



MALWARES

RAMOS BARRAZA JORGE
ARIAN ESPINOZA

.. PRIMERO... HAY QUE ENTENDER QUE ES UN MALWARE.

El malware se considera un tipo molesto o dañino de software destinado a acceder a un dispositivo de forma inadvertida, sin el conocimiento del usuario.



3 CONCEPTOS CLAVE DEL SISTEMA OPERATIVO

- ✗ Abstracción: su acceso debe estar limitado a la interfaz que el sistema le ofrece.
- ✗ Administración de recurso: debe evitar que el usuario exceda las asignaciones aceptables
- ✗ Aislamiento: separación entre los datos, procesos y recursos de sus distintos usuarios,

Los sistemas operativos, al igual que todo programa de cómputo, presentan imperfecciones, errores u omisiones, tanto en su diseño como en su implementación.



VULNERABILIDADES

Si la vulnerabilidad que aprovecha el código malicioso es resultado de un error en la implementación, el desarrollador del sistema operativo típicamente podrá corregirla

si la vulnerabilidad es consecuencia de una debilidad en el diseño, su corrección puede ser mucho más compleja

TIPOS DE MALWARE

- ✗ Gusanos / Worms
- ✗ Spyware
- ✗ Ransomware
- ✗ Exploits
- ✗ Virus
- ✗ Troyanos
- ✗ Adware



GUSANOS / WORMS

- ✗ ILoveYou (o VBS/LoveLetter) es un gusano escrito en VBScript.
- ✗ infectó aproximadamente 50 millones de computadores



RANSOMWARE

- ✗ Virus de la Policía
- ✗ Koler el ransomware móvil "de la policía" dirigida a dispositivos Android

RANSOMWARE



POLICÍA FEDERAL
Estados Unidos Mexicanos



Apoyado y Protegido por 

IP: [REDACTED]

Location: MX, Mexico, Distrito Federal, Mexico

ISP: Metro Net, S.A.P.I. de C.V.

User Name: [REDACTED]



¡ATENCIÓN! Su OP (ordenador) está bloqueado debido a al menos una de las razones especificadas siguientes.

Usted ha violado «el derecho de autor y los derechos conexos» (video, música, software) y ha utilizado de una manera ilegal con la distribución de contenido los derechos de autor, infringiendo así el artículo 128 del Criminal Code de los Estados Unidos Mexicanos.

El artículo 128 del Criminal Code prevé una multa 200 a 500 de los salarios mínimos o la privación de la libertad de 2 a 8 años.

Código PIN

Suma

2000 ▼

1

2

3

4

5

6

7

8

9

0

Pagar Ukash

Pagar PaySafeCard

¿Dónde puedo comprar PaySafeCard?

Disponible muy cerca de ti. En México puedes obtener PaySafeCard en las tiendas de 7-Eleven, extra®, Ley, Comercial mexicana, Blockbuster, Sanborns, Superette, Fast!, Del Río, Soriana y en selectos puntos de OXXO.





SPYWARE

✗ Perfect Keylogger


✗ Este programa corre en el computador una vez instalado, está completamente escondido de los usuarios y registra todo lo que pasa en el teclado



ADWARE





✗ 1ClickDownloader se ejecuta en su computadora para mostrar anuncios no deseados sin su consentimiento.

1Click Downloader

Download your files with 1Click Downloader
Review special offers while you downloading

Babylon
With Babylon you get simple one-click translation in any application, simply click on any text in any desktop application to get immediate translation and much more...

 Search 

- ☒ Install Babylon toolbar
- ☒ Set Babylon as my default home page, new tab page
- ☒ Set Babylon Search as my default search provider

By clicking "Next" you agree to install Babylon by the selected settings and to the [terms of service](#)

Decline

1Click Downloader

Next >>>

EXPLOITS

✗ Públicos

✗ zero-day



¿CÓMO PUEDE ENTRAR UN MALWARE EN UNA COMPUTADORA?

- A través de enlaces o archivos adjuntos en el correo electrónico
- Al hacer clic en ventanas emergentes
- Usar JavaScript mientras se navega por Internet
- Iniciar sesión en sitios falsos

Los ataques de malware no funcionarían sin el ingrediente más importante: nosotros.

HABLEMOS DE EXPLOITS



¿QUÉ ES UN EXPLOIT?

Es como un modelo de cerradura (sistema o aplicación) tuviera un fallo de diseño que nos permitiera crear llaves que la abrieran (exploit) y poder así acceder al sitio que trata de proteger y realizar actos delictivos (malware).

Existe confusión entre los usuarios y cierto mito de que un exploit puede considerarse malware. La realidad es que, tal y como hemos visto en el ejemplo, no es un código malicioso en sí mismo, sino que es la llave para que estos accedan a nuestro sistema.

De esta forma, puede proporcionarles los permisos necesarios para poder ejecutarse en un sistema e infectarlo aprovechándose de una vulnerabilidad.



EXPLOITS ACTIVOS

Los exploits activos son aquellos que explotan un host específico, se ejecutan hasta completarse y entonces salen.

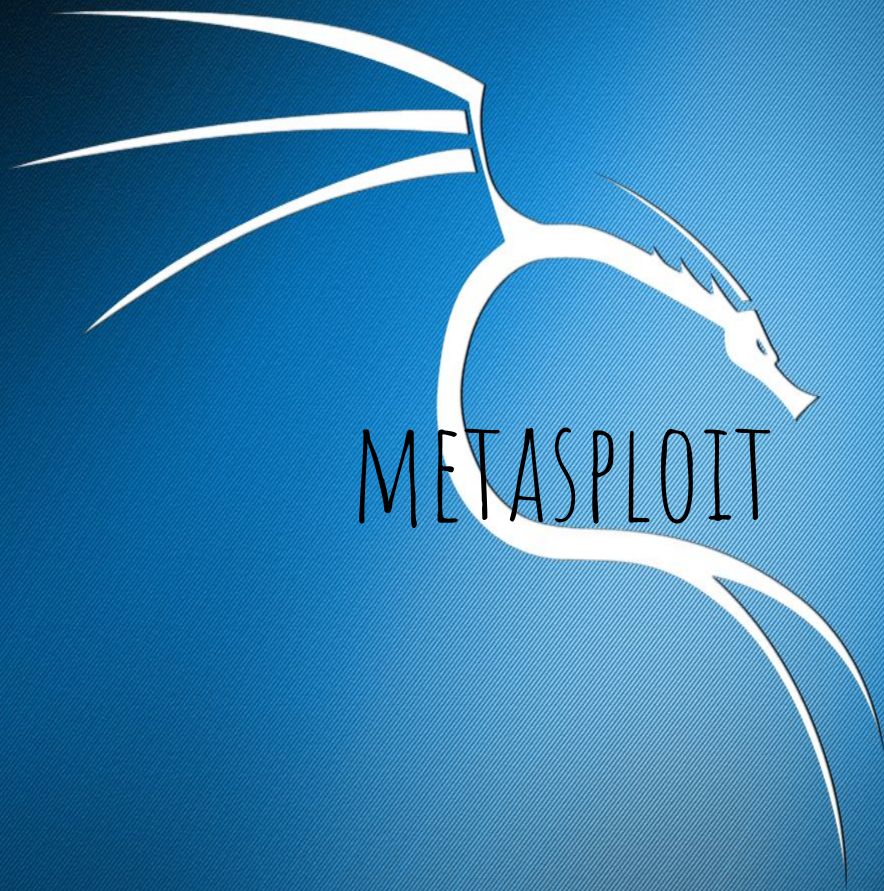
- Los módulos de fuerza bruta pueden salir cuando una shell es abierta por la víctima.
- Si un error ocurre, la ejecución del módulo se detiene.
- Usted puede forzar un módulo activo a pasar a "background" o segundo plano pasando el argumento -j al comando del exploit.

EXPLOIT PASIVO

Exploits Pasivos.

Los exploits pasivos funcionan de esta manera: esperan hasta que un host interactue con el exploit y entonces lo explotan.

- Los exploit pasivos se concentran normalmente en navegadores, clientes FTP y similares.
- Pueden ser usados en conjunto con exploits enviados por e-mail.
- Los exploits pasivos, una vez ejecutados, reportan que se ha abierto una shell y esperan ser enumerados pasando el argumento `-l` al comando `sessions`. Pasando el argumento `-i` interactuamos con una shell que se encuentre en el listado.



METASPLOIT

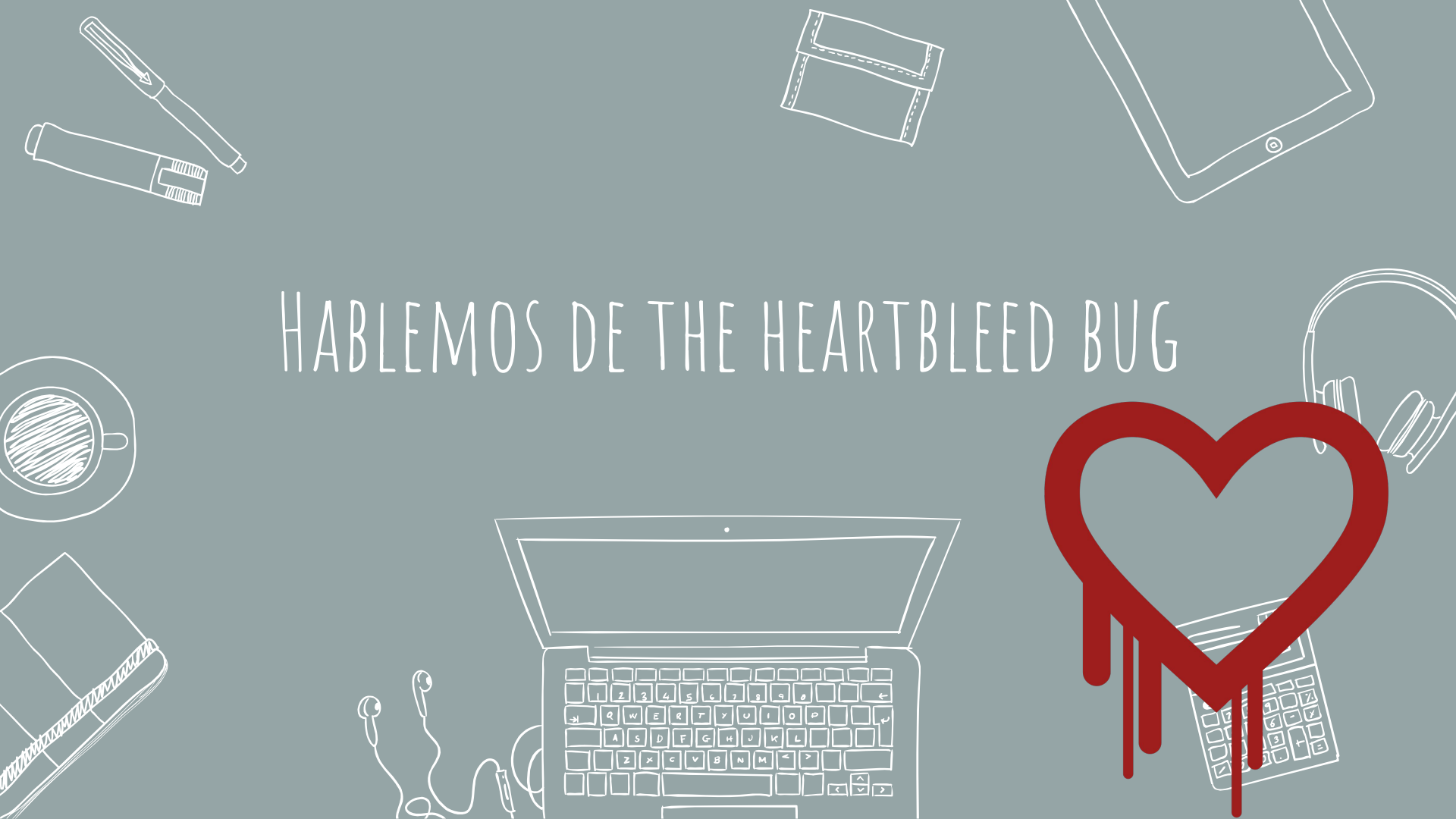




METASPLOIT FRAMEWORK

EL proyecto más conocido es el Metasploit Framework de código abierto [2], una herramienta para desarrollar y ejecutar código de explotación contra una máquina de destino remota. Otros subproyectos importantes incluyen la base de datos Opcode, el archivo shellcode e investigaciones relacionadas.

HABLEMOS DE THE HEARTBLEED BUG





THE HEARTBLEED BUG

Heartbleed es un error de seguridad divulgado en abril de 2014 en la biblioteca de criptografía OpenSSL, que se usa ampliamente para la implementación del protocolo de Seguridad de la capa de transporte (TLS). • Heartbleed puede explotarse independientemente de si la parte que utiliza una instancia de OpenSSL vulnerable para TLS es un servidor o un cliente. •



EL PROTOCOLO HEARTBEAT

El protocolo Heartbeat es un nuevo protocolo que se ejecuta sobre la capa de grabación. El protocolo en sí consta de dos tipos de mensajes: HeartbeatRequest y HeartbeatResponse. • Un mensaje HeartbeatRequest puede llegar casi en cualquier momento durante la vida útil de una conexión.



FUNCIONAMIENTO

Cuando se recibe un mensaje de HeartbeatRequest y no se prohíbe el envío de HeartbeatResponse, el receptor debe enviar un mensaje de HeartbeatResponse correspondiente con una copia exacta de la carga útil de HeartbeatRequest recibida. • Si un mensaje HeartbeatResponse recibido no contiene la carga útil esperada, el mensaje debe descartarse. Si contiene la carga útil esperada, se debe detener el temporizador de retransmisión.

EL ATAQUE HEARTBLEED

La vulnerabilidad radica en la variable de carga útil. • Idealmente, el código debe verificar la longitud de los datos de la carga útil con la longitud real de los datos enviados en la solicitud Heartbeat, pero no lo está verificando. • Entonces, si la carga útil excede la longitud estándar en la solicitud, el servidor puede devolver más datos en respuesta de lo que idealmente debería devolver. Este es un caso de desbordamiento de búfer (BoF).

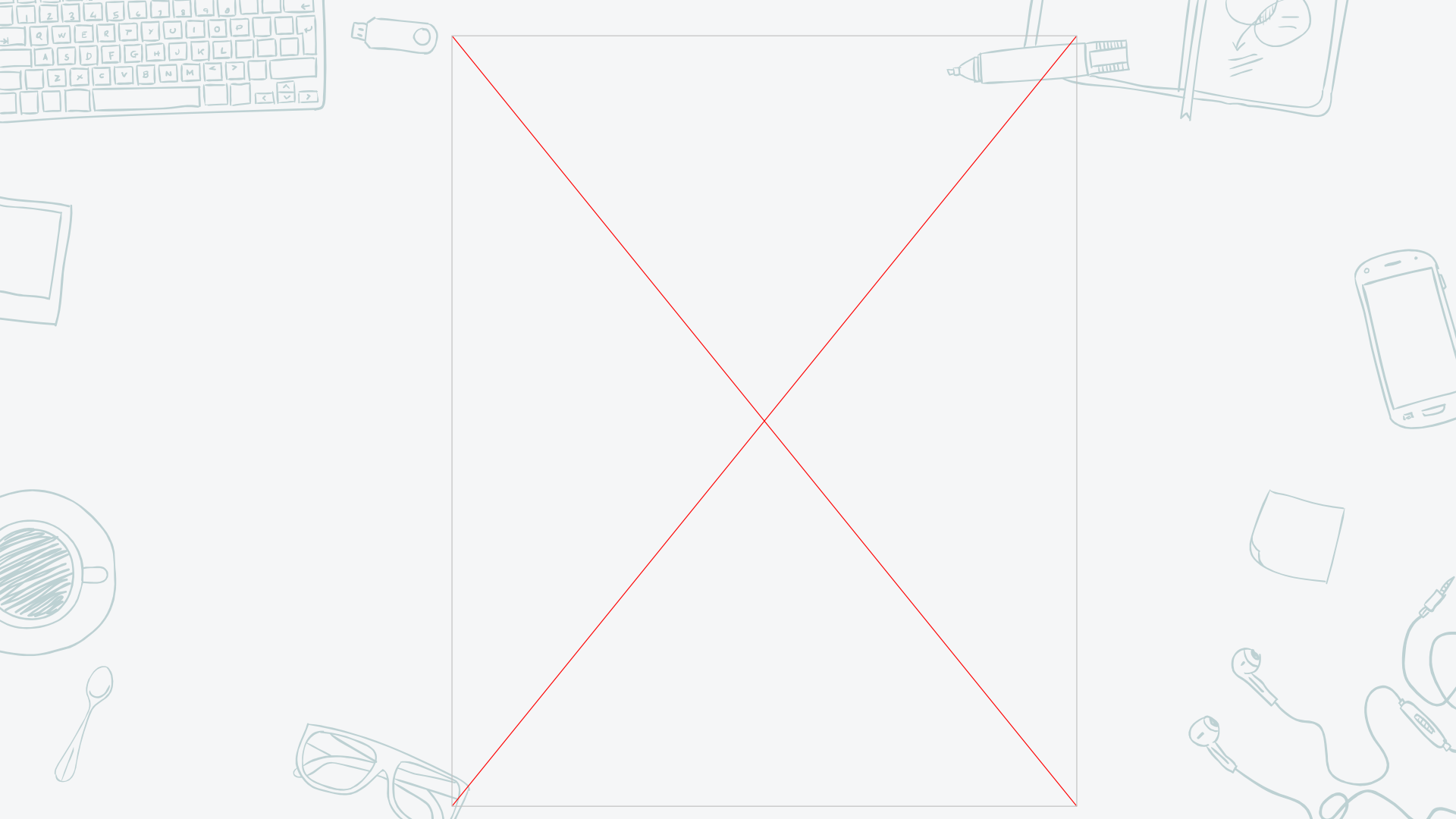
¿SOLUCIÓN?

Esta vulnerabilidad se encuentra en la versión 1.0.1f y 1.0.2 - beta1 de OpenSSL. • Los usuarios afectados deben actualizar a OpenSSL 1.0.1g. • Los usuarios que no pueden actualizar inmediatamente pueden recompilar OpenSSL alternativamente con `-DOPENSSL_NO_HEARTBEATS`. • versión OpenSSL



GRACIAS!





PRESENTATION DESIGN

- ✗ <https://www.redeszone.net/2017/09/23/asegurarnos-no-queda-malware-al-formatear-disco-duro/>
- ✗ <https://www.avg.com/es/signal/what-is-malware>
- ✗ <https://culturacion.com/diferencia-entre-exploits-y-xploits/>
- ✗ https://es.wikipedia.org/wiki/Virus_inform%C3%A1tico#Virus_inform%C3%A1ticos_y_su_propagaci%C3%B3n_en_otros_sistemas_operativos
- ✗ <https://www.seguridad.unam.mx/historico/noticia/index.html-noti=1274>