dic-2023	El malware Atomic Stealer ataca macOS a través de actualizaciones falsas del navegador.	Pág.: 1 of 6

I. DATOS GENERALES:

Clase de alerta:	Incidente
Tipo de incidente:	Malware / MacOS
Nivel de riesgo:	Alto


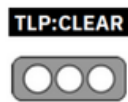
II. ALERTA

La campaña de actualización falsa del navegador 'ClearFake' se ha expandido a macOS, apuntando a computadoras Apple con malware Atomic Stealer (AMOS).

La campaña ClearFake comenzó en julio de este año para dirigirse a los usuarios de Windows con mensajes falsos de actualización de Chrome que aparecen en sitios pirateados mediante inyecciones de JavaScript.



Figura 1.- Ataque AtomicStealer – figura referencial

Nro. Alerta:	AL-2023-055	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR ALERTAS DE SEGURIDAD	 V 1.1
TLP:			
Fecha:	05-dic-2023	El malware Atomic Stealer ataca macOS a través de actualizaciones falsas del navegador.	Pág.: 2 of 6

III. INTRODUCCIÓN

Alertan de una campaña que usa actualizaciones falsas de Chrome y Safari para distribuir Atomic Stealer en MacOS. Investigadores de ciberseguridad han alertado de una campaña maliciosa que distribuye Atomic Stealer, también conocido como AMOS, a través de falsas actualizaciones de los navegadores Chrome y Safari para ordenadores con MacOS.

El ladrón de información de macOS, conocido como **Atomic**, ahora se entrega al objetivo a través de una cadena de actualización de navegador web falsa rastreada como ClearFake.

Atomic Stealer (también conocido como AMOS), documentado por primera vez en abril de 2023, es una familia de malware ladrón comercial que se vende mediante suscripción por 1.000 dólares al mes. Viene con capacidades para desviar datos de navegadores web y billeteras de criptomonedas.

Luego, en septiembre de 2023, se detalló una campaña de Atomic Stealer que aprovecha los anuncios maliciosos de Google, engañando a los usuarios de macOS que buscan una plataforma de gráficos financieros conocida como TradingView para que descarguen el malware.



En octubre de 2023, se descubrió un desarrollo significativo para la operación maliciosa, que aprovechó los contratos de Binance Smart Chain para ocultar sus scripts maliciosos que respaldan la cadena de infección en la blockchain.

A través de esta técnica, denominada "EtherHiding", los operadores distribuyeron cargas útiles dirigidas a Windows, incluido malware de robo de información como RedLine, Amadey y Lumma.

IV. VECTOR DE ATAQUE:

ClearFake, por otro lado, es una incipiente operación de distribución de malware que emplea sitios de WordPress comprometidos para enviar avisos fraudulentos de actualización del navegador web con la esperanza de implementar ladrones y otro malware.

Es la última incorporación a un grupo más grande de actores de amenazas como TA569 (también conocido como SocGhosh), RogueRticate (FakeSG), ZPHP (SmartApeSG) y EtherHiding, que se sabe que utilizan temas relacionados con actualizaciones falsas del navegador para este propósito.

Nro. Alerta:	AL-2023-055	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR ALERTAS DE SEGURIDAD	 V 1.1
TLP:			
Fecha:	05-dic-2023	El malware Atomic Stealer ataca macOS a través de actualizaciones falsas del navegador.	Pág.: 3 of 6

A partir de noviembre de 2023, la campaña ClearFake se amplió para apuntar a sistemas macOS con una cadena de infección casi idéntica, aprovechando sitios web pirateados para entregar Atomic Stealer en forma de archivo DMG.

Este desarrollo es una señal de que el malware continúa dependiendo de archivos de instalación falsos o envenenados para software legítimo a través de anuncios maliciosos, redireccionamientos de motores de búsqueda a sitios web maliciosos, descargas no autorizadas, phishing y envenenamiento de SEO para su propagación.

Los operadores del malware también han estado promocionando una nueva característica que, según afirman, puede usarse para recopilar cookies de cuentas de Google de computadoras comprometidas que no caducan ni serán revocadas incluso si el propietario cambia la contraseña.

V. IMPACTO:

Se ha observado una nueva campaña de publicidad maliciosa que distribuye una versión actualizada de un malware stealer de macOS llamado Atomic Stealer (o AMOS), lo que indica que su autor lo mantiene activamente.


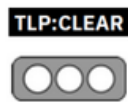
Un malware Golang disponible por \$ 1,000 por mes, Atomic Stealer salió a la luz por primera vez en abril de 2023. Poco después, se detectaron nuevas variantes con un conjunto ampliado de funciones de recopilación de información en la naturaleza, dirigidas a usuarios de criptomonedas.

La publicidad maliciosa a través de “Google Ads” se ha observado como el principal vector de distribución en el que los usuarios que buscan software popular, legítimo o agrietado, en los motores de búsqueda muestran anuncios falsos que dirigen a sitios web que alojan instaladores deshonestos.

La última campaña implica el uso de un sitio web fraudulento para TradingView, que destaca tres botones para descargar el software para los sistemas operativos Windows, macOS y Linux.

“Tanto los botones de Windows como los de Linux apuntan a un instalador MSIX alojado en Discord que deposita NetSupport RAT”.

La carga útil de macOS (“TradingView.dmg”) es una nueva versión de Atomic Stealer lanzada a finales de junio, que se incluye en una aplicación firmada ad-hoc que, una vez ejecutada, solicita a los usuarios que ingresen su contraseña en un mensaje falso y recopilen archivos, así como datos almacenados en iCloud Keychain y navegadores web.

Nro. Alerta:	AL-2023-055	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR ALERTAS DE SEGURIDAD	 V 1.1
TLP:			
Fecha:	05-dic-2023	El malware Atomic Stealer ataca macOS a través de actualizaciones falsas del navegador.	Pág.: 4 of 6

VI. INDICADORES DE COMPROMISO

“Atomic stealer también se dirige a los navegadores Chrome y Firefox y tiene una extensa lista codificada de extensiones de navegador relacionadas con criptografía para atacar”, señaló SentinelOne anteriormente en mayo de 2023. Algunas variantes también se han dirigido a las carteras Coinomi.

El objetivo final del atacante es eludir las protecciones de Gatekeeper en macOS y filtrar la información robada a un servidor bajo su control.

El desarrollo se produce cuando macOS se está convirtiendo cada vez más en un objetivo viable de ataques de malware, con una serie de ladrones de información específicos de macOS que aparecen a la venta en foros de crimeware en los últimos meses para aprovechar la amplia disponibilidad de los sistemas Apple en las organizaciones.


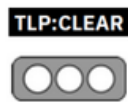
“Si bien el malware para Mac realmente existe, tiende a ser menos detectado que su contraparte de Windows”, El desarrollador o vendedor de AMOS realmente hizo un punto de venta que su kit de herramientas es capaz de evadir la detección”.

Atomic Stealer no es el único malware propagado a través de campañas de publicidad maliciosa y envenenamiento de optimización de motores de búsqueda (SEO), ya que ha surgido evidencia de que DarkGate (también conocido como MehCrypter) se aferra al mismo mecanismo de entrega.

Desde entonces, se han empleado nuevas versiones de DarkGate en ataques montados por actores de amenazas que emplean tácticas similares a las de Scattered Spider.

También se ha observado que DarkGate se propaga a través de campañas de ingeniería social utilizando mensajes de chat con temas de recursos humanos enviados a través de Microsoft Teams, según Truesec, amplificando su amenaza potencial e indicando que el cargador está siendo utilizado por múltiples actores de amenazas a través de varios canales de infección, expandiéndose a macOS. El 17 de noviembre de 2023, se informó que ClearFake había comenzado a enviar cargas útiles de DMG a los usuarios de macOS que visitaban sitios web comprometidos.

Estos ataques emplean un cebo de actualización de Safari junto con la superposición estándar de Chrome, la carga útil lanzada en estos casos es Atomic, un malware de robo de información vendido a ciberdelincuentes a través de canales de Telegram por 1.000 dólares al mes.

Nro. Alerta:	AL-2023-055	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR ALERTAS DE SEGURIDAD	 V 1.1
TLP:			
Fecha:	05-dic-2023	El malware Atomic Stealer ataca macOS a través de actualizaciones falsas del navegador.	Pág.: 5 of 6

La contraseña del llavero es el administrador de contraseñas integrado de macOS que contiene contraseñas WiFi, inicios de sesión de sitios web, datos de tarjetas de crédito y otra información cifrada, por lo que su compromiso puede resultar en una violación significativa para la víctima.

El examen de Malwarebyte de las cadenas de la carga útil revela una serie de comandos para extraer datos confidenciales como contraseñas y apuntar a archivos de documentos, imágenes, archivos de billetera criptográfica y claves.

```
find-generic-password -ga 'Chrome' | awk '{print $2}' SecKeychainSearchCopyNext:
/Chromium/Chrome /Chromium/Chrome/Local State FileGrabber tell application "Finder"
set desktopFolder to path to desktop folder
set documentsFolder to path to documents folder
set srcFiles to every file of desktopFolder whose name extension is in {"txt", "rtf", "doc", "docx", "xls", "key", "wallet", "jpg", "png", "web3", "dat"}
set docsFiles to every file of documentsFolder whose name extension is in {"txt", "rtf", "doc", "docx", "xls", "key", "wallet", "jpg", "png", "web3", "dat"}
```


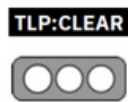
Figura 2.- Ataque AtomicStealer – Referencial

VII. RECOMENDACIONES:

- La campaña ClearFake ahora dirigida a Mac es un recordatorio para que los usuarios de Apple fortalezcan su seguridad y tengan cuidado con las descargas, especialmente con las indicaciones para actualizar su navegador cuando visitan sitios web.
- Incluso después de varios meses del descubrimiento y los informes sobre Atomic, aproximadamente el 50% de los motores antivirus de VirusTotal no detectan la carga útil.
- Además, todas las actualizaciones del navegador Safari se distribuirán a través de la Actualización de software de macOS o, para otros navegadores, dentro del propio navegador.
- Por lo tanto, si ve algún mensaje para descargar actualizaciones del navegador en sitios web, debe ignorarlo.

VIII. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta; se proporciona con fines informativos.

Nro. Alerta:	AL-2023-055	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR ALERTAS DE SEGURIDAD	 V 1.1
TLP:			
Fecha:	05-dic-2023	El malware Atomic Stealer ataca macOS a través de actualizaciones falsas del navegador.	Pág.: 6 of 6

- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

IX. REFERENCIAS:

- https://www.bleepingcomputer.com/news/security/atomic-stealer-malware-strikes-macos-via-fake-browser-updates/#google_vignette
- <https://www.europapress.es/portaltic/ciberseguridad/noticia-alertan-campana-usa-actualizaciones-falsas-chrome-safari-distribuir-atomic-stealer-macos-20231122172433.html>
- <https://www.ciberseguridadlatam.com/2023/11/22/la-campana-clearfake-se-expande-para-apuntar-a-sistemas-mac-con-atomic-stealer/>
- <https://www.bleepingcomputer.com/news/security/hackers-backdoor-russian-state-industrial-orgs-for-data-theft/>
- <https://www.bleepingcomputer.com/news/security/malware-dev-says-they-can-revive-expired-google-auth-cookies/>
- <https://devel.group/blog/advertencia-a-los-usuarios-mac-campana-de-publicidad-maliciosa-propaga-el-malware-atomic-stealer-macos/>