Nro. Alerta:	AL-2026-002	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert V 1.1
TLP:	TLP:CLEAR		
Fecha:	16-ene-2026	Malware Astaroth	Pág.: **1** of **12**

I. DATOS GENERALES:

Clase de alerta: Campaña de malware
Tipo de Incidente: Phishing - Robo de credenciales, secuestro de sesiones y persistencia
Nivel de riesgo: Alta

II. ALERTA

Figura 1.- Ataque a la cadena de Suministro Drift - Figura referencial

A diferencia del malware convencional que busca la fuerza bruta, Astaroth domina el arte del sigilo. Utilizando scripts maliciosos que se ejecutan directamente en la memoria y aprovechando procesos nativos de Windows para sus actividades delictivas, este troyano ha logrado vaciar cuentas bancarias y comprometer identidades digitales en todo el mundo. Con el reciente aumento de sus vectores de ataque, incluyendo la automatización de envíos por WhatsApp Web, entender su funcionamiento ya no es solo una tarea de especialistas, sino una necesidad de defensa crítica. Esta amenaza utiliza la “invisibilidad” para vulnerar incluso los sistemas más actualizados."

III. INTRODUCCIÓN

En el vasto ecosistema de las Ciber amenazas, pocas aplicaciones de software malicioso han demostrado una resiliencia y capacidad de adaptación tan notables como el malware Astaroth, también conocido como Guildma. Surgió inicialmente como

un troyano bancario convencional, Astaroth ha mutado hasta convertirse en una de las amenazas "fileless" (sin archivos) más sofisticadas del panorama actual. Su historia es una crónica de innovación constante, pasando de simples campañas de correo masivo a complejas operaciones que hoy, en enero de 2026, aprovechan la confianza humana a través de plataformas de mensajería instantánea como WhatsApp.

Astaroth fue detectado por primera vez alrededor de 2017, con un foco agresivo y casi exclusivo en Brasil. Su arquitectura inicial, escrita principalmente en el lenguaje de programación Delphi, ya mostraba señales de lo que vendría, un diseño modular capaz de descargar componentes adicionales según las necesidades del atacante.

En sus primeros años, su éxito radicó en el Phishing geolocalizado. Los atacantes diseñaban correos electrónicos que suplantaban a Instituciones Gubernamentales o servicios de mensajería locales, adjuntando archivos .lnk o comprimidos. El objetivo era simple pero letal, robar credenciales bancarias y datos de identidad de usuarios en una región donde la higiene digital aún estaba en desarrollo.

Tradicionalmente, Astaroth se ha difundido a través de campañas de Phishing masivo mediante correos electrónicos con facturas falsas o notificaciones gubernamentales. Sin embargo, en enero de 2026, se ha detectado una nueva y peligrosa variante, ahora utiliza mensajes de WhatsApp con archivos comprimidos (.zip) maliciosos. Una vez que infecta un equipo, el malware accede a la lista de contactos de WhatsApp Web de la víctima y se reenvía automáticamente, explotando la confianza entre conocidos para propagarse más rápido; monitorea cuando el usuario entra a sitios de bancos o servicios financieros para capturar nombres de usuario y contraseñas; es capaz de cerrar procesos de Google Chrome o Firefox para forzar al usuario a usar otros medios donde pueda registrar las pulsaciones de teclas (keylogging); utiliza herramientas legítimas del sistema operativo (como WMIC o BITSAdmin) para descargar sus componentes dañinos, una técnica llamada *Living-off-the-Land* (LotL). Si detecta ciertos antivirus, puede intentar inyectar código dentro de sus procesos para pasar desapercibido

La verdadera peligrosidad de Astaroth reside en su adopción de técnicas *Living-off-the-Land* (LotL). Para evadir los antivirus tradicionales, el malware no intenta ejecutar un código malicioso desconocido; en su lugar, utiliza herramientas legítimas del propio sistema operativo Windows para realizar sus tareas:

- **BITSAdmin y WMIC:** Utiliza estos componentes para descargar sus cargas útiles directamente en la memoria.

- **Esteganografía:** Ha ocultado sus configuraciones y módulos dentro de archivos de imagen aparentemente inofensivos (formatos .jpg o .gif) alojados en plataformas legítimas como GitHub o YouTube.

- **Evasión de Antivirus:** A diferencia de otros malwares que se detienen al detectar protección, las versiones más recientes de Astaroth intentan inyectar código malicioso dentro de los propios procesos de los antivirus (como Avast) para operar bajo su "paraguas" de confianza.

Astaroth representa la culminación del malware moderno, sigiloso, modular y profundamente integrado en los flujos de comunicación cotidiana. Su transición de los correos basura a la mensajería instantánea automatizada subraya que el eslabón más débil sigue siendo la confianza del usuario. La defensa contra esta amenaza ya no depende solo de un software antivirus, sino de una vigilancia constante sobre el comportamiento anómalo del sistema y una desconfianza saludable hacia los archivos adjuntos, sin importar quién los envíe.

IV. VECTOR DE ATAQUE

A inicios de 2026, Astaroth ha dado un salto estratégico con la campaña denominada "Boto Cor-de-Rosa". Tras años de depender del correo electrónico, los operadores han integrado un módulo tipo gusano de WhatsApp.

- **Propagación por confianza:** Una vez que un equipo es infectado, el malware utiliza scripts de Python y herramientas de automatización como Selenium para secuestrar la sesión de WhatsApp Web del usuario.

- **Automatización de mensajes:** El sistema envía de forma automática archivos .zip maliciosos a toda la lista de contactos del usuario. Al provenir de un contacto conocido y utilizar saludos dinámicos (buenos días, buenas tardes), la tasa de clics es alarmantemente alta.

- **Archivos zip/lnk:** Envía automáticamente a toda tu lista de contactos un archivo comprimido que contiene scripts (como VBS o HTA) disfrazados de documentos legítimos. Utiliza archivos .lnk (accesos directos) o archivos de instalación de Microsoft (.msi) que parecen archivos pdf o comprobantes de transferencia.

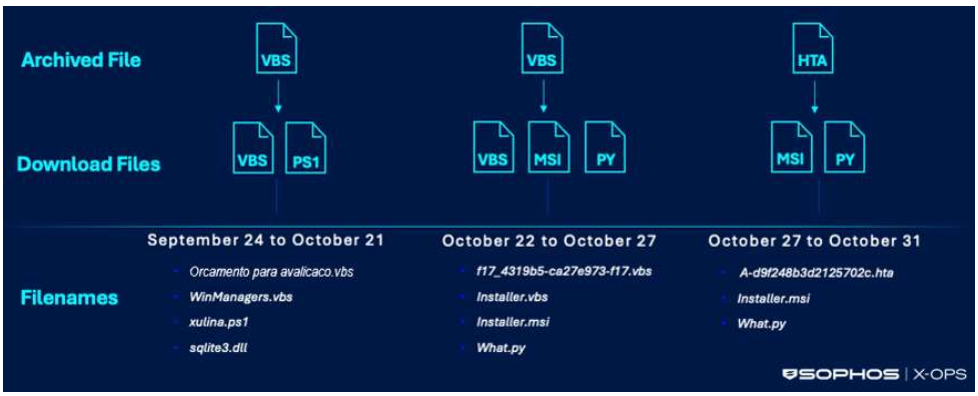

Figura: formatos de archivo utilizados en la campaña STAC3150 entre el 24 de septiembre y el 31 de octubre de 2025
Fuente: https://www.sophos.com/es-es/blog/whatsapp-compromise-leads-to-astaroth-deployment

- **Suplantación de identidad:** Correos que fingen ser de autoridades fiscales, bancos o proveedores con facturas vencidas.

- **Resiliencia en la Nube:** Si los servidores de control son dados de baja, el malware recurre a repositorios en la nube como Google Cloud Run para obtener nuevas configuraciones, garantizando que la infección no muera. Utiliza estos servicios para hospedar sus archivos de configuración y módulos maliciosos. Como el tráfico hacia Google o GitHub suele considerarse seguro, los sistemas de seguridad perimetral no suelen bloquearlo.

- **YouTube y redes sociales:** En campañas anteriores, se ha visto el uso de descripciones de videos o perfiles para esconder direcciones IP de sus servidores de comando y control (C2).

- **WMIC y BITSAdmin:** Utiliza herramientas propias de Windows para descargar y ejecutar el código directamente en la memoria RAM, sin escribir archivos sospechosos en el disco duro.

- **Inyección de código:** El malware se "esconde" dentro de procesos legítimos (como el navegador o procesos del sistema) para realizar el robo de datos sin levantar alertas.

V. IMPACTO

El impacto de Astaroth va más allá de la pérdida económica inmediata. Sus efectos se dividen en tres pilares críticos:

- **Vaciado de Cuentas:** Su función principal es el keylogging y la captura de sesiones. Monitorea activamente cuando un usuario accede a portales financieros para interceptar contraseñas y códigos de seguridad.

- **Secuestro de Identidad:** Roba tokens de sesión y cookies de navegadores, permitiendo a los atacantes entrar en correos corporativos y redes sociales sin necesidad de la contraseña original.

- **Impacto Reputacional:** Para las empresas, una infección por Astaroth significa que la cuenta de sus empleados puede ser utilizada para atacar a clientes y proveedores vía WhatsApp o correo, destruyendo la confianza comercial en cuestión de horas.

Los países más afectados incluyen Brasil, Paraguay, Argentina, Colombia, Panamá y Venezuela, siendo Brasil el que presenta el mayor número de instituciones afectadas. Esto pone de manifiesto un enfoque predominante en instituciones financieras de Latinoamérica. Sin embargo, el alcance del malware no se limita geográficamente a Latinoamérica. Países europeos como Italia, España y Portugal también han sido blanco de ataques, lo que indica un alcance operativo más amplio. Cabe destacar que también se identificó una sola referencia a una entidad japonesa, lo que subraya la capacidad del malware para atacar diversas regiones geográficas y ecosistemas financieros.

VI. INDICADORES DE COMPROMISO

Astaroth utiliza dominios de baja reputación y servicios en la nube para su comando y control (C2).

- **Dominios sospechosos detectados en 2025-2026:**

Indicador	Tipo	Contexto
manoelimoveiscaioba[.]com	Nombre de dominio	C2 server used in WhatsApp STAC3150 campaign
varegjopeaks[.]com	Nombre de dominio	Servidor C2 utilizado en la campaña STAC3150 de WhatsApp

Indicador	Tipo	Contexto
docsmoonstudioclayworks[.]online	Nombre de dominio	Servidor C2 utilizado en la campaña STAC3150 de WhatsApp
shopeeship[.]com	Nombre de dominio	Servidor C2 utilizado en la campaña STAC3150 de WhatsApp
miportuarios[.]com	Nombre de dominio	Servidor C2 utilizado en la campaña STAC3150 de WhatsApp
borizerefeicoes[.]com	Nombre de dominio	Servidor C2 utilizado en la campaña STAC3150 de WhatsApp
clhttradinglimited[.]com	Nombre de dominio	Servidor C2 utilizado en la campaña STAC3150 de WhatsApp
lefthandsuperstructures[.]com	Nombre de dominio	Servidor C2 utilizado en la campaña STAC3150 de WhatsApp
puxaofolesanfoneiro[.]quest		subdominios aleatorios de 11 caracteres

- **Uso de Proxies/Túneles:**
  - Conexiones hacia ngrok (Por ejemplo. 1.tcp.sa.ngrok[.]io).
- **Infraestructura en la nube:**
  - Tráfico inusual hacia raw.githubusercontent.com o Cloud Run para descargar imágenes que esconden código malicioso mediante esteganografía.
- **Patrones de balizamiento (Beaconing):**
  - Conexiones HTTP POST cada 2 horas exactas hacia servidores externos.
- **Rutas de archivos comunes:**
  - C:\Users\Public\Libraries\tempsys\ (donde suele descargar módulos iniciales).
  - Uso de ADS (Alternate Data Streams): Busca datos ocultos en archivos legítimos como desktop.ini (ej. desktop.ini:masihaddajjalb.jpg).
- **Procesos sospechosos:**
  - svchost.exe o userinit.exe con un uso de memoria inusual (Astaroth se inyecta en ellos).

- Ejecución de mshta.exe, bitsadmin.exe, wmic.exe o certutil.exe con argumentos que apuntan a URLs externas o archivos en la carpeta de usuario.

- **Extensiones de archivo:**
  - Presencia de archivos .LNK, .VBS o .HTA dentro de archivos .ZIP recibidos por correo o WhatsApp.

Extensión	Archivo
ZIP	1368b8d0a6e4c511e17080032b183133e920bc2f
	e92fcd723d12b6e9533e8cbb9bab374037184fe1
	efffe10b78e1eab853dd6e91bbec52b24e331af2
LNK	4c691442ae0af56d8559475f73a3482a3839462
	a835e5d99b11339056bc36cbb41d950525a5aaa
	7957de4e33259045d7da94905203ad7f1432141c
URL	hxxps://tiasr[.]olafdisney.sbs/?5/
	hxxps://screranvel[.]safezipdirect.associates/?2/
	hxxps://planbenpunwel2[.]smartconsultoria.quest/?2/

- **Run Keys:**
  - Entradas sospechosas en HKCU\Software\Microsoft\Windows\CurrentVersion\Run que apuntan a scripts en carpetas locales.

- **Carpeta de Inicio:**
  - Creación de archivos de acceso directo (.lnk) en %APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup.

- **Evasión:**
  - El malware intenta detectar si está en una máquina virtual. Si ves que un equipo se apaga repentinamente después de abrir un archivo dudoso, podría ser una técnica de evasión de Astaroth.

- **Desactivación de Seguridad:**
  - Intentos de deshabilitar Windows Defender o inyectar código en procesos de antivirus como Avast (aswRunDll.exe).

- **Actividad en WhatsApp Web:**
  - Envío masivo de mensajes con archivos adjuntos desde la sesión del usuario sin su intervención.

- **Actividades asociadas:**

Nombre	Descripción
VBS/DwnLdr-ADJT	Detección del archivo VBS inicial
VBS/DwnLdr-ADJW	Detección del archivo VBS inicial
VBS/DwnLdr-ADJS	Detección del archivo VBS de segunda fase
Troj/Mdrop-KEP	Detección del archivo MSI de segunda fase
Troj/Mdrop-KES	Detección del archivo MSI de segunda fase
Troj/AutoIt-DJB	Detección de la carga útil de AutoIt
Troj/HTADrp-CE	Detección del script HTA

- **Hashes**

SHA-1	Descripción	Nombre detectado por ESET
45c58bc40768dce6a6c611e08fd34c62441aa776	Main module loader 1	Win32/Spy.Guildma.BM
861f20b0dcc55f94b4c43e4a7e77f042c21506cf	Main module injector	Win32/Spy.Guildma.BJ

SHA-1	Descripción	Nombre detectado por ESET
37fd19b1ab1dcc25e07bc96d4c02d81cf4edb8a1	Main module loader 2	Win32/Spy.Guildma.Q
a7b10b8de2b0ef898cff31fa2d9d5cbaae2e9d0d	Main module	Win32/Spy.Guildma.BS
4f65736a9d6b94b376c58b3cdcb49bbd295cd8cc	Contacts stealer and form grabber	Win32/Spy.Guildma.D
6c9304c5862d4e0de1c86d7ae3764f5e8358daff	RAT module (DLL)	Win32/Spy.Guildma.BR
89fbffe456de850f7abf4f97d3b9da4bad6afb57	RAT module (EXE)	Win32/Spy.Guildma.BR
af0d495ecc3622b14a40ddcd8005873c5ddc3a2d	MailPassView	Win32/PSWTool.MailPassView.E
92bcf54079cbba04f584eac4486473c3abdd88cd	WebBrowserPassView	WebBrowserPassView.E
a2048f435f076988bf094274192a196216d75a5f	JScript dropper module	Win32/Spy.Guildma.BP

VII. RECOMENDACIONES:

- Desconfíar de los archivos adjuntos en WhatsApp y mensajería; dado el nuevo vector de propagación de Astaroth, no descargar ni ejecutar archivos .zip, .lnk o .html enviados por WhatsApp, incluso si vienen de un contacto conocido. Si recibe uno inesperadamente, confirmar por otro medio (llamada o audio) que la persona realmente lo envió.

- Implementar una solución EDR (Endpoint Detection and Response); a diferencia de un antivirus tradicional que busca archivos maliciosos, un EDR monitorea el comportamiento. Astaroth usa procesos legítimos (wmic.exe,

bitsadmin.exe); un EDR puede detectar si estos procesos están actuando de forma inusual (como descargar código desde un repositorio de GitHub).

- Desactivar o restringir el uso de Scripts (VBScript y PowerShell); Astaroth depende de scripts para su ejecución inicial. Desasociar la extensión .vbs de Windows Script Host para que, si se hace clic en un archivo malicioso, no se ejecute automáticamente. Usar el modo de "Lenguaje restringido" en PowerShell para usuarios que no necesiten funciones avanzadas.

- Usar autenticación de dos factores (2FA) en todas las cuentas bancarias y correos. Astaroth es un "infostealer" (ladrón de credenciales). Si logra capturar una contraseña bancaria o de correo, el 2FA (preferiblemente mediante apps de autenticación o llaves físicas, no SMS) servirá como la última línea de defensa para evitar que el atacante acceda a las cuentas de los usuarios.

- Mantener el sistema operativo actualizado, ya que Astaroth suele aprovechar vulnerabilidades de componentes antiguos de Windows.

- Mantener Microsoft Office actualizado (Parches críticos); asegurar que toda la suite de Office esté actualizada, ya que los documentos maliciosos suelen ser la puerta de entrada principal.

- Bloquear la ejecución de herramientas administrativas para usuarios comunes; si los empleados no son administradores de sistemas, no deberían poder ejecutar herramientas como cmd.exe, powershell.exe, wmic.exe o certutil.exe. Se puede usar AppLocker o Windows Defender Application Control (WDAC) para crear una lista blanca de aplicaciones permitidas.

- Monitorear el uso de Servicios Cloud en la Red; configurar los firewalls o sistemas de monitoreo para alertar sobre conexiones inusuales a servicios como GitHub, Google Cloud Run o Discord desde estaciones de trabajo

comunes, especialmente si el tráfico ocurre de forma automatizada y persistente.

- Utilizar el "Principio de Menor Privilegio"; no trabaje en una computadora diaria con una cuenta de Administrador. Si una infección de Astaroth ocurre en una cuenta de usuario estándar, el malware tendrá muchas más dificultades para inyectarse en procesos críticos del sistema o desactivar el antivirus.

- Cerrar sesiones de WhatsApp Web al terminar, para evitar que el módulo de "gusano" de Astaroth utilice la sesión activa para propagarse, adquirir el hábito de cerrar la sesión de WhatsApp Web o la aplicación de escritorio cuando no se la esté utilizando.

- La técnica más fuerte de Astaroth es el engaño, por lo que se debe realizar campañas de concientización donde los usuarios aprendan a identificar:
  - Remitentes sospechosos.
  - Urgencia falsa en el lenguaje.
  - Extensiones de archivo dobles (ej. factura.pdf.exe).

VIII. DESCARGO DE RESPONSABILIDAD

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

- 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:

- **SOPHOS (2026).** *Ataque por WhatsApp conduce al despliegue de Astaroth*. https://www.sophos.com/es-es/blog/whatsapp-compromise-leads-to-astaroth-deployment

- **FORCEPOINT (2026).** *Ataques del troyano Astaroth en Brasil y México a través de Secureserver.net*. https://www.forcepoint.com/es/blog/x-labs/astaroth-trojan-attacks-brazil-mexico-secureserver-net

- **SEGU.INFO (2026).** *Astaroth: campaña de malware basado en WhatsApp Web* https://blog.segu-info.com.ar/2026/01/astaroth-campana-de-malware-basado-en.html

- **MICROSOFT (2026).** *Los últimos ataques de Astaroth que viven de la tierra son aún más invisibles, pero no menos observables.* https://www.microsoft.com/en-us/security/blog/2020/03/23/latest-astaroth-living-off-the-land-attacks-are-even-more-invisible-but-not-less-observable/

- **DEVEL (2026).** *El troyano bancario Astaroth usa la infraestructura de GitHub para su Command & Control* https://www.microsoft.com/en-us/security/blog/2020/03/23/latest-astaroth-living-off-the-land-attacks-are-even-more-invisible-but-not-less-observable/

- **WELIVESECURITY (2026).** *Guildma: un troyano bancario muy activo en Brasil* https://www.welivesecurity.com/la-es/2020/03/05/guildma-un-troyano-bancario-muy-activo-en-brasil/

- **COCIBER (2026).** *Boletín instante 12-ene-26 Ciberinteligencia 2025-COCIBER-CINT-012.* 12. BOLETIN CAMPAÑA ACTIVA DE MALWARE ASTAROTH -DEL 12-ENE-026.pdf