RATS

Carlos Gamaliel Morales Téllez

Y

Miguel Ángel Pérez Quiroz

Sistemas Operativos

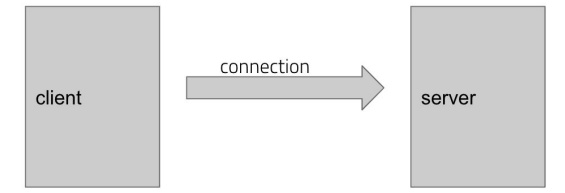
Remote Administration Tools and Remote Access Trojans

Herramienta de administración remota

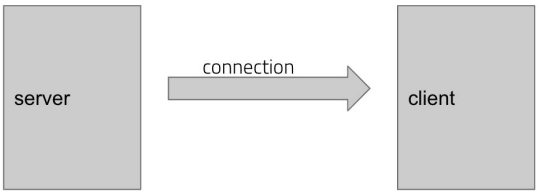
Una herramienta de administración remota o RAT es un software que le da a una persona el control total de un dispositivo de forma remota. Una RAT le da acceso al usuario a su sistema, como si tuviera acceso físico a su dispositivo. Con este acceso, la persona puede manejar archivos, grabar la pantalla,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

Existen dos tipos de conexión que se pueden utilizar en una herramienta de administración remota:

Conexión directa: El servidor abre el puerto al cual el cliente se conecta.

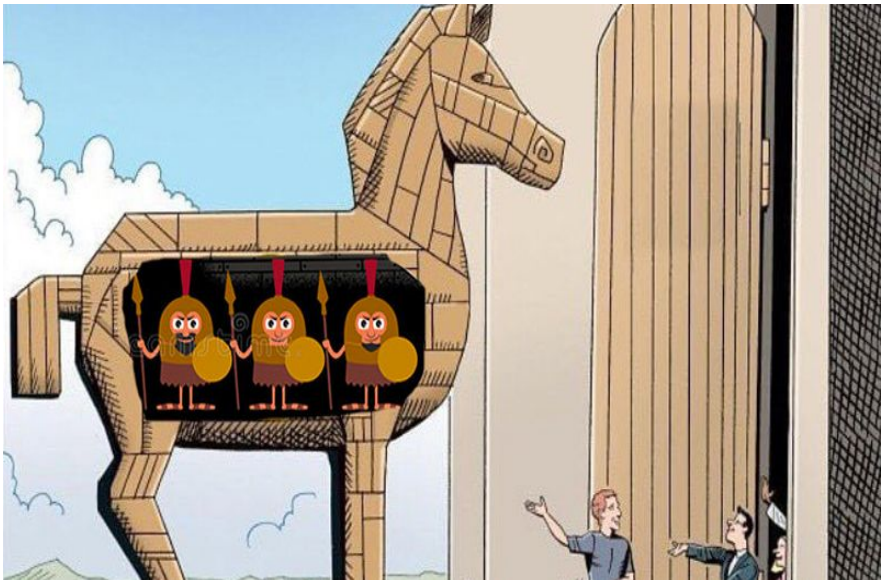


Conexión inversa: El cliente abre el puerto al cual el servidor se va a conectar.



Troyano de acceso remoto

Para comprender de qué se trata esta parte, primero debemos comprender lo que es un troyano. Por lo que daremos un salto a la historia de la guerra de Troya, en la que se presenta a un caballo de troya como un artilugio gigantesco de madera que fue usado por los griegos para introducirse a la ciudad fortificada de Troya. La estrategia fue enviar al caballo de troya, de parte de los griegos, como símbolo de victoria de los troyanos, los cuales no tenían idea de que dentro del artilugio se encontraría un conjunto de soldados griegos, mismos que saldrían en la noche, matarían a los centinelas y así abrir las puertas al ejército griego para llegar finalmente a la caída de troya.



Con lo anterior podemos decir que un troyano en cómputo es un tipo de malware que se encuentra disfrazado de software legítimo.

Para que se haga uso del término *troyano de acceso remoto* se debe cumplir que el software malicioso embebido en el software legítimo debe cumplirse que éste se comporte como una *herramienta de administración remota.*

Remote access trojan

Los troyanos de acceso remoto 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 troyano de acceso remoto

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.

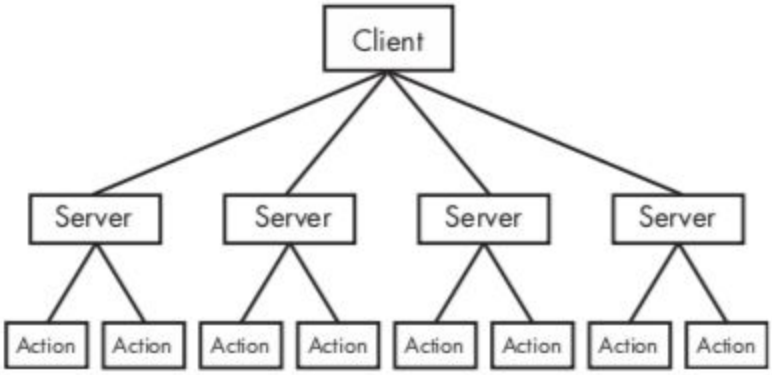


Figure 11-1: RAT network structure

Posibilidades

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

Backdoors

Los troyanos de acceso remoto son herramientas que instalan un backdoor (puerta trasera).

Una puerta trasera es un tipo de malware que proporciona acceso remoto a un equipo. Son muy comunes y existe una gran variedad de ellos.

Las puertas traseras se comunican a través de Internet de muchas maneras, pero un método común es a través del puerto 80 mediante el protocolo HTTP. HTTP es el protocolo más utilizado para el tráfico de red saliente, por lo que ofrece a los malware la mejor oportunidad de mezclarse con el resto del tráfico.

Las puertas traseras vienen con un conjunto común de funcionalidades, como la capacidad de manipular claves de registro, enumerar ventanas de visualización, crear directorios, buscar archivos, etc.

Persistencia

Una vez que el malware obtiene acceso a un sistema, a menudo parece estar allí por mucho tiempo. Este comportamiento se conoce como persistencia. Si el mecanismo de persistencia es lo suficientemente único, incluso puede servir como una excelente manera de detectar huellas digitales en una determinada pieza de malware.

Troyanización de binarios

Una forma en que el malware gana persistencia es mediante un proceso conocido como troyanización de binarios. 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. Los autores de malware suelen dirigirse a aquellos binario de sistema que se utilizan con frecuencia en el funcionamiento normal de Windows. Los DLL son un objetivo popular.

Un binario de sistema se modifica normalmente parchando la función de entrada para que salte al código malicioso. El parche sobrescribe el principio de la función o algún otro código que no es necesario para que el archivo funcione correctamente.

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*.

Típicamente, los códigos malicioso se agregan a una sección vacía del binario, de modo que no afecte el funcionamiento normal. En la tabla anterior se muestra un ejemplo de un archivo DLL modificado de tal modo que el código insertado cargue el malware cada vez que el archivo sea ejecutado. Después de que el código carga el malware, vuelve al código DLL original, para que todo funcione como lo hacía antes del parche.

```
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

La imagen anterior el contenido de la función “DLLEntryPoint_0” que es invocada en el archivo modificado de rtutils.dll. En primer lugar se respalda información necesaria para la ejecución normal del programa con la instrucción ‘pusha’.

Se realiza una llamada a la subrutina “sub_76E8A667” y dentro de esta se guarda la dirección de retorno en ‘ecx’. Este valor se copia en ‘eax’ y se utiliza para calcular una dirección de memoria.

Con ese mismo valor de retorno actualmente se calcula otra dirección de memoria con ‘ecx’ y se copia en ‘eax’.

Se hace una llamada a LoadLibraryA que se encuentra en ‘eax’ y esto causa que se cargue el archivo ‘msconf32.dll’ (archivo malicioso).

Después de que se ejecuta este código malicioso se restaura la información inicial con la instrucción ‘popa’ y se ejecuta el resto del programa de manera normal.

Prevención

Las siguientes estrategias no garantizan la prevención de cualquier ataque, pero definitivamente ayudan a mejorar la probabilidad de adquirir algún tipo de malware.

1. Mantener el software de las computadoras y teléfonos móviles actualizado
2. De manera particular, el navegador, cliente de email, aplicaciones de oficina y extensiones (Java, Flash, visualizador de PDF, etc)
3. Instalar y mantener siempre actualizados antivirus y firewalls
4. No seguir hipervínculos poco confiables ni descargar archivos de desconocidos. Ignorar mensajes sospechosos recibidos a través de e-mail o redes sociales

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://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