

Malware e Ingeniería Social

Atacantes

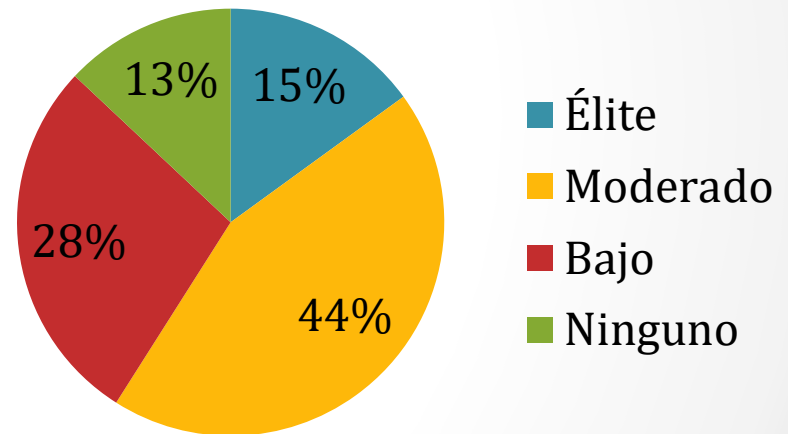
¿Quiénes son los atacantes?

- Hackers
 - Black/Grey/White hat
 - Sustituida por *atacante* independientemente de los motivos
- Script Kiddies
 - Atacantes sin conocimientos que utilizan herramientas automatizadas (scripts)
 - Las herramientas actuales tienen UI gráfica (más fáciles)
 - Anonymous emplea este enfoque habitualmente
- Espías
 - Atacante bajo contrato (mercenario)
 - El objetivo es mucho más específico
 - Nivel excelente de conocimientos
- Interno (*insiders*)
 - Alrededor del 48% de los ataques son de origen interno (empleados, contratistas y empresas aliadas)
 - Suelen consistir en sabotaje o robo de propiedad intelectual
 - Casi todos provienen de empleados recién despedidos

¿Quiénes son los atacantes?

- **Élite**
 - Métodos avanzados, recursos ingentes, conocimiento elitista
- **Moderado**
 - Métodos que requieren cierto conocimiento, alguna modificación y recursos no triviales
- **Bajo**
 - Métodos básicos, sin modificaciones ni recursos extra
- **Ninguno**
 - Usuario medio sin experiencia ni conocimientos

Nivel de Conocimientos



Malware

- Propagación
 - Virus
 - Gusanos
- Ocultación
 - Troyanos
 - Rootkits
 - Bomba lógica
 - Puerta trasera
- Beneficio
 - Botnets
 - Spyware
 - Adware
 - Keylogger
 - Ransomware

Propagación

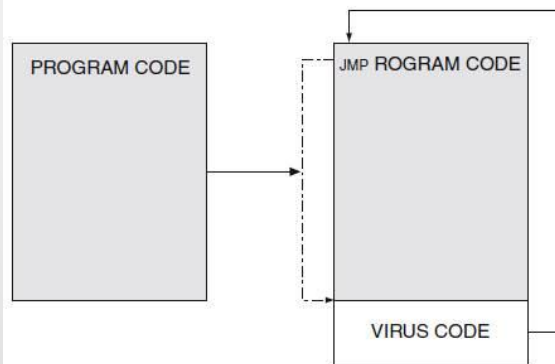
Virus

- Virus biológico
 - Infecta una célula
 - La controla para producir copias de si mismo
- Virus informático
 - Se inserta (infecta) en el código de un programa
 - Se reproduce infectando otros ficheros
 - Cada vez que arranca intenta reproducirse y/o llevar a cabo una acción maliciosa
 - Depende del usuario para saltar de máquina
- Acciones de los virus
 - Colgar el ordenador de forma repetida
 - Borrar ficheros
 - Consumir todo el espacio libre copiándose a sí mismo
 - Desactivar los sistemas de seguridad
 - Formatear el disco duro, etc.

Virus

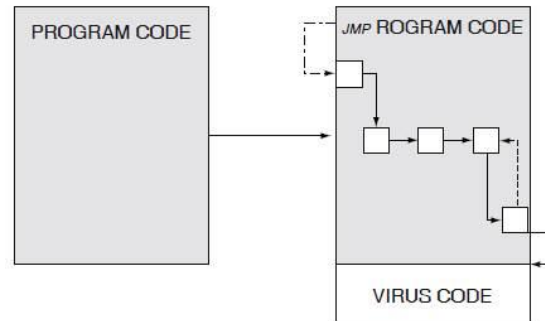
Apéndice

- Se inserta al final
- Salto inicial al virus
- Cede el control al programa tras el virus



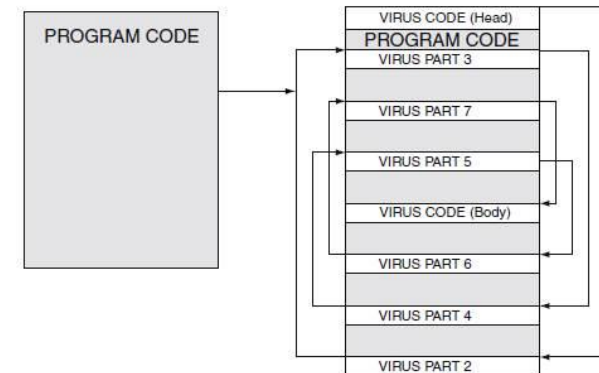
Queso Suizo

- Se inserta dentro del código del programa
- Se almacena el código sobrescrito para ejecutar el programa original correctamente



Fraccionado

- El virus se divide en muchas partes
- Se intercalan de forma aleatoria
- Se almacena el código sobrescrito



Virus

- Virus de programa
 - Infecta ficheros ejecutables
 - Se activa al ejecutar el programa
 - Hay más de 70 extensiones en windows que pueden contener un virus
- Virus de macro
 - Una macro es una serie de instrucciones para la automatización de tareas repetitivas que se almacenan en un fichero de datos (Visual Basic en Excel, etc.)
 - Se activa al abrir el documento
- Virus de arranque
 - Infecta el Master Boot Record (MBR) del disco duro. Se activa al arrancar el ordenador (antes del sistema operativo)
- Virus asociado
 - Suplanta a una herramienta legítima del sistema operativo (por ej. Notepad.com en lugar de Notepad.exe)

Gusanos

- Programa malicioso que explota una vulnerabilidad para entrar en una máquina
- Una vez ha infectado una máquina, busca otros objetivos potenciales
- Utiliza la red para enviar copias de si mismo
- Los gusanos originales simplemente se copiaban y producían un ataque de denegación de servicio
- Los actuales pueden realizar otras acciones:
 - Borrar ficheros
 - Permitir el control remoto...
- Rober T. Morris Jr. (1998)
 - Afectó a 6000 máquinas (10% del internet de entonces)

Diferencias Virus/Gusanos

Acción	Virus	Gusano
Propagación	Requiere que una persona o agente externo transfiera archivos infectados a otros sistemas	Utiliza la red para transferirse de forma autónoma entre sistemas
Infección	Se insertan en ficheros ejecutables	Explotan las vulnerabilidades de aplicaciones o SO
Requiere acción externa	Sí	No
Se puede controlar de forma remota	No	Sí

Ocultación

Troyanos

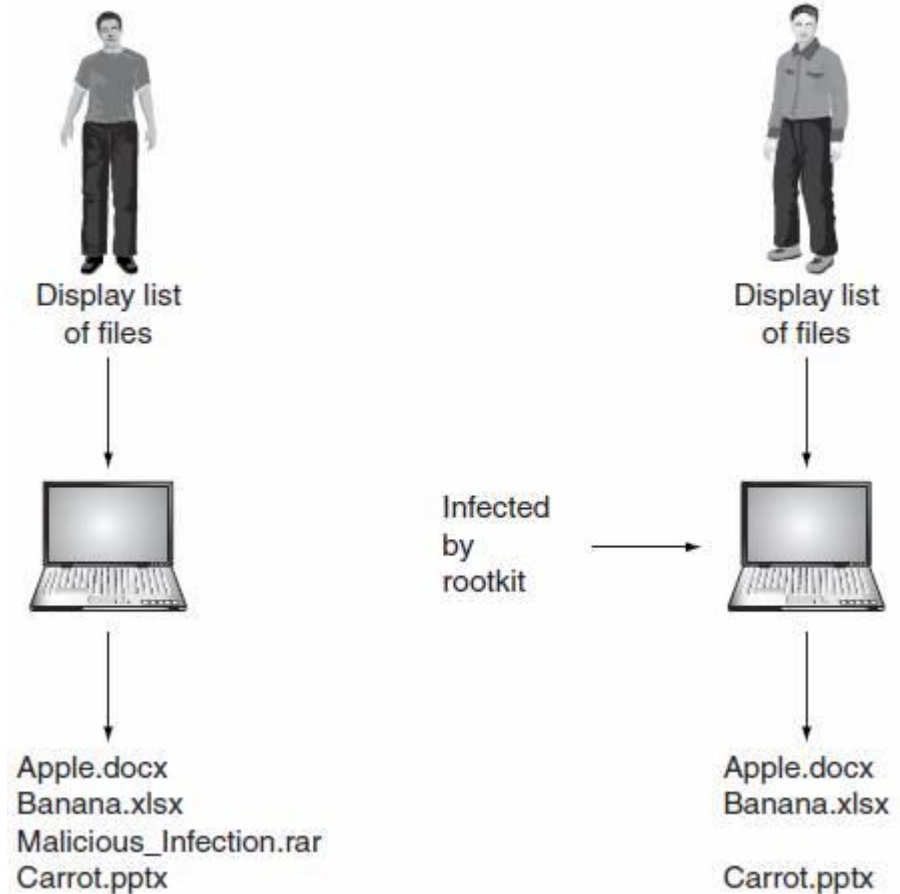
- Los griegos ganaron la guerra de Troya escondiendo soldados en un caballo de madera gigante [Leyenda]
- Un caballo de Troya (o troyano) informático es un programa que oficialmente hace una actividad pero tiene otra actividad oculta
- Ejemplo: calendario gratuito
 - Envío remoto de contraseñas y números de tarjetas de crédito
- Otra técnica
 - cupones-gratis.docx.exe
 - Etc.

Rootkits

- Un *rootkit* es un grupo de herramientas que sirve para esconder la actividad o presencia de otro malware
- Actúan escondiendo registros, logs y procesos asociados
- Modifican el SO para forzarle a ignorar actividad maliciosa
- Ejemplo:
 - Antimalware analiza todos los ficheros en cierto directorio
 - Recibe la lista del SO
 - El rootkit altera el SO para que nunca muestre los archivos maliciosos
- Con un rootkit, ni el usuario ni el SO conocen realmente lo que está ocurriendo: *todo aparenta ser normal*

Rootkits

- La detección depende del tipo de rootkit
 - Cambio de ficheros del SO
 - Comparar con versiones originales
 - Rootkits de bajo nivel
 - Mucho más difícil de detectar
- Son relativamente difíciles de eliminar una vez detectados
- [Caso de los CD de Sony]



Bombas lógicas

- Programas que permanecen dormidos hasta que se satisface cierta condición
- Pueden producir cualquier tipo de actividad maliciosa
- Son muy difíciles de detectar antes de activarse
- No deben confundirse con los “huevos de pascua” (easter eggs) [excel 95]
- Ejemplo:
 - Un empleado del gobierno de Maryland intentó destruir los contenidos de 4000 servidores
 - Bomba lógica preparada para activarse 90 días tras su despido
- Ejemplo:
 - Una bomba lógica en una red de servicios financieros
 - 1000 ordenadores borraron datos críticos
 - Un empleado descontento quería que las acciones de la empresa bajaran
 - Condenado a 8 años de prisión y \$3.1M de multa

Bombas lógicas

- Ejemplo

- Bomba lógica en un contratista de defensa diseñada para borrar información de un proyecto armamentístico
- El plan del empleado era ser contratado como un asesor altamente remunerado para arreglar el problema
- Se encontró y desactivó antes de actuar
- Acusado de fraude y manipulación de ordenadores con 5000\$ de multa

- Ejemplo

- Bomba lógica en una empresa de servicios sanitarios programada para activarse en el cumpleaños del empleado
- El empleado estaba enfadado, pensando que iba a ser despedido (no era cierto)
- Sentenciado a 30 meses en prisión federal y 81200\$ de multa

Puertas traseras

- Código que permite el acceso a un programa o servicio sin las restricciones de seguridad normales.
- Es una práctica normal en el desarrollo de muchos programas para obtener un acceso rápido o de depuración al mismo. A veces se olvida de eliminar antes del lanzamiento.
- Malware puede dejar una puerta trasera para que el atacante vuelva después sin pasar por los sistemas de seguridad.
- [Compilador de C, Ken Thompson – “Trusting trust”]

Beneficio

Botnets

- Una de las cargas más habituales de troyanos, gusanos y virus es un programa que permita el control remoto de la máquina infectada
- Este robot infectado (*bot*) se conoce como *zombie*
- Cuando cientos, miles o cientos de miles de zombies forman una red de ordenadores bajo control de un atacante se llama **botnet**
- Dada la capacidad de cómputo y multitarea de las máquinas actuales son capaces de actuar como *zombies* y llevar a cabo las tareas normales sin despertar sospechas en el usuario legítimo
- Ha existido una botnet de un europeo con 1.5M zombies.
- Las botnets originales usaban IRC para controlar las máquinas
- Recientemente, se ha sustituido IRC por HTTP. De esta forma es más difícil de detectar y bloquear además de permitir más independencia entre el atacante y la botnet
- Sirven para
 - Spam
 - Distribuir malware
 - Manipular encuestas y juegos
 - Denegación de servicio (anonymous)
- Plataforma ideal
 - Sigiloso, ataques encubiertos
 - Permanecen activas durante años
 - Un gran porcentaje de máquinas está siempre disponible

Comercio co: Botnets

- Basic crypter (for inserting rogue code into a benign file): \$10-30
- SOCKS bot (to get around firewalls): \$100
- Hiring a DDoS attack: \$30-70 for a day, \$1,200 for a month
- Email spam: \$10 per one million e-mails
- Expensive email spam (using a customer database): \$50-500 per one million e-mails
- SMS spam: \$3-150 per 100-100,000 messages
- Bots for a botnet: \$200 for 2,000 bots
- DDoS botnet: \$700
- Zeus source code: \$200-\$500
- Windows rootkit (for installing malicious drivers): \$292
- Hacking a Facebook or Twitter account: \$130
- Hacking a Gmail account: \$162
- Hacking a corporate mailbox: \$500
- Scans of legitimate passports: \$5 each
- Winlocker ransomware: \$10-20
- Unintelligent exploit bundle: \$25
- Intelligent exploit bundle: \$10-3,000
- Traffic: \$7-15 per 1,000 visitors for the most valuable traffic (from the US and EU)

Spyware

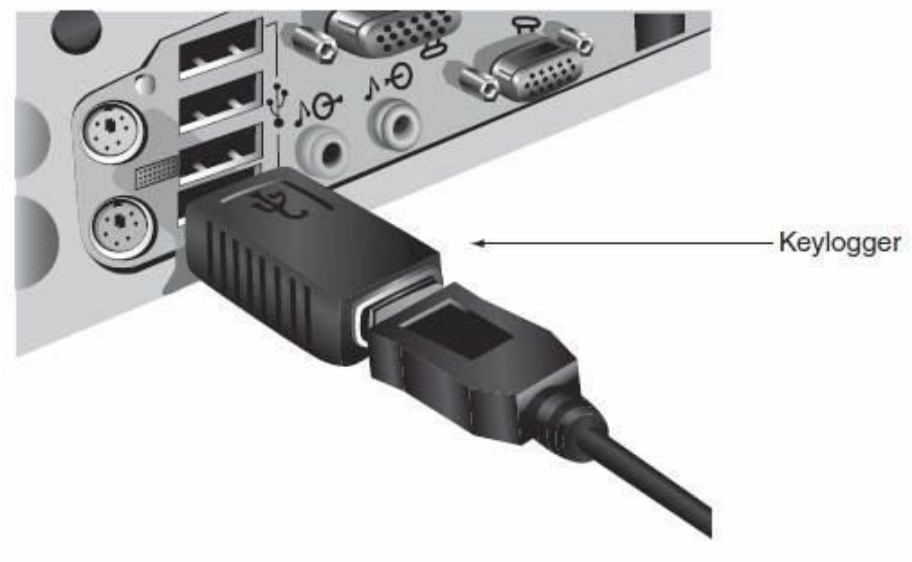
- Software que espía a los usuarios obteniendo información sin su consentimiento:
 - Uso de recursos del sistema, instalación de programa
 - Recolección y distribución de información personal o sensible
 - Cambios en la experiencia del usuario, privacidad o seguridad del sistema
- Produce efectos adversos
 - Reducir el rendimiento
 - Inestabilidad del sistema
 - Barras de navegador, enlaces o página de inicio
 - Pop-ups
- Tecnologías
 - Descarga automática de software
 - Tracking y monitoreo
 - Software de modificación del sistema
- Georgia atacó e identificó a un hacker ruso mediante spyware
- Problema cada vez mayor con la cantidad de dispositivos con cámara y localización que llevamos continuamente

Adware

- Proporciona publicidad de manera inesperada e indeseada
- Puede provenir de otro malware (virus, gusano, troyano...)
- Una vez instalado
 - Muestra banners
 - Pop-ups
 - Abre páginas web...
- Efectos negativos
 - Contenido inapropiado
 - Afecta a la productividad
 - Pueden provocar que la máquina deje de responder, etc.
- Seguimiento de intención comercial
 - Venta de historial a anunciantes
 - Anuncios ad-hoc
- Similar a spyware

Keyloggers

- Captura y almacena cada pulsación en el teclado.
- Puede ser recuperado más adelante o transmitido a una localización remota
- El objetivo puede ser
 - Contraseñas
 - Números de tarjetas de crédito
 - Información personal, etc.
- Puede ser
 - Dispositivo hardware intercalado entre el teclado y el ordenador
 - Receptor inalámbrico
 - Software



Ransomware

cifrado

- PC Cyborg (1989)
 - cifrado de ficheros en disco
 - usaba licencia expirada como excusa
 - el creador fue declarado incapaz mentalmente y prometió donar el dinero a la investigación contra el SIDA
- Extorsión criptoviral (Young & Yung)
 - Uso de criptografía de clave pública
- Reveton (2012)
- Cryptolocker (2013)

no cifrado

- WinLock (Rusia, 2010)
 - Restringe el acceso al sistema con imágenes pornográficas.
- WPA (2011)
 - Imita la activación de windows
 - Obligaba a llamar a un teléfono internacional con coste elevado
- Stamp.EK (2013)
 - Distribuido por GitHub y Sourceforge
 - Ofrecía fotos de famosos desnudos.
- Pedófilo se autoinculpa (USA, 2013)

Ingeniería social

Caso verídico

1. Antes de entrar en el edificio, llaman a recursos humanos para obtener el nombre de ciertos empleados clave.
2. Al acercarse al edificio, un atacante simula haber perdido la llave. Un empleado les permite entrar.
3. Saben que el CFO está fuera por su buzón de voz. Entran en su oficina y obtienen información de su ordenador y documentos en papel.
4. Lllaman a los técnicos desde la oficina del CFO suplantándole. Solicitan su contraseña puesto que la ha olvidado y está de camino a una reunión importante.

Suplantación de identidad

- Suplantación
 - Actuar como un personaje ficticio
 - Por ejemplo: técnico preguntando por contraseña y usuario a la víctima
 - Personajes estándar
 - Servicio de reparación
 - Técnico informático
 - Gestor
 - Una entidad de confianza
 - Antiguo empleado, etc.
 - Suplantación de alguien de autoridad y esperar a solicitud de información
- Phishing
 - Enviar un e-mail o mostrar un anuncio que simula provenir de una fuente legítima con el objetivo de engañar al usuario para que proporcione información privada
 - El atacante copia logos, colores, texto, url y direcciones de e-mail para incrementar autenticidad
 - Phishing proviene de fishing (pescar).
 - Una web de phishing está activa 3.8 días de media. En ese tiempo es capaz de obtener más de 50,000\$
 - Existen variaciones: pharming, spear phishing, whaling, vishing, etc.

Spam : Hoax

- Spam

- E-mail no solicitado con fines comerciales
- Cuesta 874\$ por persona en pérdida de productividad (EEUU)
- Es uno de los vehículos primarios para otro malware
- El beneficio económico es sorprendentemente alto
 - 6M emails, 0.001% eficacia con 45\$ de beneficio: \$270K
- Para evitar los filtros de texto, se hace spam con imágenes
- Existe el Spim (mensajería instantánea)

- Engaño (hoax)

- Aviso falso que proviene de los técnicos informáticos indica una alerta por un virus especialmente malicioso.
- Insta a modificar ciertos ficheros o cambiar los ajustes de seguridad, así como reenviar a otros empleados.
- El atacante tiene, de esta forma, vía libre para atacar el sistema.
- Otro enfoque consiste en solicitar cambios que hagan inestable el sistema para que el usuario llame al teléfono falso proporcionado en el hoax.