

!#Think/divergent

GUÍA: ANALIZANDO LOS **MAGIC BYTES**

Una Mirada desde la
Ciberseguridad Ofensiva y
Defensiva

Samuel Rincón
consultoriapnl2015@gmail.com



¿Alguna vez te has preguntado cómo un sistema operativo o una aplicación "adivinan" el tipo de archivo con el que están tratando?

La respuesta a menudo reside en los **Magic Bytes**.

01

¿QUÉ SON LOS MAGIC BYTES?

Los Magic Bytes, también conocidos como números mágicos, son una secuencia de bytes al principio de un archivo que identifican su formato. Actúan como una "firma" que le dice al sistema qué tipo de datos contiene el archivo (por ejemplo, una imagen PNG siempre comienza con los bytes 89 50 4E 47 0D 0A 1A 0A).

```
# file Watson-2.0.zip
Watson-2.0.zip: Zip archive data, at least v1.0 to extract
# xxd Watson-2.0.zip|head
00000000: 504b 0304 0a00 0000 0000 6f27 c34e 0000  PK.....o'.N..
00000010: 0000 0000 0000 0000 0000 0b00 0900 5761  .....
00000020: 7473 6f6e 2d32 2e30 2f55 5405 0001 a30b  tsон-2.0/UT.....
00000030: f55c 504b 0304 0a00 0000 0800 6f27 c34e  .\PK.....o'.N
00000040: 37ee 5ddc 3e00 0000 4200 0000 1900 0900  7.]>...B.....
00000050: 5761 7473 6f6e 2d32 2e30 2f2e 6769 7461  Watson-2.0/.gita
00000060: 7474 7269 6275 7465 7355 5405 0001 a30b  ttributesUT.....
00000070: f55c 5356 702c 2dc9 5748 492d 494d 2e51  .\SVp,-.WHI-IM.Q
00000080: 2849 ad28 5148 cbcc 492d 5648 cc4b 5128  (I.(QH..I-VH.KQ(
00000090: 482d 4acb 2fca 55f0 7153 c803 d289 3999  H-J./.U.qS....9.
```

02

¿POR QUÉ SON IMPORTANTES EN **CIBERSEGURIDAD?**

Desde la perspectiva de la ciberseguridad ofensiva, los atacantes pueden manipular los Magic Bytes para disfrazar archivos maliciosos.

Desde la ciberseguridad defensiva, entender y analizar los Magic Bytes es crucial para detectar y prevenir este tipo de ataques.

03

¿CÓMO ANALIZAR LOS MAGIC BYTES?

1. Inspección Hexadecimal: La forma más directa es abrir el archivo con un editor hexadecimal. Los primeros bytes revelarán el "número mágico".

2. Comandos de Línea:

- **Linux/macOS:** El comando file a menudo utiliza una base de datos de Magic Bytes para identificar el tipo de archivo. Por ejemplo: file tu_archivo. También puedes usar xxd -p tu_archivo | head -n 1 para ver los bytes hexadecimales.
- **Windows:** Puedes usar PowerShell con Get-Content -Path "tu_archivo" -Encoding Byte | Select-Object -First 8 para obtener los primeros 8 bytes.

3. Herramientas Especializadas: Existen herramientas como TrID que utilizan una extensa base de datos de firmas para identificar el tipo de archivo incluso si la extensión es incorrecta. Tambien hay herramientas como ImHex el cual es un editor para ingeniería inversa que puede servirnos para ir más allá de los magic bytes y realizar un análisis exhaustivo de los ficheros.



gmh5225/Tool-
ImHex



EDITORES Y COMANDOS ÚTILES

- **Editores Hexadecimales:**
 - **HxD (Windows):** Gratuito y potente.
 - **Okteta (Linux):** Parte del entorno KDE.
 - **Hex Fiend (macOS):** Sencillo y eficiente.
 - **Online Hex Editors:** Numerosas opciones disponibles en línea para análisis rápidos.
- **Comandos de Línea:**
 - file (Linux/macOS)
 - xxd (Linux/macOS)
 - hexdump (Linux/macOS)
 - Get-Content (PowerShell - Windows)

PERSPECTIVA DE CIBERSEGURIDAD OFENSIVA

Los atacantes pueden explotar la confianza que los sistemas operativos y las aplicaciones depositan en los Magic Bytes para:

- **Bypass de Filtros:** Cambiar la extensión de un archivo malicioso (ej. de .exe a .jpg) pero mantener los Magic Bytes del ejecutable para que, al ser ejecutado por un usuario desprevenido, el sistema lo interprete correctamente.

- **Camuflaje:** Insertar código malicioso dentro de archivos aparentemente inofensivos (como imágenes o documentos) manipulando los Magic Bytes o aprovechando vulnerabilidades en el procesamiento de ciertos formatos.

PERSPECTIVA DE CIBERSEGURIDAD DEFENSIVA

La detección y prevención de ataques que involucran manipulación de Magic Bytes son cruciales:

- **Validación de Magic Bytes:** Los sistemas de seguridad (firewalls de aplicaciones web, antivirus, sistemas de detección de intrusiones) deben validar los Magic Bytes de los archivos entrantes independientemente de su extensión.

- **Análisis Forense:** En investigaciones de incidentes, la inspección de los Magic Bytes puede revelar la verdadera naturaleza de archivos sospechosos o confirmar si un archivo fue manipulado.
- **Políticas de Seguridad:** Implementar políticas que restrinjan la ejecución de archivos basados únicamente en su extensión y que promuevan el análisis del contenido.

EJEMPLOS CONCRETOS DE USO EN ATAQUES CONOCIDOS

1. Phishing con Archivos Disfrazados: Un atacante podría enviar un correo electrónico con un archivo adjunto que parece ser una imagen (.jpg o .png) pero que en realidad es un ejecutable malicioso (.exe) con los Magic Bytes correspondientes. Si el usuario ejecuta el archivo, el malware se activará.

2. Explotación de Vulnerabilidades en el Procesamiento de Formatos: Algunos ataques aprovechan vulnerabilidades en cómo ciertas aplicaciones procesan formatos de archivo específicos. Un atacante podría manipular los Magic Bytes y otros campos internos de un archivo para desencadenar un buffer overflow u otra vulnerabilidad al ser abierto por la aplicación vulnerable.

3. Bypass de Filtros de Carga de Archivos: En aplicaciones web con funcionalidades de carga de archivos, un atacante podría intentar subir un script malicioso (ej. .php, .jsp) disfrazándolo con la extensión de un archivo permitido (ej. .txt, .pdf) pero manteniendo los Magic Bytes del script. Si la aplicación solo verifica la extensión, el atacante podría lograr ejecutar código en el servidor.

CONCLUSIÓN

Los Magic Bytes son un concepto fundamental en la informática y juegan un papel importante en la ciberseguridad. Tanto los profesionales de la seguridad ofensiva como defensiva deben comprender cómo funcionan y cómo pueden ser utilizados o abusados para proteger los sistemas y la información.

¡Mantente atento a los bytes!

Samuel Rincón
consultoriapnl2015@gmail.com

Sígueme
para más

Información
y recursos
como este

!#Think/divergent

