Hacker Highschool
SECURITY AWARENESS FOR TEENS

LECCIÓN 6
MALWARE

Hacker Highschool
SECURITY AWARENESS FOR TEENS

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

"License for Use" Information

The following lessons and workbooks are open and publicly available under the following terms and conditions of ISECOM:

All works in the Hacker Highschool project are provided for non-commercial use with elementary school students, junior high school students, and high school students whether in a public institution, private institution, or a part of home-schooling. These materials may not be reproduced for sale in any form. The provision of any class, course, training, or camp with these materials for which a fee is charged is expressly forbidden without a license including college classes, university classes, trade-school classes, summer or computer camps, and similar. To purchase a license, visit the LICENSE section of the Hacker Highschool web page at www.hackerhighschool.org/license.

The HHS Project is a learning tool and as with any learning tool, the instruction is the influence of the instructor and not the tool. ISECOM cannot accept responsibility for how any information herein is applied or abused.

The HHS Project is an open community effort and if you find value in this project, we do ask you support us through the purchase of a license, a donation, or sponsorship.

All works copyright ISECOM, 2004.

Información sobre la "Licencia de Uso"

Las lecciones y cuadernos de trabajo siguientes son de acceso público y están disponibles bajo las siguientes condiciones de ISECOM:

Todos los trabajos del proyecto "Hacker Highschool" son proporcionados para su uso no comercial con estudiantes de escuelas primarias, secundarias, bachilleratos y ciclos formativos dentro de las actividades académicas propias de la institución. Dichos materiales no pueden ser reproducidos con fines comerciales de ningún tipo. La impartición con estos materiales de cualquier clase, curso o actividad de formación para el que sea necesario pagar un importe, queda totalmente prohibida sin la licencia correspondiente, incluyendo cursos en escuelas y universidades, cursos comerciales o cualquier otro similar. Para la compra de una licencia visite la sección "LICENSE" de la página web del proyecto "Hacker Highschool" en www.hackerhighschool.org/license.
El proyecto HHS es una herramienta de aprendizaje y, como tal, la formación final debe proceder realmente de la influencia del instructor y no basarse únicamente en el uso de la herramienta.

ISECOM no puede aceptar bajo ningún concepto responsabilidad alguna sobre la forma de aplicar, ni sus consecuencias, de cualquier información disponible dentro del proyecto. El proyecto HHS es un esfuerzo de una comunidad abierta, por lo que si encuentra útil este proyecto le invitamos a patrocinarlo a través de la compra de una licencia, una donación o un patrocinio.

Todos los Derechos Reservados ISECOM, 2004.

Índice

Contribuciones

Simon Biles, Computer Security Online Ltd.

Kim Truett, ISECOM

Pete Herzog, ISECOM

Marta Barceló, ISECOM

Frank Craig, RAN Ingeniería de Sistemas SRL

Jaume Abella, La Salle URL - ISECOM

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

LA SALLE
Enginyeria
Arquitectura
Universitat Ramon Llull

6.0 Introducción

"Malware" son aquellos programas o partes de ellos que tienen un efecto malicioso en la seguridad de tu ordenador. Este término engloba muchas definiciones las cuales de seguro ya has oído hablar como "Virus", "Worm (gusano)" y "Trojan (troyano)" y otras de las que posiblemente no hayas oído hablar como "Rootkit", "Logicbomb (bomba lógica)" y "Spyware". Este capítulo presentará, definirá y explicará cada una de estas subclases de malware, brindará ejemplos y explicará algunas de las contramedidas que pueden ser puestas en práctica para restringir los problemas que causa el malware.

6.1 Virus

6.1.1 Introducción

Virus – este es el tipo de malware del cual la gente está más concienzada. La razón de que se conozca como "virus" es solamente histórica. Al mismo tiempo que se dio a conocer la aparición del primer virus informático los medios publicaban artículos acerca de la distribución del virus del SIDA. Los paralelismos que se daban entre ambos, la propagación debido a la interacción con un medio infectado, la dependencia de un medio transmisor y la eventual "muerte" de todo anfitrión infectado fomentaron esta definición. Este paralelismo hizo creer, y aún lo hace, que la gente podría llegar a infectarse con un virus informático.

6.1.2 Descripción

Los virus son programas auto replicantes que al igual que un virus biológico se adjuntan a otro programa, o en el caso de virus "macro" se adjuntan a otro archivo. El virus se ejecuta solamente cuando se ejecuta el programa o se abre el archivo infectado. Esto es lo que diferencia a los virus de los gusanos: si no se accede al programa o archivo entonces el virus no se ejecutará y por lo tanto no se replicará.

Existen distintos tipos de virus aunque la forma más común de encontrarlos hoy en día es en el formato "*virus macro*", mientras otros como los virus de sector de arranque (boot sector) sólo se encuentran en "cautividad".

6.1.2.1 Virus de Sector de Arranque (Boot Sector Viruses)

El virus de sector de arranque fue el primer virus en ser creado. Se esconde en el código ejecutable del sector de arranque de los discos de arranque, lo que significaba que para infectar un ordenador había que iniciarlo desde un diskette de arranque infectado. Hace mucho tiempo atrás (15 años aproximadamente) iniciar el ordenador desde un diskette de arranque era algo bastante usual, lo que significó que los virus se distribuían rápidamente, antes de que la gente se diera cuenta de lo que estaba ocurriendo. Este tipo de virus (y también los demás) deben dejar una marca digital para evitar que se infecte repetidamente el mismo objetivo. Es esta firma la que permite que ciertos programas (como por ejemplo los antivirus) detecten la infección.

6.1.2.2 Virus de Archivos Ejecutables

El virus de Archivos Ejecutables se adjunta a archivos del tipo .exe o .com. Algunos virus buscaban programas que formaran parte específicamente del sistema operativo y por ello se ejecutaban cada vez que se encendía el ordenador, aumentando así sus posibilidades de una exitosa propagación del virus. Existían unas cuantas maneras de adjuntar un virus a un archivo ejecutable, aunque algunas funcionaban mejor que otras. El método más simple y menos sutil era la de sobrescribir la primer parte del archivo con código de virus, lo que significaba que el virus se ejecutaba pero el resto del programa no funcionaba correctamente. Esto era una clara señal que había una infección – especialmente si el programa era una parte esencial del sistema operativo.

6.1.2.3 Virus Residentes en Memoria (Terminate and Stay Resident - TSR)

La sigla TSR viene del DOS y significa que un programa se carga en memoria y queda residente en segundo plano permitiendo al ordenador trabajar en primer plano de manera normal. Estos virus más avanzados podían interceptar llamadas al sistema operativo (system calls) que podrían exponer su existencia y respondían con respuestas falsas, evitando de esta manera su descubrimiento y/o limpieza. Otros se adjuntaban al comando 'dir' e infectaban todas las aplicaciones listadas en el directorio. Algunos hasta detenían (o borraban) los programas anti-virus.

6.1.2.4 Virus Polimórfico

Los primeros virus eran bastante fáciles de detectar ya que poseían una cierta firma digital dentro de ellos para evitar una re-infección o simplemente porque poseían una estructura específica que permitía su detección. Luego aparecieron los virus polimórficos. Poli (muchas) Mórficos (formas). Estos virus se modificaban cada vez que se replicaban, reordenando su código, cambiando de encriptación, generando un nuevo código que parecía totalmente distinto al original.

Esto creó un gran problema ya que las firmas a detectar eran cada vez más pequeñas y los más avanzados solo se detectaban mediante algoritmos que comparaban combinaciones. Esto se acentuó por la aparición de kits de generación de virus polimórficos que se distribuyeron en la comunidad de autores de virus que permitían generar cualquier virus como polimórfico.

6.1.2.5 Virus de Macro

Los virus de Macro hacen uso de la habilidad de muchos programas de ejecutar código. Los programas como Word y Excel poseen versiones de lenguaje de programación Visual Basic limitados en funciones pero muy poderosos. Esto permite la automatización de tareas repetitivas y la configuración automática de ciertos parámetros. Estos lenguajes de macros se utilizan maliciosamente para adosar código viral a los documentos los cuales copiarán el código viral a otros documentos, lo que resulta en una propagación del virus. Aunque Microsoft ha desactivado esa propiedad en las nuevas versiones, Outlook (el programa de correo) ejecutaba cierto tipo de código adosado a los mensajes de correo de manera automática apenas eran abiertos. Eso significaba que los virus se propagaban rápidamente enviándose a toda la lista de direcciones de correo que había en el ordenador infectado. Esto ya ha sido solucionado en las últimas versiones del producto.

Ejercicios:

1) Utilizando Internet intenta encontrar un ejemplo de cada tipo de virus definido previamente.

2) Investiga el virus Klez :

- ¿cual es su "carga destructiva" (payload)?

- el virus Klez es muy conocido por su técnica de SPOOFING. ¿Qué es SPOOFING y como es utilizado por el virus Eles?

- acabas de enterarte que tu ordenador está infectado con el virus Klez. Investiga como eliminar el virus.

3) Acabas de recibir un mensaje de correo con el asunto "Warning about your email account" (advertencia acerca de tu cuenta de correo). El cuerpo del mensaje explica que tu uso indebido del correo electrónico resultará en la pérdida de tus privilegios de Internet y que deberías ver el archivo adjunto para más información. Pero que a ti te conste tú no has hecho nada raro con el correo electrónico. ¿Sospechas? Deberías. Investiga esta información y determina que virus se encuentra adjunto al mensaje.

6.2 Gusanos

6.2.1 Introducción

Los Gusanos son antecesores a los Virus. El primer gusano fue creado muchos años antes del primer virus. Este gusano hacía un uso indebido del comando finger de UNIX para rápidamente detener el acceso a Internet (que era sustancialmente menor en esos días). La siguiente sección trata el tema de los gusanos.

6.2.2 Descripción

Un gusano es un programa que una vez ejecutado se replica sin necesidad de la intervención humana. Se propagará de anfitrión en anfitrión haciendo uso indebido de un servicio(s) desprotegido(s). Atravesará la red sin la necesidad de que un usuario envíe un archivo o correo infectado. Debes tener en cuenta que la mayoría de los sucesos que han aparecido en los medios últimamente se deben a gusanos y no a virus.

Ejercicios:

1) Utilizando Internet, intenta encontrar información del primer gusano que se haya creado.
2) Averigua cual es la vulnerabilidad que utilizan el gusano Code Red y Nimda para propagarse.

6.3 Troyanos y Spyware

6.3.1 Introducción

El primer Caballo de Troya fue creado por los Griegos hace miles de años (piensa en la película Troya si la has visto). El concepto básico es que dentro de un sistema que parece seguro se introduce algo malicioso pero disfrazado como sano. Este disfraz podrá ser desde el anticipo de un juego bajado de Internet hasta un mensaje de correo electrónico prometiendo imágenes pornográficas de tu celebridad preferida. Esta sección cubre en detalle los troyanos y el spyware.

6.3.2 Descripción

Los Troyanos son códigos maliciosos que intentan mostrarse como algo útil o apetecible para que uno lo ejecute. Una vez ejecutados intentarán instalar un backdoor o rootkit (ver sección

6.4), o aún peor, intentarán marcar un número de teléfono de acceso a Internet de alto coste, lo que te costará mucho dinero.

Spyware es código que se instala clandestinamente casi siempre de sitios de Internet que tú puedas visitar. Una vez instalado buscará en tu ordenador información que considere de valor. Esto podrán ser o estadísticas de tu utilización de Internet o hasta tu número de tarjeta de crédito. Algunas versiones de Spyware inadvertidamente se dan a conocer porque hacen aparecer avisos en tu escritorio de manera irritante.

Ejercicios:

1) Mediante Internet encuentra un ejemplo de troyanos y spyware.

6.4 Rootkits y Backdoors

6.4.1 Introducción

A menudo cuando un ordenador ha sido vulnerado por un hacker, él mismo intentará instalar un método para poder accederlo fácilmente a voluntad. Existen muchas variaciones de estos programas algunos de los cuales se han vuelto bastante famosos – ¡busca en Internet "Back Orifice" !

6.4.2 Descripción

Rootkits y backdoors son códigos maliciosos que elaboran metodologías para permitir el acceso a un ordenador. Van desde los más simples (un programa escuchando en un puerto determinado) hasta los más complejos (un programa que esconderá sus procesos en memoria, modificará los archivos de registros y escuchará en un puerto). A menudo un backdoor será tan simple como crear un usuario que tiene privilegios de super-usuario con la esperanza de que no se note. Esto se debe porque un backdoor está diseñado para evitar el control normal de autenticación de un sistema. Tanto el virus Sobig como el virus MyDoom instalan backdoors como parte de su carga destructiva.

Ejercicios:

1) Encuentra en Internet ejemplos de rootkits y backdoors.

2) Investiga acerca de "Back Orifice" y compara sus funcionalidades con las de los programas de acceso remoto promocionados por Microsoft.

6.5 Bombas Lógicas y Bombas de Tiempo

6.5.1 Introducción

Algunos programadores o administradores de sistemas pueden ser bastante peculiares. Se ha sabido de ciertos sistemas donde se han ejecutado algunos comandos en base a la ocurrencia de ciertas condiciones específicas. Por ejemplo: se puede crear un programa donde si el administrador no entra en el sistema en tres semanas él mismo empezará a borrar bits al azar del disco. En el año 1992 se dio un caso que cobró notoriedad en la compañía General Dynamics que involucró a un programador. El programador creó una bomba lógica que se activaría una vez que se fuera y que borraría información crítica. Él esperaba que la compañía le pagara una buena suma para volver y arreglar el problema. Sin embargo otro programador descubrió la bomba lógica antes que explotara y el programador malicioso fue sentenciado y multado con 5.000 US$. Aparentemente el juez fue benevolente ya que los cargos por los que fue sentenciado podían tener una sentencia de prisión y hasta 500.000 US$ de multa.

6.5.2 Descripción

Las Bombas lógicas y bombas de tiempo son programas que no poseen rutinas de replicación y no pueden crear accesos remotos, pero son o forman parte de aplicaciones que causarán daño o modificaciones a los datos si son activados. Pueden ser entes individuales o formar parte de gusanos o virus. Las bombas de tiempo están programadas para liberar su carga destructiva en un momento determinado. Las bombas lógicas están programadas para liberar su carga destructiva cuando ocurren determinados eventos. El principio de una bomba de tiempo también se puede aplicar en programaciones no maliciosas. Por ejemplo el concepto de bomba de tiempo nos permite evaluar un programa por un período de tiempo, normalmente treinta días, después del cual el programa cesa de funcionar. Este es un ejemplo de programación no maliciosa que involucra el concepto de bomba de tiempo.

Ejercicios:

1) ¿Que otros usos razonables (y legales) pueden darse a los conceptos de bomba de tiempo y bomba lógica?

2) Piensa como puedes detectar un programa de este tipo en tu ordenador.

6.6 Contramedidas

6.6.1 Introducción

Existen muchos métodos por los cuales se puede detectar, eliminar y prevenir el malware. Algunos métodos no son más que sentido común mientras otros involucran cierta tecnología. La siguiente sección resalta algunos de estos métodos e incluye una breve explicación y brinda ejemplos.

6.6.2 Anti-Virus

El software anti-virus está disponible en varias versiones comerciales y también en Open Source. Todas funcionan con la misma metodología. Poseen una base de datos de las firmas de los virus y las comparan con los archivos del sistema para ver si existe alguna infección. A menudo con los virus actuales las firmas son muy pequeñas y pueden dar falsos positivos, es decir, detecciones que aparentan ser virus y no lo son. Algunos programas anti-virus utilizan una técnica conocida como "heurística", que significa que en base al concepto de qué forma debiera tener un virus pueden determinar si un programa desconocido se adecua a este concepto. Recientemente los anti-virus han cruzado el umbral de los sistemas de prevención de intrusiones de host, verificando que no se produzcan anomalías en el funcionamiento de los programas estándar.

6.6.3 NIDS (Sistemas de detección de intrusiones de red)

Los sistemas de detección de intrusiones de red son similares a los anti-virus pero aplicado al tráfico de la red. Buscan en el tráfico de red firmas o comportamientos debidos a un virus o gusano. Pueden alertar al usuario atacado o detener el tráfico de red que intenta distribuir el malware.

6.6.4 HIDS (Sistemas de detección de intrusiones de host)

Los sistemas de detección de intrusión de host, tal como Tripwire, son capaces de detectar cambios realizados sobre archivos en un servidor. Es razonable esperar que un archivo una vez compilado no necesite ser modificado. Luego, mediante el control de sus características, tales como tamaño, fecha de creación y control de integridad pueden detectar inmediatamente si ha ocurrido algo irregular.

6.6.5 Firewalls (Cortafuegos)

Los gusanos se propagan por la red conectándose a servicios vulnerables en cada sistema. Además de asegurarte que estos servicios vulnerables no se estén ejecutando en tu ordenador el siguiente paso es verificar que tu firewall no permita conexiones a estos servicios. Muchos firewalls modernos realizan algún tipo de filtrado de paquetes similar a un NIDS lo cual frenará los paquetes que coincidan con ciertas firmas. (Analizaremos los firewalls con más detalle en la sección 7.1.2).

6.6.6 Sandboxes (Cajas de arena)

El concepto de sandboxes es simple: una aplicación o programa tiene su propio entorno para ejecutarse y no puede afectar al resto del sistema. Este concepto se implementa como estándar en el lenguaje de programación Java y también puede implementarse a través de otras utilidades como chroot en Linux. Esto restringe el daño que un malware pueda ocasionarle al sistema operativo anfitrión simplemente restringiéndole los accesos requeridos. Otra opción es la de crear un ordenador virtual completo mediante un producto como VMWare. Esto aísla al ordenador virtual del sistema anfitrión limitando el acceso del mismo según lo haya configurado el usuario.

Ejemplo – http://www.vmware.com – VMWare virtual machines

Ejercicios:

1. El juego de las coincidencias: investiga cada una de las siguientes referencias y asocia el tipo de contramedida que le corresponda:

1. http://www.vmware.com	a. NIDS
2. http://www.tripwire.org	b. Antivirus
3. http://www.snort.org	c. Firewalls
4. http://www.checkpoint.com	d. Sandboxes
5. http://www.sophos.com	e. HIDS

2. Investiga "Spybot Search and Destroy" y determina de que tipo de malware protege.

3. Averigua como funcionan los NIDS y HIDS.

4. Analiza las soluciones de Firewalls en la red.

5. Busca "chroot" en Internet e infórmate acerca de este tipo de "cárcel" o "caja de arena".

6.7 Sanos Consejos de Seguridad

Existen varios procedimientos simples que minimizarán tu exposición al Malware.

- Descarga información únicamente de sitios confiables (esto significa no W4R3Z, por favor)
- No abras nunca ficheros anexados de un e-mail de gente que no conozcas.
- No dejes las macros activadas por defecto en tus aplicaciones.
- Mantén tu sistema operativo y aplicaciones actualizadas con las últimas versiones.
- Si descargas o instalas software acompañado de un checksum – comprueba dicho checksum.

Más Información

Sitios de proveedores de Anti-Virus

http://www.sophos.com

http://www.symantec.com

http://www.fsecure.com

http://www.mcafee.com

Todos estos sitios poseen bases de datos donde enumeran las propiedades de troyanos, virus y otros malware. También hay descripciones de sus funcionamientos

http://www.cess.org/adware.htm

http://www.microsoft.com/technet/security/topics/virus/malware.mspx

http://www.zeltser.com/sans/gcih-practical/revmalw.html

http://www.securityfocus.com/infocus/1666

http://www.spywareguide.com/

http://www.brettglass.com/spam/paper.html

http://www.lavasoft.nu/ - AdAware Cleaning Software (Freeware Version)

http://www.claymania.com/removal-tools-vendors.html

http://www.io.com/~cwagner/spyware.html

http://www.bo2k.com/

http://www.sans.org/rr/catindex.php?cat_id=36