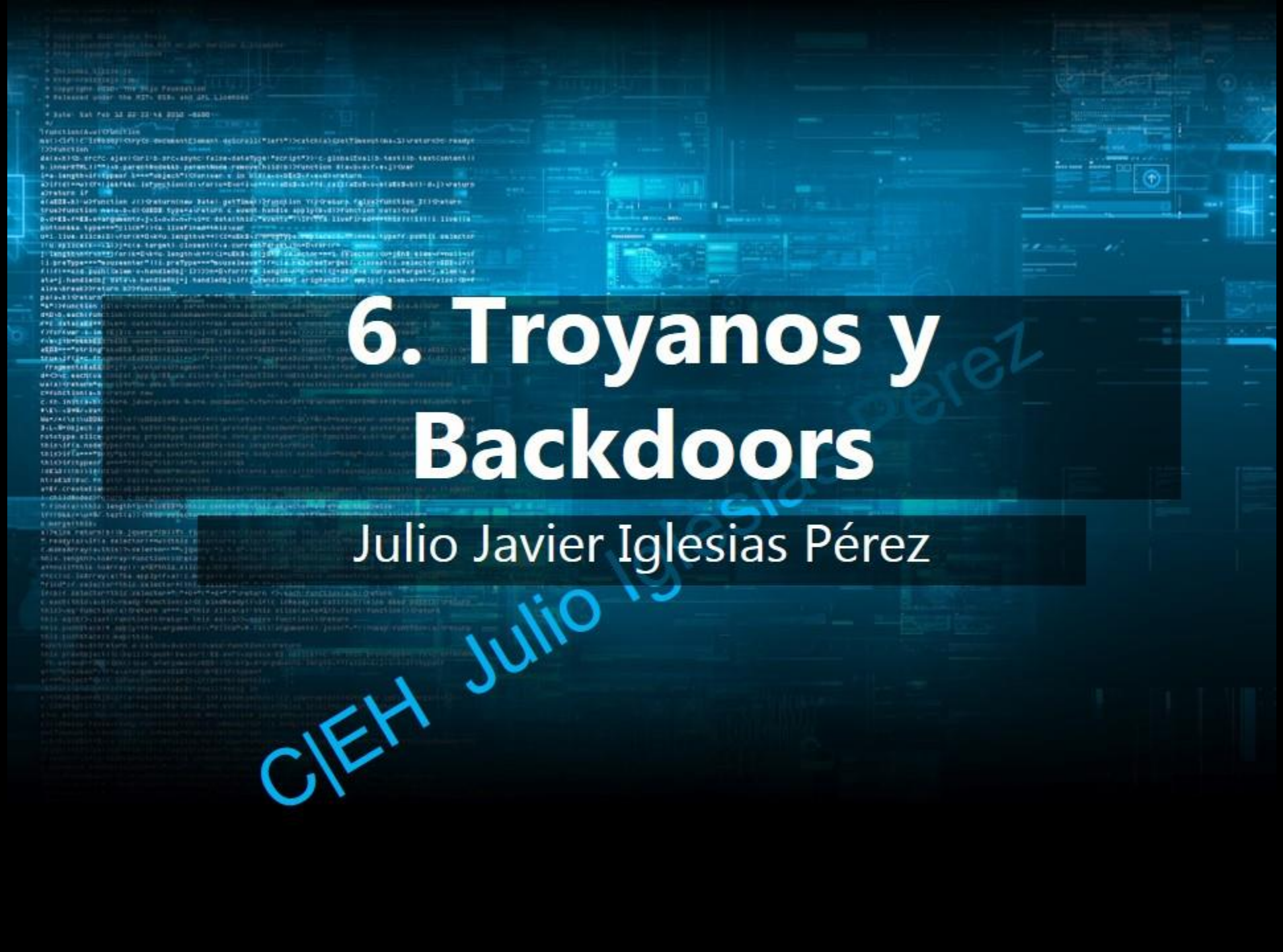

6. Troyanos y Backdoors
Julio Javier Iglesias Pérez
C|EH Julio Iglesias Perez

Troyanos

Programa malicioso que se encuentra dentro de un programa aparentemente inofensivo que puede obtener acceso y causar daño.

Con la ayuda de un troyano un atacante puede obtener acceso a las contraseñas almacenadas en el equipo, también puede leer documentos personales, borrar archivos y mostrar imágenes y/o mostrar mensajes en la pantalla

Su propósito

El propósito de los troyanos son variados, por ejemplo, robar información como contraseñas, códigos de seguridad utilizando keyloggers. Borrar o remplazar archivos críticos del S.O. Generar tráfico para crear ataques DoS. Descargar spyware, adwares y archivos maliciosos. Deshabilitar firewalls y antivirus. Capturar pantallas, audio y video. Infectar el equipo como un proxy server. Utilizar el equipo para hacer spamm o blasting mensajes de correo. Utilizar el equipo como botnet para realizar ataques DoS.

Su propósito

Generalmente busca información sobre: tarjetas de crédito, cuentas, documentos confidenciales, datos financieros, calendario, utilizar el equipo infectado para propósitos ilegales.

Indicaciones de ataque troyano

El DVD se abre o cierra solo, navegador se redirige solo, antivirus se deshabilita, la barra de tareas desaparece, extrañas cajas aparecen, el color del S.O. cambia, contraseñas cambiadas sin autorización, la pantalla se vuelve extraña, cambia la configuración del fondo de pantalla o protector de pantalla. IPS se queja de que el IP del equipo está haciendo escaneos. Compras extrañas en la tarjeta de crédito. Inversión en los botones del mouse. Que la gente sepa mucha información personal de una victima. El monitor se enciende y apaga solo. Documentos y mensajes se imprimen solos. El puntero del mouse desaparece o mueve solo. El equipo se apaga solo. Ctrl Alt Surp no funciona.

Infectando un sistema con un Troyano

1. Crear un nuevo troyano utilizando un Trojan Horse Construction Kit
2. Crear un dropper, que es parte de un paquete troyanizado que instala el código malicioso en el sistema.

Ejemplo de dropper:

Ruta de instalación: C:\Windows\system32\svchosts.exe

Autostart:

HKLM\Software\Micr....\run\Iexplorer.exe

Código Malicioso:

Client address: cliente.attacker.com

Dropzone: dropzone.attacker.com

Wrapper

File name: my_name.jpg

Wrapper data: Graphic file

Infectando un sistema con un Troyano

3. Crear un wrapper utilizando herramientas para instalar el troyano en el equipo de la victima
4. Propagar el troyano (generalmente se contagian las redes P2P como el kazaa)
5. Ejecutar el dropper
6. Ejecutar la damage routine

Wrapper

Une un troyano ejecutable a una aplicación .exe con aspecto inocente, como juegos, etc.

Cuando la víctima ejecuta el .exe, primero se instala el troyano en background y luego ejecuta la aplicación wrapping en foreground.

Ambos programas están unidos dentro de un archivo simple.

Ejemplos de wrapper conver programs.
Kriptomatik. Advanced file joiner

¿Cómo un troyano puede entrar a un sistema?

- Programa falso.
- Descargando archivos, juegos, programas, etc.
- Sitios de descarga de software freeware.
- NetBIOS (filesharing).
- Aplicaciones Instant Messenger. IRC.
- Archivos adjuntos.
- Acceso físico.
- Bugs en mails y navegadores.

Desplegar un troyano

1. Se crea el software troyano.
2. Se lo une en un archivo wrapped.
3. Se lo pone en el equipo de la víctima.
4. Se instala
5. Víctima comprometida

Técnicas para evadir antivirus.

- Nunca utilizar troyanos descargados desde la web (los antivirus pueden detectarlos fácilmente).
- Dividir el archivo troyano en varias piezas y comprimirlas en un archivo simple.
- SIEMPRE escribir sus propios troyanos e incrustarlo dentro de una aplicación.
- Convertir el .exe en vbscript, doc, ppt, pdf
- Cambiar el contexto del troyano utilizando un editor hex, revisar y cifrar el archivo.

Tipos de troyanos

Generalmente se los caracteriza por lo que hace, troyanos http, de comando, destructivos, shell, etc.

Troyanos Command Shell

Estos troyanos proporcionan control remoto a través de línea de comandos en el equipo de la maquina

El servidor troyano es instalado en la maquina virtual de la victima que abre un puerto para que se pueda conectar el atacante. El cliente se instala en el equipo del atacante que ejecuta un command shell en el equipo de la víctima.

Ejemplo con netcat

nc <ip> <puerto>

nc -L -p <puerto> -t -e cmd.exe

Troyanos Botnet

Tiene como objetivo utilizar a las maquinas "secundarias" para atacar al objetivo principal.

Ejemplo: Illusion BOT, netbot attacker

Troyanos Proxy Server

Los atacantes usan los equipos de las victimas para conectarse a internet

Ejemplo: W3bPrOxy Tr0j4nCr34t0r

Troyanos FTP

Instalan un servidor FTP en el equipo de la victima, el cual abre los puertos FTP

Ejemplo: TinyFTPD

Troyanos VNC

Inicia un Servidor VNC deamon en el sistema. Se puede conectar utilizando cualquier visor VNC. Se tiene acceso remoto total, escritorio, pantalla, mouse, teclado, etc.

Ejemplo: WinVNC, aunque no sea un troyano en sí, sirve para "controlar" a los empleados, "que están haciendo"

Troyanos HTTP/HTTPS

Sirven para saltar los firewalls creando una conexión por los puertos 80 y 443, de esa manera se crea un "túnel". Se ejecutan en el host interno.

Ejemplo: HTTP RAT: Muestra datos, keystrokes, archivos, deshabilita programas, floodea las conexines a internet, distribuye threads, hace seguimiento de las actividades de navegación, jihackea el navegador, hace fraude, etc.

Shttpd Trojan: Es un pequeño servidor http que puede ser incrustado en cualquier programa, por ej (chess.exe) cuando este se ejecute el servidor web se ejecuta en segundo plano.

Troyanos ICMP

Esto se estudia precisamente para conocer que se puede crear troyanos de todo tipo.

Ejemplo: icmpsend (old)

Troyanos de acceso remoto

Trabaja como un acceso al escritorio. El hacker consigue un acceso GUI completo al sistema remoto.

Ejemplo

1. Se infecta el equipo con "server.exe" y planta un Reverse Connecting Trojan.
2.- El troyano conecta el puerto 80 al atacante y establece una conexión reversa
3.- El atacante tiene el control total sobre el equipo.

Ejemplo: Beast, RAT DarkComet, Apocalypse

Troyanos CCTT (Covert Channel Tunneling Trojan)

1. Presenta varias técnicas de explotación, creando canales de transferencia de datos arbitrarias para enviar streams autorizados por un sistema de control de acceso a la red.
2. Habilita a los atacantes de obtener shell externa del servidor desde una red interna y viceversa.
3. Utiliza TCP/UDP/HTTP CONNECT|POST channel permitiendo TCP data streams (SSH, SMTP, POP, etc) entre el servidor externo y el interno.

Troyanos E-banking

Intercepta información de la cuenta de la víctima antes de que se cifre y la envía al comando del troyano del atacante y el centro de control.

Ejemplo: ZeuS

Troyanos destructivos

Peligrosos. Cuando se ejecutan destruyen el S.O. El usuario no podrá iniciar el S.O. Formatea todos las unidades locales y de red.

Troyanos de notificación

Envía la locación del IP de la víctima, cuando la víctima se conecta, el atacante recibe la notificación.

Troyanos de tarjetas de crédito

Tienen un propósito, el de robar la información de la tarjeta de crédito de las víctimas. Engaña a los usuarios con sitios web de bancos falsos para que estos ingresen su información. Los servidores transmiten los datos robados a hackers remotos utilizando mail, FTP, IRC, etc.

Troyanos Data Hiding (Troyanos encriptados)

Son difíciles de detectar, puesto que están encriptados o cifran información en el sistema, cifran comunicaciones.

Troyano de Blakberry: PhoneSnoop

Activa remotamente el micrófono de los blackberry escuchando sonidos alrededor.

Troyano MAC OS X: DNSChanger

Le dice al usuario que se descargó un códec que al instalarlo hace un DNS Poison. Incluso luego ejecuta un video para que no haya sospecha. Posteriormente el atacante es notificado mediante un HTTP Post message que el equipo fue infectado. Los hackers toman control total del equipo de la víctima.

Otro Troyano para MAC es el Hell Raiser

Como detectar Troyanos

1. Escaneando puertos sospechosos

netstat -an

netstat -anb

Además muestra los binarios que están utilizando los puertos

Otras Herramientas: IceSword, CurrPorts, TCPView (GUI)

Como detectar Troyanos

2. Escaneando Procesos sospechosos

Por ejemplo vemos que iexplore.exe está en ejecución pero no está abierto... sospechoso

Otro ejemplo, spytector keylogger (o algo así) utiliza al navegador y mailer por defecto para enviar sus logs. El firewall nunca se dará cuenta porque las aplicaciones son legítimas.

Herramientas: What's Running, etc.

Como detectar Troyanos

3. Escaneando entradas al registro sospechosas

Windows ejecuta automáticamente instrucciones en las siguientes secciones del registro:

HKEY_CURRENT_USER

HKEY_LOCAL_MACHINE

Que contienen: Run, RunServices, RunServicesOnce, HKEY_CLASSES_ROOT\exefile\shell\open\command "%" %*

Como detectar Troyanos

4. Escaneando Controladores de dispositivo sospechosos

Los Troyanos del tipo drivers son generalmente descargados de fuentes no confiadas. Escanear y verificar que los dispositivos son de una fuente original o sitio original.

Herramientas: DriverView

Como detectar Troyanos

5. Escaneando Servicios de Windows sospechosos

Permite a los atacantes generar servicios de Windows permitiéndoles tener control remoto sobre el equipo de la víctima y pasar instrucciones maliciosas. Los troyanos renombran sus procesos para parecer servicios originales de Windows de esa manera impedir detección.

Los troyanos emplean técnicas rootkit para manipular HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services para esconder sus procesos.

Herramientas: Windows Service Manager (SrvMan)

Como detectar Troyanos

6. Escaneando programas sospechosos de inicio

Primero revisar la carpeta Inicio para ver accesos directos de los programas que se inician automáticamente. Revisar los servicios de Windows que se inician automáticamente. Revisar los programas de inicio en el registro. Revisar controladores que se cargan automáticamente. Revisar el inicio del Explorer

Como detectar Troyanos

Entradas del registro con relación al inicio:

Explorer Startup Setting

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders, Common Startup

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders, Common Startup

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders, Startup

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders, Startup

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows, load

Como detectar Troyanos

Windows Startup Setting

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce

HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce

Como detectar Troyanos

IE Startup Setting

HKCU\Software\Microsoft\Internet Explorer\UrlSearchHooks

HKLM\Software\Microsoft\Internet Explorer\Toolbar

HKLM\Software\Microsoft\Internet Explorer\Extensions

HKCU\Software\Microsoft\Internet Explorer\MenuExt

Como detectar Troyanos

Herramientas: Starter, Security AutoRun, What's Running? 2.2

Como detectar Troyanos

7. Escaneando archivos y carpetas sospechosas

Los troyanos normalmente modificar los archivos y carpetas del sistema. Utilice estas herramientas para detectar los cambios.

, WinMD5

Como detectar Troyanos

FCIV: Es una aplicación de línea de comandos que computa los hashes (MD5 o SHA1) de los archivos.

Tripwire: Sistema de clase empresarial verificador de integridad que escanea y reporta archivos del sistema críticos cambiados.

Sigverif: Revisa la integridad de los archivos críticos que son firmados digitalmente por Microsoft.

Otras herramientas: FastSu

Como detectar Troyanos

8. Escaneando actividades de red sospechosas

Se debe revisar puertos, tanto puertos no permitidos o comunes, como permitidos o comunes.

La herramienta Capsa Network Analyzer es una herramienta intuitiva, que provee información detallada para ayudar a revisar si hay actividades troyanas en la red.

Contramedidas para los troyanos

1. Evitar descargar y ejecutar aplicaciones de fuentes no confiadas.
2. Evitar abrir archivos adjuntos por mail de remitentes no conocidos.
3. Instalar parches de seguridad y actualizaciones para los S.O. y aplicaciones
4. Escanear CDS, DVDs, Discos, USB con antivirus

Contramedidas para los troyanos

5. Evitar aceptar programas transferidos por programas de mensajería.
6. Bloquear puertos innecesarios en el equipo y firewall
7. Fortalecer las configuraciones débiles por defecto.
8. Deshabilitar funcionalidades que no se utilizan, incluyendo protocolos y servicios
9. Evitar ejecutar aplicaciones, scripts, etc. a ciegas.

Contramedidas para los troyanos

10. Monitorear el tráfico interno de la red de puertos extraños o tráfico encriptado.
11. Administrar los archivos de integridad del sistema realizando revisiones, auditorías y escaneo de puertos
12. Ejecutar versiones locales de antivirus, firewall e IDS.
13. Restringir permisos entre los ambientes de escritorio para prevenir la instalación de aplicaciones maliciosas. *(cont.)*

Contramedidas para los troyanos

Y especialmente ¡EDUCAR A LOS USUARIOS!

Contramedidas para los troyanos

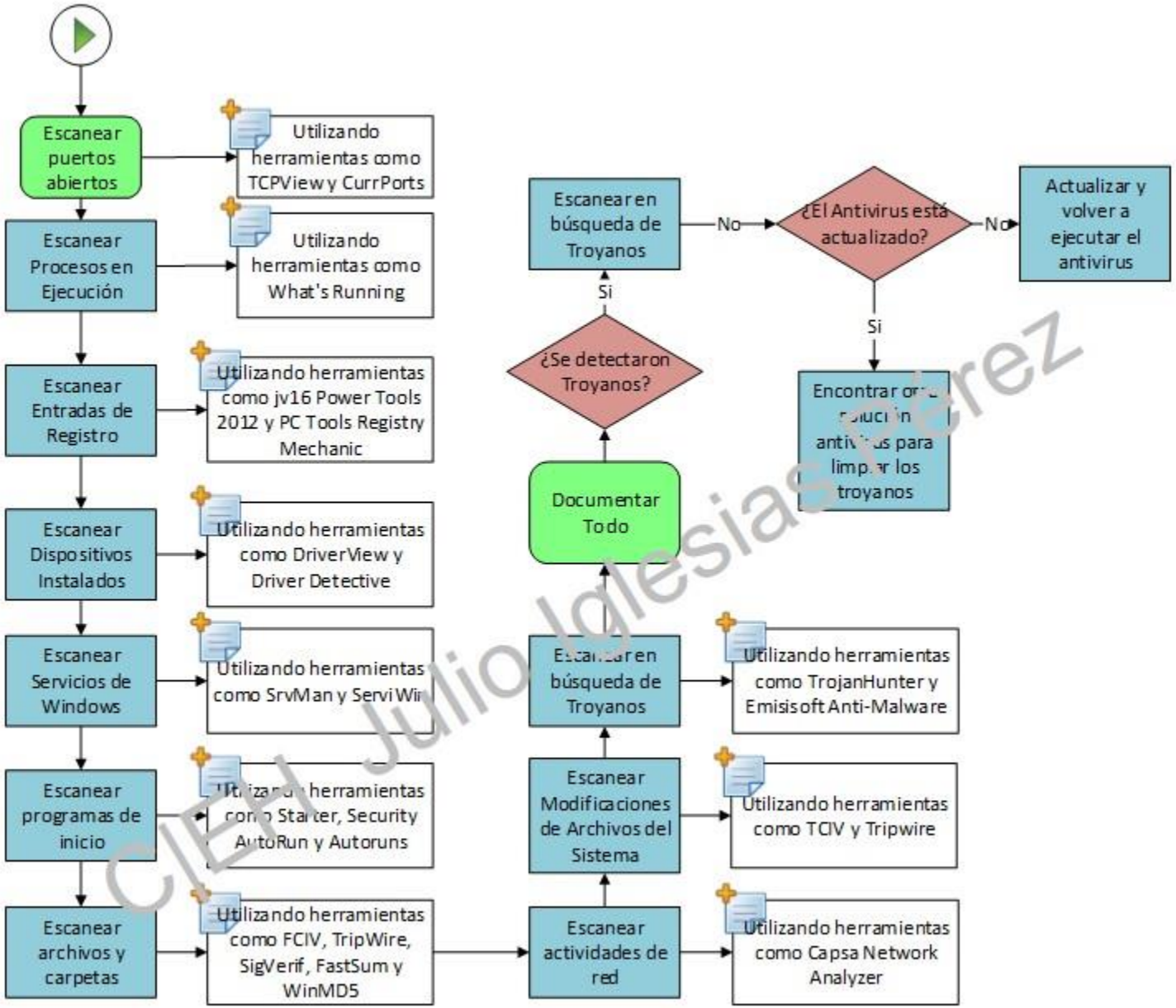
Trojan Horse Contruction Kit

Ayuda a los atacantes a crear sus propios troyanos. Estas herramientas pueden ser peligrosas si no se ejecutan apropiadamente. También pueden ser detectadas puesto que utilizan código redundante.

Software Anti-Troyano

TrojanHunter, Emsisoft Anti-Malware, etc.


Test de Intrusión para Troyanos
C|EH
Julio Iglesias




¡Muchas Gracias!
C|EH Julio Iglesias Perez