# INFORME AMENAZAS

# Amenaza 1: trojan horse.

* **Descripción de la amenza.**

Un troyano es un tipo de malware que puede acceder de forma remota a cualquier dispositivo sin el conocimiento del usuario. Según el tipo, las finalidades pueden variar desde bloquear, modificar o eliminar datos hasta recopilar información y enviarla a terceros.

Su nombre se basa en el mítico caballo de Troya que hace uso del engaño para pasar desapercibido. Disfrazado como un programa o software legítimo, un caballo de Troya se instala inadvertidamente sin el conocimiento del usuario, creando una puerta trasera que permite a los atacantes acceder a toda la información almacenada en él.

Los troyanos generalmente se propagan mediante algún tipo de ingeniería social, por ejemplo, cuando un usuario es persuadido para hacer click en un correo con un archivo adjunto que no hace sospechar.

Se diferencian de los virus informáticos y gusanos en que generalmente no intentan inyectarse en otros archivos o replicarse a sí mismos.

Hay diferentes tipos de troyanos:

* **Rootkit**: están diseñados para ocultar ciertos objetos o actividades del sistema infectado. Normalmente su propósito principal es prevenir que el usuario se de cuenta de la existencia de programas maliciosos en su sistema, para así extender el tiempo que permanecen en este. Afecta principalmente a la **integridad**.
* **Spyware**: este tipo se basa en obeservar la actividad realizada por el usuario, recolectando así información sensisble como por ejemplo credenciales de cuentas o datos bancarios. Estos datos son enviados al atacante. Afecta principalmente a la **confidencialidad**.
* **Backdoor**: aunque es uno de los tipos más simples, a su vez es uno de los más peligrosos. Esto es porque es capaz de abrir un tunel de comunicación secreto que permite al malware desplegado comunicarse con el atacante y recibir sus órdenes. Por lo tanto, puede permitir que el atacante controle el dispositivo infectado, monitorize o robe datos, e incluso instale nuevo software. Afecta principalmente a la **confidencialidad**.
* **Troyano DDoS**: un troyano de tipo DDoS convierte el equipo de la víctima en un zombie que participará en una red de ordenadores que se suele llamar botnet. El objetivo del atacante es hacerse con el poder de el máximo número de máquinas y utilizarlas para propósitos maliciosos sin el conocimiento ni consentimiento de los propietarios de estas. Típicamente el uso principal que hace el atacante es el de inhundar servidores con tráfico ficticio como parte de un ataque DDoS. Afecta principalmente a la **disponibilidad**.
* **Troyano downloader**: la funcionalidad principal de este tipo es la descarga de una o más amenazas de la red, que se encargarán de llevar a cabo las acciones maliciosas que el atacante quiera. Un downloader no contiene una carga maliciosa por sí solo, hecho que hace que sea más difícil detectarlo. Una de sus características principales es que configura el sistema infectado para que ejecute el conjunto de programas maliciosos automáticamente cuando esta arranca.

Requieren la interacción del usuario, es decir, necesitan que el usuario ejecute el archivo malicioso, y una de sus peculiaridades es que realiza la descarga legítima del software por el que se hacían pasar, camuflando de esta manera su presencia.

Suele confundirse por el troyano **dropper** pero no es exactamente lo mismo, ya que el dropper ya contiene la amenaza embedida en sí mismo. Afecta principalmente a la **integridad**.

* **Riesgos que supone.**
* **Eliminación de archivos**: uno de los principales problemas de los troyanos, que se intuye fácilmente, es la eliminación y corrupción de archivos contenidos en el sitema atacado. La gravedad de este problema variará en función de los sistemas de recuperación de archivos de los que el usuario disponía en el momento del ataque.

**\*SUSTITUIR POR OTRO RIESGO\***

* **Uso del sistema atacado para infectar a otros sistemas**: si por ejemplo un sistema de una emprea es infectado con un troyano, uno de los riesgos que corre esta empresa es el de que el troyano identifique otros ordenadores en la red y envíe correos en masa con archivos maliciosos adjuntos para infectar así más sitemas en una reacción en cadena. Uno de los mecanismos más utilizados es el phising. **\*SUSTITUIR POR OTRO RIESGO\***
* **Espiar a los usuarios**: uno de los usos que los atacantes dan a los troyanos es el de observar a los usuarios haciendo uso de la webcam de su sitema, comprometiendo la privacidad del usuario.
* **Keylogging**: un troyano dedicado al keylogging es capaz de registrar las teclas presionadas por el usuario, guardándolas en un archivo que es enviado al autor del ataque. De esta manera el atacante podra filtrar entre todo el texto contenido en el fichero para encontrar información sensible como contraseñas, números de tarjeta, etc. Algunos troyanos de este tipo que son más avanzados que el resto tienen la capacidad de distinguir actividad específica del usuario como el acceso al navegador apuntando a una web o tipo de web específico, por ejemplo webs bancarias.
* **Obtención de información sensible**:consiste en que el troyano es capaz de identificar y enviar al atacante archivos almacenados en el sitema de la víctima que contienen información sensible. Afecta principalmente a las compañías industriales, que suelen ser el objetivo más apuntado por los atacantes, ya que contienen una inmensa cantidad de información sensisble en sus servidores que es de mayor interés para el atacante que la que puedan encontrar en un PC de escritorio de una persona media.
* **Medidas correctivas(para evitar la amenaza).**
* **Adquisión de un nuevo producto**: implementación de una zona demilitarizada (DMZ) para controlar el tráfico que entra y sale de la empresa al exterior e instalación de sistemas NIDS para anlizar constantemente la red. No recomendamos HIDS ya que al instalarse en el host lo ralentizan, y ya contamos con software antivirus para contrarestar esto.
* **Contratación de un nuevo servicio**: contratación de un data center de respaldo, situado en un área geográfica algo alejada CPD principal para mitigar problemas causados por catástrofes naturales y gestionado por una empresa externa (outsorcing). Envío de datos entre data centers mediante copias diferenciales. Si se dispara el precio de almacenamiento recomendaríamos el cambio a copias incrementales, ya que que requieren menor almacenamiento, sin embargo habría que tener en cuenta que provocan que el tiempo de restauración sea mayor.
* **Ejecución de un cambio interno**: se recomienda a la alta dirección la inversión de tiempo y recursos en implementar cursos de formación relacionados con el phising para todos los empleados cuya actividad requiere el uso de un ordenador.

Además, se debería comprobar que el sistema de inventariado controle que todos los usuarios tengan la versión más reciente del antivirus utilizado por la empresa. También es importante que el sistema de activos tenga bien identificado y localizado a cada sistema, ya que en caso de que haya una infección masiva, será mucho más fácil mitigar el problema.

Se debería de definir un apartado específico para la gestión de esta amenaza dentro de la política de seguridad de la empresa para tener bien documentada toda la información referente a esta amenaza y actuar de manera ágil en caso de que ocurra.

Finalmente, recomendamos la formalización del proceso de gestión de riesgo, llevando a cabo las actividades de análisis, estimación, aceptación, evaluación y tratamiento del riesgo.

* Ejemplos de troyanos (casos reales).
* **Zeus(2007)**: es un troyano distribuido a través de archivos maliciosos escondidos en correos electrónicos y webs falsas. Es conocido por propagarse rápidamente y por registrar keystrokes, lo que ha hecho que se use principalmente para el robo de credenciales y contraseñas, como cuentas bancarias.

Se ha usado para a atacar a grandes empresas como Amazon, el Banco Americano y Cisco. Se estima que desde su creación en 2007, ha provocado daños valorados en más de 100 millones de dólares. No solo se ha utilizado el troyano original, sino que también han ido surgiendo variantes a partir de este.

* **Stuxnet**: fue un troyano especializado en el SO Windows diseñado para atacar sistemas de control industriales (ICS). Concretamente, se utilizó para atacar la central nuclear de Iran, haciendo que las centrifugadoras alcanzaran muchas revoluciones por segundo causando la explosión de estas. Provocó graves pérdidas para el gobierno de Irán.
* **Emotet**: fue descubierto por primera vez en 2014 por investigadores de seguridad. Se diseño originalmente como un malware bancario que intentaba colarse en el ordenador y robar información privada y sensible.

Utiliza funcionalidad específica que le ayuda a evadir la detección por parte de productos anti-malware. Se distribuye principalmente a través de emails.

En febrero de 2022, se habían confirmado más de 2.7 millones de casos confirmados utilizando Emotet tan solo en el último año. Los daños causados en cada caso por Emotet provocan pérdidas de hasta 1 millón de euros.