

Descripción de las amenazas de Internet

Prólogo

Por favor, consulte la [introducción](#) a nuestra sección Glosarios, para una mejor comprensión de los criterios, terminología y convenciones utilizadas.

🔍 Presionando el atajo de teclado **Control + F** podrá hacer búsquedas simples en esta página.

Definiciones de programas y códigos maliciosos

Adware

Ver [Publicidad no solicitada](#).

Bulo

Hoax

Los bulos son generalmente bromas, y suelen formar parte de una cadena de correo electrónico, y a menudo también, configuran las llamadas leyendas urbanas.

Estos bulos cibernéticos intentan generar miedo, incertidumbre y dudas en el receptor del mensaje, haciéndole creer que existe un "virus indetectable" en el sistema.

Algunos son maliciosos en contenido y logran que el receptor elimine archivos de su sistema.

Sólo hay que eliminarlos. No es verdad lo de la buena suerte al enviar 20 copias a todos los amigos, ni tampoco le va a enseñar nada sobre la seguridad del ordenador.

Algunos sitios con información sobre bulos:

<http://www.encyclopediavirus.com/enciclopedia/ver.php?id=12> (en español)

<http://www.vsantivirus.com/hoaxes.htm> (en español)

<http://www.snopes.com/> (en inglés)

<http://www.virushoax.co.uk/> (en inglés)

***Caballo de Troya**

Ver [Trojano](#).

Capturadores de pantalla

Programas de seguimiento que registran imágenes de la actividad en pantalla.

Los capturadores de pantallas, por lo general, almacenan las imágenes y vídeos registrados para su posterior recuperación, o los transmiten a un proceso o persona remota.

Existen algunos usos legales de los capturadores de pantallas, pero a menudo son utilizados por los agresores para realizar un seguimiento escondido del comportamiento del usuario en Internet, y para realizar otras acciones indeseadas y sin autorización, entre las que puede contarse el hurto de identidad.

Carga adicional

Payload

Es la función adicional, por ejemplo al robo de información, la eliminación de archivos, formateo de disco, la actualización de la memoria BIOS, entre otros, que pueden estar incluidos en los gusanos o trojanos.

No es necesario que la carga adicional sea dañina.

Por ejemplo el *payload* del virus **Form.A** provocaba que el teclado hiciera ciertos ruidos un día en el mes, y no hacía más daño que eso.

En el caso de un trojano, el acceso remoto y secreto es la función oculta, y adicional, que el programador desea alcanzar.

Cifrado

El cuerpo de los virus cifrados está dividido en dos partes básicas.

La parte ejecutable está codificada. Para poder ser procesada, se utiliza el sector del código llamado "descifrador", que la descodifica antes de su ejecución.

El cifrado fue hecho para hacer más dificultoso el análisis y la detección de un virus. En la actualidad no abundan los descifradores polimorfos en uso, pero tampoco escasean. Los que acarrearán más inconvenientes son los de gran tamaño, múltiples y distribuidos.

Código malicioso

Malware

Bajo el término *Malware*, derivado de la unión de dos palabras (en inglés): **malicious software**, se cobija una gran cantidad de diversos tipos de aplicaciones y códigos dañinos y/o potencialmente peligrosos, que actúan en un ordenador sin el conocimiento ni consentimiento del usuario.

Si bien no hay consenso absoluto sobre la traducción, al español, del término *malware*, ya que se ha utilizado "código malintencionado" y "código potencialmente dañino" entre otros, en este glosario utilizaremos, como traducción, "código malicioso" a pesar que el término "malicioso" está definido como "que tiende a pensar mal", más que a la acción concreta del daño potencial.

Técnicamente, tanto un programa (o aplicación) como un código (*Script* o guión) se basan en sentencias escritas en un orden determinado, en un lenguaje específico, que puede ser interpretado en un ordenador, bajo un entorno operativo definido, para su ejecución.

Generalmente, un código (*Script* o guión) consta de pocas sentencias mientras que un programa, puede llegar a comprender hasta miles de instrucciones en su interior.

Existen otras grandes diferencias operativas entre estos dos tipos básicos de "código" pero escapa, su detalle, de la intención de este documento.

Por lo tanto, y a los efectos de este glosario, utilizaremos el término *malware* o su traducción, código malicioso, en su acepción más amplia.

***Dropper**

Ver [Liberador de virus](#).

Espía

Ver [Programas espía](#).

EXE

Los archivos con extensión .EXE contienen código de procesamiento ejecutable, capaces de modificar su ubicación y operar en más de un segmento.

Falsificación de sitios

Phishing

Este es un ataque de ingeniería social que intenta obtener, de forma fraudulenta, información privada, como claves personales y/o detalles de las tarjetas de crédito.

Generalmente esto se logra por medio de un correo electrónico (o alguna comunicación similar) simulando ser emitida por una persona o entidad confiable con un pedido de información aparentemente legítimo.

Los casos de *Phishing* más comunes, simulan provenir de conocidos bancos y generalmente contienen algún aviso de discontinuación de servicios u otras consecuencias indeseables, si no se siguen ciertas instrucciones y en un plazo perentorio.

Muchas veces el correo se ve como genuino y hasta contiene información que originalmente pudo haber pertenecido a la fuente que ahora intenta simular.

Usualmente hay un vínculo en el correo que lleva, al receptor, a un sitio de Internet (que también se ve bastante similar al sitio Web legítimo), y este se utiliza para capturar todos los detalles e información personal del usuario.

Es importante recordar que tanto los bancos como las empresas importantes nunca solicitarán nombres de usuarios ni claves personales por medio de correos electrónicos. También hay que tener en cuenta que los vínculos en los mensajes de correo que implementan técnicas *Phishing*, aunque parezcan legítimos, siempre apuntan a un sitio diferente y oculto.

Por eso, es recomendable abrir una nueva sesión en el navegador y escribir la dirección habitual (previamente conocida) en la barra de direcciones, tal como cuando el usuario intenta entrar a la página Web de su banco o realizar otras operaciones en Internet.

Y, ante la duda, consulte telefónicamente con su banco o entidad de confianza antes de completar una operación de este tipo.

Fraude

Scam

La técnica denominada *Scam* es muy similar al *Phishing*, pero con la diferencia que no busca obtener detalles del usuario, sino que apela a la compasión o a la ambición humana para obtener un rédito económico.

Por ejemplo, casi todas las catástrofes (terremotos, inundaciones, guerra, hambre, etcétera) han generado una gran cantidad de *Scams*, generalmente en el formato de pedidos de ayuda por una causa real.

Las estafas cibernéticas, como por ejemplo *Advanced Fee Fraud* (conocido también como *Scam 419*) ofrece a los usuarios la oportunidad de conseguir grandes sumas de dinero con sólo ayudar al emisor del *Scam* (*Scammer*) a sacar sumas de dinero aún más grandes fuera de un país determinado (generalmente países africanos como Nigeria).

Estos *Scams* siempre piden al usuario el envío de dinero para cubrir los gastos "administrativos" (generalmente miles de euros). A veces estos *Scams* tienen como resultado el secuestro o desaparición de la persona engañada al viajar a otro país a encontrarse con su "benefactor". En los casos menos extremos, mucha gente ha perdido miles de euros a causa de estos fraudes cibernéticos.

Algunas sugerencias para evitar esta técnica:

- Las instituciones de caridad legítimas sólo mandan correos electrónicos pidiendo ayuda a las personas que han expresado explícitamente su deseo de recibir esos mensajes.
Los correos electrónicos como estos, que no fueron solicitados, son generalmente fraudulentos, especialmente si aparecen justo después de alguna catástrofe.
- No hay que dejarse engañar por las apariencias. Los correos electrónicos pueden parecer legítimos con sólo copiar los gráficos y el lenguaje de alguna organización legítima.
Muchos incluyen historias trágicas de las víctimas de las catástrofes. En caso de alguna duda, diríjase directamente al sitio Web de la organización, donde sí podrá realizar donaciones legítimas y de forma segura. El usuario interesado puede verificar la legitimidad de gran cantidad de estos sitios en <http://www.charity-navigator.org/>
- Hay que tener cuidado con los vínculos en los correos electrónicos, estos generalmente llevan a sitios Web engañosos que simulan la apariencia de una organización genuina.
Algunos sitios de control (en inglés):
<http://www.scambusters.org/> y <http://hoaxbusters.ciac.org/HBScams.shtml>

Gusano

También denominado Gusano de Internet

Worm, I-Worm, Internet Worm

En términos informáticos, los gusanos son en realidad una subclase de virus, pero tienen la habilidad de reproducirse por ellos mismos, no necesitando de un archivo anfitrión.

Una aproximación simple a sus diferencias, indica que, los virus infectan archivos (anfitriones), mientras que los gusanos infectan sistemas.

A menudo los gusanos se aprovechan de las vulnerabilidades existentes en las redes. Estos gusanos pueden esparcirse muy rápidamente por las redes de sistemas vulnerables, ya que ellos no necesitan de la intervención del usuario para ejecutarse.

Sin embargo, la clase más común de gusanos, se propaga por medio de correos electrónicos (es importante aclarar que no son los correos los infectados sino los archivos gusanos que ellos transportan).

En estos casos, el correo suele contener asuntos y mensajes llamativos y, la vulnerabilidad, se genera en el receptor del mismo. Habitualmente, los gusanos son mucho más fáciles de eliminar de un sistema que un virus, porque ellos no infectan archivos.

Los gusanos intentan agregarse a la carpeta de inicio, o modificar las claves del registro para asegurarse que sean cargados cada vez que el sistema se inicia. Una de las consecuencias de la infección por gusanos suele ser una sensible merma en el ancho de banda disponible por un uso intensivo de la misma.

Otra vez, es importante aclarar que los gusanos no necesariamente tienen que ocasionar algún daño.

📄 Ver [Carga adicional](#).

***Hoax**

Ver [Bulo](#).

***Keylogger**

Ver [Registrador de pulsaciones](#).

***Keystroke Logger**

Ver [Registrador de pulsaciones](#).

Liberador de virus

Dropper

Un *dropper* (liberador de virus) es un archivo ejecutable de baja complejidad. Su única función es instalar virus en la memoria o atacar archivos mediante los mismos.

La aplicación *dropper*, es normalmente utilizada por su autor, para propagar diversos tipos de código malicioso "en bruto" que son generados al ejecutar el programa. Estos virus, una vez creados, continúan actuando por su cuenta y expandiendo la infección a su manera.

En el caso de virus polimorfos el programa dropper, generalmente, no contiene un descifrador polimorfo, sino sólo el cuerpo del virus.

***Malware**

Ver [Código malicioso](#).

***Payload**

Ver [Carga adicional](#).

***Phishing**

Ver [Falsificación de sitios](#).


Programas espía

Spyware

Originalmente, era usual que los programas espía sólo recolectaran información con fines de mercadeo, la que era enviada, sin el conocimiento del usuario, al autor u organización que había originado dichos programas maliciosos.

Con el transcurso del tiempo y el desarrollo de nuevas técnicas delictuales, algunos han sido preparados para enviar información sensible, como números de cuentas bancarias y datos de tarjetas de crédito. Este término ha sido utilizado de dos formas:

- En el sentido más estricto, “programas espía” es una denominación para describir programas de rastreo ubicados sin el control, consentimiento o conocimiento del usuario.
A menudo el seguimiento se hace pasando información a terceras partes (cualquier cosa puede ser incluida en esta categoría, desde el historial de búsqueda hasta números de tarjetas de crédito o detalles personales). Algunos programas espía se entregan como parte de otras aplicaciones (muy similares a los [caballos de Troya](#)), pero algunos son introducidos como elementos adicionales en los gusanos ([Carga adicional](#)) o a través de los sitios de Internet que aprovechan vulnerabilidades en los buscadores para instalar programas en segundo plano. También existen muchos programas que dicen ser anti-espía, pero en la realidad son programas espía.

 Puede consultar varias listas de anti-espías falsos en:
<http://www.vsanvirus.com/lista-nospyware.htm> (español)
<http://www.spywarewarrior.org/> (inglés)
- En el sentido más amplio del término, “programas espía” es utilizado como sinónimo de lo que la Coalición de programas anti-espía llama “Programas espía y otras tecnologías potencialmente indeseadas”. En este grupo se pueden incluir algunas clases de *cookies*, capturadores comerciales de teclado, y otras tecnologías de rastreo, como *Snoopware*.

En configuraciones técnicas, ASC utiliza el término programa espía solamente en su sentido más acotado y siempre lo indica como tal [programaespía(acotado)]. Sin embargo, entendemos que es imposible evitar las connotaciones más amplias del término en el uso coloquial o popular y no intentamos hacerlo.

Publicidad no solicitada

Adware

Es una clase de programa que muestra publicidad emergente, específicamente ciertas aplicaciones ejecutables cuyo propósito principal es mostrar contenidos de mercadeo en una forma o contexto que no es esperado ni solicitado por el usuario. Muchas aplicaciones que contienen publicidad no deseada también realizan funciones de seguimiento, y por lo tanto se las puede categorizar dentro de las Tecnologías de rastreo.

Algunos consumidores pueden eliminar esta publicidad si se niegan a tal intromisión a su privacidad, si no desean ver los anuncios generados por el programa, o si encuentran frustrante los efectos de las mismas en el rendimiento del sistema.

Por otro lado, algunos usuarios prefieren mantener algunos mensajes con este tipo de información si su presencia costea un cierto producto o servicio, o si proporcionan datos que le son útiles o deseados, tales como la publicidad que pudiera ser competitiva o complementaria a lo que el usuario está buscando.

Registrador de pulsaciones

Keylogger o Keystroke Logger

Programa de seguimiento que registra la actividad del teclado y/o del ratón. Los registradores de pulsaciones (*keyloggers*) habitualmente almacenan las pulsaciones registradas para una posterior recuperación, o las transmiten a un proceso o persona remota que esté utilizando este programa.

Si bien existen algunos usos legales de los registradores de pulsaciones, a menudo los agresores los utilizan de manera maliciosa para realizar un seguimiento escondido del comportamiento y efectuar acciones no deseadas o no autorizadas, incluyendo el hurto de identidad, aunque no limitándose a este delito.

Rootkit

Conjunto de herramientas de administración

Un *rootkit* es una colección de una o más herramientas diseñadas para controlar de forma encubierta un ordenador y obtiene o mantiene, de manera fraudulenta, un acceso a nivel de administrador que puede también ejecutarse de forma indetectable.

Una vez que el programa obtiene acceso, puede utilizarse para controlar el tráfico y las pulsaciones de teclas; crear una puerta trasera hacia el sistema para que sea utilizada por un agresor, editar archivos del registro, atacar otros equipos en la red o modificar herramientas existentes en el sistema para sortear la detección.

Los *rootkits* reemplazan el comando original del sistema para ejecutar instrucciones maliciosas elegidas por el agresor, y para esconder su presencia en el sistema al modificar los resultados devueltos, eliminando toda evidencia de su operación.

Inicialmente, los *rootkits* aparecieron en los sistemas operativos Unix (inclusive Linux) y consistían en una o más herramientas, que permitían al atacante acceder como usuario más privilegiado en el ordenador (en el sistema UNIX a este usuario se lo denomina *root* –raíz, de allí su nombre)

En los sistemas con plataforma Windows, los *rootkits* han sido asociados con herramientas, para ocultarle al usuario, programas o procesos. Cuando se instala un *rootkit* en Windows, este utiliza funciones del sistema operativo para ocultarse a sí mismo, y así no ser detectado, y a veces también es utilizado para ocultar otros programas maliciosos como capturadores de pulsaciones de teclado.

El uso de los *rootkits* no es necesariamente nocivo, pero es asociado cada vez más a programas maliciosos y a conductas indeseadas y constituyen una forma extrema de los programas de modificación del sistema.

Scam

Ver [Fraude](#).

Secuestrador

Programa de modificación de sistemas implantado sin aviso, consentimiento o control adecuado del usuario.

Los secuestradores a menudo modifican de manera inesperada las configuraciones del navegador, vuelven a dirigir búsquedas en Internet y/o pedidos de redes hacia sitios no buscados, o reemplazan contenidos de Internet.

Los secuestradores también pueden frustrar los intentos de los usuarios para deshacer estos cambios, al restaurar las configuraciones secuestradas cada vez que se inicia el sistema.

***Snoopware**

Ver [Programas espía](#).

***Spyware**

Ver [Programas espía](#).

***Trojan**

Ver [Troyano](#).

***Trojan horse**

Ver [Troyano](#).

Troyano

Trojan horse

Un caballo de Troya, a menudo denominado también como Troyano, es un programa que tiene como propósito visible realizar cierta acción, cuando en realidad, realiza otra. No siempre son dañinos ni maliciosos aunque las consecuencias de su instalación, potencialmente pueden serlo, y generalmente están relacionados con acciones tales como la eliminación de archivos, el formateo de los discos duros, o se los utiliza para darle acceso, al atacante remoto, a un sistema vulnerable.

Dentro de los Troyanos clásicos, encontramos a los capturadores de pulsaciones de teclado, los cuales son enviados como archivos de juego, o eliminadores de archivos disfrazados de herramientas útiles.

Los caballos de Troya pueden ser utilizados con varios propósitos incluyendo:

- Acceso Remoto (a menudo llamado herramientas de acceso remoto o RAT- *Remote Access Tools*, o puerta trasera).
- Captura de pulsaciones de teclado (*Keyloggers*) y robo de contraseñas (la mayoría de los programas espía están dentro de esta categoría).

Virus

Un virus es un programa que se copia a sí mismo, ya sea exactamente igual o en un formato modificado, como parte de un código ejecutable.

Los virus pueden utilizar varias clases de anfitriones, y algunos de los más comunes son:

- Archivos ejecutables (como los programas en el ordenador)
- Sectores de arranque
- *Boot* (partes de un código que le dice al ordenador dónde encontrar las instrucciones que utiliza para iniciarse)
- Archivos de guiones (como Windows Scripting o un guión de Visual Basic)
- Macros dentro de los documentos (esto hoy en día es mucho menos factible, ya que los macros, por ejemplo, en Microsoft Word, no se ejecutan en forma predeterminada)

Cuando un virus se inserta dentro de algún código ejecutable, se asegura su aplicación al mismo tiempo que dicho código y así se esparce en busca de otros anfitriones "limpios". Algunos virus sobrescriben los archivos originales, destruyéndolos de forma efectiva, pero muchos sólo se insertan de forma tal que pasan a formar parte del programa que los aloja, y de esta forma sobreviven los dos, el programa y el virus.

De acuerdo a la codificación del virus, este puede esparcirse hacia varios archivos en el sistema, y por la red, a través de archivos compartidos, alojándose en documentos y sectores de arranque de los discos. Aunque algunos virus se propagan por correo electrónico, no es esto lo que los define como virus. En realidad, la mayoría de las amenazas que se propagan por correo son gusanos.

Para ser un virus, el código simplemente tiene que reproducirse, no es necesario que ocasione mucho daño, ni siquiera que se propague ampliamente. Esta descripción no es taxativa y puede variar entre distintas empresas desarrolladoras de programas antivirus, así como en algunos casos, también efectúan la clasificación según la plataforma operativa: DOS, Windows, Linux, etc.

Si bien a este tipo de programas se los conoce genéricamente como virus, una mirada más profunda permite clasificarlos según el método de funcionamiento, aún cuando algunos virus pueden estar incluidos en más de una categoría:

- Bromas (*Joke*)
- Código malicioso (*Badware* o *Malware*)
- [Gusanos de Internet](#)
- Hoax o falsos virus
- Troyanos
- Virus de inicio
- Virus de la ayuda de Windows (HLP)
- Virus de macro o macrovirus
- Virus de Script
- Virus en Java
- Virus multifuncionales (archivos e inicio)
- Virus multi-plataforma

 Ver [Carga adicional](#).

Virus polimorfos

El polimorfismo es una tecnología que le permite a cada nueva generación de virus asumir una forma diferente que es, desde el punto de vista funcional, idéntica a la anterior.

El objetivo de usar polimorfismo es evitar la detección del virus mediante el uso de una muestra.

Virus satélite

Los virus satélite utilizan una técnica especial de infiltración, recurriendo a las variadas prioridades de inicio de los archivos ejecutables.

Cuando hay más de un archivo con el mismo nombre, pero con distintas extensiones en el directorio, y el sistema operativo recibe un pedido de ejecución de un programa, procesará primero aquel que tenga la extensión con prioridad de inicio más alta.

Los archivos con extensión BAT son los de prioridad más alta, seguidos por los COM, y finalmente, los EXE. El virus coloca su cuerpo en el archivo de igual nombre, pero con la extensión de máxima prioridad.

Entre los virus satélite, se encuentran también aquellos que colocan su cuerpo dentro de cualquier archivo, y crean una copia con el mismo nombre, pero con una extensión de mayor prioridad. De este modo consiguen que el cuerpo del virus sea leído y ejecutado.

***Worms**

Ver [Gusano](#).

Zombie

Sistema que ha sido tomado utilizando un programa de control remoto.

Los ordenadores *zombies* se utilizan a menudo para enviar correo electrónico no deseado o para atacar servidores remotos con una cantidad abrumadora de tráfico (un ataque distribuido de denegación de servicio).

Un grupo de varios *zombies* conforman un *Botnet*.