RAT

(Remote Administration Tool / Remote Access Trojan)

Elaborado por:
Morales Téllez Carlos Gamaliel
Pérez Quiroz Miguel Ángel

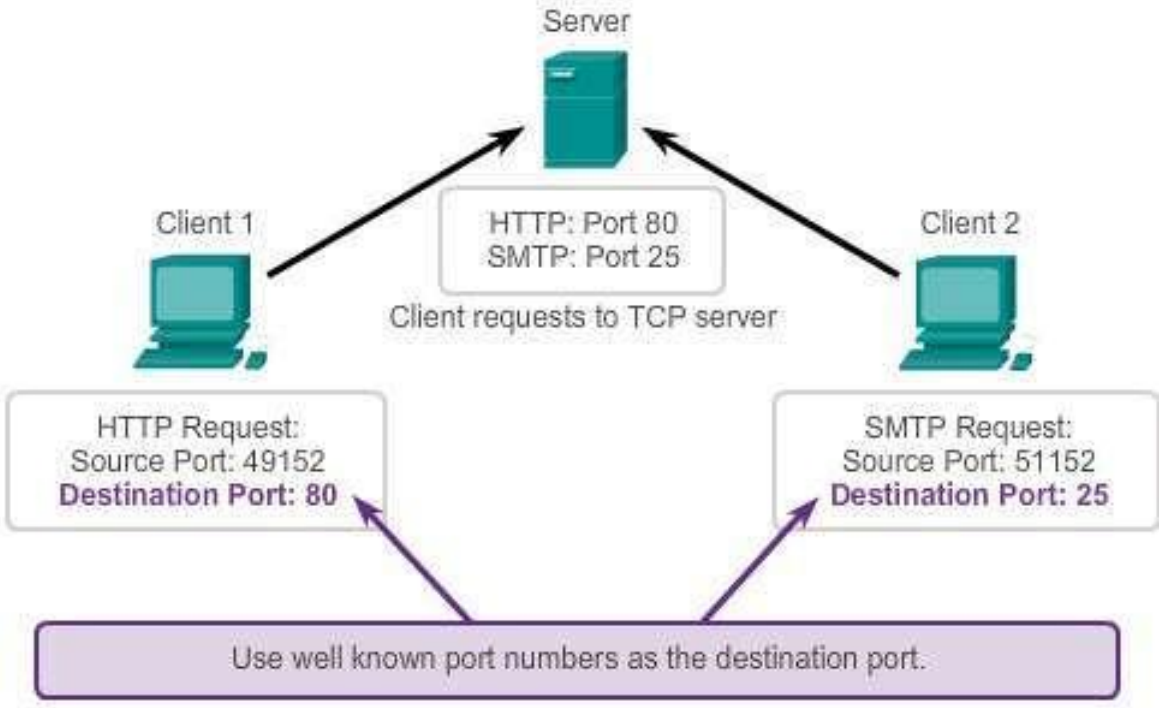
1. Antecedentes

SSH (22), HTTP (80) y HTTPS (443)

El protocolo SSH (también conocido como Secure Shell) es un método para el inicio de sesión remoto seguro desde una computadora a otra.

Los puertos 80 y 443 son utilizados en páginas web, para el casos de las RATs se pueden utilizar para administración remota a través de una aplicación web.

Conexiones cliente-servidor



2. ¿Qué es una RAT?

El lado del bien

Herramienta de administración remota.

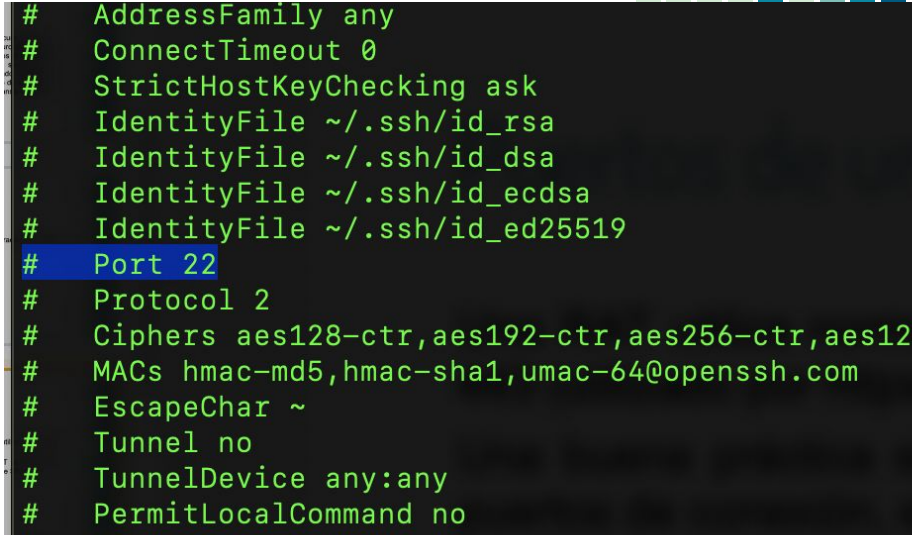
Una herramienta de administración remota o RAT es un software que le da a una persona el control total de un dispositivo de forma remota. Una RAT le da acceso al usuario a su sistema, como si tuviera acceso físico a su dispositivo. Con este acceso, la persona puede manejar archivos, grabar la pantalla, capturar información del teclado e incluso encender / apagar el dispositivo.

Modificación de los puertos.

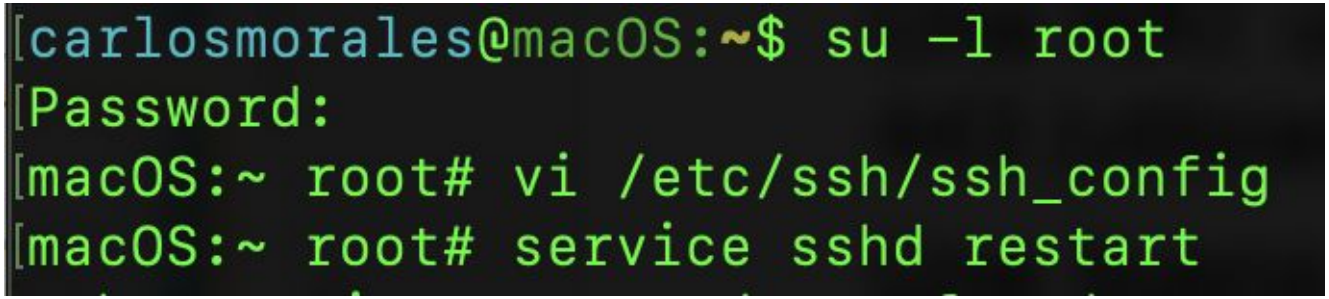
Una buena práctica si se va a utilizar una RAT es cambiar los puertos de conexión, especialmente el de Secure Shell.

Ejemplo:

Empleando al usuario root o administrador se debe editar el archivo de configuración de ssh (/etc/ssh/sshd_config) descomentando la línea que diga “#Port 22”

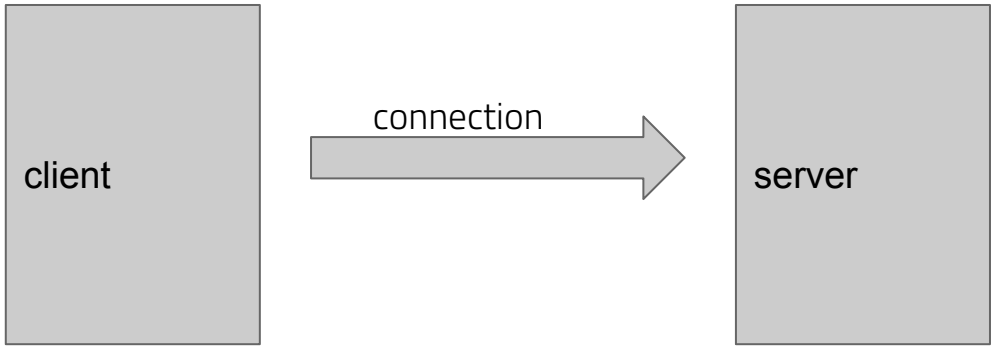



IdentityFile ~/.ssh/id_ed25519
Port 11154
Protocol 2
Ciphers aes128-ctr,aes192-ctr,aes256


carlosmorales@macOS:~$ su -l root
Password:
macOS:~ root# vi /etc/ssh/ssh_config
macOS:~ root# service sshd restart

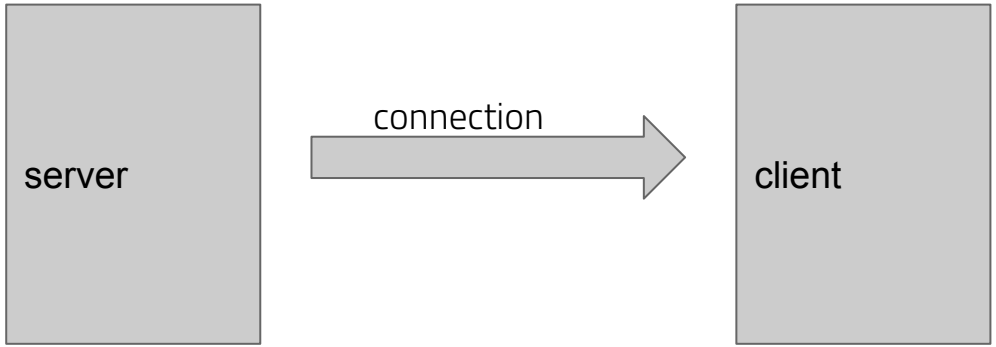
RAT de conexión directa

En una conexión directa un servidor abre el puerto al cual el cliente se conecta.



RAT de conexión inversa

En una conexión inversa el cliente abre el puerto al cual el servidor se va a conectar.



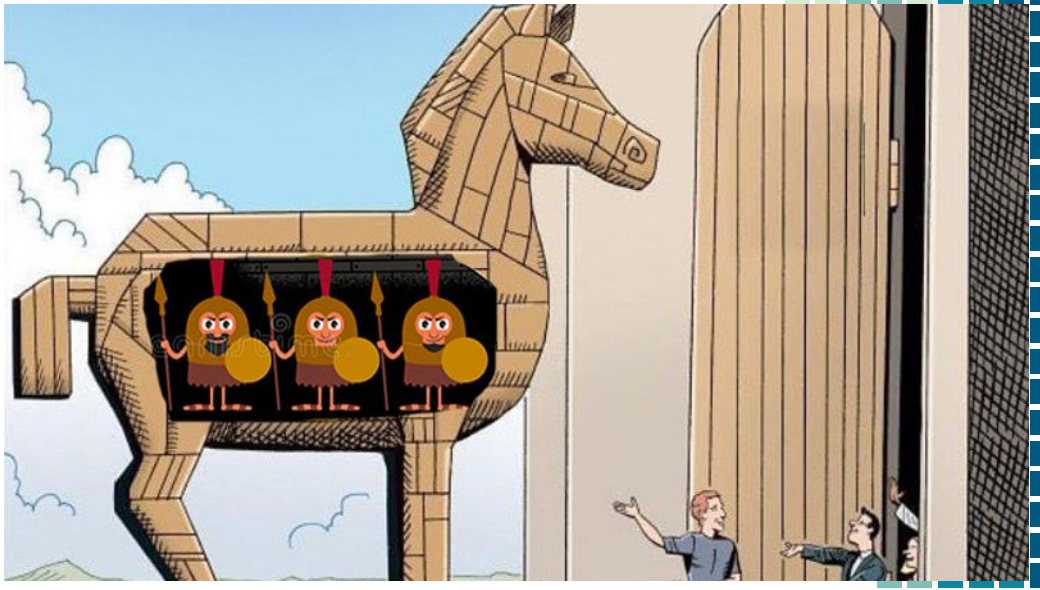
3. ¿Qué es un RAT?

El lado del mal

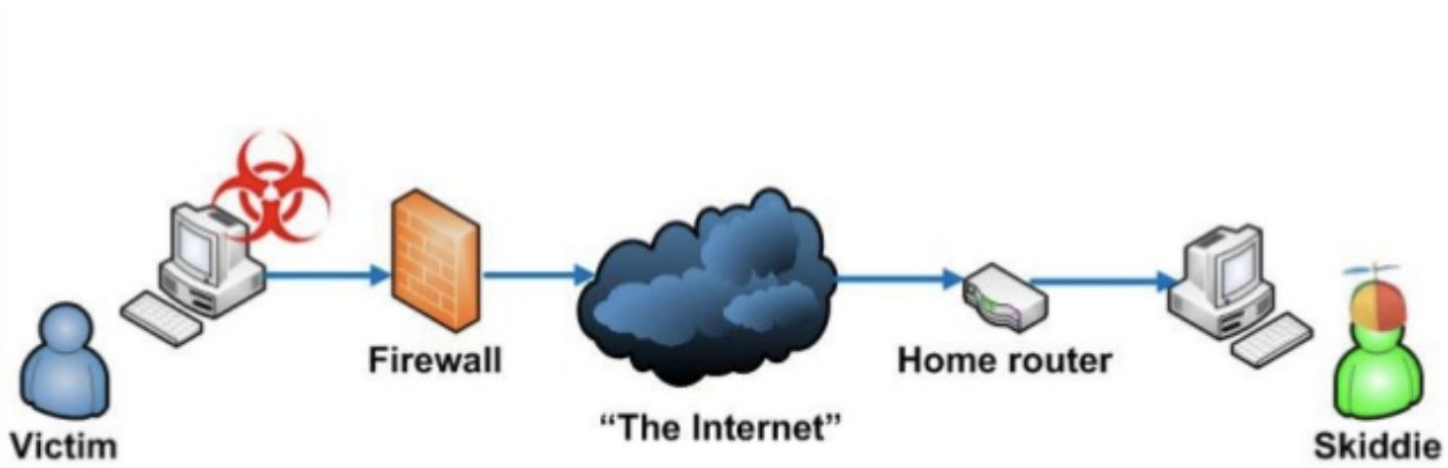
Troyano de acceso remoto.

Troyano

Un troyano puede encontrarse adherido a un software corrupto o dentro de archivos de texto, imágenes, canciones, videos, etc.



Escenario típico de un RAT (Troyano)



Formas de adquirir un troyano

- A través de un dispositivo de almacenamiento externo (USB,SD,CD,etc.).
- A través de una descarga de un paquete corrupto.

REMOTE ACCESS TROJAN

Los RATs se utilizan a menudo en ataques dirigidos con objetivos específicos, como como robar información o moverse lateralmente a través de una red.

Estructura de un RAT

El servidor corre en la computadora de la víctima infectada con malware.

El cliente corre de manera remota a través de una unidad de control operada por el atacante.

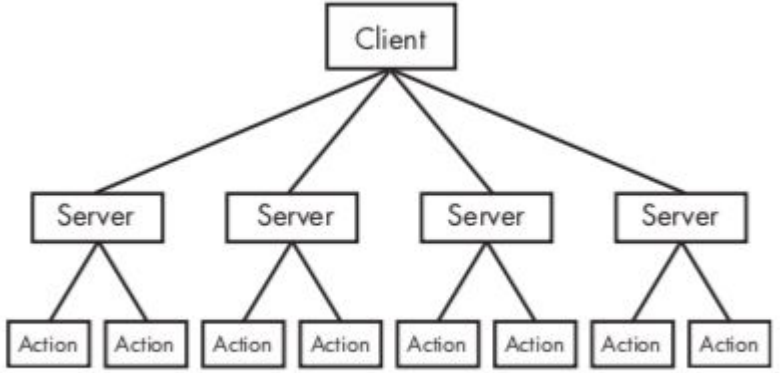


Figure 11-1: RAT network structure

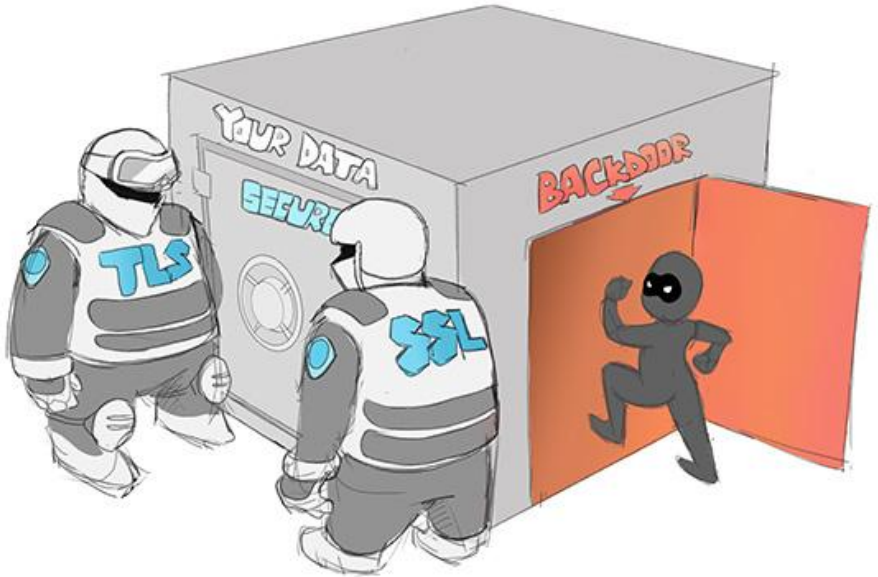
Cuando un RAT (Remote Access Trojan) se activa, el atacante puede ver lo que más le convenga a cada momento:

- Saltar los procesos de comprobación de identidad más comunes.
- Monitorear el comportamiento del usuario.
- Recopilar información personal de la víctima.
- Sustraer archivos e incluir nuevos.
- Formatear unidades o descargar, eliminar o alterar sistemas de archivo.
- Distribuir software malicioso.
- Borrar las cookies de un navegador

4. ¿Cómo funciona?

Hace uso de un Backdoor

Los RAT son herramientas que instalan un Backdoor.



¿QUÉ ES UN BACKDOOR?

- Un Backdoor es un tipo de malware que proporciona al atacante acceso remoto al equipo de la víctima. Son el tipo más común de malware y vienen en todas formas y tamaños.

Troyanización de binarios

Otra forma en que el malware gana persistencia es mediante la troyanización de los binarios del sistema. Con esta técnica, el malware altera los bytes de un binario del sistema para forzar al sistema a ejecutar el malware la próxima vez que se ejecute o se cargue el binario infectado.

Ejemplo

Original code	Trojanized code
`DllEntryPoint(HINSTANCE hinstDLL,` `  DWORD fdwReason, LPVOID lpReserved)`	`DllEntryPoint(HINSTANCE hinstDLL,` `  DWORD fdwReason, LPVOID lpReserved)`

`mov  edi, edi`
`push  ebp`
`mov  ebp, esp`
`push  ebx`
`mov  ebx, [ebp+8]`
`push  esi`
`mov  esi, [ebp+0Ch]`
	`jmp  DllEntryPoint_0`

Listing 11-5 shows the malicious code that was inserted into the infected *rtutils.dll*.

```
6E8A660 DllEntryPoint_0
6E8A660         pusha
6E8A661         call  sub_76E8A667 ❶
6E8A666         nop
6E8A667 sub_76E8A667
6E8A667         pop   ecx
6E8A668         mov   eax, ecx
6E8A66A         add   eax, 24h
6E8A66D         push  eax
6E8A66E         add   ecx, 0FFFF69E2h
6E8A674         mov   eax, [ecx]
6E8A677         add   eax, 0FFF00D7Bh
6E8A67C         call  eax ; LoadLibraryA
6E8A67E         popa
6E8A67F         mov   edi, edi ❷
6E8A681         push  ebp
6E8A682         mov   ebp, esp
6E8A684         jmp   loc_76E81BB2
..
6E8A68A         aMsconf32_dll db 'msconf32.dll',0 ❸
```

'sting 11-5: Malicious patch of code inserted into a system DLL

pusha guarda el estado inicial del registro.
Se hace una llamada a una subrutina.

Dentro de la subrutina:
Se guarda la dirección de la instrucción después de call en ecx.
Se mueve el valor del registro ecx a eax.
Se calcula una localidad de memoria con eax y se almacena en la pila.
Se calcula otra dirección de memoria con ecx y se pasa a eax.
Se hace una llamada a LoadLibraryA que se encuentra en eax. Esto causa que se cargue el archivo 'msconf32.dll'.
Posteriormente se restaura el estado del registro a y se ejecuta el resto del programa de manera normal.

5. Prevención

¿CÓMO PREVENIRNOS?

Mantener el software de las computadoras y teléfonos móviles actualizado

De manera particular, el navegador, cliente de email, aplicaciones de oficina y extensiones (Java, Flash, visualizador de PDF, etc)

¿CÓMO PREVENIRNOS?

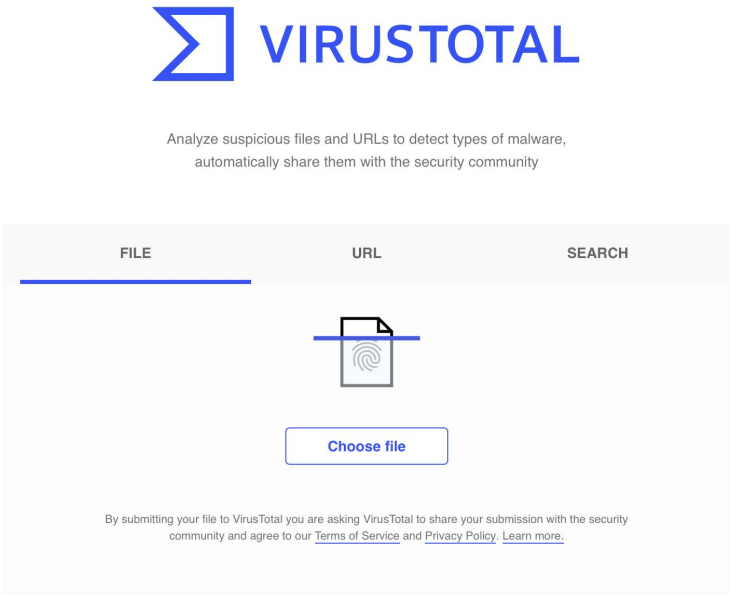
Instalar y mantener siempre actualizados antivirus y firewalls

No seguir hipervínculos poco confiables ni descargar archivos de desconocidos. Ignorar mensajes sospechosos recibidos a través de e-mail o redes sociales

Verificación de la integridad de los paquetes descargados

```
root# echo "Hola, compañeros" > expo.txt
root# cat expo.txt
Hola, compañeros
root# sha256 expo.txt
SHA256 (expo.txt) = c643680f36badd7af70fba39991ac1cd72d8075e86024c86f91f2d3ae8a6
f286
root# echo "Código malicioso muajaja" >> expo.txt
root# sha256 expo.txt
SHA256 (expo.txt) = 351a519fd4188b3524d87111e1dea55056097e5d817287cde9455cd38ca0
5d1c
root#
```

Virus Total


VIRUSTOTAL
Analyze suspicious files and URLs to detect types of malware,
automatically share them with the security community
FILE
URL
SEARCH
Choose file
By submitting your file to VirusTotal you are asking VirusTotal to share your submission with the security community and agree to our Terms of Service and Privacy Policy. Learn more.

37 engines detected this file

5f99db1b097eeb24c0e490f86fab019c5a2680d8433fadbfc0e1b8907e12bfd5

Zer0.tar.gz

gzip tar-bundle

136.44 KB
Size

2018-10-26 18:19:08 UTC
5 months ago

DETECTION DETAILS RELATIONS COMMUNITY

AegisLab	Worm.Linux.Lion.p!c	AhnLab-V3	Linux/Agent
Antiy-AVL	Worm[Net]/Linux.Lion	Arcabit	Trojan.Linux.Rootkit.C
Avast	BV:Agent-ACS [Rtk]	AVG	BV:Agent-ACS [Rtk]
Avira	LINUX/Lion.14	Baidu	Multi.Threats.InArchive
BitDefender	Linux.Worm.Lion.A	CAT-QuickHeal	Linux.Lion
ClamAV	Win.Trojan.U-7	Cyren	Unix/Lion
DrWeb	Linux.Lion	Emsisoft	Linux.Worm.Lion.A (B)
eScan	Linux.Worm.Lion.A	ESET-NOD32	Linux/Lion
F-Prot	Unix/Lion	F-Secure	Linux.Worm.Lion.A
Fortinet	Linux/T0rn.A!tr	GData	Trojan.Hacktool.Linux.Kldhide.A
Ikarus	Net-Worm.Linux.Lion	Jiangmin	Backdoor/Linux.hl

Referencias

- Sikorski, Michael. Honing, Andrew. (2012). Practical Malware Analysis. San Francisco, no stach press.
- https://cdn2.hubspot.net/hubfs/2264844/website/pdf/Los_troyanos_de_acceso_remoto_en_el_sector_bancario.pdf?t=1508366427685
- https://sites.google.com/site/gestionderedesdedatossmt/puertos-y-servicios/puertos-fisicos/puertos-fisicos
- https://securingtomorrow.mcafee.com/consumer/identity-protection/what-is-rat/
- https://www.2-spyware.com/remote-administration-tools-removal
- https://www.wordfence.com/learn/finding-removing-backdoors/
- https://www.washingtonpost.com/apps/g/page/world/how-to-implant-a-trojan-horse-a-user-manual/1257/?noredirect=on
- https://www.fireeye.com/content/dam/fireeye-www/regional/mx_ES/current-threats/pdfs/rpt-poison-ivy.pdf
- https://www.cyber.nj.gov/threat-profiles/trojan-variants/poison-ivy

RAT

(Remote Administration Tool / Remote Access Trojan)

Elaborado por:
Morales Téllez Carlos Gamaliel
Pérez Quiroz Miguel Ángel