UNIVERSIDAD CATOLICA DE HONDURAS

“NUESTRA SEÑORA REINA DE LA PAZ”



CLASE: SEGURIDAD INFORMATICA Y GESTION DE RIESGO

TEMA: AMENAZAS EN UN SISTEMA INFORMATIICO

ING . PATRICIA MEDINA

ESTUDIANTE : ANTONIA ROSIBEL PERDOMO AMAYA

CUENTA: 1305200000366

FECHA: 22-OCTUBRE-2022

Malware

El malware es un software creado con fines maliciosos, diseñado para infectar y dañar un sistema.

Dado que es un término amplio, [el malware](https://es.godaddy.com/blog/que-es-malware-y-como-proteger-wordpress/) abarca las vulnerabilidades que van desde virus informático hasta adware que pueden infectar tanto los ordenadores como las páginas web.

Las consecuencias de un ciberataque por malware supone la exposición de datos confidenciales, incluida la información de tus clientes.

Los ataques de malware pueden ser muy perjudiciales para las empresas, especialmente para aquellas que no son capaces de reconocerlos.

En el segundo trimestre de 2021, McAfee Labs monitoreó un [promedio de 688 amenazas por malware por minuto](https://revistabyte.es/ciberseguridad/malware-2021/). Una cifra un 3% superior a la del primer trimestre de este mismo año.

Dos de los tipos de malware más comunes son:

* Defacement, que cambia la apariencia de una web. Usualmente, la página mostrará un mensaje que contiene el nombre del hacker.
* Redirección maliciosa: en esta situación, cuando los usuarios acceden a tu web, se les redirige a otra página que contiene contenido malicioso. Esto puede hacer que ciertas páginas, o incluso toda la web, sean inaccesibles para los usuarios.

[Seguridad de la página web de GoDaddy](https://www.godaddy.com/es-es/seguridad-web/seguridad-pagina-web) ofrece varias opciones para mantener tu web segura, incluido el análisis, la prevención y la [eliminación de malware](https://es.godaddy.com/blog/como-funciona-la-eliminacion-de-malware-express-de-godaddy-para-limpiar-el-malware/).

Esta herramienta es ideal para propietarios de pequeñas empresas que no tienen tiempo, conocimientos especiales ni recursos tecnológicos necesarios para proteger adecuadamente sus páginas contra amenazas en Internet.

Inyección SQL

Las vulnerabilidades suelen ocurrir cuando una página contiene un fallo de seguridad en el código que permite que aquellos con intenciones maliciosas ataquen o consigan el control.

Esto es comúnmente causado por problemas en [plugins de WordPress](https://es.godaddy.com/blog/plugins-para-wordpress/) desactualizados u otras herramientas utilizadas en tu web.

La Inyección SQL es un tipo de ciberataque que involucra declaraciones SQL maliciosas o códigos de aplicación que se inyectan en los campos de entrada del usuario. Este proceso permite a los atacantes obtener acceso al backend de la web o al contenido corrupto de la base de datos.

Si el ataque se completa con éxito, pueden robar información del cliente, modificar o eliminar datos, o para conseguir un control absoluto de la web.

Esta es una de las amenazas informáticas más extendida en el mundo.

Un firewall de aplicaciones web (WAF), incluido en el paquete de Seguridad de la página web de GoDaddy, puede proteger tu web contra ataques de Inyección SQL.

Un WAF es un servicio de firewall basado en la nube que criba y protege el tráfico de tu web en tiempo real contra amenazas tales como ataques de Inyección SQL y spammers, a la vez que evita los ataques DDoS.

Cross-site scripting (XSS)

Este tipo de vulnerabilidad, también denominada XSS, es otro de los tipos comunes de amenazas informáticas más habituales que puede sufrir tu web.

A diferencia de la Inyección SQL, XSS ocurre cuando las líneas de código JavaScript malicioso se inyectan en una página para dirigirse a los usuarios de dicha web, manipulando scripts del lado del cliente.

Estos scripts secuestran las sesiones de los usuarios a través de la barra de búsqueda de una página web o comentarios (a través del backend).

Esto puede alterar la web y redirigir a los usuarios a otras páginas maliciosas que pueden manifestarse como páginas aparentemente de apariencia normal, pero que, en realidad, pueden robar su información.

Intercepción

Un ataque por Intercepción ocurre cuando un hacker captura datos que los usuarios envían a una web, y luego los utiliza para su propio beneficio. Puede ser información de contacto o datos sensibles como la tarjeta de crédito.

Los ciberdelincuentes luego venden estos datos o hacen sus propias compras.

Entre muchos ejemplos, [un grupo de ciberdelincuentes](https://www.globalsign.com/en/blog/what-is-a-man-in-the-middle-attack/) hackeó en Bélgica varias empresas europeas en 2015 para acceder a datos financieros confidenciales. Robaron 6 millones de euros como resultado de estas actividades criminales.

Es importante [instalar en tu web un certificado SSL](https://www.godaddy.com/es-es/seguridad-web/certificado-ssl) para proteger los datos confidenciales.

El certificado SSL encripta las conexiones entre el navegador del visitante y el servidor web, para establecer una sesión segura. Esto protege a los compradores de ataques cibernéticos, como el de por Intercepción.

Entonces, ¿[tu web necesita un certificado SSL aunque no vendas online](https://es.godaddy.com/blog/tener-una-conexion-cifrada-con-ssl-si-no-vendo-online/)? La respuesta es sí.

Ataques de contraseñas

Algunos hackers adivinan contraseñas o usan herramientas y programas de diccionario para probar diferentes combinaciones hasta que las encuentran.

En algunos casos, el registro de teclas también se usa para conseguir el acceso a cuentas de usuario. El registro de teclas reconoce cada golpe de teclado realizado por un usuario. Los resultados se comunican nuevamente a los hackers que inicialmente instalaron estos programas.

¡Ojo! Ten cuidado al usar los ordenadores y redes de WIFI públicas.

Muchas webs carecen de contraseñas seguras, lo que hace que los intentos de iniciar sesión sean increíblemente fáciles. Estas son algunas formas de proteger tu página web:

* Solicita una combinación segura y única de contraseñas.
* Pídeles a los usuarios que cambien regularmente sus contraseñas.
* Requiere autenticación de dos pasos para confirmar el acceso del usuario.

Y, por favor, no dejes “admin” como tu nombre de usuario en WordPress.

Ataque DDoS

Un [ataque de denegación de servicio distribuido](https://es.godaddy.com/blog/que-es-un-ataque-ddos-y-como-prevenirlo/) (DDoS) se da cuando un servidor web recibe mucho tráfico o solicita que se sobrecargue o que se inunde el sistema.

Se trata de tráfico falso de equipos controlados por atacantes, a menudo llamados botnets. Una botnet es una cantidad de dispositivos conectados a Internet que ejecutan uno o más bots.

Cuando el servidor web se ve sobrecargado por el tráfico o las solicitudes, la web se carga mal o no llega a cargarse. Con la fuerza suficiente detrás de estos ataques, el servidor de la web puede bloquearse, lo que desactiva completamente la página.

Según un análisis de F5 Labs, los ataques DDoS han aumentado un 55% en 2021 con respecto al año anterior.

¿La moraleja? ¡Los ataques DDoS siguen en aumento, tanto en número como en complejidad!

Afortunadamente, prevenir los ataques DDoS no tiene que ser complicado. La supervisión avanzada de seguridad y el firewall de aplicaciones web (WAF) de la Seguridad de la página web de GoDaddy pueden evitar este tipo de amenazas informáticas.

Configuración de seguridad incorrecta

Este ataque ocurre cuando las configuraciones de seguridad de una web tienen agujeros de seguridad que pueden conducir a varias vulnerabilidades.

Esto ocurre a menudo debido a la falta de un [mantenimiento adecuado de tu página](https://es.godaddy.com/blog/empieza-a-usar-pro-sites-para-el-mantenimiento-de-tu-pagina-web/) o una configuración inadecuada de la aplicación web.

Una configuración de seguridad incorrecta permite a los piratas informáticos acceder a datos privados o funciones de la web que pueden comprometer completamente el sistema. En estas situaciones, los datos también pueden ser robados o modificados.