Nro. Alerta:	AL-2024-025	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR ALERTAS DE SEGURIDAD	ecucert V 1.1
TLP:	TLP:CLEAR		
Fecha:	30-oct-2024	Malware AsyncRAT	Pág.: **1** of **5**

I. DATOS GENERALES:

Clase de alerta: Incidente

Tipo de incidente: Malware

Nivel de riesgo: Alto

II. ALERTA

AsyncRAT es un *malware* de tipo *troyano* de acceso remoto (RAT) que se enfoca en infectar dispositivos Windows para monitorizarlos y controlarlos remotamente a través de conexiones seguras y encriptadas. Además, proporciona una puerta trasera a los atacantes que permite incluir el dispositivo como parte de una *botnet* para realizar otras actividades maliciosas.

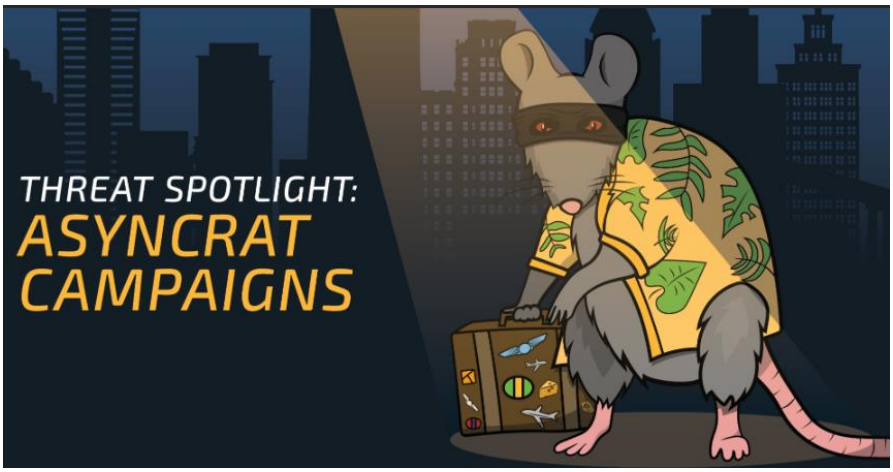

Figura 1.- *Ilustración asociada a AsyncRAT* ***Fuente: blog.talosintelligence.com/asyncrat-3losh-***

III. INTRODUCCIÓN

AsyncRAT es un troyano de acceso remoto (RAT) lanzado en 2019, principalmente como ladrón de credenciales y cargador de otro malware, incluido el ransomware. AsyncRAT tiene capacidades de botnet y una interfaz de comando y control (C2) que permite a los operadores controlar los hosts infectados de forma remota. A pesar de

un descargo de responsabilidad legal en su página oficial de GitHub y la autopromoción como una herramienta legítima de administración remota de código abierto, AsyncRAT es utilizado casi exclusivamente por actores de amenazas cibercriminales.

El uso de AsyncRAT ha crecido constantemente y ha experimentado fuertes aumentos de popularidad desde su lanzamiento. Ahora se considera una de las principales amenazas. AsyncRAT está afiliado a otras cepas de malware; Surgió de la cepa de malware QuasaRAT y se utilizó como punto de partida para RevengeRAT y BoratRAT.

AsyncRAT ha sido utilizado por todo tipo de actores de amenazas, desde estados-nación y bandas de ransomware de primer nivel hasta pequeños grupos emergentes de delitos cibernéticos en países en desarrollo, en campañas contra un conjunto igualmente diverso de víctimas a nivel mundial. Campañas notables que aprovechan AsyncRAT se han dirigido a los sectores aeroespacial, hotelero, de TI, de servicios empresariales y de transporte y a organizaciones gubernamentales en todas las regiones.

IV. VECTOR DE ATAQUE:

Este *malware* infecta a los dispositivos a través de la descarga de adjuntos en correos de *phishing* y de archivos maliciosos de Internet, a través de la explotación de vulnerabilidades conocidas no parcheadas y a través de conexiones con dispositivos extraíbles (USB).

V. INDICADORES DE COMPROMISO

Los siguientes IoC han sido observados para ser asociados a esta campaña de malware:

- 4567abc4645a8f9414c6d642763d47a2678bf00fefe9e02677664b1c1b35c226
  64836303a8eb58b7c5660211e085e3e42b2f4a068aeee88ede30eaa1b9cc4898
  c174daa66473073d55fca74107642b43938c832b6c57a2e35c5b6998b89becc8
  ed22a3a0314aa108d3e2a5f89fc90eb4d32a07a83e4a16a0e778ec3dae8e3406

- 0e1d80e1868067b61194539818ac5cd517fb17ab6644492b8d9926f7c400efbb
  15ebbc7c74e36fdfb677c56fb94db874a29ed995548c226fc38bd2977f4462c6

1a072171f489d1ae560368b82eeaf6dc4797fcfc7c0a8e53a635311c33fd061d
1cecb3e057afa5ad2150c74e1db583d5fda9780cba9d0e3bbaf2c6a4a345173a
26716b84938ec82bd3847d6c45fa2b2b502d1475dc31e735fd443b7a7c70dd442b9
229dd6d60c44b28afea7fddd30ec889583184ff51cba03b156d8a96a41c92336d41e
4e6380dccd03791f4b25c840de9268f750b7e9db1e842f5cea60342d5

- 4fb011aa84514cd8cf5896134383b327abe213d28f2bb4bff614e8beb03540b5
8595efa76a38e37ee168f811382cb46b801582cedc6a11b6399e50eaa3c92f2d
b8fb2174816014c9033236a62469308542aa02d76c9219f8569ac3a4e4db3b7ec0a
62c7b8100381f3562413a33b8edcdcf7996ce6663918a1f0e08a0a14c0632c137cb7
cc4bdd9fa2376b8fc4329b31a6cf5fbff2c094e820d73929e2215af94
df710408a6c93ad71c6bca3133ac6e767c269908be26352793b11b2fdee56f68
fd664f3203418b3188ef00dac1b17bf1c4322946797cfdcce6ff10c0f50ca560

Se ha observado que las siguientes URL albergan contenido malicioso recuperado durante el proceso de infección.

hXXp[:]//ia801400[.]us[.]archive[.]org/26/items/auto_20220216/auto.txt
hXXps[:]//afomas[.]com/wp-admin/images/Feb_MA2.mp3
hXXps[:]//archive[.]org/download/auto_20220216/auto.txt
hXXps[:]//archive[.]org/download/my44_20220211/my44.txt
hXXps[:]//blankinstall[.]info/build/x.mp3
hXXps[:]//cdn[.]discordapp[.]com/attachments/777508363029184525/935168254744358952/log.mp3
hXXps[:]//cozumreklamkayseri[.]com/.Fainl.txt
hXXps[:]//isoeducationjo[.]com/.well-known/mo.mp3
hXXps[:]//kediricab[.]dindik[.]jatimprov[.]go[.]id/wp-admin/x.txt
hXXps[:]//onedrive[.]live[.]com/Download?cid=358166AEFCA69E90&resid=358166AEFCA69E90!124&authkey=AGvLNowfByqo5eo
hXXps[:]//usaymaboutique[.]com/assets/assets.txt
hXXps[:]//uxsingh[.]com/uxsingh.jpg
hXXps[:]//v3-fastupload[.]s3-accelerate[.]amazonaws[.]com/1643406871-d.mp3
hXXps[:]//www[.]atgame888[.]com/wp-admin/Feb_MO2.mp3
hXXps[:]//www[.]wordpressthemesall[.]com/wp-admin/Feb_MA2.mp3
hXXps[:]//y-menu[.]com/wp-admin/MA.txt

Los siguientes dominios para ser asociados a esta campaña de malware:

141[.]95[.]89[.]79
3laallah[.]myvnc[.]com
94[.]130[.]207[.]164
anderione[.]com
invoice-update[.]myiphost[.]com
mekhocairos[.]linkpc[.]net
n[.]myvnc[.]com
python[.]blogsyte[.]com

VI. IMPACTO:

Este *malware*, una vez se instala en el equipo, tiene capacidad para realizar las siguientes acciones:

- Accede y roba la información del dispositivo.
- Captura y registra los datos introducidos con el teclado.
- Captura las imágenes de pantalla del dispositivo infectado.
- Crea una clave de registro en el sistema del dispositivo afectado para crear persistencia.
- Deshabilita la protección antivirus del dispositivo infectado.
- Obtiene privilegios de administrador.
- Realiza conexiones con sitios no legítimos y descarga otros ficheros y programas maliciosos.
- Toma el control del dispositivo remotamente.

Los principales dispositivos afectados son los que disponen de sistema operativo Windows.

VII. RECOMENDACIONES:

- Si bien no existen soluciones inmediatas para bloquear el malware en general, el uso de soluciones de seguridad tanto en la capa de red como en la de host es una regla crucial en estos días. Los delincuentes utilizan a diario diferentes técnicas para eludir los mecanismos de defensa. Utilizando un archivo .bat simple con mucha basura y líneas de código ofuscadas, fue posible inyectar código en la memoria y romper la barrera de seguridad inicial.

- De esta forma, es necesario utilizar software contra las ciberamenazas y aplicar medidas capaces de monitorear una perspectiva de 360 grados de todo el ecosistema.
- Las principales firmas de antivirus contienen reglas para detectar y eliminar este *malware.*

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:

- https://www.incibe.es/servicio-antibotnet/info/AsyncRAT
- https://www.blackberry.com/us/en/solutions/endpoint-security/ransomware-protection/asyncrat
- https://www.welivesecurity.com/la-es/2023/02/23/campana-espionaje-empresas-organismos-gubernamentales-colombia-asyncrat/
- https://seguranca-informatica.pt/how-asyncrat-is-escaping-security-defenses/
- https://blog.talosintelligence.com/asyncrat-3losh-update/