RAT

(Remote Administration Tool / Remote Access Trojan)

Elaborado por:
Morales Téllez Carlos Gamaliel
Pérez Quiroz Miguel Ángel

1. Antecedentes

Puerto Lógico

El Puerto Lógico es una zona, o localización, de la memoria de una computadora que se asocia con un puerto físico o con un canal de comunicación, y que proporciona un espacio para el almacenamiento temporal de la información que se va a transferir entre la localización de memoria y el canal de comunicación.

Protocolo

Un protocolo en informática se refiere a un conjunto de reglas predefinidas con el propósito de estandarizar el intercambio de información en actividades informáticas.

- Al seguir un mismo protocolo se garantiza que habrá compatibilidad entre dispositivos de ubicados en diferentes puntos de un sistema informático.

SSH (22)

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

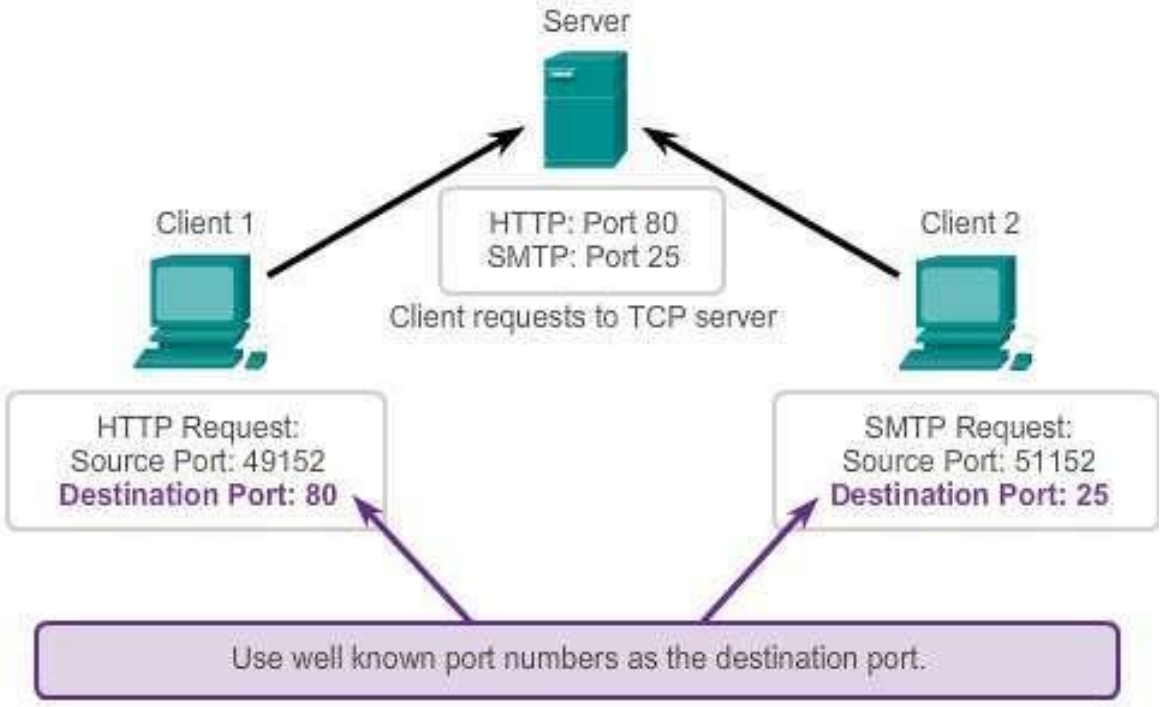
- Proporciona varias opciones alternativas para una autenticación sólida.
- Protege la seguridad e integridad de las comunicaciones con un cifrado sólido.

Es una alternativa segura a los protocolos de inicio de sesión no protegidos (como telnet, rlogin) y métodos de transferencia de archivos inseguros (como FTP).

HTTP (80) y HTTPS (443)

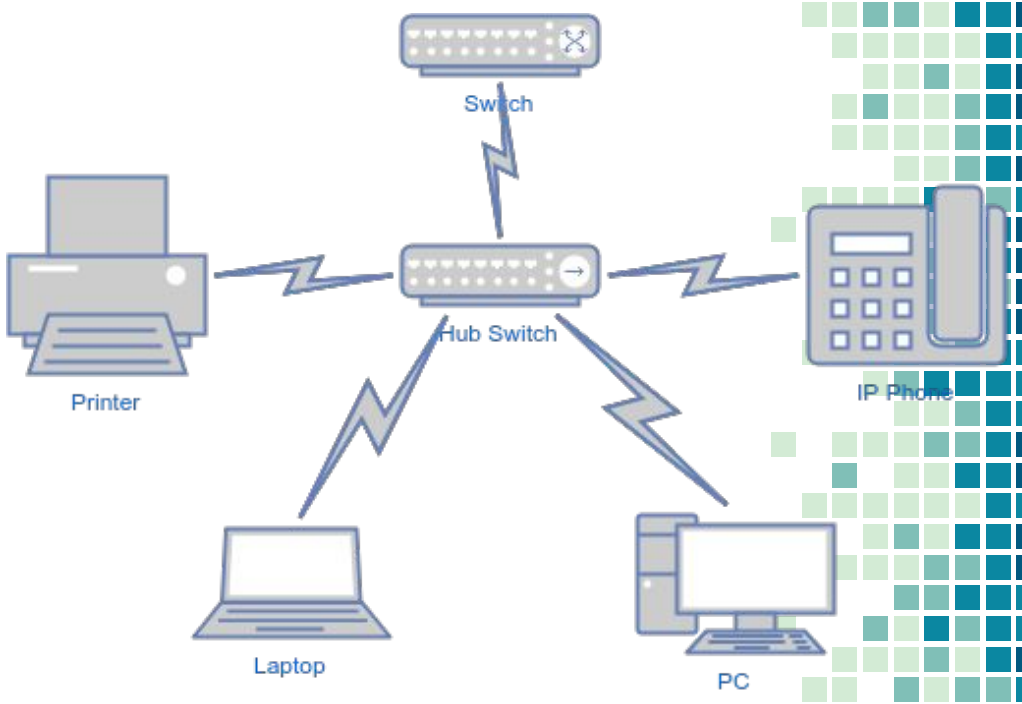
Son utilizados en herramientas de administración remota a través de una aplicación web.

Conexiones cliente-servidor



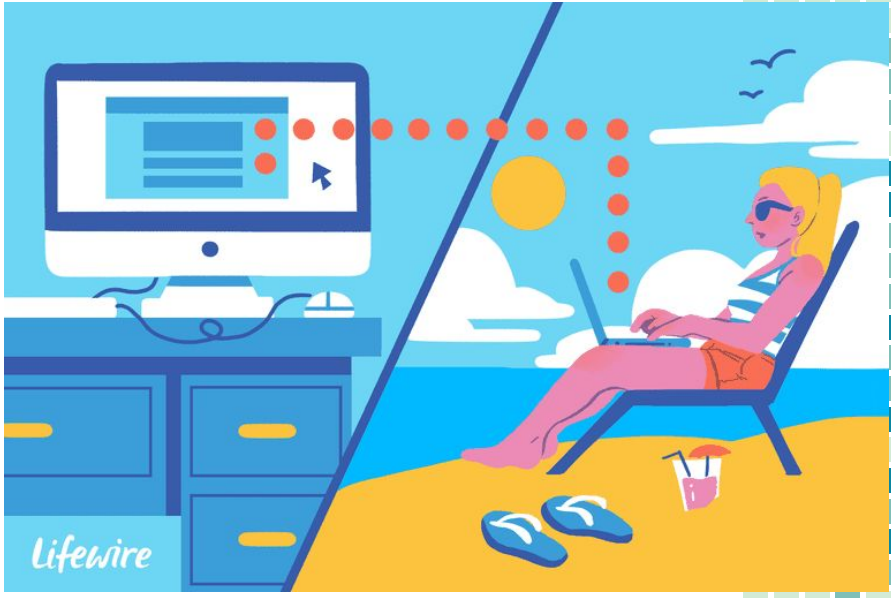
Conexión en LAN

La conexión hacia un equipo remoto a través de una RAT debe ser dentro de una red de área local.



VPN

También podemos tener acceso a una red local desde un lugar distinto a través de una VPN.



2. ¿Qué es una RAT?

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 sus archivos, usar su cámara e incluso encender / apagar su dispositivo.

Puertos de una RAT

Una RAT utiliza normalmente los puertos 22 (utilizado por ssh), 443 (utilizado por https) y 80 (utilizado por http).

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

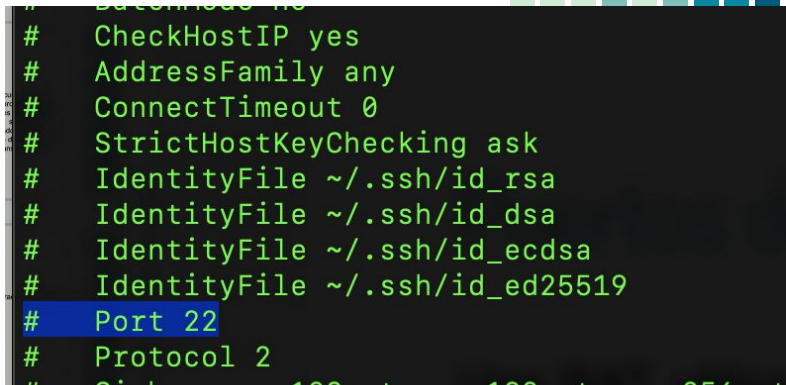
Ejemplo:

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

Una RAT de conexión directa es una configuración simple donde el cliente se conecta a uno o varios servidores directamente. Los servidores estables tienen múltiples subprocesos, lo que permite la conexión de múltiples clientes, junto con una mayor confiabilidad.

RAT de conexión inversa

En este caso se tiene una conexión desde un servidor hacia un cliente.

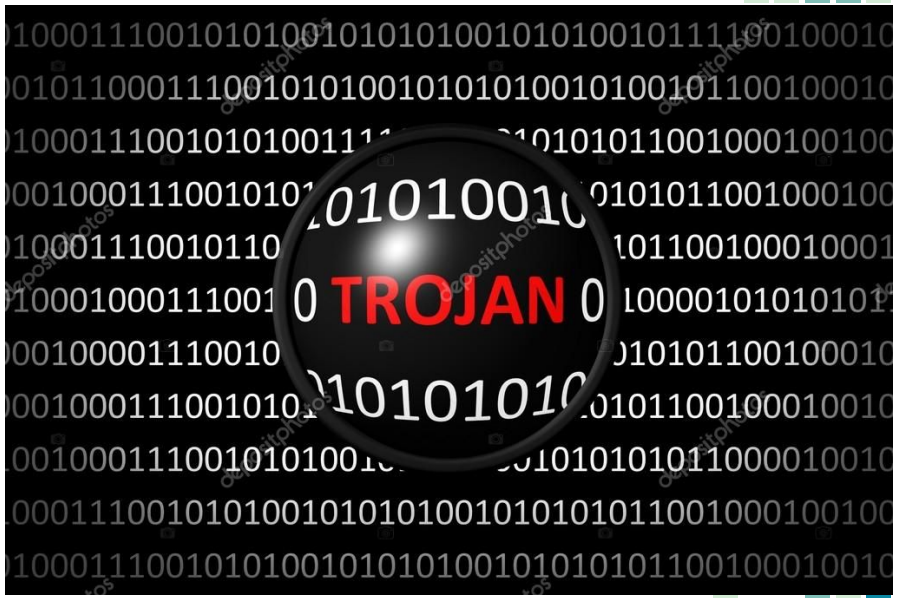
- Es posible revisar el tráfico proveniente del servidor a través de un sniffer.

3. ¿Qué es un RAT?

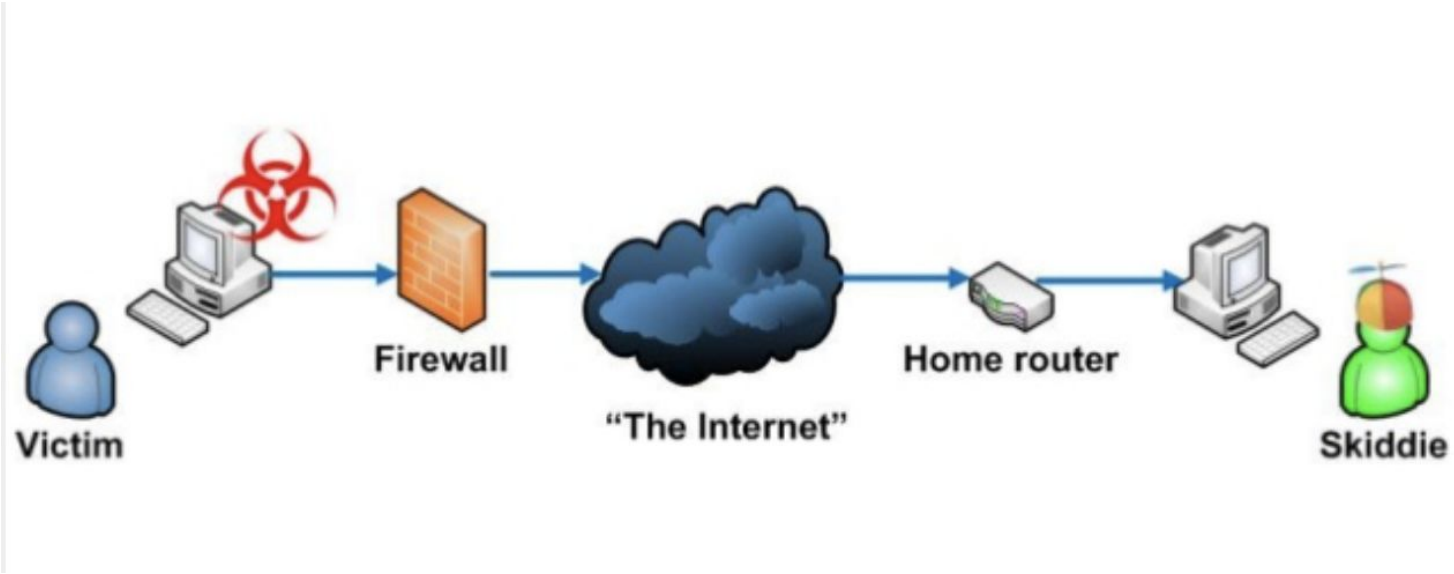
Troyano de acceso remoto.

Troyano

Existen dos tipos de troyanos. Aquellos que se encuentran adheridos a un software corrupto y aquellos que se encuentran 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 con la siguiente forma:

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.

La comunicación de RATs es usualmente a través de los puertos 80 y 443

MOVIMIENTO LATERAL

Es la capacidad del malware para explotar otros recursos de la red a la que se ha conectado, así como la recopilación de información sensible que se encuentre en la misma.

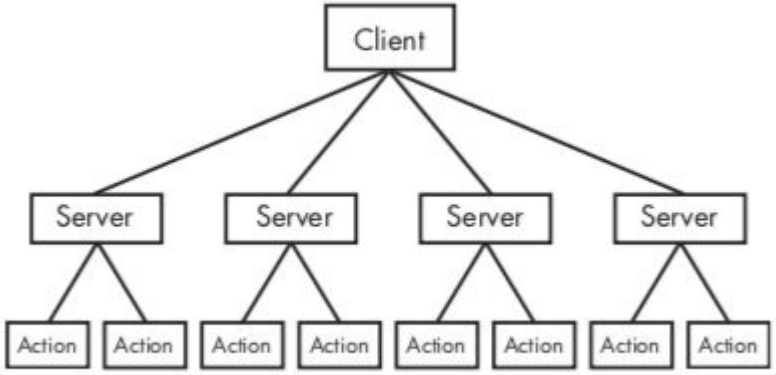


Figure 11-1: RAT network structure

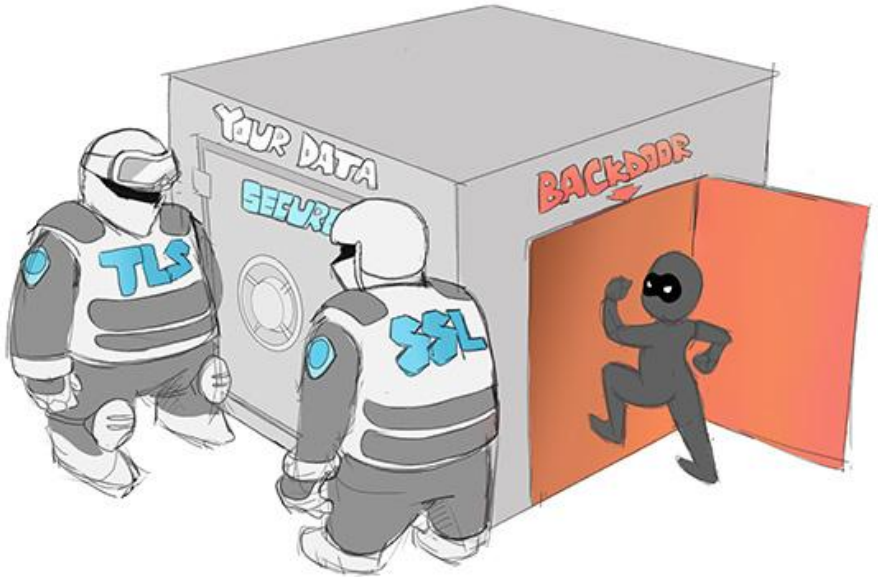
Cuando un RAT (Remote Access Trojan) se activa, el atacante puede ver lo que más le convenga a cada momento:

- Saltar los procesos de comprobación de identidad más comunes.
- Monitorizar el comportamiento del usuario.
- Recopilar información de la víctima, incluidos sus números de tarjeta de crédito y de seguridad social.
- Sustraer archivos e incluir nuevos.
- Activar cámaras web y grabar vídeos, así como realizar capturas de pantalla.
- 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 utilizan el método de conexión Backdoor.



¿QUÉ ES UN BACKDOOR?

Una puerta trasera es una técnica en la que un mecanismo de seguridad del sistema se pasa por alto y se accede a una computadora sin ser detectado.

- El método de acceso de puerta trasera a veces lo escribe el programador que desarrolla un programa.
- Una puerta trasera también se conoce como una trampilla.

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*.

```
76E8A660 DllEntryPoint_0
76E8A660         pusha
76E8A661         call  sub_76E8A667 ❶
76E8A666         nop
76E8A667 sub_76E8A667
76E8A667         pop   ecx
76E8A668         mov   eax, ecx
76E8A66A         add   eax, 24h
76E8A66D         push  eax
76E8A66E         add   ecx, 0FFFF69E2h
76E8A674         mov   eax, [ecx]
76E8A677         add   eax, 0FFF00D7Bh
76E8A67C         call  eax ; LoadLibraryA
76E8A67E         popa
76E8A67F         mov   edi, edi ❷
76E8A681         push  ebp
76E8A682         mov   ebp, esp
76E8A684         jmp   loc_76E81BB2
...
76E8A68A         aMsconf32_dll db 'msconf32.dll',0 ❸
```

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

Poison Ivy (PIVY)

Poison Ivy es un RAT disponible de manera gratuita y muy popular.
Puede ser una herramienta bastante útil para generar muestras de malware para probar o analizar.
Disponible en (http://www.poisonivy-rat.com/)

Reportes

Poison Ivy se ha utilizado en varias campañas destacadas de malware, siendo la más célebre el robo de los datos sobre la solución SecurID de RSA en 2011. Ese mismo año, Poison Ivy impulsó un ataque coordinado denominado Nitro, contra fabricantes de productos químicos, organismos públicos, empresas de defensa y grupos en favor de los derechos humanos.

Operación

En 2013, FIreEye difundió un informe detallado sobre Poison Ivy y proporcionó su secuencia de ataque típica:

1. El atacante configura un servidor personalizado de PIVY, que incorpora detalles sobre cómo se instalará la RAT en la computadora del objetivo, las funciones habilitadas y la contraseña de cifrado, entre otras.
2. El atacante envía el archivo de instalación del servidor PIVY a la computadora del objetivo. El objetivo abre el correo electrónico infectado y ejecuta el archivo, o visita un sitio web comprometido.

Operación

3. El archivo de instalación del servidor se ejecuta en la computadora del objetivo y descarga código adicional a través de un canal de comunicación cifrado para evitar la detección de antivirus.
4. Una vez que el servidor PIVY se ejecuta en la máquina de destino, el atacante usa un cliente de GUI de Windows para controlar la computadora de destino.

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

Bloqueo de acceso a dispositivos externos. (Ejemplo en CentOS)

Modificar el archivo de configuración de almacenamiento de usb.

/etc/modprobe.d/usb-storage.conf

Añadir la siguiente línea

cat “install usb-storage /bin/true” >> /etc/modprobe.d/usb-storage.conf

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
-