Malware World Edición I

BY ANTRAX

Contacto: antrax.labs@gmail.com

Introducción:

Hola a todos soy ANTRAX, en esta ocasión iré haciendo varias ediciones hablando sobre los malwares en general.

En esta primera edición estudiaremos definiciones generales, que servirán en un futuro para podernos ubicar mejor en el tema.

Todos aquellos que quieran colaborar con futuras ediciones que tratare de sacar lo mas seguido que pueda, ustedes pueden contactarme por mail y así poder trabajar en conjunto para entregar estas revistas lo más rápido y completas posibles. Por supuesto que aparecerán los créditos de todos los colaboradores interesados

Con gusto resolveré sus dudas e inquietudes en caso de que las tengan si las envían por mail.

Les dejare unos links que podrán usar como fuente para ampliar sus conocimientos, y para poder resolver dudas de manera rápida.

http://antrax-labs.blogspot.com: Mi Blog, Encontraran información sobre programación, malwares, Telefonía móvil y fija, Hacking, Trucos, Descargas, Juegos de Hacking, Novedades, Noticias, Los mejores video tutoriales de la red, Modding – Overlocking, entre otras cosas de interés.

http://foro.infiernohacker.com: En mi opinión el mejor Foro de hacking general de la red. Me verán por ahí con rango de colaborador ayudando en todo lo posible a los administradores con proyectos y a los usuarios con sus dudas. A demás de esto, es un gran foro con muy buena gente de cada rincón del mundo interesados en el hacking.

Quiero aprovechar para resaltar la gran labor de los administradores de este foro, Skywalker, Pasqui y TXS. Personas muy responsables y con un gran nivel ético, a demás de eso son grandes personas. No quiero dejar de lado tampoco al Staff que es bastante movedizo y anda constantemente en proyectos interesantes. Estoy muy agradecido y contento de poder pertenecer a esa comunidad

http://indetectables.net/foro: Sin dudas el mejor foro de malwares de la red, posee un gran grupo de personas desarrolladoras de programas, diariamente se publican mods de Crypters y otras aplicaciones muy útiles. Tiene usuarios de medio y alto nivel. Es notable lo rápido que aprenden los novatos de ese foro gracias a los moderadores y administradores que siempre están disponibles para aclarar dudas. Quiero darles las gracias a Polifemo y a Verbal por recibirme con los brazos abiertos en su comunidad y resaltar el gran nivel que poseen los administradores DSR/Shimpei y 4n0nym0us.

Sin nada mas que decir, ya podemos ponernos en marcha con las definiciones a tener en cuenta.

Definiciones:

Comenzaremos nombrando y definiendo las diferentes ramas que posee este gran mundo lleno de misterios, en mi opinión siempre hay que comenzar por aquí, para saber que cosas nos interesan y que cosas nos llaman la atención para aprender.

HACKER:

Persona que posee habilidades con los ordenadores, por lo general son programadores, o personas de gran nivel y conocimiento en alguna de sus ramas.

Dentro de estos hay subdivisiones, existen criterios para clasificarlos según su ética. Esta el Hacker de sombrero blanco, sombrero gris y sombrero negro.

El hacker de sombrero blanco: es el administrador de sistemas, o el experto de seguridad, que tiene una ética muy alta y utiliza sus conocimientos para evitar actividades ilícitas. Por lo general se encarga de la seguridad y no hace daños ni cosas perjudiciales a los demás.

El hacker de sombrero gris: no se preocupa mucho por la ética, sino por realizar su trabajo, si necesita alguna información o herramienta y para ello requieren penetrar en un sistema de computo, lo hace, además disfruta poniendo a prueba su ingenio contra los sistemas de seguridad, sin malicia y difundiendo su conocimiento, lo que a la larga mejora la seguridad de los sistemas.

El hacker de sombrero negro: Es aquel que no le interesa ayudar ni colaborar. Posee conocimientos pero no los usa para actos buenos. No le importan los daños que pueda causar en sistemas a los que penetra.

Definitivamente no posee ética, y hace lo que desea sin importar consecuencias ni daños que pueda causar.

CRACKER

Existen dos formas de definirlo. Por un lado están los que dicen que rompen la seguridad en sistemas y programas que es la mas acertada. Y por otro lado los que dicen que son personas dañinas que destrozan todo lo que encuentran a su paso con virus y herramientas que desarrollan.

PHREAKER

Son aquellos con habilidades en la telefonía móvil como en la telefonía fija. Son los que hacen pinchados de líneas, clonaciones de teléfonos, escuchas telefónicas, flasheos de teléfonos móviles, liberaciones, entre otras cosas.

SAMURAI

Son Personas que poseen gran nivel contratados por el gobierno para proteger sistemas en empresas o gubernamentales.

NEWBIE

Es aquel que recién se inicia en el mundo del hacking y posee pocos conocimientos. Suele ser principiante, pero no ignorante

LAMMER

Sinónimo de LUSER=LOOSER+USER Personas ignorantes, que utilizan lo poco que saben para hacer daños. Utilizan programas hechos para hacerse pasar por hackers y demostrar que saben.

Script Kiddies

Personas que poseen pocos conocimientos y utilizan herramientas hechas por los demás, a veces los usan para realizar ataques y otras para uso personal.

PROGRAMER - CODER

Personas con capacidad de poder desarrollar sus propios programas.

CARDER

Persona que se dedica al falsificado o robo de tarjetas de crédito

BANKING

Personas que se dedican al robo de las cuentas y transacciones bancarias.

Teniendo en cuenta las definiciones anteriormente definidas, ahora podemos pasar a las que veremos normalmente en el mundo de los malwares.

Modders: Proviene de modificar o moldear algún programa, en nuestro caso, son aquellos que modifican Crypters, Binders, Stubs, entre otras herramientas.

Coders: Aquellos que desarrollan sus propios malwares o herramientas

Malware: Programa malicioso y dañino.

Troyano: El nombre proviene del caballo de Troya. Programa que se queda residente en un sistema informático y facilita información sobre los que ocurre en el mismo (passwords, logins, etc.). También es aplicable a programas que parecen normales y al ejecutarse despiertan un virus que se introduce en el sistema. Se divide en dos partes, Cliente y Servidor.

Server: (Servidor) Ejecutable que se envía a nuestro objetivo con el fin de infectarlo y obtener información.

Cliente: Es aquel que usaremos nosotros para podernos conectar al servidor enviado a nuestro objetivo para poderlo manipular.

Crypter: Archivo ejecutable que se encarga de encriptar el contenido de nuestro servidor para evitar ser detectado por los AVs.

AVs: Forma abreviada de Anti Virus.

Enrutador: (Router) Un Router es un dispositivo para la interconexión de redes informáticas que permite asegurar el enrutamiento de paquetes entre redes o determinar la ruta que debe tomar el paquete de datos. Lo usaremos en los troyanos para abrir puertos.

Puertos: Son abiertos en routers para poder establecer un puente de conexión y enviar paquetes de datos por el.

IP: Conjunto de protocolos básico sobre los que se fundamenta Internet. Se sitúan en torno al nivel tres y cuatro del modelo OSI. En otras palabras es una serie de números que nos identifica en internet.

DNS: Alternativa a la IP, una de las más utilizadas son NO-IP y DNS de CDMON para la conexión de troyanos en caso de que no se tenga una IP estable.

Virus: Código malicioso con la capacidad de dañar una PC.

Stub: Corazón de un ejecutable, es en donde contiene toda la información que lo hace funcionar.

VIRII: Programación de Virus

Edición Hexadecimal: Se lo llama a la modificación hexadecimal de archivos ejecutables para evitar ser detectados.

Registro del sistema: Es en donde se guarda todo lo que debe hacer el sistema. Los malwares se añaden en el registro para iniciar junto con el sistema operativo. Esto ocurre en la plataforma Windows.

EOF Data: "End of file" o EOF (Final de código en español), es conocido como una herramienta vista en ejecutables como los Crypters, y q ayuda a los ejecutables que terminan con código a no deformarse cuando se encriptan.

Spread: Métodos o formas de propagación de los malwares.

Binders – Joiners: Programas que sirven para unir o camuflajear nuestros servidores para que pasen desapercibidos.

Bomba lógica: Código que ejecuta una particular manera de ataque cuando una determinada condición se produce. Por ejemplo una bomba lógica puede Formatear el disco duro un día determinado, pero a diferencia de un virus.

Backdoor: Puerta trasera. Mecanismo que tiene o que se debe crear en un software para acceder de manera indebida.

Gusanos o Worms: Programas que se reproducen ellos mismos copiándose una y otra vez de sistema a sistema y que usa recursos de los sistemas atacados.

Ingeniería Social: Obtención de información por medios ajenos a la informática. En otras palabras la Ingeniería Social hace referencia a usar la cabeza.

Tracear: Seguir un rastro o pista para dar con una persona.

Bonet: Gusano que se propaga con la finalidad de ganar muchas PCs zombies que luego son utilizadas para atacar servidores webs.

Un poco de historia:

Se denomina troyano (o caballo de Troya, traducción fiel del inglés Trojan horse aunque no tan utilizada) a un programa malicioso capaz de alojarse en computadoras y permitir el acceso a usuarios externos, a través de una red local o de Internet, con el fin de recabar información o controlar remotamente a la máquina anfitriona.

Un troyano no es en sí un virus, aún cuando teóricamente pueda ser distribuido y funcionar como tal. La diferencia fundamental entre un troyano y un virus consiste en su finalidad. Para que un programa sea un "troyano" solo tiene que acceder y controlar la máquina anfitriona sin ser advertido, normalmente bajo una apariencia inocua. Al contrario que un virus, que es un huésped destructivo, el troyano no necesariamente provoca daños porque no es su objetivo.

Suele ser un programa alojado dentro de una aplicación, una imagen,

un archivo de música u otro elemento de apariencia inocente, que se instala en el sistema al ejecutar el archivo que lo contiene. Una vez instalado parece realizar una función útil (aunque cierto tipo de troyanos permanecen ocultos y por tal motivo los antivirus o anti troyanos no los eliminan) pero internamente realiza otras tareas de las que el usuario no es consciente, de igual forma que el Caballo de Troya que los griegos regalaron a los troyanos.

Habitualmente se utiliza para espiar, usando la técnica para instalar un software de acceso remoto que permite monitorizar lo que el usuario legítimo de la computadora hace (en este caso el troyano es un spyware o programa espía) y, por ejemplo, capturar las pulsaciones del teclado con el fin de obtener contraseñas (cuando un troyano hace esto se le cataloga de keylogger) u otra información sensible.

La mejor defensa contra los troyanos es no ejecutar nada de lo cual se desconozca el origen y mantener software antivirus actualizado y dotado de buena heurística; es recomendable también instalar algún software anti troyano, de los cuales existen versiones gratis aunque muchas de ellas constituyen a su vez un troyano. Otra solución bastante eficaz contra los troyanos es tener instalado un firewall.

Otra manera de detectarlos es inspeccionando frecuentemente la lista de procesos activos en memoria en busca de elementos extraños, vigilar accesos a disco innecesarios, etc.

Lo peor de todo es que últimamente los troyanos están siendo diseñados de tal manera que, es imposible poder detectarlos excepto por programas que a su vez contienen otro tipo de troyano, inclusive y aunque no confirmado, existen troyanos dentro de los programas para poder saber cual es el tipo de uso que se les da y poder sacar

mejores herramientas al mercado llamados también "troyanos sociales"

Los troyanos están actualmente ilegalizados, pero hay muchos crackers que lo utilizan.

Las cuatro partes de los troyanos

Los troyanos están compuestos principalmente por dos programas: un cliente (es quién envía las funciones que se deben realizar en la computadora infectada) y un servidor (recibe las funciones del cliente y las realiza, estando situado en la computadora infectada). También hay un archivo secundario llamado Librería (con la extensión *.dll)(pero que no todos los troyanos tienen de hecho los más peligrosos no lo tienen) que es necesaria para el funcionamiento del troyano pero no se debe abrir, modificar ni eliminar. Algunos troyanos también incluyen el llamado EditServer, que permite modificar el Servidor para que haga en el ordenador de la víctima lo que el hacker quiera.

Troyanos de conexión directa e inversa

Los troyanos de conexión directa son aquellos que hacen que el cliente se conecte al servidor; a diferencia de éstos, los troyanos de conexión inversa son los que hacen que el servidor sea el que se conecte al cliente; las ventajas de éste son que traspasan la mayoría de los firewall y pueden ser usados en redes situadas detrás de un Router sin problemas. El motivo de por qué éste obtiene esas ventajas es que la mayoría de los firewall no analizan los paquetes que salen de la computadora infectada, pero que sí analizan los que entran (por eso los troyanos de conexión directa no poseen tal ventaja); y se

dice que traspasan redes porque no es necesario que se redirijan los puertos hacia una computadora que se encuentre en la red.

Tipos de troyanos

Los troyanos, a pesar de haber algunos ejemplos inofensivos, son casi siempre diseñados con propósitos dañinos. Se clasifican según la forma de penetración en los sistemas y el daño que pueden causar. Los ocho tipos principales de troyanos según los efectos que producen son:

- Acceso remoto
- Envío automático de e-mails
- Destrucción de datos
- Troyanos proxy, que asumen ante otras computadoras la identidad de la infectada
- Troyanos FTP (que añaden o copian datos de la computadora infectada)
- Deshabilitador es de programas de seguridad (antivirus, cortafuegos…)
- Ataque DOS a servidores (denial-of-service) hasta su bloqueo.
- Troyanos URL (Que conectan a la máquina infectada a través de conexiones de módem, normalmente de alto coste)

Algunos ejemplos de sus efectos son:

• Borrar o sobrescribir datos en un equipo infectado.

• Cifrar archivos de la máquina, llevando al usuario al pago para recibir un código que le permita descifrarlos.

• Corromper archivos

• Descargar o subir archivos a la red.

• Permitir el acceso remoto al ordenador de la víctima. (Herramientas de administración remota o R.A.T)

• Reproducir otros programas maliciosos, como otros virus informáticos. En este caso se les denomina 'droppers' o 'vectores'.

• Crear redes de 'computadoras zombie' infectadas para el lanzamiento de ataques de denegación de servicio contra servidores (DDoS) de forma distribuida entre varios equipos o envío de correo no deseado (spam).

• Espiar y recolectar información sobre un usuario y enviar de incógnito los datos, como preferencias de navegación y estadísticas a otras personas (Véase el artículo sobre software espía – spyware)

• Tomar capturas de pantalla en determinados momentos para saber lo que está viendo el usuario y así capaz detectar las contraseñas que se escriben en los teclados virtuales.

• Monitorizar las pulsaciones de teclas para robar información, nombres de usuario, contraseñas o números de tarjetas de crédito (keyloggers).

• Engañar al usuario mediante ingeniería social para conseguir sus datos y números bancarios y otros datos de su cuenta que pueden ser usados para propósitos delictivos.

• Instalación de puertas traseras en una computadora.

• Control de funciones físicas del equipo, como la apertura y cierre de los lectores de discos.

• Recolectar direcciones de correo electrónico y usarlas para enviar correo masivo o spam.

• Reiniciar el equipo cuando se ejecuta el programa.

Precauciones para protegerse de los troyanos.

En definitiva, se puede considerar a los troyanos un tipo de virus informáticos, y el usuario final se puede proteger de ellos de modo similar al que lo haría de otro cualquiera. Los virus informáticos pueden causar grandes daños a ordenadores personales, pero este aún puede ser mayor si se trata de un negocio, particularmente negocios pequeños que no pueden tener la misma capacidad de protección contra virus que pueden permitirse las grandes empresas. Una vez que un troyano se ha ocultado en un equipo, es más complicado protegerse de él, pero aún así hay precauciones que se pueden tomar.

La forma de transmisión más común de los troyanos en la actualidad es el correo electrónico, al igual que muchos otros tipos de virus. La única diferencia con ellos es que los troyanos suelen tener mayor capacidad para ocultarse. Las mejores maneras de protegerse contra los troyanos son las siguientes:

1. Si recibes un correo electrónico de un remitente desconocido con datos adjuntos también sin identificar, nunca lo abras. Como usuario de correo electrónico deberías confirmar la fuente de la que proviene cualquier correo. Algunos crackers roban la lista de direcciones de otros usuarios, así que en algunos casos a pesar de que conozcas al remitente del mensaje, no por ello es necesariamente seguro.

2. Cuando configures tus programas cliente de correo electrónico, asegúrate de desactivar la apertura automática de datos adjuntos a los mensajes, de modo que puedas decidir cuando abrirlos y cuando no. Algunos clientes de correo electrónico vienen de fábrica con programas antivirus que escanean los datos adjuntos antes de ser abiertos, o se pueden sincronizar con antivirus que tengas instalados para hacer esto. Si tu cliente no tiene esa posibilidad, quizás sea el momento de comprar otro o descargar uno gratuito que sí pueda hacerlo.

3. Asegúrate también de que dispones en tu equipo de un programa antivirus actualizado regularmente para estar protegido contra las últimas amenazas en este sentido. Actualmente, la mayoría incluye la opción de actualizarse automáticamente. Esta debería estar activada para que el antivirus aproveche nuestras conexiones a internet para descargar las últimas actualizaciones e instalarlas. De este modo,

también se actualizará aunque te olvides de hacerlo.

4. Los sistemas operativos actuales ofrecen parches y actualizaciones de seguridad a sus usuarios para protegerlos de determinadas vulnerabilidad es de seguridad descubiertas tras su salida al mercado, bloqueando las vías de expansión y entrada de algunos troyanos. Llevando al día estas actualizaciones de seguridad del fabricante del sistema operativo, tu equipo será mucho menos vulnerable ante los troyanos.

5. Evita en lo posible el uso de redes peer-to-peer o P2P redes de compartición de archivos como eMule, Kazaa, Limewire, Ares, Imesh o Gnutella porque generalmente están desprotegidos de troyanos y virus en general y estos se expanden utilizándolas libremente para alcanzar a nuevos usuarios a los que infectar de forma especialmente sencilla. Algunos de estos programas ofrecen protección antivirus, pero normalmente no suele ser lo suficientemente fuerte. Si aún así usas redes de este tipo, suele ser bastante seguro evitar descargarte archivos calificados como canciones, películas, libros o fotos "raras", desconocidas o maquetas no publicadas etc.

¿Cómo eliminar un troyano si ya estás infectado?

A pesar de estas precauciones, también es recomendable instalar en los sistemas programas anti-troyano, de los cuales la mayoría son gratuitos o freeware, sobre todo teniendo en cuenta el uso tan amplio que ahora mismo hay de internet y la cantidad de datos personales que proteger de personas y programas malintencionad os.

Formas de infectarse con troyanos

La mayoría de infecciones con troyanos ocurren cuando se engaña al usuario para ejecutar un programa infectado – por ello se avisa de no abrir datos adjuntos de correos electrónicos desconocidos -. El programa es normalmente una animación interesante o una foto llamativa, pero tras la escena, el troyano infecta la computadora una vez abierta, mientras el usuario lo desconoce totalmente. El programa infectado no tiene por qué llegar exclusivamente en forma de e-mail. Puede ser enviado en forma de mensaje instantáneo, descargado de una página de internet o un sitio FTP, o incluso estar incluido en un CD o un diskette (La infección por vía física es poco común, pero de ser un objetivo específico de un ataque, sería una forma sencilla de infectar tu sistema) Es más, un programa infectado puede venir de alguien que utiliza tu equipo y lo carga manualmente. Las probabilidades de recibir un virus de este tipo por medio de mensajería instantánea son mínimas, y normalmente, como se ha dicho, el modo más común de infectarse es por medio de una descarga.

Por medio de sitios web: Tu ordenador puede infectarse mediante visitas a sitios web poco confiables.

Correo electrónico: Si usas Microsoft Outlook, eres vulnerable a la mayoría de problemas de protección contra programas de este tipo que tiene Internet Explorer, incluso si no usas IE directamente.

Puertos abiertos: Los ordenadores que ejecutan sus propios servidores (HTTP, FTP, o SMTP, por ejemplo), permitiendo la compartición de archivos de Windows, o ejecutando programas con capacidad para compartir archivos, como los de mensajería instantánea (AOL's AIM, MSN Messenger, etc.) pueden tener vulnerabilidad es similares a las descritas anteriormente. Estos

programas y servicios suelen abrir algún puerto de red proporcionando a los atacantes modos de interacción con estos programas mediantes ellos desde cualquier lugar. Este tipo de vulnerabilidad es que permiten la entrada remota no autorizada a los sistemas se encuentran regularmente en muchos programas, de modo que estos deberían evitarse en lo posible o asegurarse de que se ha protegido el equipo mediante software de seguridad.

Se pueden usar un determinado tipo de programas llamados cortafuegos para controlar y limitar el acceso a los puertos abiertos en un equipo. Los cortafuegos se utilizan ampliamente y ayudan a mitigar los problemas de entrada remota de troyanos por medio de puertos de red abiertos, pero en cualquier caso no existe ninguna solución perfecta e impenetrable.

Algunos troyanos modernos se distribuyen por medio de mensajes. Se presentan al usuario como mensajes de aspecto realmente importante o avisos críticos del sistema, pero contienen troyanos, en los que el archivo ejecutable es el mismo o aparenta ser el propio sistema operativo, ayudando a su camuflaje. Algunos procesos de este tipo son:

- Svchost32.exe
- Svhost.exe
- back.exe

Métodos de borrado

Debido a la gran variedad de troyanos existente, su borrado no se realiza siempre del mismo modo. La forma normal de borrar muchos troyanos adquiridos a través de internet es borrar los archivos temporales, o encontrar el archivo y borrándolo manualmente, tanto en modo normal como en el modo seguro del sistema operativo. Esto es porque muchos troyanos se camuflan como procesos de sistema que este no permite "matar" manualmente si se encuentran en ejecución. En algunos casos también se hace necesario editar el registro y limpiarlo de todas las entradas relativas al troyano, puesto que algunos tienen la habilidad de copiarse automáticamente a otros emplazamientos en el sistema, como carpetas con archivos de sistema que el usuario normalmente no suele visitar y donde hay una gran cantidad de archivos entre los que camuflarse a los ojos de este, además de introducir entradas en el registro para ejecutarse automáticamente al arrancar el sistema o bajo determinadas condiciones. En caso de tener que limpiar el registro de estas entradas, bajo Windows, vaya a Inicio > Ejecutar > regedit y borre o repare cualquier entrada que el troyano haya introducido o corrompido en el registro.

Espero que les sea útil, en la segunda edición comenzaremos viendo lo que es la NO-IP y para que se la utiliza.

Las dudas como bien dije antes, pueden hacerlas por mail.

Es probable que no las tengan con esta primera parte debido a que es solo teoría, pero si quedo alguna definición colgando, pueden decirme y yo tratare de hacer todo lo que pueda para resolvérselas.

No es obligación saberse todo esto, simplemente para que vean el funcionamiento de las cosas, o por si encuentran algún día alguna palabra extraña, puedan acudir aquí para entenderla.

Saludos! Y hasta la próxima!