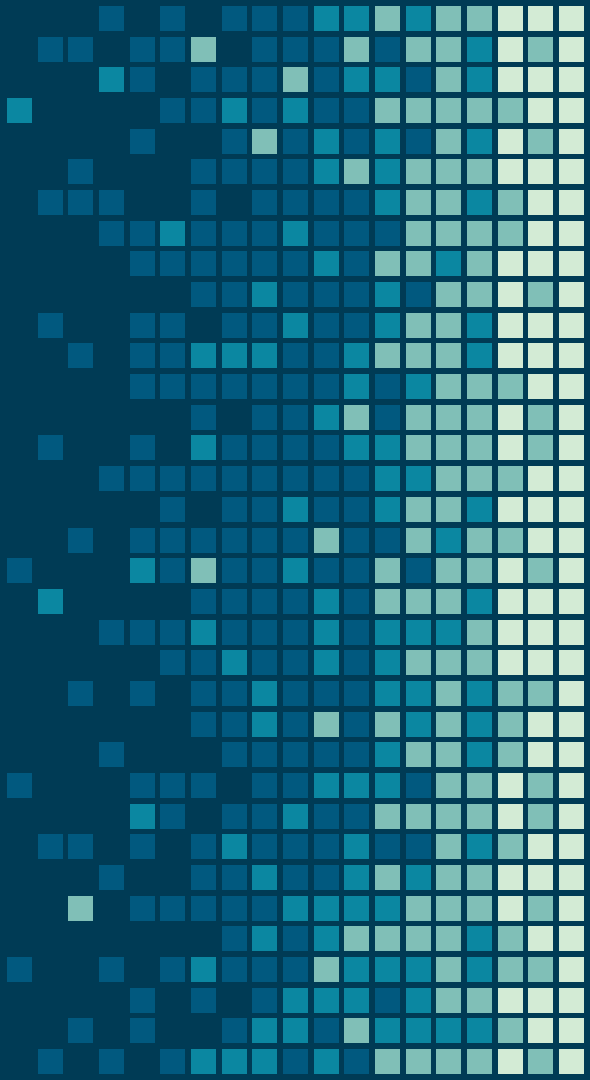
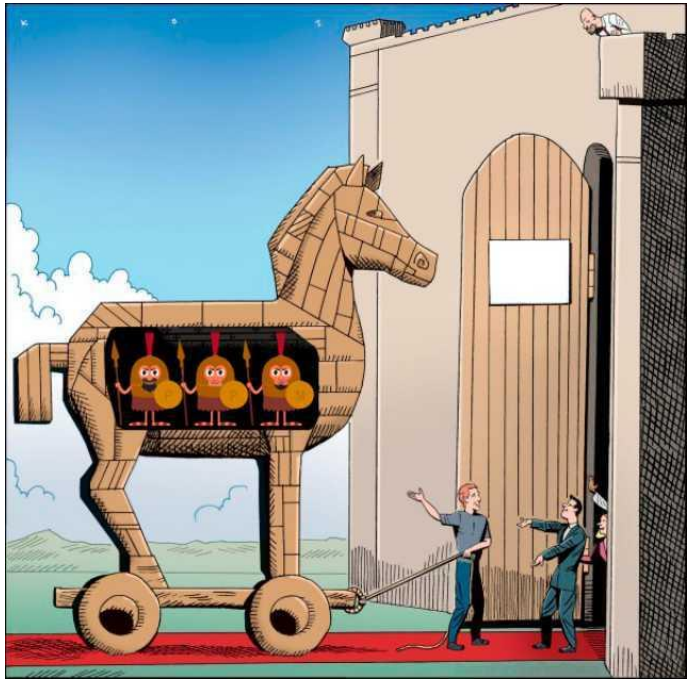
RAT (Remote Access Trojan)

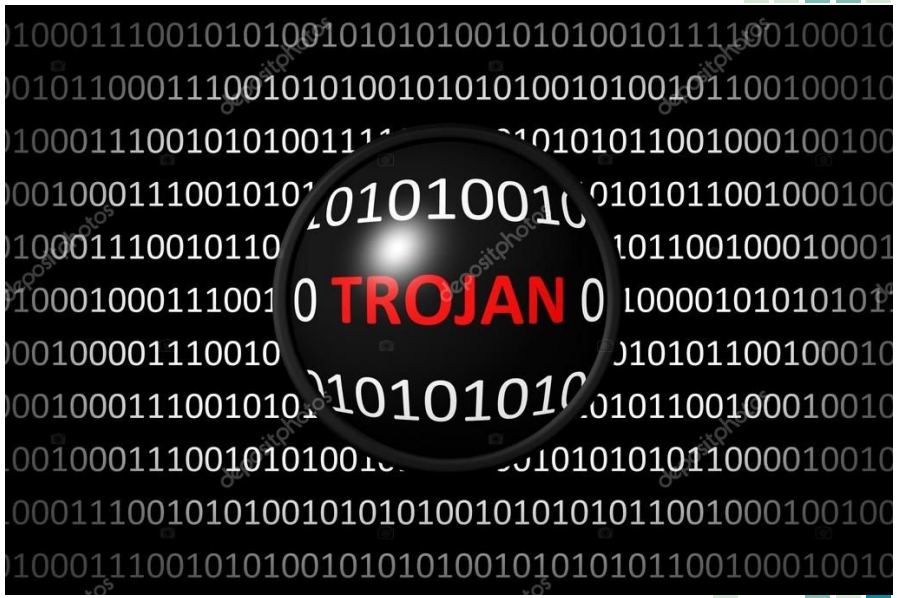


¿QUÉ ES UN CABALLO DE TROYA?



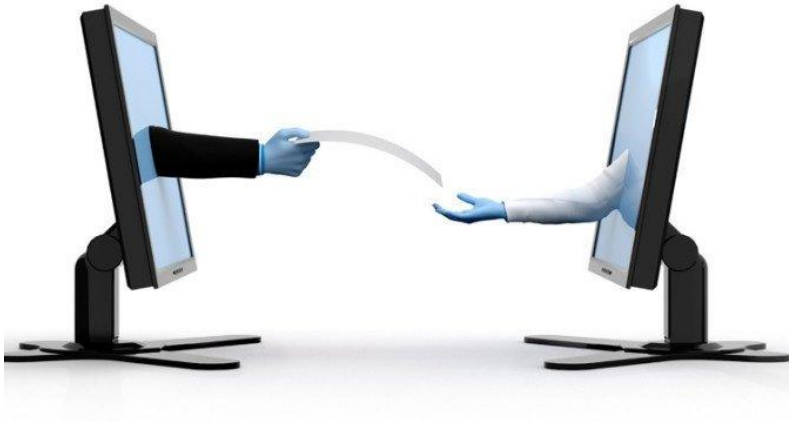
Aterrizando ésto a lo que ocurre en el mundo del cómputo...

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.

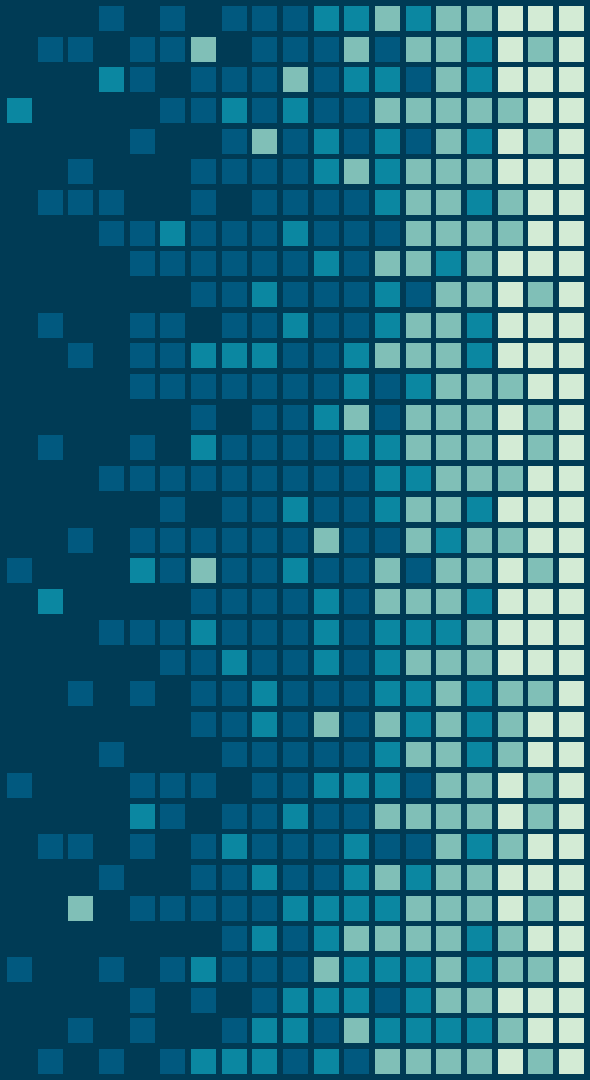


¿QUÉ ES EL ACCESO REMOTO?

Un acceso remoto es poder acceder desde una computadora a un recurso ubicado físicamente en otra computadora que se encuentra geográficamente en otro lugar, a través de una red local o externa (como Internet).



RAT (REMOTE ACCESS TOOL)



REMOTE ADMINISTRATION TOOL

Son usados para administrar remotamente una computadora o computadoras

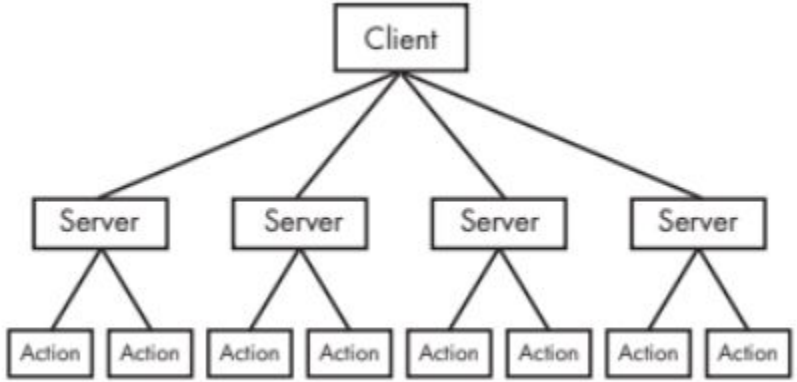


Figure 11-1: RAT network structure

Son utilizados para conectarse remotamente y manejar funcionalidades de una o más computadoras.

- Gestión de archivos (descargas, cargas, ejecuciones, etc.)
- Control del sistema (apagado / encendido)
- Gestión de registros (query, delete, add, modify)
- Control de una shell a través de una terminal

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

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.

¿QUÉ ES UN BACKDOOR?

Un backdoor es un tipo de malware que proporciona a un atacante acceso remoto a la máquina de una víctima.
Las puertas traseras son el tipo más común de malware y vienen en todas las formas y tamaños con una amplia variedad de capacidades.

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.

Troyanos

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*.

¿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

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