M-ZINE I

Malware Magazine #1

Tema: Historia e introducción a los Malwares

ANTRAX

www.antrax-labs.net

Tipos de hackers

Existen dos grandes grupos de hackers, aunque también hay uno intermedio. Estos grupos están divididos según la forma de pensar que tienen los individuos a la hora de interactuar con un remoto.

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.

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.

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.

Ética Hacker

¿Qué es la ética Hacker?

Se denomina Ética Hacker a la actitud que se tiene a la hora de entrar a un sistema. Cuando digo actitud, hago referencia a el grado de maldad que se puede llegar a tener en cuanto a la producción de daños que se pueden ocasionar una vez dentro.

Es de poca ética entrar a un sistema y dañarlo con malas intensiones.

Volcando esto en los Malwares, podemos decir que es poco ético entrar a una PC y destrozarlo sin tener una buena finalidad.

Por lo general cuando se entra a una PC es para robar cierto tipo de información, espiar conversaciones de chats, revisar correos, pero nunca para borrar documentación, a menos de que esa información sea muy intima. Por ejemplo fotos muy personales, archivos nuestros, etc.

Cuando hablo de borrar, hago referencia a subir un virus al PC remoto con la finalidad de dañarlo.

Por lo general cuando alguien entra a un sistema, modifica o borra información o rastros que dejo con un zapper, para evitar ser traceado.

Lo ideal es encontrar una falla de seguridad en un sistema y reportarlo para que sea reparado antes de que ese bug caiga en manos equivocadas y puedan ocasionar daños severos.

¿Qué significa la palabra Malware?

La palabra Malware viene del ingles **Mal**icious Soft**ware**, hace referencia a programas o scripts que afectan a nuestro ordenador y que puedan llegar a dañarlo.

Estos daños pueden afectar tanto al Software, como al Hardware. El nivel del daño lo determina el lenguaje con el cual fue programado el Malware y el nivel del programador, y por supuesto la finalidad con la cual fue creado.

Muchas veces decimos que un Malware es dañino, pero esto no siempre es así. Por ejemplo los Stealers, son Malwares diseñados únicamente para robar logs o passwords almacenadas en un ordenador y tienen la capacidad de enviarnos esos logs por mail o a un FTP propio. No quiero entrar en detalle con esto, ya que en las próximas entregas le hare una especial para hablar de esto. Lo que nos interesa ahora, es saber diferenciar los tipos y finalidades de los Malwares.

Definiciones

Malware: Programa malicioso que puede o no dañar nuestro ordenador

Modder: Persona que modifica el Stub de algún Malware para volverlo indetectable.

Codder: Persona que programa o crea sus propios Malwares o herramientas.

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.). El troyano consta de 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.

Regedit: 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.

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

webs.

Remoto: Se denomina remoto al ordenador de la persona infectada con un troyano.

Keylogger: Programa diseñado para capturar teclas pulsadas por un teclado.

Clicklogger: Programa diseñado para capturar Clicks del mouse.

Filemanager: Opción que traen los troyanos que sirve para subir, bajar, borrar, modificar archivos de nuestro remoto

ScreenCapture: Captura de pantalla.

Escritorio Remoto: Permite manipular el Teclado y Mouse de nuestro Remoto.

Remote Shell: Shell remota, nos deja ejecutar comandos de consola en nuestro remoto.

Cam Capture: Captura de Webcam (permite ver la webcam de nuestro remoto en caso de que tenga).

System Manager: Permite ver propiedades del equipo remoto.

ClipBoard: Portapapeles, Esta opción se activa cada vez que el remoto copia algún texto.

Zapper o Cloacker: Programa utilizado para borrar huellas.

Proxy: Programa utilizado para escondernos en la red.

FTP: (File Transfer Protocol) Protocolo de transferencia de archivos. Se utiliza para subir y bajar archivos de un servidor de internet o viceversa.

LAN: Red de área local

Password: Contraseña

IRC: Chat antiguo, compuesto por servidores y canales. Utilizado para montar una Botnet.

Firewall: Utilizado para bloquear conexiones no deseadas.

Bug: agujero o falla de seguridad

Debbuger: programa que permite la ejecución de otros programas

Sniffer: Programa encargado de interceptar paquetes de datos con el fin de obtener información.

Rootkit: Son técnicas utilizadas para esconder un malware y evitar ser identificado.

FUD: Full UnDetected (indetectable al 100%)

UD: Undetected (Indetectable a ciertos antivirus)

En la próxima entrega la dedicaremos a saber que es un troyano. Como funciona, Los avances y características de cada uno.

Esto es todo por ahora.

Saludos!

ANTRAX