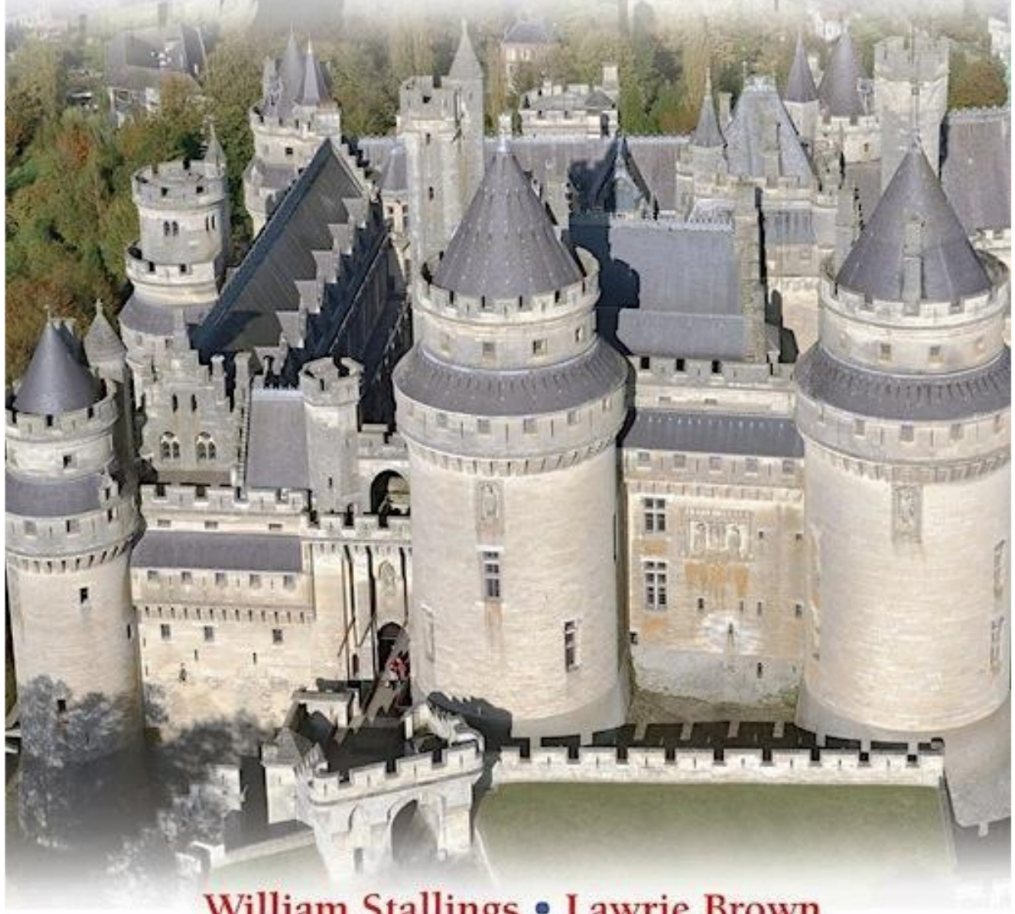
COMPUTER SECURITY

PRINCIPLES AND PRACTICE

Third Edition



William Stallings • Lawrie Brown

Capítulo 6

Software malicioso

Software malicioso

[SOUP13] define malware como:

"un programa que se inserta en un sistema, generalmente de forma encubierta, con la intención de comprometer la confidencialidad, integridad o disponibilidad de los datos, aplicaciones o sistema operativo de la víctima o de molestar o perturbar de otro modo a la víctima".

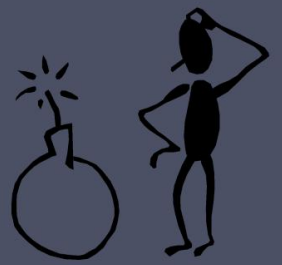
Name	Description
Advanced persistent threat	Cybercrime directed at business and political targets, using a wide variety of intrusion technologies and malware, applied persistently and effectively to specific targets over an extended period, often attributed to state-sponsored organizations.
Adware	Advertising that is integrated into software. It can result in pop-up ads or redirection of a browser to a commercial site.
Attack Kit	Set of tools for generating new malware automatically using a variety of supplied propagation and payload mechanisms.
Auto-rooter	Malicious hacker tools used to break into new machines remotely.
Backdoor (trapdoor)	Any mechanisms that bypasses a normal security check; it may allow unauthorized access to functionality in a program, or onto a compromised system.
Downloaders	Code that installs other items on a machine that is under attack. It is normally included in the malware code first inserted on to a compromised system to then import a larger malware package.
Drive-by download	An attack using code in a compromised web site that exploits a browser vulnerability to attack a client system when the site is viewed.
Exploits	Code specific to a single vulnerability or set of vulnerabilities.
Flooders (DoS client)	Used to generate a large volume of data to attack networked computer systems, by carrying out some form of denial-of-service (DoS) attack.
Keyloggers	Captures keystrokes on a compromised system.
Logic bomb	Code inserted into malware by an intruder. A logic bomb lies dormant until a predefined condition is met; the code then triggers an unauthorized act.
Macro Virus	A type of virus that uses macro or scripting code, typically embedded in a document, and triggered when the document is viewed or edited, to run and replicate itself into other such documents.
Mobile Code	Software (e.g., script, macro, or other portable instruction) that can be shipped unchanged to a heterogeneous collection of platforms and execute with identical semantics.
Rootkit	Set of hacker tools used after attacker has broken into a computer system and gained root-level access.
Spammer Programs	Used to send large volumes of unwanted e-mail.
Spyware	Software that collects information from a computer and transmits it to another system by monitoring keystrokes, screen data and/or network traffic; or by scanning files on the system for sensitive information.
Trojan horse	A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the Trojan horse program.
Virus	Malware that, when executed, tries to replicate itself into other executable machine or script code; when it succeeds the code is said to be infected. When the infected code is executed, the virus also executes.
Worm	A computer program that can run independently and can propagate a complete working version of itself onto other hosts on a network, usually by exploiting software vulnerabilities in the target system.
Zombie, bot	Program activated on an infected machine that is activated to launch attacks on other machines.

Tabla 6.1

Software malicioso

Terminología

(La tabla se puede encontrar en la página 201 del libro de texto).



Clasificación de malware

Clasificados en dos grandes categorías:

Basado primero en cómo se propaga para alcanzar los objetivos deseados.

Luego, sobre las acciones o cargas útiles que realiza una vez que se alcanza un objetivo.

También clasificado por:

Aquellos que necesitan un programa anfitrión (código parásito como virus)

Aquellos que son programas independientes y autónomos (gusanos, troyanos y bots)

Malware que no se replica (troyanos y correo electrónico spam)

Malware que se replica (virus y gusanos)

Tipos de software malicioso

(Software malicioso)

Los mecanismos de propagación incluyen:

- Infección de contenido existente por virus que posteriormente se propaga a otros sistemas.
- Explotación de vulnerabilidades de software mediante gusanos o descargas automáticas para permitir que el malware se replique.
- Ataques de ingeniería social que convencen a los usuarios de eludir los mecanismos de seguridad para instalar troyanos o responder a ataques de phishing.

Las acciones de carga útil que realiza el malware una vez que llega a un sistema de destino pueden incluir:

- Corrupción del sistema o de archivos de datos.
- Robo de servicio/convertir el sistema en un agente zombi de ataque como parte de una botnet
- Robo de información del sistema/keylogging
- Ocultar/mantener oculta su presencia en el sistema

Kits de ataque

- Inicialmente el desarrollo y despliegue de

  El malware requirió considerables habilidades técnicas por parte de los autores del software

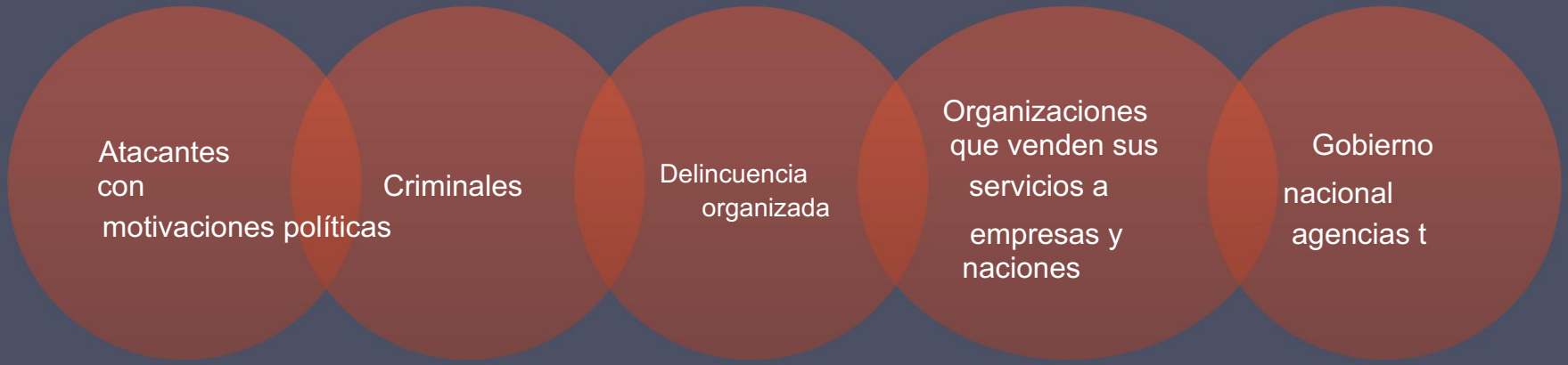
  - El desarrollo de kits de herramientas para la creación de virus a principios de la década de 1990 y luego
    Los kits de ataque más generales de la década de 2000 ayudaron en gran medida al desarrollo y la implementación de malware.
- Los kits de herramientas a menudo se conocen como "crimeware"
  - Incluir una variedad de mecanismos de propagación y módulos de carga útil que
    Incluso los novatos pueden implementarlo
  - Las variantes que pueden generar los atacantes que utilizan estos kits de herramientas crean un problema importante para quienes defienden los sistemas contra ellos.
- Los kits de herramientas más utilizados incluyen:
  - Zeus
  - Agujero negro

  sakura

  sobre Phoenix

Fuentes de ataque

- Otro desarrollo significativo del malware es el cambio de los atacantes, que a menudo son individuos motivados por demostrar su competencia técnica a sus pares, a fuentes de ataque más organizadas y peligrosas como:



- Esto ha cambiado significativamente los recursos disponibles. y la motivación detrás del auge del malware y ha llevado al desarrollo de una gran economía subterránea que involucra la venta de kits de ataque, acceso a hosts comprometidos y a información robada.

Persistente avanzado Amenazas (APT)

- Aplicación persistente y con recursos suficientes de una amplia variedad de tecnologías de intrusión y malware a objetivos seleccionados (generalmente comerciales o políticos)
- Generalmente se atribuye a organizaciones patrocinadas por el Estado y empresas criminales.
- Se diferencian de otros tipos de ataque por su cuidado. Selección de objetivos y esfuerzos de intrusión sigilosos durante períodos prolongados
- Los ataques de alto perfil incluyen Aurora, RSA, APT1 y Stuxnet

Características de APT

Avanzado

- Utilizado por los atacantes de una amplia variedad de tecnologías de intrusión y malware, incluido el desarrollo de malware personalizado si es necesario.
- Los componentes individuales pueden no ser necesariamente técnicamente avanzados, pero se seleccionan cuidadosamente para adaptarse al objetivo elegido.

Persistente

- Aplicación determinada de los ataques durante un período prolongado contra el objetivo elegido para maximizar las posibilidades de éxito.
- Se pueden aplicar progresivamente diversos ataques hasta que el objetivo se vea comprometido.

Amenazas

- Amenazas a los objetivos seleccionados como resultado de la intención de atacantes organizados, capaces y bien financiados de comprometer los objetivos específicamente elegidos.
- La participación activa de las personas en el proceso aumenta en gran medida el nivel de amenaza debido a las herramientas de ataques automatizados, y también la probabilidad de ataques exitosos.

Ataques APT

- Apuntar:
  - Varía desde el robo de propiedad intelectual o de datos relacionados con la seguridad y la infraestructura hasta la interrupción física de la infraestructura.
- Técnicas utilizadas:
  - Ingeniería social
  - Correo electrónico de phishing
  - Descargas automáticas desde sitios web comprometidos seleccionados que probablemente sean visitados por personal de la organización objetivo
- Intención:
  - Infectar el objetivo con malware sofisticado con propagación múltiple. mecanismos y cargas útiles
  - Una vez que han obtenido acceso inicial a los sistemas de la organización objetivo, se utiliza una gama adicional de herramientas de ataque para mantener y ampliar su acceso

Virus

- Pieza de software que infecta programas o Los modifica para incluir una copia del virus o Se replica y continúa infectando otros contenidos o Se propaga fácilmente a través de entornos de red • Cuando se adjunta a un programa ejecutable, un virus puede hacer cualquier cosa que el programa tenga permitido hacer o Se ejecuta en secreto cuando se ejecuta el programa anfitrión • Específico del sistema operativo y el hardware o Se aprovecha de sus detalles y debilidades

Componentes del virus

Mecanismo de infección

• Medio por el cual un virus se propaga o se esparce • También conocido como vector de infección

Desencadenar

• Evento o condición que determina cuándo se carga útil. activado o entregado • A veces conocido como bomba lógica

Carga útil

• Qué hace el virus (además de propagarse) • Puede implicar daños o una actividad benigna pero notable

Fases del virus

Fase latente

El virus está inactivo	Eventualmente se activará por algún evento.	No todos los virus tienen esta etapa.

Fase de activación

El virus se activa para realizar la función para la que fue diseñado.	Puede ser causado por una variedad de eventos del sistema.

Fase de propagación

El virus coloca una copia de sí mismo en otros programas o en ciertas áreas del sistema en el disco.	Puede no ser idéntico a la versión propagada	Cada programa infectado contendrá ahora un clon del virus que entrará en una fase de propagación.

Fase de ejecución

La función se realiza	Puede ser inofensivo o dañino.

Estructura del virus

```
program V
1234567;

procedure attach-to-program;
begin
   repeat
      file := get-random-program;
   until first-program-line ≠ 1234567;
   prepend V to file;
end;

procedure execute-payload;
begin
   (* perform payload actions *)
end;

procedure trigger-condition;
begin
   (* return true if trigger condition is true *)
end;

begin (* main action block *)
   attach-to-program;
   if trigger-condition then execute-payload;
   goto main;
end;
```

(a) A simple virus

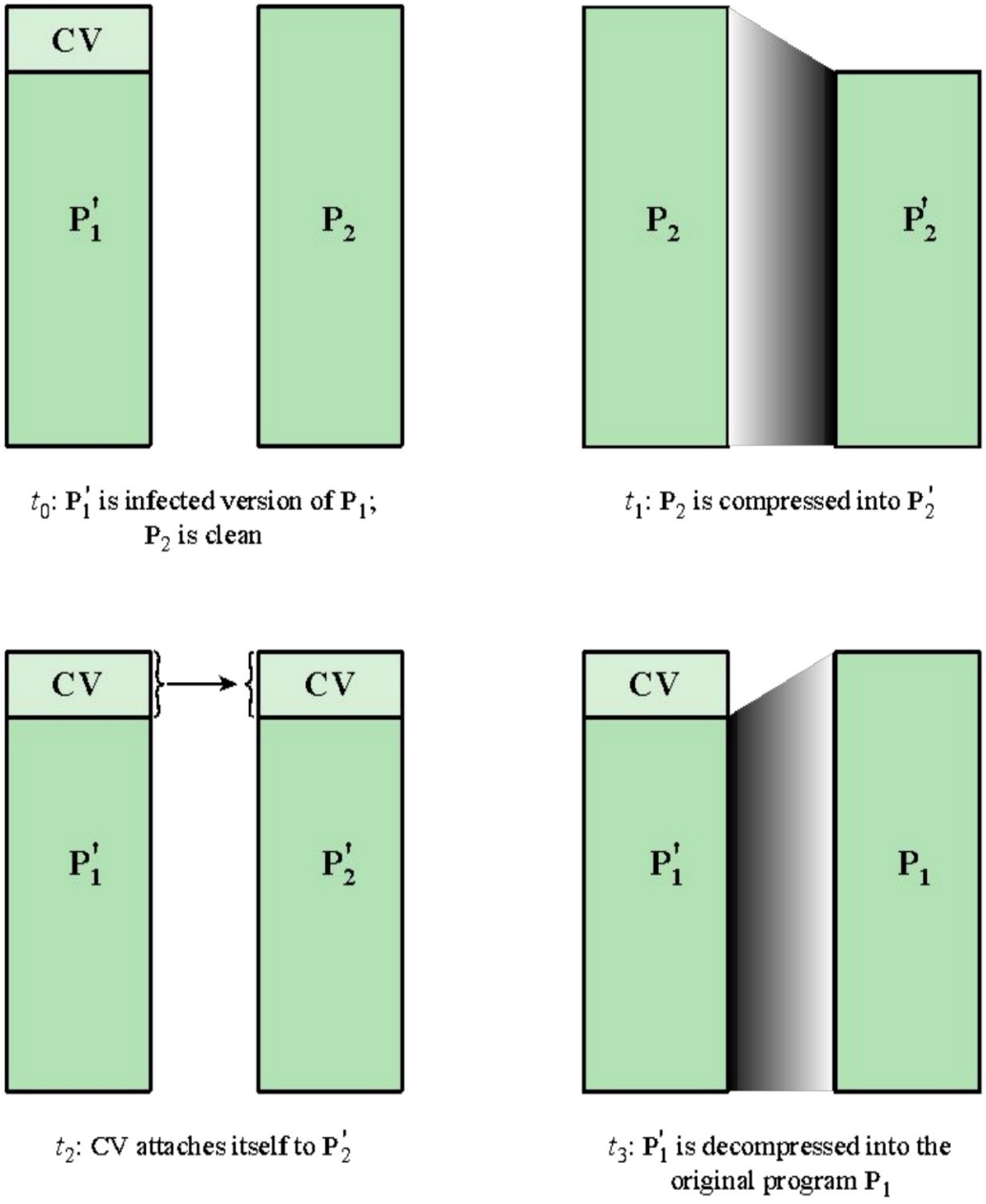
```
program CV
1234567;

procedure attach-to-program;
begin
   repeat
      file := get-random-program;
   until first-program-line ≠ 1234567;
   compress file;   (* t1 *)
   prepend CV to file;   (* t2 *)
end;

begin (* main action block *)
   attach-to-program;
   uncompress rest of this file into tempfile;   (* t3 *)
   execute tempfile;   (* t4 *)
end;
```

(b) A compression virus

Figure 6.1 Example Virus Logic



t_0: P_1' is infected version of P_1; P_2 is clean

t_1: P_2 is compressed into P_2'

t_2: CV attaches itself to P_2'

t_3: P_1' is decompressed into the original program P_1

Figure 6.2 A Compression Virus

Clasificaciones de virus

Clasificación por objetivo

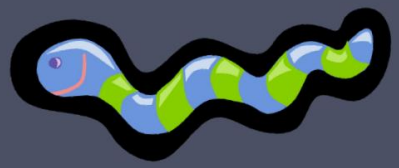
- Infector del sector de arranque
  - o Infecta un registro de arranque maestro
    - o un registro de arranque y se propaga cuando un sistema se inicia desde el disco que contiene el virus.
- Infectador de
  - archivos : Infecta archivos
    - que el sistema operativo o el shell considera ejecutables.
- Virus de macro
  - o Infecta archivos con macros o códigos
    - de secuencias de comandos que son interpretados por una aplicación.
- Virus multipartito
  - o Infecta archivos de múltiples maneras

Clasificación por estrategia de ocultamiento

- Virus encriptado
  - o Una parte del virus crea una clave de cifrado aleatoria y cifra el resto del virus.
- Virus sigiloso
  - o Una forma de virus explícitamente Diseñado para ocultarse de la detección por parte del software antivirus.
- Virus polimórfico
  - o Un virus que muta con cada infección.
- Virus metamórfico
  - o Un virus que muta y
    - Se reescribe completamente en cada iteración y puede cambiar tanto el comportamiento como la apariencia.

Macro y secuencias de comandos Virus

- Muy común a mediados de la década de 1990.
  - Independiente de la plataforma
  - Infecta documentos (no partes ejecutables del código)
  - Se propaga fácilmente
- Explota la capacidad de macro de las aplicaciones de MS Office
  - Las versiones más recientes de productos incluyen protección
- Se han desarrollado varios programas antivirus, por lo que estos ya no son la amenaza de virus predominante.



Gusanos

- Programa que busca activamente más máquinas para infectar y cada una
  La máquina infectada sirve como plataforma de lanzamiento automatizada para ataques a otras máquinas.

- Explota vulnerabilidades de software en programas cliente o servidor.

- Puede utilizar conexiones de red para propagarse de un sistema a otro.

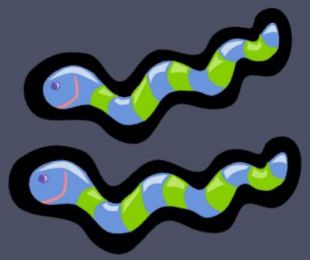
- Se propaga a través de medios compartidos (unidades USB, CD, discos de datos DVD)

- Los gusanos de correo electrónico se propagan en códigos de macro o scripts incluidos en archivos adjuntos y transferencias de archivos de mensajería instantánea.

- Al activarse, el gusano puede replicarse y propagarse nuevamente.

- Generalmente lleva algún tipo de carga útil.

- La primera implementación conocida se realizó en Xerox Palo Alto Labs en el
  principios de los años 1980



Replicación de gusanos

Servicio de correo electrónico o mensajería instantánea	•El gusano envía por correo electrónico una copia de sí mismo a otros sistemas. •Se envía como archivo adjunto a través de un servicio de mensajería instantánea.
Intercambio de archivos	•Crea una copia de sí mismo o infecta un archivo como un virus en un medio extraíble
Capacidad de ejecución remota	
Capacidad de acceso o transferencia remota de archivos	
Capacidad de inicio de sesión remoto	

Descubrimiento de objetivos

- Escaneo (o toma de huellas dactilares)
  - o Primera función en la fase de propagación de un gusano de red
  - o Busca otros sistemas para infectar

Estrategias de escaneo que puede utilizar un gusano:

- Aleatorio
  - Cada host comprometido sondea direcciones aleatorias en el espacio de direcciones IP utilizando un semilla diferente
  - Esto produce un alto volumen de tráfico de Internet que puede causar problemas generalizados. Interrupción incluso antes de que se lance el ataque real

- Lista de objetivos
  - El atacante primero compila una larga lista de máquinas potencialmente vulnerables.
  - Una vez compilada la lista, el atacante comienza a infectar las máquinas de la lista.
  - A cada máquina infectada se le proporciona una parte de la lista para escanear.
  - Esto da como resultado un período de escaneo muy corto, lo que puede dificultar la detección de una infección.

- Topológico
  - Este método utiliza información contenida en una máquina víctima infectada para encontrar más hosts para escanear

- Subred local
  - Si un host puede infectarse detrás de un firewall, ese host busca objetivos en su propia red local.
  - El host utiliza la estructura de dirección de subred para encontrar otros hosts que de otro modo no encontrarían. estar protegido por el firewall

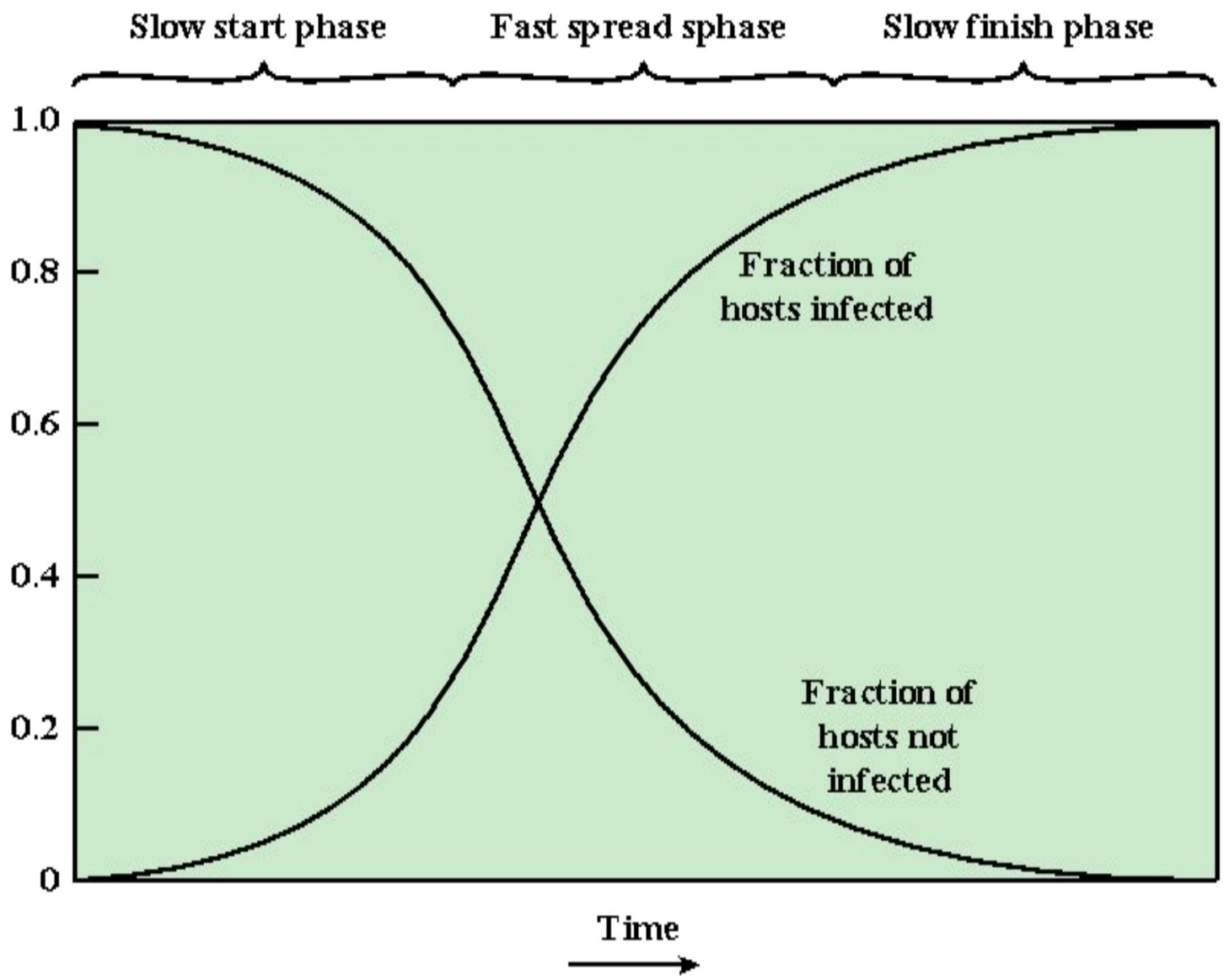


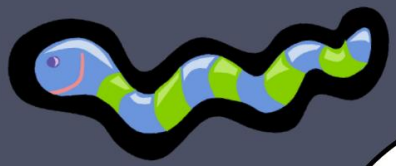
Figure 6.3 Worm Propagation Model

Gusano Morris

- Infección por gusanos significativa más temprana
- Lanzado por Robert Morris en 1988
- Diseñado para propagarse en sistemas UNIX
  - Se intentó descifrar el archivo de contraseña local para usar el nombre de usuario y la contraseña. Iniciar sesión en otros sistemas
  - Se aprovechó un error en el protocolo de dedo que informa el paradero de un usuario remoto
  - Se explotó una trampa en la opción de depuración del proceso remoto que recibe y envía correo.
- Los ataques exitosos lograron comunicarse con el intérprete de comandos del sistema operativo.
  - Envió al intérprete un programa de arranque para copiar el gusano

Ataques recientes de gusanos

Toronjil	1998	gusano de correo electrónico El primero en incluir virus, gusanos y troyanos en un solo paquete
Código rojo	Julio de 2001	Error explotado de Microsoft IIS Sondea direcciones IP aleatorias consume una capacidad significativa de Internet cuando está activo
Código Rojo II	Agosto de 2001	También se dirigió a Microsoft IIS instala una puerta trasera para acceder
ellos saben	Septiembre de 2001	Tenía características de gusano, virus y código móvil. Se propaga mediante correo electrónico, recursos compartidos de Windows, servidores web, clientes web y puertas traseras.
Delincuente de SQL	Principios de 2003	Explotó una vulnerabilidad de desbordamiento de búfer en el servidor SQL Compacto y extendido rápidamente
Sobig.F	Finales de 2003	Explotó servidores proxy abiertos para convertir las máquinas infectadas en motores de spam
Mi perdición	2004	gusano de correo electrónico de envío masivo instaló una puerta trasera en las máquinas infectadas
Warezov	2006	Crea ejecutables en directorios del sistema. Se envía como archivo adjunto en un correo electrónico. Puede desactivar productos relacionados con la seguridad.
Conficante (Abajo arriba)	Noviembre de 2008	Explota una vulnerabilidad de desbordamiento de búfer de Windows La infección más extendida desde SQL Slammer
Stuxnet	2010	Tasa de propagación restringida para reducir las posibilidades de detección sistemas de control industrial específicos



Gusano Tecnólogo y

- Multiplataforma
- Exploit múltiple
- Propagación ultrarrápida
- Polimórfico
- Metamórfico

Código móvil

- Programas que se pueden enviar sin cambios a una variedad de plataformas
- Se transmite desde un sistema remoto a un sistema local y luego se ejecuta en el sistema local.
- A menudo actúa como mecanismo de un virus, gusano o troyano. caballo
- Aprovecha las vulnerabilidades para realizar sus propias acciones. hazañas
- Los vehículos populares incluyen applets de Java, ActiveX, JavaScript y VBScript

Gusanos de telefonía móvil

- El primer descubrimiento fue el gusano Cabir en 2004
- Luego Lasco y CommWarrior en 2005
- Comunicarse a través de conexiones inalámbricas Bluetooth o MMS
- El objetivo es el teléfono inteligente
- Puede deshabilitar completamente el teléfono, eliminar datos del teléfono o forzar al dispositivo a enviar mensajes costosos.
- CommWarrior se replica mediante Bluetooth a otros teléfonos, se envía como un archivo MMS a los contactos y como una respuesta automática a los mensajes de texto entrantes.

Descargas automáticas

- Aprovecha las vulnerabilidades del navegador para descargar y Instala malware en el sistema cuando el usuario visita una página web controlada por el atacante
- En la mayoría de los casos no se propaga activamente.
- Se propaga cuando los usuarios visitan la página web maliciosa.

Secuestro de clics

- También conocido como

  ataque de reparación de interfaz de usuario (UI)

- Utilizando una técnica similar, las

  pulsaciones de teclas también

  pueden ser secuestradas.

  - Se puede hacer creer a un usuario que está escribiendo la contraseña de su correo electrónico o cuenta bancaria, pero en realidad está escribiendo en un marco invisible controlado por el atacante.

- Vulnerabilidad utilizada por un atacante para recopilar los clics de un usuario infectado

  - El atacante puede obligar al usuario a Realizar una variedad de cosas, desde ajustar la configuración de la computadora del usuario hasta enviar involuntariamente al usuario a sitios web que podrían tener código malicios

  - Aprovechando Adobe Flash o JavaScript: un atacante podría incluso colocar un botón debajo o encima de un botón legítimo, dificultando que los usuarios lo detecten.

  - Un ataque típico utiliza múltiples Capas transparentes u opacas para engañar a un usuario para que haga clic en un botón o enlace en otra página cuando tenía la intención de hacer clic en la página de nivel superior.

  - El atacante está secuestrando clics. destinados a una página y enrutarlos a otra página

Ingeniería social

- “Engañar” a los usuarios para que ayuden a comprometer sus propios sistemas.

Correo basura

- Envío masivo no solicitado
  - correo electrónico
- Portador importante de malware
- Se utiliza para ataques de phishing

Caballo de Troya

- Programa o utilidad que contiene código oculto dañino
- Se utiliza para realizar funciones que el atacante no podría realizar directamente

Troyanos de telefonía móvil

- Apareció por primera vez en 2004 (debería)
- El objetivo es el teléfono inteligente

Carga útil

Corrupción del sistema

Virus de Chernóbil

- Visto por primera vez en 1998 • Virus de Windows 95 y 98
- Infecta archivos ejecutables y Corrompe todo el sistema de archivos cuando se alcanza una fecha de activación

Klez

- Gusano que infecta mediante correo masivo Sistemas Windows 95 a XP
- La fecha de activación hace que los archivos del disco duro queden vacíos.

Ransomware

- Cifra los datos del usuario y exige el pago para acceder a la clave necesaria para recuperar la información.

- El troyano cibernético de PC (1989)
- Troyano Gpcode (2006)

Carga útil

Corrupción del sistema

- Daños en el mundo real • Provoca daños a equipos físicos o El virus Chernobyl reescribe el código BIOS • Gusano Stuxnet o Ataca software de sistemas de control industrial específico • Existen preocupaciones sobre el uso de ataques sofisticados y dirigidos malware para sabotaje industrial

- Bomba lógica
  - Código incrustado en el malware que está configurado para "explotar" cuando se cumplen ciertas condiciones

Carga útil – Agentes de ataque

Bots

- Se apodera de otra computadora conectada a Internet y la utiliza para lanzar o administrar ataques. • Botnet : conjunto de bots capaces de actuar de manera coordinada.

- Usos: •
  - Ataques distribuidos de denegación de servicio (DDoS) •
  - Spam •
  - Espionaje de tráfico
  - • Registro de pulsaciones de teclas • Difusión de nuevo malware • Instalación de complementos publicitarios y objetos auxiliares del navegador (BHO) • Ataques a redes de chat IRC • Manipulación de encuestas y juegos en línea

Mando a distancia

Instalación

- Distingue un bot de un gusano • El gusano se propaga y se activa a sí mismo
  - El bot se controla inicialmente desde alguna instalación central.
- El medio típico para implementar la función de control remoto es en un servidor IRC.
  - Los bots se unen a un canal específico en este servidor y tratan los mensajes entrantes como comandos
  - Las botnets más recientes utilizan canales de comunicación encubiertos a través de protocolos como HTTP
  - Los mecanismos de control distribuido utilizan protocolos peer-to-peer para evitar un único punto de falla.

Carga útil – Robo de información

Keyloggers y spyware

Registro de teclas

a

- Captura pulsaciones de teclas para permitir que el atacante controle información confidencial.
  información
- Generalmente utiliza algún tipo de mecanismo de filtrado que solo devuelve información cercana a las palabras clave ("inicio de sesión", "contraseña")

Programa espía

- Subvierte la máquina comprometida para permitir el monitoreo de una amplia gama de actividades en el sistema.
  - Monitoreo del historial y contenido de la actividad de navegación.
  - Redirigir ciertas solicitudes de páginas web a sitios falsos
  - Modificar dinámicamente los datos intercambiados entre el navegador y ciertos sitios web de interés

Carga útil – Robo de información

Suplantación de identidad (phishing)

- Explota la ingeniería social para aprovecharse de la confianza del usuario haciéndose pasar por una comunicación de una persona de confianza. fuente
  - Incluir una URL en un correo electrónico no deseado que enlace a un sitio falso
    Sitio web que imita la página de inicio de sesión de un sitio bancario, de juegos o similar
  - Sugiere que el usuario debe tomar una acción urgente para autenticar su cuenta.
  - El atacante explota la cuenta utilizando las credenciales capturadas

• Suplantación de identidad (spear phishing)

- El atacante investiga cuidadosamente a los destinatarios.
- El correo electrónico está diseñado específicamente para adaptarse a su destinatario, a menudo citando una variedad de información para convencerlo de su autenticidad.

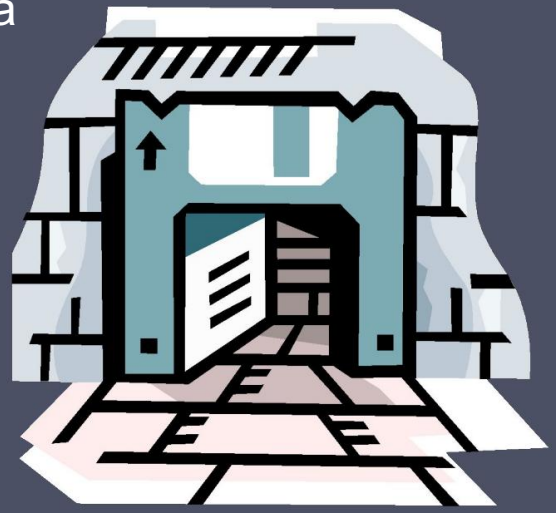
Contramedidas contra gusanos

- Superposición considerable en las técnicas para tratar los virus y gusanos
- Una vez que un gusano reside en una máquina, se puede utilizar un software antivirus para detectarlo y posiblemente eliminarlo.
- La actividad de la red perimetral y el monitoreo del uso pueden formar la Base de una defensa contra gusanos
- Los enfoques de defensa contra gusanos incluyen:
  - o Filtrado de escaneo de gusanos basado en firmas
  - o Contención de gusanos basada en filtros
  - o Contención de gusanos basada en la clasificación de carga útil
  - o Detección de escaneo de umbral de paseo aleatorio (TRW)
  - o Limitación de velocidad
  - o Detención de la tasa

Carga útil: sigilo

Puerta trasera

- También conocida como trampilla
- Punto de entrada secreto a un programa que permite Atacante para obtener acceso y eludir los procedimientos de acceso de seguridad.
- El gancho de mantenimiento es una puerta trasera utilizada por Programadores para depurar y probar programas.
- Es difícil implementar controles del sistema operativo para puertas traseras en aplicaciones.



Carga útil: sigilo

Kit de raíz

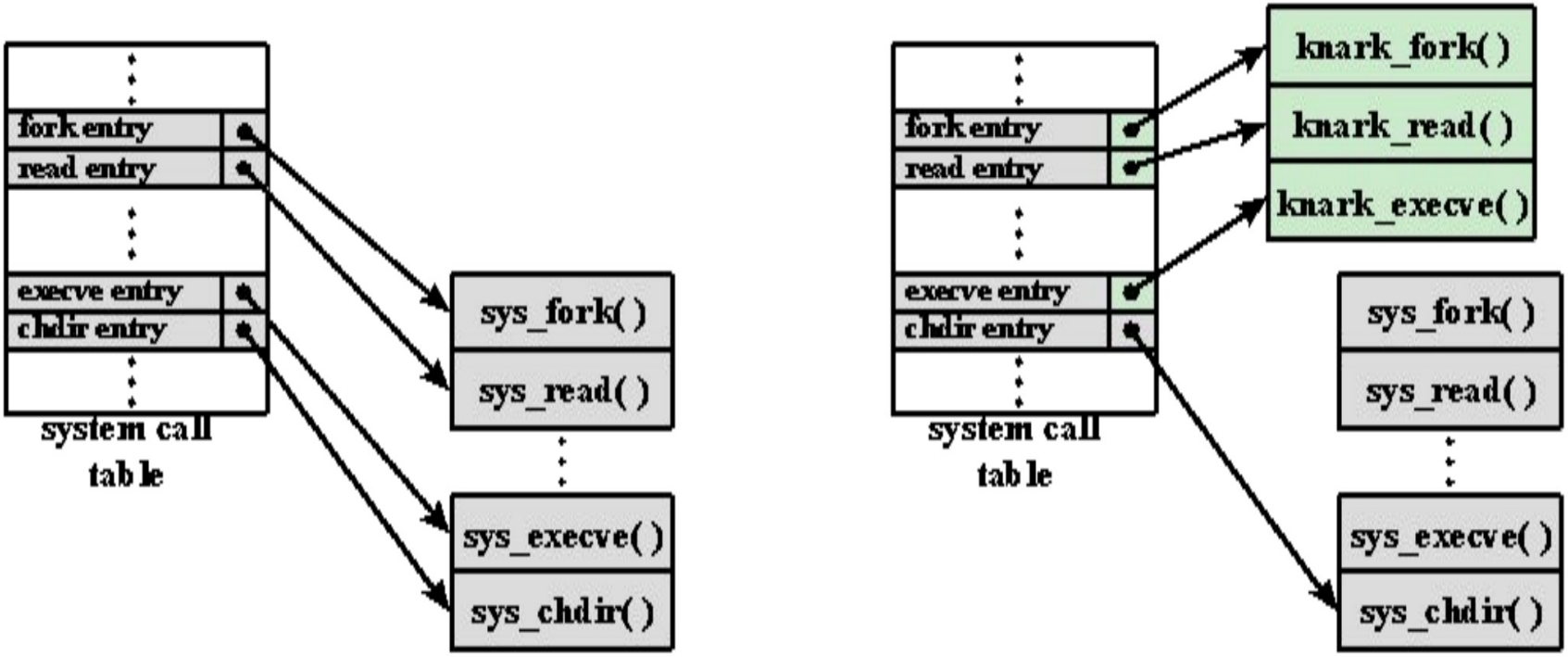
- Conjunto de programas ocultos instalados en un sistema para mantener acceso encubierto a ese sistema
- Se oculta subvirtiendo los mecanismos que monitorean e informan sobre los procesos, archivos y registros de una computadora
- Otorga privilegios de administrador (o root) al atacante

  - Puede agregar o cambiar programas y archivos, monitorear procesos, enviar y recibir tráfico de red y obtener acceso de puerta trasera a pedido.

Clasificación de rootkits

Características

Persistente	Basado en la memoria	Modo de usuario
Modo kernel	Basado en máquina virtual	Modo externo



(a) Normal kernel memory layout

(b) After nkark install

Figure 6.4 System Call Table Modification by Rootkit

Contramedidas contra malware

Aproches

- La solución ideal a la amenaza del malware es la prevención.

Cuatro elementos principales de la prevención:

- Política
- Conciencia
- Mitigación de vulnerabilidades
- Mitigación de amenazas

- Si la prevención falla, se pueden utilizar mecanismos técnicos para apoyar las siguientes opciones de mitigación de amenazas:
  - Detección
  - Identificación
  - Eliminación

Generaciones de software antivirus

Primera generación: escáneres simples

- Requiere una firma de malware para identificar el malware.
- Limitado a la detección de malware conocido

Segunda generación: escáneres heurísticos

- Utiliza reglas heurísticas para buscar posibles instancias de malware
- Otro enfoque es la comprobación de la integridad.

Tercera generación: trampas de actividad

- Programas residentes en la memoria que identifican el malware por sus acciones en lugar de por su estructura en un programa infectado

Cuarta generación: protección completa

- Paquetes que consisten en una variedad de técnicas antivirus utilizadas en conjunto
- Incluye componentes de escaneo y captura de actividad y capacidad de control de acceso.

Descifrado genérico (GD)

- Permite que el programa antivirus detecte fácilmente Virus polimórficos complejos y otro malware manteniendo velocidades de escaneo rápidas
- Los archivos ejecutables se ejecutan a través de un escáner GD que contiene los siguientes elementos:
  - Emulador de CPU
  - Escáner de firmas de virus
  - Módulo de control de emulación
- El problema de diseño más difícil con un escáner GD es determinar cuánto tiempo se debe ejecutar cada interpretación.

Software de bloqueo de comportamiento basado en host

- Se integra con el sistema operativo de un host

  Computadora y monitorea el comportamiento del programa en tiempo real para detectar acciones maliciosas.

  - Bloquea acciones potencialmente maliciosas antes de que tengan la oportunidad de ocurrir. afectar el sistema
  - Bloquea el software en tiempo real, por lo que tiene una ventaja sobre las técnicas de detección de antivirus, como la toma de huellas dactilares o la heurística.

Limitaciones

- Porque el código malicioso debe ejecutarse en el objetivo máquina antes de que se puedan identificar todos sus comportamientos, puede causar daño antes de que haya sido detectada y bloqueada

Enfoques de escaneo perimetral

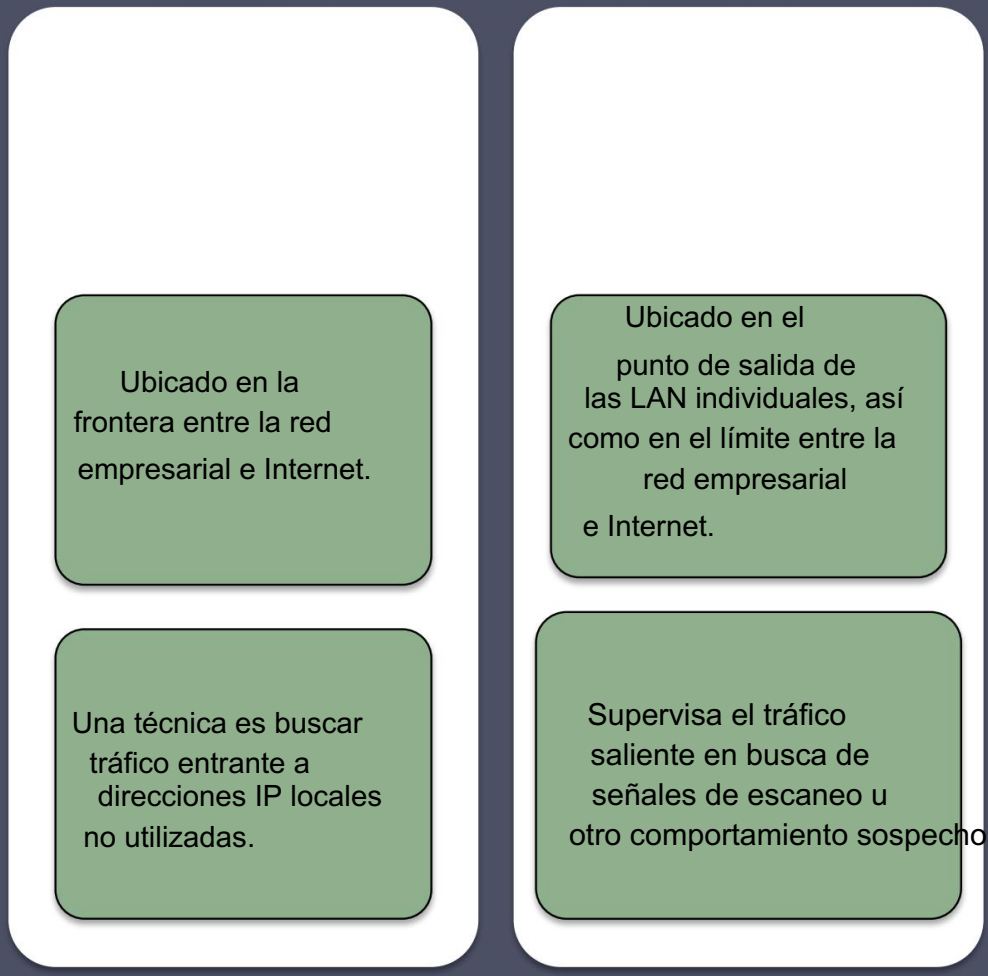
- Software antivirus

  Generalmente se incluye en servicios de proxy web y de correo electrónico que se ejecutan en el firewall y el IDS de una organización.

- También puede incluirse en el componente de análisis de tráfico de un IDS.

- Puede incluir medidas de prevención de intrusiones, bloqueando el flujo de cualquier tráfico sospechoso.

- El enfoque se limita al escaneo de malware.



Dos tipos de software de monitorización

Resumen

- Tipos de software malicioso (malware)
- Amenaza persistente avanzada
- Propagación
  - o Contenido infectado
    - • virus
  - o Explotación de vulnerabilidad
    - • gusanos
  - o Ingeniería social
    - • spam • correo electrónico
    - • Troyanos

- Carga útil
  - o Corrupción del sistema
  - o Agente de ataque
    - • Zombi
    - • Bots
  - o Robo de información
    - • Registradores de teclas
    - • Suplantación de identidad (phishing)
    - • Spyware
  - o sigilo
- Contramedidas