

Código malicioso

Capítulo destinado a acciones de respuesta ante incidentes de malware

- [Wordpress comprometido](#)
- [SEO Japonés](#)
- [Joomla comprometido](#)
- [Ransomware](#)
- [Adware](#)
- [Backdoors/webshells](#)
- [Herramientas sandbox](#)

Wordpress comprometido

Revisión Online

Verificar que no tenga instalado malware:

- <https://www.virustotal.com/#/home/upload>
- <https://sitecheck.sucuri.net/>

Verificar con herramientas de google el grado de compromiso del sitio:

- <https://transparencyreport.google.com/safe-browsing/overview>
- <https://www.youtube.com/watch?v=IG5IOix9b9k>

Es necesario acceder a la consola de búsqueda de google:

- <https://search.google.com/search-console/welcome>

Para verificar enlaces comprometidos, obtener el contenido en línea, recuperar posible código malicioso.

Coordinación con el RSI

- Solicitar al RSI que no debe eliminar ningún archivo ni realice cambios en la base de datos.
- Si el sitio web sufrió un defacement solicitar al RSI que mueva los archivos de la instalación wordpress a otra ruta que no sea accesible desde el servidor web. Ej. /home/[USUARIO] y que establezca un sitio web temporal mientras dure la investigación.
- Solicitar los archivos de la instalación de wordpress.
- Solicitar el envío del backup de la base de datos.
- Solicitar el envío de los logs del servidor web.

Revisión Offline

1. Comprobar la integridad de los archivos WordPress (Core y Plugins)

- Descargar la versión de wordpress que se tiene instalada de

<https://wordpress.org/download/releases/>

```
diff -r wordpress_Instalado wordpress_descargado
```

- De manera similar proceder con los plugins y themes.
- Alternativamente se puede usar:

```
wp core verify-checksums --allow-root
```

2. Buscando patrones de cadena maliciosos:

2.1. Buscar webshells/backdoors en el sistema de archivos

2.1.1. Usando GREP

Guardar en el archivo pattern.txt

```
eval($_REQUEST
eval($_GET
eval($_POST
eval(
$GLOBALS[
$strrev(' dedoce
base64_decode
str_replace
preg_replace
gzinflate
$f53[
hacked
FilesMan
\x73\x74\x72\x5f
str_rot13
Location:
google.com
bing.com
```

Ejecutar el comando:

```
fgrep -rf pattern.txt folderInstalacion | egrep -iv "\.js|\.css|\.po|\.html| Binary" >
resultado.txt
```

Eliminar los falsos positivos.

Otros patrones sospechosos (ejecutar dentro del directorio principal):

```
grep -r '\\x' * | egrep -iv "\.gif|\.js|\.png|\\# entities"
grep -r '\\057' * | egrep -iv
"\.gif|\.js|\.png|\\# binary|Crypto|zip|case|elseif|ChaCha|\\x00|pie|escaper"
```

2.1.2. Usando la herramienta webshell-scanner-client

Descargar e instalar webshell-scanner-client

```
wget https://github.com/baidu-security/webshell-scanner-client/releases/download/v1.0/webdir-
linux32.bin
sudo mv webdir-linux32.bin /usr/bin/webshell-scanner-client
sudo chmod a+x /usr/bin/webshell-scanner-client
```

Escanear un archivo

```
webshell-scanner-client.bin archivo.php-
Solicitar al RSI que mueva los archivos de la instalacion wordpress a otra ruta que no sea
accesible desde el servidor web.
Ej: /home/[USUARIO]
```

2.1.3. Usando la herramienta webshell-scan

Descargar e instalar webshell-scan:

```
git clone https://github.com/tstillz/webshell-scan
go build main.go
sudo mv main /usr/bin/webshell-scan
```

Escanear en busca de webshells con extensión en php:

```
webshell-scan -dir . -exts php
```

2.1.4. Usando findbot

Instalación:

```
wget https://raw.githubusercontent.com/wellr00t3d/findbot.pl/master/findbot.pl
chmod a+x findbot.pl
sudo mv findbot.pl /usr/bin
```

Buscar archivos maliciosos:

```
findbot.pl directorio
```

Verificando archivos de wordpress

- .htaccess
- wp-config.php
- Revisar los archivos functions.php

```
find . -iname "functions.php"
```

- Verificar que archivos se han modificado recientemente:

```
find . -type f -printf "%-.22T+ %M %n %-8u %-8g %8s %Tx %.8TX %p\n" | sort | cut -f 2- -d ' '
```

Escanear el servidor en busca de códigos maliciosos en los archivos

Buscar código malicioso en archivos y carpetas de WordPress:

```
find wp-includes -iname "*.php"
find wp-content/uploads -name "*.php" -print
```

Escanear la base de datos en busca de códigos maliciosos

- Descargar un back de la base de datos "backup.sql"
- Guardar en el archivo pattern.txt

```
<script>
eval
base64_decode
gzinflate
preg_replace
str_rot13
```

- Ejecutar el comando:

```
fgrep -rf pattern.txt backup.sql > resultado.txt
```

- Eliminar los falsos positivos.

Detección de cuentas de administrador falsas

Encuentre y elimine nuevos usuarios administradores o cuentas FTP que no ha creado.

Restauración del sitio:

- Eliminar los backdoors identificados y restaurar el sitio web con los archivos antiguos.
- Borrar themes no usados.
- Borrar plugins no usados.
- Actualizar el core, theme y plugins.
- Instalar el plugin WP Hardening (<https://wordpress.org/plugins/wp-security-hardening/>)
- Cambiar la contraseña de los usuarios de :
 - WordPress
 - Base de datos
 - Hosting/Cpanel

Herramientas

<https://malwaredecoder.com>

Anexos

Instalar wp-cli y checksum:

```
curl -O https://raw.githubusercontent.com/wp-cli/builds/gh-pages/phar/wp-cli.phar
chmod +x wp-cli.phar
sudo mv wp-cli.phar /usr/local/bin/wp
wp package install git@github.com:wp-cli/checksum-command.git --allow-root
```

SEO Japonés

Joomla comprometido

Revisiones Online

Verificar que no tenga instalado malware:

- <https://www.virustotal.com/#/home/upload>
- <https://sitecheck.sucuri.net/>
- <https://transparencyreport.google.com/safe-browsing/search>

Coordinación con el RSI

- Solicitar al RSI que no debe elimine ningun archivo ni realice cambios en la base de datos
- Si es un incidente de defacement, solicitar al RSI que establezca un sitio web temporal mientras dure la investigacion. En el archivo configuration.php configurar la variable \$offline = '1';
- Solicitar los archivos de la instalacion de jomla
- Solicitar el envio del backup de la base de datos
- Solicitar el envio de los logs del servidor web

Revisiones Offline

- Borrar themes no usados
- Borrar plugins no usados
- Revisar el archivo .htaccess, verificar que no hay redirecciones extrañas
- Verificar integridad de archivos core de la instalación de joomla con <https://audit-fs.co.za/>
- Descargar los componentes usados del repositorio oficial
- Actualizar el core: <https://www.youtube.com/watch?v=Duba0GEj2L8>
- Revisar integridad de archivos, comparar con los archivos descargados
<https://downloads.joomla.org/es/latest>

```
diff -r joomla-3.6.4 ./public_html
```

Restauración del sitio

- Eliminar los backdoors identificados y restaurar el sitio web con los archivos antiguos

- Cambiar las contraseñas de los usuarios de:
 - Joomla
 - Base de datos
 - hosting/Cpanel

Modificar permisos:

- `chmod 444 .htaccess`
- `chmod 444 index.php`

Instalar las extensiones

- <https://extensions.joomla.org/extension/securitycheck/> (Revisa componentes con vulnerabilidades)
- <https://www.akeebabackup.com/products/akeeba-backup.html> (Realizar backups)
- <https://extensions.joomla.org/extension/brute-force-stop/>
- <https://www.richeyweb.com/software/joomla/plugins/1-adminexile/>

Reemplazar el contenido del archivo `.htaccess` con:

Herramientas

<https://malwaredecoder.com>

Actualización del core de Joomla a la última versión

1. Descargar el paquete de actualización <https://downloadas.joomla.org/es/>
2. Sobre escribir los archivos en el servidor con los del paquete de actualización.
3. Si sale el error "Fatal error: Call to undefined method JApplicationSite::set()"
 1. Reemplazar la carpeta `libraries` con las de la instalación completa.
4. Si sale un error "Unknown column 'a.cliente_id' in 'where clause': Unknown column 'a.client_id' in 'where clause'" en el panel de administración.
 1. Ejecutar (Reemplazar XXXXX por el prefijo usado en la base de datos):

```
ALTER TABLE `XXXXXX_menu_types` ADD COLUMN `client_id` int(11) NOT NULL DEFAULT 0 AFTER `description`;
```

```
UPDATE `XXXXXX_menu` SET `published` = 1 WHERE `menutype` = 'main' OR `menutype` = 'menu';
```

Realizar correcciones en la base de datos. En el menú de administración:

Extensiones> Gestor de extensiones> Database> Corregir

Hardening de Joomla

- Cambiar el nombre del usuario administrador (admin) y crear un password robusto
- Los archivos deben tener los siguientes permisos:

Tipo de archivo	Permisos
Archivos PHP	644
Archivos de configuración	644
Otros folders	755

- Cambiar la ruta por defecto del panel de administración
- Deshabilitar el registro de usuarios:

tudominio.com/administrador/index.php?option=com_config&view=component&component=com_users

Ransomware

El ransomware es un tipo de software malicioso (malware) que se utiliza para bloquear el acceso a los archivos o sistemas de una víctima y exigir un rescate para restaurar el acceso. Los atacantes utilizan el ransomware para extorsionar a individuos y empresas mediante el cifrado de archivos o el bloqueo del acceso a sistemas críticos, lo que les impide acceder a sus datos y archivos importantes.

Una vez que el ransomware infecta un sistema, se suele mostrar una pantalla de advertencia que exige un pago en criptomonedas para obtener una clave de cifrado que permita desbloquear los archivos o sistemas afectados. En algunos casos, los atacantes también amenazan con publicar los datos de la víctima si no se paga el rescate.

El ransomware se propaga a menudo mediante técnicas de ingeniería social, como correos electrónicos de phishing, enlaces maliciosos o descargas de software ilegal. Además, algunos tipos de ransomware también pueden propagarse a través de vulnerabilidades en el software o sistemas no actualizados.

Es importante destacar que no se recomienda pagar el rescate exigido por los atacantes ya que no hay garantía de que los archivos o sistemas afectados sean restaurados, además de que esto puede animar a los ciberdelincuentes a continuar con sus actividades ilícitas. En lugar de pagar el rescate, es recomendable tomar medidas preventivas para evitar la infección por ransomware, como mantener el software actualizado, utilizar software de seguridad y educar a los empleados en técnicas de seguridad informática.

Intentar recuperar "shadow copy"

Listar si existen "shadow copies"

```
vssadmin list shadows
```

En caso que hubiera copias, usar ShadowExplorer.exe (portable) para recuperar archivos.

Determinar la forma de infección

- Información básica del sistema

```
systeminfo
```

- Información de red

```
ipconfig/all
```

- Identificar con que equipos se comunicó

```
arp -a
```

- Extraer el historial de navegación (Ejecutar como el usuario que infecto el equipo)
 - Chrome History View (AGAVE)
 - Mozilla History View (AGAVE)
 - IE History View (AGAVE)
- Registro de actividades (Necesita permisos de administrador)
 - LastActivityView
 - MyEventViewer
 - RecentFileView
 - USBDBView

Nota: Transformar los archivos a UTF-8 con el comando dos2unix.

Análisis forense

- Realizar el apagado brusco del equipo. Desconectar el cable (PC de escritorio), Usar el boton de apagado (Laptop)
- Realizar copia bit a bit del disco duro

```
dd if=/dev/sdc of=/media/parrot/disk600Gb/backup.img bs=64M conv=sync,noerror status=progress
```

Si fuera necesario convertir la imagen forense en disco virtual

```
qemu-img convert -O vmdk -o compat6 backup.img vmdkname.vmdk  
qemu-img convert -f raw -O vmdk rawdisk200gb.img vdisk200gb.vmdk
```

Herramientas útiles

- Identificar exactamente que variante de ransomware infecto al host
 - <https://id-ransomware.malwarehunterteam.com/index.php>
 - <https://www.nomoreransom.org/crypto-sheriff.php?lang=en>
 - Buscar IoC (IPs, dominios, etc) en los logs del firewall/proxy

Identificar si el ransomware usa llave simetrica (AES) o asimetrica (RSA). Si el ransomware usa una llave simetrica buscar la llave de encriptación en la copia de la memoria RAM.

Buscar herramientas para desencirptar

- <https://docs.google.com/spreadsheets/d/1TWS238xacAto-fLK1n5uTsdijWdCEsGIM0Y0Hvmc5g/pub?output=html>
- <https://heimdalsecurity.com/blog/ransomware-decryption-tools/>
- <https://www.nomoreransom.org/en/decryption-tools.html>
- <https://www.avast.com/ransomware-decryption-tools>
- <https://decrypter.emsisoft.com/>
- <https://support.kaspersky.com/viruses/utility>
- <https://noransom.kaspersky.com/?tool=>. [EXTENSION ARCHIVOS CIFRADOS]
- <https://malpedia.caad.fkie.fraunhofer.de/>

Intentar recuperar archivos de la copia forense

- Usar Autopsy con la copia forense
- Usar FTK para montar la imagen forense y usar el software de recuperacion "recuva"

Anexos

- Links de descarga:
 - <https://www.shadowexplorer.com/downloads.html>
 - <http://devcdn.avanquest.com/rw/WindowsDataRecovery.exe>
- Extracción de llave de cifrada estático (AES) de memoria RAM
 - <https://medium.com/@0xINT3/jigsaw-ransomware-analysis-using-volatility-2047fc3d9be9>
- Posibles vectores:
 - pop-ups
 - facebook messenger
 - mail
 - Cracks

Adware

Backdoors/webshells

1. Usando GREP

- Guardar en el archivo pattern.txt

```
eval($_REQUEST
eval($_GET
eval($_POST
eval(
$GLOBALS[
$strrev('dedoce
base64_decode
str_replace
preg_replace
gzinflate
$f53[
hacked
FilesMan
\x73\x74\x72\x5f
str_rot13
Location:
google.com
bing.com
```

- Ejecutar al comando

```
fgrep -rf pattern.txt folderInstalacion | egrep -iv "\.js|\.css|\.po|\.html|Binary" >
resultado.txt
```

- Eliminar los falsos positivos
- Otros patrones sospechosos (Ejecutar dentro del directorio principal)

```
grep -r '\\x' * | egrep -iv "\.gif|\.js|\.png|\\#|entities"
grep -r '\\057' * | egrep -iv
```



```
"\.\ gif| \. js| \. png| \#| binary| Crypto| zip| case| elseif| ChaCha| \\x00| pie| escaper"
```

2. Usando la herramienta webshell-scanner-client

- Descargar e instalar webshell-scanner-client

```
wget https://github.com/baidu-security/webshell-scanner-client/releases/download/v1.0/webdir-linux32.bin
sudo mv webdir-linux32.bin /usr/bin/webshell-scanner-client
sudo chmod a+x /usr/bin/webshell-scanner-client
```

- Escanear un archivo

webshell-scanner-client.bin archivo.php- Solicitar al RSI que mueva los archivos de la instalacion wordpress a otra ruta que no sea accesible desde el servidor web. Ej: /home/{usuario}

3. Usando la herramienta webshell-scan

- Descargar e instalar webshell-scan

```
git clone https://github.com/tstillz/webshell-scan
go build main.go
sudo mv main /usr/bin/webshell-scan
```

- Escanear en busca de webshells con extensión en php

```
webshell-scan -dir . -exts php
```

4. Usando findbot

- Instalar

```
wget https://raw.githubusercontent.com/wellr00t3d/findbot.pl/master/findbot.pl
chmod a+x findbot.pl
sudo mv findbot.pl /usr/bin
```

- Buscar archivos maliciosos

```
findbot.pl directorio
```


Herramientas sandbox

Una sandbox (en español, caja de arena) es un entorno aislado y seguro en el que se pueden ejecutar aplicaciones y procesos sin afectar al sistema principal. La idea detrás de una sandbox es crear un espacio limitado en el que los programas pueden ejecutarse sin afectar el resto del sistema, lo que permite a los usuarios probar o ejecutar aplicaciones sin preocuparse por los posibles efectos negativos.

Las sandboxes se utilizan a menudo para ejecutar software no confiable o potencialmente peligroso, como archivos de correo electrónico adjuntos, scripts descargados de Internet, software malicioso o programas que pueden dañar el sistema. Al ejecutar estos programas en una sandbox, el usuario puede analizarlos o probarlos sin exponer su sistema a posibles amenazas.

Además, las sandboxes también se utilizan para desarrollar y probar aplicaciones en un entorno seguro y aislado. Esto permite a los desarrolladores probar sus aplicaciones sin preocuparse por los posibles efectos negativos en el sistema principal.

Sandbox Online

Puede utilizar las siguientes sandbox:

- <https://sandbox.anlyz.io/>
- <https://app.any.run/>
- <https://www.hybrid-analysis.com/>
- <https://www.joesandbox.com>