# **Unpacking UPX Manually**

kausrini.github.io/2021-06-20-unpacking-upx-manually/

Detect It Easy v3.01				_
File name	12 Martin Martin States	the the file	all a stable	MARIAN,
C:/Users/Admin/Deskto	p/sample	1. 11. 1.1.	and a state of the	Red and the the
File type	Entry point		Base address	alling the Lin
PE32 -	00486970	Disasm	00400000	Memory map
PE	Export	Resources	.NET TLS	Overlay
Sections	TimeDateStamp Siz	eOfImage	Resources	1. 1. H. M. C. S.
0003 >	2013-10-14 05:10:28	00089000	Manife	est Version
Scan	Endianness	Mode	Architecture	4 Type
Detect It Easy(DiE)	LE	32	1386	GUI
packer	UPX(3.05	)[LZMA,brute]	1121411	S ?
compiler	Microsoft Vis	ual C/C++(2008	0[-]	S
linker	Microsoft L	inker(9.0)[GUI32	2]	S ?
State Libra	all and the second	and the	Chelder Ha	and the second
Signatures			Deep scar	n
Carlana and	100%	>	.og 83 msec	Scan

UPX [1] is one of the most common packers used by malware authors to obfuscate their binaries. Obfuscated binaries are harder to analyze than the original binary. UPX is a packer, so it does have legitimate usage like compressing a binary for reduced file size. Not all UPX packed files are malicious but for this blogpost, we will be choosing something malicious.

UPX packed executables can be automatically unpacked by UPX tool (which available online for free). To prevent this, malware authors often tamper with the packed binary in such a way that they can't be unpacked by UPX tool but the binary unpacks itself in memory without any issues. So, learning to unpack them manually always helps. Moreover, the general principle mentioned below can be used to unpack any custom packer or obfuscation techniques used by malware authors.

I took a long time to search for a sample malicious file and in the end, chose one randomly in VirusTotal (VT) by searching for "UPX Ransomware" [2]. I used Detect It Easy (DIE) [3] tool to confirm that the binary is UPX packed.

For the purpose of this post, I'll be using packed and obfuscated interchangeably. I've renamed the downloaded binary to "sample". Using the long hash value as the binary name makes the x32dbg debug windows look cluttered as the function names are referred to as *filename.memory\_address* in the debugger.

## **Theory Crafting**

Before we proceed, we need to talk about how a packed binary is unpacked. A packed binary, when executed (starts from a point called Entry Point - EP), allocates memory space to unpack itself and then populates it with the unpacked instructions. This process of writing to the memory is unpacking.

Once unpacked, the packer will start executing instructions from the unpacked section (The starting address is called Original Entry Point - OEP). By debugging the packed executable, we can execute/debug until we can identify the OEP. Once we identify OEP, we can dump the instructions into a binary file and this is the unpacked code. This can be considered as the standard process for unpacking manually.

We already know it's packed. If we did not know that, we can use a tool like PeID [4] or Detect It Easy to check for packers. Before we start debugging, let's take a look at the packed binary in the tool - PeStudio. It gives us a quick look at the PeFile structure, strings and imported libraries. Each of these sections provides us with more context to focus on while analyzing the binary.

property	value	value	value
name	UPX0	UPX1	.rsrc
md5	n/a	24A7744756FEFA4B187566A	820662818CDAF57E63206FC
entropy	n/a	7.998	3.791
file-ratio (97.27%)	n/a	96.50 %	0.77 %
raw-address	0x00000400	0x00000400	0x0004EA00
raw-size (323584 bytes)	0x00000000 (0 bytes)	0x0004E600 (321024 bytes)	0x00000A00 (2560 bytes)
virtual-address	0x00401000	0x00439000	0x00488000
virtual-size (557056 bytes)	0x00038000 (229376 bytes)	0x0004F000 (323584 bytes)	0x00001000 (4096 bytes)
entry-point	-	0x00086970	-
characteristics	0xE0000080	0xE0000040	0x C0000040
writable	x	x	x
executable	x	x	-

## Pe File Structure

### Figure 1: PE File Structure

The basic unit of code within a PE file is contained within a section [5]. There are 3 sections, *UPX0*, *UPX1* and *.rsrc* in the packed binary. Sections being named as UPX is a hint to what packer might be used.

**Warning:** PE File section names can be anything and is not a reliable indicator of the contents within.

The section UPX0 has raw size of 0 bytes but virtual size of 0x3800 bytes. And the section UPX1 has 96.5% entropy. High entropy value indicates packed or encrypted data. In this case, the packed data in UPX1 will be unpacked into the empty space of UPX0.

**Note:** Sections with high entropy indicate compressed or encrypted data. Sections with 0 raw size but large virtual size might be used to write instructions dynamically and execute them during runtime.

## Strings

It shows 3935 strings, but majority of it is unreadable/gibberish. The small percentage of readable strings also indicates that binary might be obfuscated. There is not much more to do here, let's move on.

## Imports

PeStudio shows only 15 functions imported. The small number of library imports is another indicator of packed or obfuscated content. Malicious files might often contain obfuscate module and library names (won't show up in simple string analysis). These obfuscated libraries names, can then be deobfuscated during runtime and then loaded using LoadLibraryA api call followed by GetProcAddress to obtain the address to specific module/function within that library.

This binary has the following interesting imports

- VirtualProtect
- VirtualAlloc
- ShellExecuteW
- LoadLibraryA
- GetProcAddress

These are sufficient for the binary to unpack itself in memory and run the deobfuscated code. For the sake of this blogpost size and your time, I'll not go into details of how they are used. We can discuss them in future posts.

## Identifying OEP

Let's load the binary into x32dbg. As soon as it is loaded, the execution is paused at the very beginning. As stated above, the next set of instructions are meant to unpack the original binary instructions and execute them. So, we are looking for an unconditional jump or a call instruction to a specific memory location.

You can verify that you are still in packed section of instructions by searching for the "Intermodular calls" and "String references" in the "current region". Both these will open a new window displaying limited data. This is an indicator that you are still in packed executable region.



Figure 2: Search for Intermodular Calls

Address	Disassembly		Destination
77222726	mov dword ptr	ds:[70020006],eax	kernelbase.75FF5656
77240E93	call ws2_32.7	710A31C	WS2_32.7710A31C
772464CE	mov dword ptr	ds: [77345D64], eax	apphelp.75030000
77284C96	mov esi, dword	ptr ds:[773465E4]	kernel32.7561F0E0
77287A81	mov esi, dword	<pre>ptr ds:[&lt;&amp;BaseThreadInitThunk&gt;]</pre>	<kernel32.basethreadinitthunk></kernel32.basethreadinitthunk>
7728CCD8	mov dword ptr	ds:[773465E4],eax	kernel32.7561F0E0
7728CCE0	mov dword ptr	ds:[773465E0],eax	kerne132.7563A680
7728CCE8	mov dword ptr	ds:[<&ReleaseActCtx>],eax	<kernelbase.releaseactctx></kernelbase.releaseactctx>
772A999A	mov dword ptr	ds: [77345D64], ebx	apphe1p.75030000
77282378	mov esi, dword	ptr ds: [773465E0]	kerne132.7563A680
772B247B	mov edi, dword	ptr ds:[<&ReleaseActCtx>]	<kernelbase.releaseactctx></kernelbase.releaseactctx>
772C44AC	mov esi, dword	<pre>ptr ds:[&lt;&amp;BaseQueryModuleData&gt;]</pre>	<kernel32.basequerymoduledata></kernel32.basequerymoduledata>
772CA67C	mov dword ptr	ds:[77345D0C],ed1	sample.004000F0
772CBC90	mov dword ptr	ds:[<&BaseQueryModuleData>],ebx	<kernel32.basequerymoduledata></kernel32.basequerymoduledata>
772CC153	mov eax, dword	ptr ds:[<&BaseThreadInitThunk>]	<kernel32.basethreadinitthunk></kernel32.basethreadinitthunk>
772CC314	mov dword ptr	ds: 77345D64 ,ebx	apphe1p.75030000
772D1505	mov dword ptr	ds: [77345D64],es1	apphe1p.75030000
772D1D05	mov aword ptr	ds:[77345D64],eax	appne1p.75030000
772D3E31	mov eax, dword	ptr ds:[77345D0C]	sample.004000F0

#### Figure 3: Intermodular calls **before** the code is unpacked

Continue to "step over" the instructions to avoid jumping into function calls. As you continue, keep an eye on the title of the debugger. If it has ntdll.dll or some other system library, it means you are in the library code and that does not interest you (usually) as a malware analyst. You can select "Run to user code" to get back to your binary code.

After a few step instructions, you'll notice that you are now at the very end of the binary. If you scroll further down, you'll notice an unconditional jump right before a series of opcodes **0000** signaling the end of the binary.

0048751C       804424 80       lea eax,dword ptr ss:[esp-80]         00487520       > GA 00       gush 0         00487521       > 75 FA       jme sample.416520         00487522       00487522       0000         00487523       > E9 F2EFF8FF         00487530       48       dec eax         00487531       0000       add byte ptr ds:[eax],al         00487533       0000       add byte ptr ds:[eax],al         00487533       0000       add byte ptr ds:[eax],al         00487533       0000       add byte ptr ds:[eax],al         00487535       0000       add byte ptr ds:[eax],al         00487537       0000       add byte ptr ds:[eax],al         00487538       0000       add byte ptr ds:[eax],al         00487541       0000       add byte ptr ds:[eax],al         00487543       0000       add byte ptr ds:[eax],al         00487544       0000       add byte ptr ds:[eax],al         00487545       0000       add byte ptr ds:[eax],al         00487548       0000       add byte ptr ds:[eax],al         00487549       0000       add byte ptr ds:[eax],al         00487548       0000       add byte ptr ds:[eax],al         00487551       0000 </th <th>1</th> <th></th> <th>00101220</th> <th></th> <th>-</th> <th>popua</th>	1		00101220		-	popua
00487520       > 6A 00       push 0         00487522       39C4       cmp esp, eax         00487524       75 FA       sample.487520         00487524       83EC 80       sub esp, FFFFFF80         00487524       83EC 80       sub esp, FFFFFF80         00487524       83EC 80       add byte ptr ds: [eax], al         00487523       48       oot487531         00487534       0000       add byte ptr ds: [eax], al         00487535       0000       add byte ptr ds: [eax], al         00487537       0000       add byte ptr ds: [eax], al         00487538       0000       add byte ptr ds: [eax], al         00487539       0000       add byte ptr ds: [eax], al         00487538       0000       add byte ptr ds: [eax], al         00487541       0000       add byte ptr ds: [eax], al         00487542       0000       add byte ptr ds: [eax], al         00487549       0000       add byte ptr ds: [eax], al         00487540       0000       add byte ptr ds: [eax], al         00487551       0000       add byte ptr ds: [eax], al         00487551       0000       add byte ptr ds: [eax], al         00487551       0000       add byte ptr ds: [eax], al      <		0	0048751C		8D4424 80	lea eax,dword ptr ss:[esp-80]
Image: Note of the second se		·	00487520	>	6A 00	push 0
Image         Sample.487520           Image         Sample.487520           Image         Sample.416520           Image         Sample.41620		0	00487522		39C4	cmp esp,eax
III:       01457525       83EC 80       sub esp,FFFFFF80         00487529       ^ E9 F2EFF8FF       jmp sample.416520         00487530       48       dec eax         00487531       0000       add byte ptr ds: [eax],al         00487535       0000       add byte ptr ds: [eax],al         00487537       0000       add byte ptr ds: [eax],al         00487538       0000       add byte ptr ds: [eax],al         00487539       0000       add byte ptr ds: [eax],al         00487538       0000       add byte ptr ds: [eax],al         00487539       0000       add byte ptr ds: [eax],al         00487530       0000       add byte ptr ds: [eax],al         00487538       0000       add byte ptr ds: [eax],al         00487541       0000       add byte ptr ds: [eax],al         00487545       0000       add byte ptr ds: [eax],al         00487549       0000       add byte ptr ds: [eax],al         00487540       0000		i0	00487524	~	75 FA	jne sample.487520
<ul> <li>00487529</li> <li>CO487520</li> <li>0000</li> <li>00487530</li> <li>00487531</li> <li>0000</li> <li>add byte ptr ds: [eax],al</li> <li>00487533</li> <li>0000</li> <li>add byte ptr ds: [eax],al</li> <li>00487533</li> <li>0000</li> <li>add byte ptr ds: [eax],al</li> <li>00487535</li> <li>0000</li> <li>add byte ptr ds: [eax],al</li> <li>00487537</li> <li>0000</li> <li>add byte ptr ds: [eax],al</li> <li>00487538</li> <li>0000</li> <li>add byte ptr ds: [eax],al</li> <li>00487539</li> <li>0000</li> <li>add byte ptr ds: [eax],al</li> <li>00487538</li> <li>0000</li> <li>add byte ptr ds: [eax],al</li> <li>00487538</li> <li>0000</li> <li>add byte ptr ds: [eax],al</li> <li>00487539</li> <li>0000</li> <li>add byte ptr ds: [eax],al</li> <li>00487541</li> <li>0000</li> <li>add byte ptr ds: [eax],al</li> <li>00487543</li> <li>0000</li> <li>add byte ptr ds: [eax],al</li> <li>00487549</li> <li>0000</li> <li>add byte ptr ds: [eax],al</li> <li>00487551</li> <li>0000</li> <li>add byte ptr ds: [eax],al</li> <li>00487557</li> <li>0000</li> <li>add byte ptr ds: [eax],al</li> <li>00487558</li> <li>0000</li> <li>add byte ptr ds: [eax],al</li> <li>00487559</li> <li>0000</li> <li>add byte ptr ds: [eax],al</li> <li>00487551</li> <li>0000</li> <li>add byte ptr ds: [eax],al</li> <li>00487558</li> <li>0000</li> <li>add byte ptr ds: [eax],al</li> <li>00487561</li> <li>0000</li> <li>add byte ptr</li></ul>		EIP	00487526		83EC 80	sub esp, FFFFF80
0048752E         0000         add         byte         ptr         ds:         [eax], a]           00487530         48         dec         eax         dec         eax         a]           00487531         0000         add         byte         ptr         ds:         [eax], a]           00487533         0000         add         byte         ptr         ds:         [eax], a]           00487537         0000         add         byte         ptr         ds:         [eax], a]           00487539         0000         add         byte         ptr         ds:         [eax], a]           00487539         0000         add         byte         ptr         ds:         [eax], a]           00487539         0000         add         byte         ptr         ds:         [eax], a]           00487549         0000         add		0	00487529	^	E9 F2EFF8FF	jmp sample.416520
00487530         48         dec eax           00487531         0000         add byte ptr ds: [eax], al           00487533         0000         add byte ptr ds: [eax], al           00487535         0000         add byte ptr ds: [eax], al           00487537         0000         add byte ptr ds: [eax], al           00487539         0000         add byte ptr ds: [eax], al           00487539         0000         add byte ptr ds: [eax], al           00487530         0000         add byte ptr ds: [eax], al           00487531         0000         add byte ptr ds: [eax], al           00487530         0000         add byte ptr ds: [eax], al           00487541         0000         add byte ptr ds: [eax], al           00487543         0000         add byte ptr ds: [eax], al           00487545         0000         add byte ptr ds: [eax], al           00487545         0000         add byte ptr ds: [eax], al           00487549         0000         add byte ptr ds: [eax], al           00487551         0000 <t< th=""><th></th><th></th><th>0048752E</th><th></th><th>0000</th><th>add byte ptr ds:[eax],al</th></t<>			0048752E		0000	add byte ptr ds:[eax],al
00487531         0000         add byte ptr ds: [eax], a]           00487533         0000         add byte ptr ds: [eax], a]           00487535         0000         add byte ptr ds: [eax], a]           00487537         0000         add byte ptr ds: [eax], a]           00487538         0000         add byte ptr ds: [eax], a]           00487541         0000         add byte ptr ds: [eax], a]           00487543         0000         add byte ptr ds: [eax], a]           00487545         0000         add byte ptr ds: [eax], a]           00487547         0000         add byte ptr ds: [eax], a]           00487548         0000         add byte ptr ds: [eax], a]           00487549         0000         add byte ptr ds: [eax], a]           00487551         0000         add byte ptr ds: [eax], a]           00487553         0000         add byte ptr ds: [eax], a]           00487559         0000         add byte ptr ds: [eax], a]           00487559 <td< th=""><th></th><th>0</th><th>00487530</th><th></th><th>48</th><th>dec eax</th></td<>		0	00487530		48	dec eax
00487533         0000         add         byte         ptr         ds:         [eax]         al           00487535         0000         add         byte         ptr         ds:         [eax]         al           00487537         0000         add         byte         ptr         ds:         [eax]         al           00487539         0000         add         byte         ptr         ds:         [eax]         al           00487538         0000         add         byte         ptr         ds:         [eax]         al           00487538         0000         add         byte         ptr         ds:         [eax]         al           00487541         0000         add         byte         ptr         ds:         [eax]         al           00487543         0000         add         byte         ptr         ds:         [eax]         al           00487547         0000         add         byte         ptr         ds:         [eax]         al           00487548         0000         add         byte         ptr         ds:         [eax]         al           00487551         0000         add         byte		0	00487531		0000	add byte ptr ds:[eax],a]
•       00487535       0000       add byte ptr ds: [eax], a]         •       00487537       0000       add byte ptr ds: [eax], a]         •       00487538       0000       add byte ptr ds: [eax], a]         •       00487538       0000       add byte ptr ds: [eax], a]         •       00487538       0000       add byte ptr ds: [eax], a]         •       00487537       0000       add byte ptr ds: [eax], a]         •       00487538       0000       add byte ptr ds: [eax], a]         •       00487541       0000       add byte ptr ds: [eax], a]         •       00487545       0000       add byte ptr ds: [eax], a]         •       00487549       0000       add byte ptr ds: [eax], a]         •       00487549       0000       add byte ptr ds: [eax], a]         •       00487549       0000       add byte ptr ds: [eax], a]         •       00487549       0000       add byte ptr ds: [eax], a]         •       00487549       0000       add byte ptr ds: [eax], a]         •       00487551       0000       add byte ptr ds: [eax], a]         •       00487552       0000       add byte ptr ds: [eax], a]         •       00487559       0000       ad			00487533		0000	add byte ptr ds:[eax],a]
•       00487537       0000       add byte ptr ds: [eax], a]         •       00487538       0000       add byte ptr ds: [eax], a]         •       0048753B       0000       add byte ptr ds: [eax], a]         •       0048753D       0000       add byte ptr ds: [eax], a]         •       0048753F       0000       add byte ptr ds: [eax], a]         •       00487541       0000       add byte ptr ds: [eax], a]         •       00487543       0000       add byte ptr ds: [eax], a]         •       00487543       0000       add byte ptr ds: [eax], a]         •       00487543       0000       add byte ptr ds: [eax], a]         •       00487549       0000       add byte ptr ds: [eax], a]         •       00487549       0000       add byte ptr ds: [eax], a]         •       00487549       0000       add byte ptr ds: [eax], a]         •       00487549       0000       add byte ptr ds: [eax], a]         •       00487549       0000       add byte ptr ds: [eax], a]         •       00487551       0000       add byte ptr ds: [eax], a]         •       00487553       0000       add byte ptr ds: [eax], a]         •       00487559       0000       ad		0	00487535		0000	add byte ptr ds:[eax],al
00487539       0000       add byte ptr ds: [eax],a]         0048753B       0000       add byte ptr ds: [eax],a]         0048753D       0000       add byte ptr ds: [eax],a]         0048753F       0000       add byte ptr ds: [eax],a]         00487541       0000       add byte ptr ds: [eax],a]         00487543       0000       add byte ptr ds: [eax],a]         00487543       0000       add byte ptr ds: [eax],a]         00487545       0000       add byte ptr ds: [eax],a]         00487547       0000       add byte ptr ds: [eax],a]         00487549       0000       add byte ptr ds: [eax],a]         00487540       0000       add byte ptr ds: [eax],a]         00487540       0000       add byte ptr ds: [eax],a]         00487551       0000       add byte ptr ds: [eax],a]         00487552       0000       add byte ptr ds: [eax],a]         00487553       0000       add byte ptr ds: [eax],a]         00487559       0000		•	00487537		0000	add byte ptr ds:[eax],a]
00487538       0000       add byte ptr ds: [eax],al         0048753D       0000       add byte ptr ds: [eax],al         0048753F       0000       add byte ptr ds: [eax],al         00487541       0000       add byte ptr ds: [eax],al         00487543       0000       add byte ptr ds: [eax],al         00487543       0000       add byte ptr ds: [eax],al         00487545       0000       add byte ptr ds: [eax],al         00487547       0000       add byte ptr ds: [eax],al         00487549       0000       add byte ptr ds: [eax],al         00487548       0000       add byte ptr ds: [eax],al         00487549       0000       add byte ptr ds: [eax],al         00487551       0000       add byte ptr ds: [eax],al         00487553       0000       add byte ptr ds: [eax],al         00487559       0000       add byte ptr ds: [eax],al         00487559       0000       add byte ptr ds: [eax],al         00487550       0000       add byte ptr ds: [eax],al         00487551       0000			00487539		0000	add byte ptr ds:[eax],a]
•       0048753D       0000       add byte ptr ds: [eax],a]         •       0048753F       0000       add byte ptr ds: [eax],a]         •       00487541       0000       add byte ptr ds: [eax],a]         •       00487543       0000       add byte ptr ds: [eax],a]         •       00487545       0000       add byte ptr ds: [eax],a]         •       00487547       0000       add byte ptr ds: [eax],a]         •       00487549       0000       add byte ptr ds: [eax],a]         •       00487551       0000       add byte ptr ds: [eax],a]         •       00487553       0000       add byte ptr ds: [eax],a]         •       00487559       0000       add byte ptr ds: [eax],a]         •       00487550       0000       add byte ptr ds: [		0	0048753B		0000	add byte ptr ds:[eax],al
0048753F         0000         add         byte ptr         ds:         [eax], a]           00487541         0000         add         byte ptr         ds:         [eax], a]           00487543         0000         add         byte ptr         ds:         [eax], a]           00487545         0000         add         byte ptr         ds:         [eax], a]           00487547         0000         add         byte ptr         ds:         [eax], a]           00487549         0000         add         byte ptr         ds:         [eax], a]           00487548         0000         add         byte ptr         ds:         [eax], a]           00487549         0000         add         byte ptr         ds:         [eax], a]           00487551         0000         add         byte ptr         ds:         [eax], a]           00487559         00000         add         byte ptr<		•	0048753D		0000	add byte ptr ds:[eax],al
00487541       0000       add byte ptr ds: [eax],a]         00487543       0000       add byte ptr ds: [eax],a]         00487545       0000       add byte ptr ds: [eax],a]         00487547       0000       add byte ptr ds: [eax],a]         00487549       0000       add byte ptr ds: [eax],a]         00487549       0000       add byte ptr ds: [eax],a]         00487540       0000       add byte ptr ds: [eax],a]         00487540       0000       add byte ptr ds: [eax],a]         00487540       0000       add byte ptr ds: [eax],a]         00487551       0000       add byte ptr ds: [eax],a]         00487553       0000       add byte ptr ds: [eax],a]         00487555       0000       add byte ptr ds: [eax],a]         00487557       0000       add byte ptr ds: [eax],a]         00487558       0000       add byte ptr ds: [eax],a]         00487559       0000       add byte ptr ds: [eax],a]         00487559       0000       add byte ptr ds: [eax],a]         00487551       0000       add byte ptr ds: [eax],a]         00487559       0000       add byte ptr ds: [eax],a]         00487561       0000       add byte ptr ds: [eax],a]         00487563       0000		0	0048753F		0000	add byte ptr ds:[eax],al
00487543       0000       add byte ptr ds: [eax],a]         00487545       0000       add byte ptr ds: [eax],a]         00487547       0000       add byte ptr ds: [eax],a]         00487549       0000       add byte ptr ds: [eax],a]         00487540       0000       add byte ptr ds: [eax],a]         00487540       0000       add byte ptr ds: [eax],a]         00487540       0000       add byte ptr ds: [eax],a]         00487551       0000       add byte ptr ds: [eax],a]         00487553       0000       add byte ptr ds: [eax],a]         00487555       0000       add byte ptr ds: [eax],a]         00487557       0000       add byte ptr ds: [eax],a]         00487559       0000       add byte ptr ds: [eax],a]         00487551       0000       add byte ptr ds: [eax],a]         00487550       0000       add byte ptr ds: [eax],a]         00487561       0000       add byte ptr ds: [eax],a]         00487563       0000		0	00487541		0000	add byte ptr ds:[eax],al
00487545       0000       add byte ptr ds: [eax],a]         00487547       0000       add byte ptr ds: [eax],a]         00487549       0000       add byte ptr ds: [eax],a]         00487548       0000       add byte ptr ds: [eax],a]         00487549       0000       add byte ptr ds: [eax],a]         00487548       0000       add byte ptr ds: [eax],a]         00487549       0000       add byte ptr ds: [eax],a]         00487551       0000       add byte ptr ds: [eax],a]         00487553       0000       add byte ptr ds: [eax],a]         00487559       0000       add byte ptr ds: [eax],a]         00487561       0000       add byte ptr ds: [eax],a]         00487563       0000       add byte ptr ds: [eax],a]         00487563       0000       add byte ptr ds: [eax],a]         00487563       0000			00487543		0000	add byte ptr ds:[eax],a]
00487547       0000       add byte ptr ds: [eax],a]         00487549       0000       add byte ptr ds: [eax],a]         00487548       0000       add byte ptr ds: [eax],a]         00487549       0000       add byte ptr ds: [eax],a]         00487540       0000       add byte ptr ds: [eax],a]         00487547       0000       add byte ptr ds: [eax],a]         00487547       0000       add byte ptr ds: [eax],a]         00487551       0000       add byte ptr ds: [eax],a]         00487553       0000       add byte ptr ds: [eax],a]         00487555       0000       add byte ptr ds: [eax],a]         00487559       0000       add byte ptr ds: [eax],a]         00487559       0000       add byte ptr ds: [eax],a]         00487559       0000       add byte ptr ds: [eax],a]         00487550       0000       add byte ptr ds: [eax],a]         00487551       0000       add byte ptr ds: [eax],a]         00487551       0000       add byte ptr ds: [eax],a]         00487561       0000       add byte ptr ds: [eax],a]         00487563       0000       add byte ptr ds: [eax],a]         00487563       0000       add byte ptr ds: [eax],a]         00487563       0000		0	00487545		0000	add byte ptr ds:[eax],al
00487549       0000       add byte ptr ds: [eax], a]         00487548       0000       add byte ptr ds: [eax], a]         00487540       0000       add byte ptr ds: [eax], a]         00487540       0000       add byte ptr ds: [eax], a]         00487540       0000       add byte ptr ds: [eax], a]         00487547       0000       add byte ptr ds: [eax], a]         00487551       0000       add byte ptr ds: [eax], a]         00487553       0000       add byte ptr ds: [eax], a]         00487555       0000       add byte ptr ds: [eax], a]         00487559       0000       add byte ptr ds: [eax], a]         00487559       0000       add byte ptr ds: [eax], a]         00487550       0000       add byte ptr ds: [eax], a]         00487550       0000       add byte ptr ds: [eax], a]         00487551       0000       add byte ptr ds: [eax], a]         00487551       0000       add byte ptr ds: [eax], a]         00487561       0000       add byte ptr ds: [eax], a]         00487563       0000       add byte ptr ds: [eax], a]         00487563       0000       add byte ptr ds: [eax], a]         00487565       0000       add byte ptr ds: [eax], a]         00487567		•	00487547		0000	add byte ptr ds:[eax],al
00487548       0000       add byte ptr ds: [eax], a]         00487540       0000       add byte ptr ds: [eax], a]         00487547       0000       add byte ptr ds: [eax], a]         00487551       0000       add byte ptr ds: [eax], a]         00487553       0000       add byte ptr ds: [eax], a]         00487555       0000       add byte ptr ds: [eax], a]         00487557       0000       add byte ptr ds: [eax], a]         00487559       0000       add byte ptr ds: [eax], a]         00487559       0000       add byte ptr ds: [eax], a]         00487559       0000       add byte ptr ds: [eax], a]         00487550       0000       add byte ptr ds: [eax], a]         00487550       0000       add byte ptr ds: [eax], a]         00487551       0000       add byte ptr ds: [eax], a]         00487561       0000       add byte ptr ds: [eax], a]         00487563       0000       add byte ptr ds: [eax], a]         00487565       0000       add byte ptr ds: [eax], a]         00487567       0000       add byte ptr ds: [eax], a]         00487569       0000       add byte ptr ds: [eax], a]         00487569       0000       add byte ptr ds: [eax], a]		•	00487549		0000	add byte ptr ds:[eax],al
•       0048754D       0000       add byte ptr ds: [eax], a]         •       0048754F       0000       add byte ptr ds: [eax], a]         •       00487551       0000       add byte ptr ds: [eax], a]         •       00487553       0000       add byte ptr ds: [eax], a]         •       00487555       0000       add byte ptr ds: [eax], a]         •       00487557       0000       add byte ptr ds: [eax], a]         •       00487559       0000       add byte ptr ds: [eax], a]         •       00487558       0000       add byte ptr ds: [eax], a]         •       00487558       0000       add byte ptr ds: [eax], a]         •       00487558       0000       add byte ptr ds: [eax], a]         •       00487558       0000       add byte ptr ds: [eax], a]         •       00487561       0000       add byte ptr ds: [eax], a]         •       00487563       0000       add byte ptr ds: [eax], a]         •       00487563       0000       add byte ptr ds: [eax], a]         •       00487567       0000       add byte ptr ds: [eax], a]         •       00487567       0000       add byte ptr ds: [eax], a]         •       00487569       0000       ad		0	0048754B		0000	add byte ptr ds:[eax],al
0048754F       0000       add byte ptr ds: [eax], a]         00487551       0000       add byte ptr ds: [eax], a]         00487553       0000       add byte ptr ds: [eax], a]         00487555       0000       add byte ptr ds: [eax], a]         00487555       0000       add byte ptr ds: [eax], a]         00487557       0000       add byte ptr ds: [eax], a]         00487559       0000       add byte ptr ds: [eax], a]         00487558       0000       add byte ptr ds: [eax], a]         00487558       0000       add byte ptr ds: [eax], a]         00487559       0000       add byte ptr ds: [eax], a]         00487558       0000       add byte ptr ds: [eax], a]         00487561       0000       add byte ptr ds: [eax], a]         00487563       0000       add byte ptr ds: [eax], a]         00487563       0000       add byte ptr ds: [eax], a]         00487565       0000       add byte ptr ds: [eax], a]         00487567       0000       add byte ptr ds: [eax], a]         00487569       0000       add byte ptr ds: [eax], a]		•	0048754D		0000	add byte ptr ds:[eax],al
00487551       0000       add byte ptr ds: [eax], a]         00487553       0000       add byte ptr ds: [eax], a]         00487555       0000       add byte ptr ds: [eax], a]         00487557       0000       add byte ptr ds: [eax], a]         00487559       0000       add byte ptr ds: [eax], a]         00487559       0000       add byte ptr ds: [eax], a]         00487559       0000       add byte ptr ds: [eax], a]         00487550       0000       add byte ptr ds: [eax], a]         00487551       0000       add byte ptr ds: [eax], a]         00487561       0000       add byte ptr ds: [eax], a]         00487563       0000       add byte ptr ds: [eax], a]         00487563       0000       add byte ptr ds: [eax], a]         00487565       0000       add byte ptr ds: [eax], a]         00487567       0000       add byte ptr ds: [eax], a]         00487569       0000       add byte ptr ds: [eax], a]         00487569       0000       add byte ptr ds: [eax], a]		0	0048754F		0000	add byte ptr ds:[eax],al
00487553       0000       add byte ptr ds: [eax], a]         00487555       0000       add byte ptr ds: [eax], a]         00487557       0000       add byte ptr ds: [eax], a]         00487559       0000       add byte ptr ds: [eax], a]         00487559       0000       add byte ptr ds: [eax], a]         00487559       0000       add byte ptr ds: [eax], a]         00487550       0000       add byte ptr ds: [eax], a]         00487551       0000       add byte ptr ds: [eax], a]         00487561       0000       add byte ptr ds: [eax], a]         00487563       0000       add byte ptr ds: [eax], a]         00487563       0000       add byte ptr ds: [eax], a]         00487563       0000       add byte ptr ds: [eax], a]         00487569       0000       add byte ptr ds: [eax], a]         00487569       0000       add byte ptr ds: [eax], a]         00487569       0000       add byte ptr ds: [eax], a]		0	00487551		0000	add byte ptr ds:[eax],al
00487555       0000       add byte ptr ds: [eax], a]         00487557       0000       add byte ptr ds: [eax], a]         00487559       0000       add byte ptr ds: [eax], a]         00487558       0000       add byte ptr ds: [eax], a]         00487550       0000       add byte ptr ds: [eax], a]         00487550       0000       add byte ptr ds: [eax], a]         00487557       0000       add byte ptr ds: [eax], a]         00487557       0000       add byte ptr ds: [eax], a]         00487561       0000       add byte ptr ds: [eax], a]         00487563       0000       add byte ptr ds: [eax], a]         00487565       0000       add byte ptr ds: [eax], a]         00487567       0000       add byte ptr ds: [eax], a]         00487569       0000       add byte ptr ds: [eax], a]		•	00487553		0000	add byte ptr ds:[eax],al
00487557       0000       add byte ptr ds: [eax], al         00487559       0000       add byte ptr ds: [eax], al         00487559       0000       add byte ptr ds: [eax], al         00487558       0000       add byte ptr ds: [eax], al         00487550       0000       add byte ptr ds: [eax], al         00487551       0000       add byte ptr ds: [eax], al         00487561       0000       add byte ptr ds: [eax], al         00487563       0000       add byte ptr ds: [eax], al         00487563       0000       add byte ptr ds: [eax], al         00487565       0000       add byte ptr ds: [eax], al         00487567       0000       add byte ptr ds: [eax], al         00487569       0000       add byte ptr ds: [eax], al		0	00487555		0000	add byte ptr ds:[eax],a]
00487559       0000       add byte ptr ds: [eax], al         00487558       0000       add byte ptr ds: [eax], al         00487550       0000       add byte ptr ds: [eax], al         00487557       0000       add byte ptr ds: [eax], al         00487561       0000       add byte ptr ds: [eax], al         00487563       0000       add byte ptr ds: [eax], al         00487563       0000       add byte ptr ds: [eax], al         00487563       0000       add byte ptr ds: [eax], al         00487565       0000       add byte ptr ds: [eax], al         00487567       0000       add byte ptr ds: [eax], al         00487569       0000       add byte ptr ds: [eax], al		•	00487557		0000	add byte ptr ds:[eax],al
00487558         0000         add byte ptr ds: [eax],a]           0048755D         0000         add byte ptr ds: [eax],a]           0048755F         0000         add byte ptr ds: [eax],a]           00487561         0000         add byte ptr ds: [eax],a]           00487563         0000         add byte ptr ds: [eax],a]           00487563         0000         add byte ptr ds: [eax],a]           00487565         0000         add byte ptr ds: [eax],a]           00487565         0000         add byte ptr ds: [eax],a]           00487567         0000         add byte ptr ds: [eax],a]           00487569         0000         add byte ptr ds: [eax],a]			00487559		0000	add byte ptr ds:[eax],a]
0048755D         0000         add byte ptr ds: [eax],a]           0048755F         0000         add byte ptr ds: [eax],a]           00487561         0000         add byte ptr ds: [eax],a]           00487563         0000         add byte ptr ds: [eax],a]           00487565         0000         add byte ptr ds: [eax],a]           00487565         0000         add byte ptr ds: [eax],a]           00487565         0000         add byte ptr ds: [eax],a]           00487567         0000         add byte ptr ds: [eax],a]           00487569         0000         add byte ptr ds: [eax],a]		0	0048755B		0000	add byte ptr ds:[eax],a]
0048755F         0000         add byte ptr ds: [eax], a]           00487561         0000         add byte ptr ds: [eax], a]           00487563         0000         add byte ptr ds: [eax], a]           00487565         0000         add byte ptr ds: [eax], a]           00487565         0000         add byte ptr ds: [eax], a]           00487567         0000         add byte ptr ds: [eax], a]           00487569         0000         add byte ptr ds: [eax], a]			0048755D		0000	add byte ptr ds:[eax],al
00487561         0000         add byte ptr ds: [eax], a]           00487563         0000         add byte ptr ds: [eax], a]           00487565         0000         add byte ptr ds: [eax], a]           00487565         0000         add byte ptr ds: [eax], a]           00487567         0000         add byte ptr ds: [eax], a]           00487569         0000         add byte ptr ds: [eax], a]		0	0048755F		0000	add byte ptr ds:[eax],al
<ul> <li>00487563</li> <li>00487563</li> <li>00487565</li> <li>0000</li> <li>add byte ptr ds: [eax], a]</li> <li>00487567</li> <li>0000</li> <li>add byte ptr ds: [eax], a]</li> <li>00487569</li> <li>0000</li> <li>add byte ptr ds: [eax], a]</li> </ul>		0	00487561		0000	add byte ptr ds:[eax],al
<ul> <li>00487565</li> <li>00487567</li> <li>00487567</li> <li>0000</li> <li>add byte ptr ds: [eax], al</li> <li>add byte ptr ds: [eax], al</li> <li>add byte ptr ds: [eax], al</li> </ul>			00487563		0000	add byte ptr ds:[eax],a]
00487567 0000 add byte ptr ds:[eax],al     00487569 0000 add byte ptr ds:[eax],al		0	00487565		0000	add byte ptr ds:[eax],al
00487569 0000 add byte ptr ds:[eax],al		•	00487567		0000	add byte ptr ds:[eax],al
		•	00487569		0000	add byte ptr ds:[eax],al

### Figure 4: Likely End of the Packed Section

Set a breakpoint right before the jmp sample.416520 instruction and check for intermodular calls again. You will still see limited number of calls indicating packed data. Now, step over this instruction, which will jump or change the instruction pointer to a new location.

This new location is the beginning of the the unpacked called or also called as OEP. the address location **0x416520 is the OEP** where the unpacked code (instructions) resides. You can (and need to) verify this by checking for intermodular calls which will show a larger number of function calls, indicating that the binary has been packed.

Address	Disassembly	Destination
00401037	call dword ptr ds:[<&GetVersionExW>]	<kernel32.getversionexw></kernel32.getversionexw>
0040130A	call dword ptr ds:[<&GetModuleFileNameW>]	<kernel32.getmodulefilenamew></kernel32.getmodulefilenamew>
0040131D	call dword ptr ds:[<&GetTempPathW>]	<kernel32.gettemppathw></kernel32.gettemppathw>
00401352	<pre>mov edi,dword ptr ds:[&lt;&amp;GetFileAttributesW&gt;]</pre>	<kernel32.getfileattributesw></kernel32.getfileattributesw>
00401375	call dword ptr ds:[<&DeleteFileW>]	<kernel32.deletefilew></kernel32.deletefilew>
00401392	call dword ptr ds:[<&GetTempPathW>]	<kernel32.gettemppathw></kernel32.gettemppathw>
0040144A	call dword ptr ds:[<&DeleteFileW>]	<kernel32.deletefilew></kernel32.deletefilew>
004014EA	mov edi,dword ptr ds:[<&OpenEventW>]	<kernel32.openeventw></kernel32.openeventw>
0040150F	mov ebp, dword ptr ds: [<&S]eep>]	<kernel32.sleep></kernel32.sleep>
00401519	mov ebx,dword ptr ds:[<&CloseHandle>]	<kernel32.closehandle></kernel32.closehandle>
00401530	<pre>call dword ptr ds:[&lt;&amp;CreateEventW&gt;]</pre>	<kernel32.createeventw></kernel32.createeventw>
00401584	call dword ptr ds:[<&DeleteFileW>]	<kernel32.deletefilew></kernel32.deletefilew>
0040175A	call dword ptr ds:[<&GetTempPathW>]	<kernel32.gettemppathw></kernel32.gettemppathw>
0040176F	call dword ptr ds:[<&GetSystemDirectoryW>]	<kernel32.getsystemdirectoryw></kernel32.getsystemdirectoryw>
004017DA	call dword ptr ds:[<&DeleteFileW>]	<kernel32.deletefilew></kernel32.deletefilew>
00401927	call dword ptr ds:[<&GetTickCount>]	<kernel32.gettickcount></kernel32.gettickcount>
00401B45	call dword ptr ds:[<&RegOpenKeyExW>]	<advapi32.regopenkeyexw></advapi32.regopenkeyexw>
00401B7E	call dword ptr ds:[<&RegSetValueExW>]	<advapi32.regsetvalueexw></advapi32.regsetvalueexw>
00401B8D	call dword ptr ds:[<&RegCloseKey>]	<advapi32.regclosekey></advapi32.regclosekey>
00401BA8	call dword ptr ds:[<&ShellExecuteW>]	<shell32.shellexecutew></shell32.shellexecutew>
00401CE0	call dword ptr ds:[<&GetTempPathW>]	<kernel32.gettemppathw></kernel32.gettemppathw>
00401DDD	call dword ptr ds:[<&GetSystemDirectoryW>]	<kernel32.getsystemdirectoryw></kernel32.getsystemdirectoryw>
00401E06	call dword ptr ds:[<&GetTempPathW>]	<kernel32.gettemppathw></kernel32.gettemppathw>
00401ED1	call dword ptr ds:[<&GetSystemDirectoryW>]	<kernel32.getsystemdirectoryw></kernel32.getsystemdirectoryw>
00401EF9	call dword ptr ds:[<&GetTempPathw>]	<kernel32.gettemppathw></kernel32.gettemppathw>
00401F0B	call dword ptr ds:[<&wsprintfw>]	<user32.wsprintfw></user32.wsprintfw>
00401FBC	call dword ptr ds:[<&GetModuleFileNameW>]	<kernel32.getmodulefilenamew></kernel32.getmodulefilenamew>
0040211E	call dword ptr ds:[<&GetSystemDirectoryw>]	<kernel32.getsystemdirectoryw></kernel32.getsystemdirectoryw>
004021AE	call dword ptr ds:[<&CreateFileW>]	<kernel32.createfilew></kernel32.createfilew>
00402209	call dword ptr ds:[<&sleep>]	<kernel32.sleep></kernel32.sleep>
0040224F	call dword ptr ds:[<&DeviceIocontrol>]	<kernel32.devicelocontrol></kernel32.devicelocontrol>
00402320	call dword ptr ds:[<&sleep>]	<kernel32.steep></kernel32.steep>
00402388	call dword ptr ds:[<&ReadFile>]	<kernel32.readfile></kernel32.readfile>
00402433	call dword ptr ds:[<&createFilew>]	<kernel32.createfilew></kernel32.createfilew>
00402458	call dword ptr ds:[<&DeviceIoControl>]	<kernel32.devicelocontrol></kernel32.devicelocontrol>
00402484	call dword ptr ds:[<&closeHandle>]	<kernel32.closehandle></kernel32.closehandle>
00402769	call dword ptr ds: [<&GetTickCounts]	<kernel32.gettickcounty< th=""></kernel32.gettickcounty<>
00402800	call dword ptr ds: [<&GetTickCount>]	<kernel32.gettickcount></kernel32.gettickcount>
00402936	call dword ptr ds: [<@GetNeduleFileNameAs]	<kernel32.getmedule5ilenameas< th=""></kernel32.getmedule5ilenameas<>
00402962	call dword ptr ds: [<@GetModuleriteNameA>]	<pre>kernel32.GetModulerTieNameA&gt;</pre>
00402983	call dword ptr ds: [<@writeFiles]	skernel22 WriteFiles
00402465	call dword ntr ds: [<@loseHandles]	skernel22 CloseHandles
00402464	call dword ntr ds: [<&ChallEvecuteAs]	shell22 shellEveruteAs
00402462	call dword ntr ds: [<&wsAstartuns]	ZWE2 22 WEAStartuns
0040ZAEF	call unor u per us [sawsAstar cups]	Swaz_az.waAatar tupa

#### Figure 5: Truncated Image of Intermodular calls **after** the code is unpacked

**Note:** Figure 5 has significantly greater number of function calls than Figure 3. Furthermore, the function names are indicated clearly and not obfuscated. This indicates that we have successfully unpacked the binary.

Before we proceed, make sure your Instruction Pointer is pointing to the OEP we have identified above.

### **Dump Unpacked Binary From Memory**

Once we have the unpacked binary instructions and the instruction pointer is pointing to the OEP, we can use the "OllyDumpEx" plugin [6] for x32dbg to dump the process to a file. Make sure that the OEP is pointing to the very first instruction after the Jump instruction we previously identified. This makes sure that we are dumping only the unpacked code in memory to a file. This plugin takes care of building the PE file structure around the dumped file. There is no need to change any parameters in the OllyDumpEx window. Select Dump and you will have the unpacked binary.

		Jumpic							
Module -	<u></u>								
Base:	Mod	tule U:\U	sers\Admin\l	Jesktop\san	nple				Dump
	OMen	nory 0040	00000 (00001	000) / Imag	/R /	sample / F	Έ		× .
	⊖ Add	ress 0040	0000						Cancel
List Secti	ion: 💿 l	Base Only		ny 🔿 A	ddress F	ange 00	400000 -	03400000	
Dump Ma	ode: 💿 l	Rebuild	O Binary (R	law) 🔘 B	inary (Vir	tual)			
mage So	ource: 💿 l	Memory	🔿 Disk				F	leScan Memo	ny
Search							1.1		
Search A	Area: 🔘 🤅	Select		ory (exclude l	isted mo	dule)		Search Image	Format
Search M	1ode: 💽 🤅	Strict	O Fuzzy (sl	ow)			<u>(1917</u>		• PE
Search F	Result:								○ ELF
mage Si: Entry Poi	ze: 0008 int: 0008	39000 36970	Get EIP	as OEP		<pre> Pix Corru  Disable  Auto Ad  Rebuild</pre>	upted Image He Relocation just Image Base DataDirectorv (	ader Structur e Address Follow Imagel	e Base Chance)
mage Si: Entry Poi Section	ze: 0008 int: 0008	39000	Get EIP	as OEP		<ul> <li>Pix Corru</li> <li>Disable</li> <li>Auto Ad</li> <li>Rebuild</li> <li>Search /</li> </ul>	upted Image He Relocation just Image Base DataDirectory ( All Occurrences	ader Structur e Address Follow Imagel s	e Base Change)
mage Si Entry Poi Section Select A	ze: 0008 int: 0008	39000 36970 ect BaseMoo	Get EIP	as OEP	Selec	<ul> <li>Pix Corru</li> <li>Disable</li> <li>Auto Ad</li> <li>Rebuild</li> <li>Search /</li> </ul>	upted Image He Relocation just Image Base DataDirectory ( All Occurrences	ader Structum e Address Follow Imagel s	e Base Change) DeSelect Al
mage Si Entry Poi Section Select A	ze: 0008 int: 0008 All Sele	39000 36970 ect BaseMoo Size	Get EIP dule Selec Owner	as OEP t Private/All Section	Selec Type	Prix Corru     Disable     Auto Ad     Rebuild     Search	upted Image He Relocation just Image Base DataDirectory ( All Occurrences Exec VirtualOffset	ader Structum e Address Follow Imagel s VirtualSize	e Base Change) DeSelect Al Characteristics
mage Si: Entry Poi Section Select A 4 2 00	ze: 0008 int: 0008 All Sele Address 1401000	39000 36970 ect BaseMoo Size 00038000	Get EIP dule Selec Owner sample	as OEP t Private/All Section UPX0	Select Type Imag	Fix Corru Disable Auto Ad Rebuild Search Search Access RWE	upted Image He Relocation just Image Base DataDirectory ( All Occurrences Exec VirtualOffset 00001000	ader Structur Address Follow Imagel VirtualSize 00038000	e Base Change) DeSelect Al Characteristics 60000080
mage Si Entry Poi Section Select A 2 00 2 00	ze: 0008 int: 0008 All Sele Address 1401000 1439000	39000 36970 cct BaseMod Size 00038000 0004F000	Get EIP dule Selec Owner sample sample	t Private/All Section UPX0 UPX1	Select Type Imag Imag	Prix Corru Disable Auto Ad Rebuild Search Ct Private/E Access RWE RWE RWE	upted Image He Relocation just Image Base DataDirectory ( All Occurrences Exec VirtualOffset 00001000 00039000	ader Structum e Address Follow Imagel s VirtualSize 00038000 0004F000	e Base Change) DeSelect Al Characteristics 60000080 60000040
mage Si Entry Poi Section Select A 2 00 2 00 2 00	ze: 0008 int: 0008 All Sele Address 1401000 1439000 1488000	39000 36970 ect BaseMoo Size 00038000 0004F000 00001000	Get EIP dule Selec Owner sample sample sample	as OEP t Private/All Section UPX0 UPX1 .rsrc	Select Type Imag Imag Imag	Fix Corru Disable Auto Ad Rebuild Search Search Access RWE RWE RWE RWE	upted Image He Relocation just Image Base DataDirectory ( All Occurrences Exec VirtualOffset 00001000 00039000 00088000	Address Follow Imagel VirtualSize 00038000 0004F000 00001000	e Base Change) DeSelect Al Characteristics 60000080 60000040 C0000040
mage Si Entry Poi Select A 2 00 2 00 2 00	ze: 0008 int: 0008 All Sele Address 1401000 1439000	39000 36970 ect BaseMod Size 00038000 0004F000 00001000	Get EIP dule Selec Owner sample sample sample	as OEP t Private/All Section UPX0 UPX1 .rsrc	Select Type Imag Imag Imag	<pre>Prix Corru Disable Auto Ad Rebuild Search Corrute/E Access RWE RWE RWE RWE</pre>	Ipted Image He Relocation just Image Base DataDirectory ( All Occurrences Xec VirtualOffset 00001000 00039000 00088000	Address Follow Imagel VirtualSize 00038000 0004F000 00001000	e Base Change) DeSelect Al Characteristics 60000080 60000040 C0000040

### Figure 6: OllyDumpEx Plugin

The dumped file is named as "sample\_dump.exe". Opening this file in PeStudio, will show you 15 imports with no name values. This is because the OllyDumpEx does not take care of rebuilding the imports while dumping it from memory. Imports on a file and imports in memory have different address offsets and this causes the dumped binary to be 'incomplete' in some ways as shown in the image below.

ď	pestudio 9.12 ·	Malware Initial Assessment	- www.winitor.com	[c:\users\admin\desktop\sample_	_dump.exe]
---	-----------------	----------------------------	-------------------	---------------------------------	------------

file settings about

c:\users\admin\desktop\sample_dump.exe	name (15)	hint (0)	thunk (0)	group (0)	type (1)
indicators (52) *		n/a	n/a	-	implicit
Virustotal (error)		n/a	n/a	2	implicit
dos-header (64 bytes)		n/a	n/a		implicit
dos-stub (1/b bytes)		n/a	n/a	-	implicit
		n/a	n/a	12	implicit
<ul> <li>File-neader (Oct.2013)</li> <li>Antional header (CUI)</li> </ul>		n/a	n/a		implicit
directories (3)		n/a	n/a		implicit
sections (file)		n/a	n/a	-	implicit
libraries (10) *		n/a	n/a	-	implicit
imports (count) *		n/a	n/a	2	implicit
exports (n/a)		n/a	n/a	5	implicit
∯ exceptions (n/a)		n/a	n/a		implicit
⊶o tls-callbacks (n/a)		n/a	n/a	12	implicit
ŷ relocations (n/a)		n/a	n/a		implicit
		n/a	n/a	4	implicit
abc strings (4667)					
🚓 debug (n/a)					
,🗐 manifest (aslnvoker)					
certificate (n/a)					
🗋 overlay (n/a)					

#### Figure 7: PeStudio Output For The Dumped File

To rebuild the import table, we will use a different plugin - Scylla x86 [7] which searches for the Import Address Table in the packed binary and obtains the imports from it. Select "IAT Autosearch" and when prompted for advanced search choose no. The plugin will return with the starting address of the IAT. Now select "Get Imports" to obtain the list of imports for the binary.

In this case, it will return with 247 valid APIs and missing 4 APIs as shown below. If there were large number of missing APIs, try the advanced search mentioned earlier and check if it returns better results.



File Imports Trace Misc Help

Imports	4720	) - sample - C	:\Users\Admin\	Desktop\sample		~	Pick DLL
<ul> <li>advapi32.dll (4) FThunk: 00029000</li> <li>gdi32.dll (23) FThunk: 00029074</li> <li>gdi32.dll (23) FThunk: 00029074</li> <li>getApiByVirtualAddress :: No Api found 750A16C0</li> <li>getApiByVirtualAddress :: No Api found 750A1620</li> </ul>				Impo	rts		
Image: User 32 dll (8) FThunk: 00029364       Cle         Show Invalid       Show Suspect       Cle         IAT Info       Actions       Dump         DEP       00416520       IAT Autosearch       Autotrace       Dump       PE Reb         VA       00428FFC       Get Imports       Elog       Elog         Log         getApiByVirtualAddress :: No Api found 750A 16C0 getApiByVirtualAddress :: No Api found 750A 1370 getApiByVirtualAddress :: No Api found 750A 2040		<ul> <li>advapi32</li> <li>gdi32.dll</li> <li>IPHLPAP</li> <li>kernel32</li> <li>oleact.dl</li> <li>oleaut32.dl</li> <li>shell32.dl</li> <li>user32.dl</li> <li>? (2) FTh</li> <li>user32.dl</li> <li>? (1) FTh</li> </ul>	2.dll (4) FThunk: (23) FThunk: 0 I.DLL (1) FThun .dll (114) FThur I (2) FThunk: 0 .dll (3) FThunk: 0 III (2) FThunk: 0 III (51) FThunk: 0 III (51) FThunk: 0 III (7) FThunk: 0 III (7) FThunk: 0	00029000 0029014 k: 00029074 k: 0002907C 0029248 00029254 00029264 00029270			
IAT Info DEP 00416520 IAT Autosearch A 00428FFC Get Imports Cog getApiByVirtualAddress :: No Api found 750A16C0 getApiByVirtualAddress :: No Api found 750A1370 getApiByVirtualAddress :: No Api found 750A2040	Sh	ow Invalid	Show Suspe	0029364 ect			Clear
DEP 00416520 IAT Autosearch Autotrace Dump PE Ret A 00428FFC Get Imports Fix Dump Unp PE Ret Expression Fix Dump Get ApiByVirtualAddress :: No Api found 750A16C0 getApiByVirtualAddress :: No Api found 750A1370 getApiByVirtualAddress :: No Api found 750A2040			IAT Info		Actions	Dum	Þ
A 00428FFC Size 00000414 Get Imports Fix Dump Log getApiByVirtualAddress :: No Api found 750A16C0 getApiByVirtualAddress :: No Api found 750A1370 getApiByVirtualAddress :: No Api found 750A2040	DEP	00416520		IAT Autosearch	Autotrace	Dump	E Rebuild
Log getApiByVirtualAddress :: No Api found 750A16C0 getApiByVirtualAddress :: No Api found 750A1370 getApiByVirtualAddress :: No Api found 750A2040	/A Size	00428FFC 00000414		Get Imports		Fix Du	mp
getApiByVirtualAddress :: No Api found 750A16C0 getApiByVirtualAddress :: No Api found 750A1370 getApiByVirtualAddress :: No Api found 750A2040				Log	9		
getApiByVirtualAddress :: No Api found 750A41D0 IAT parsing finished, found 247 valid APIs, missed 4 APIs DIRECT IMPORTS - Found 0 possible direct imports with 0 unique APIs!	getA getA getA getA IAT	ApiByVirtualAc ApiByVirtualAc ApiByVirtualAc ApiByVirtualAc parsing finish	ddress :: No Ap ddress :: No Ap ddress :: No Ap ddress :: No Ap ddress :: No Ap ed, found 247 5 - Found 0 pos	found 750A16C0 found 750A1370 found 750A2040 found 750A41D0 /alid APIs, missed 4 APIs ible direct imports with 0	) unique APIs!		ŕ

#### Figure 8: Scyllax86 Plugin

Once Scylla returns the above response, select "Fix Dump", and this will generate a new file called "sample\_dump\_scy.exe". As shown in the image below, opening

"sample\_dump\_scy.exe" in the PeStudio shows that the imports are now populated.

🧭 pestudio 9.12 - Malware Initial Assessment - www.winitor.com [c:\users\admin\desktop\sample\_dump.exe]

c:\users\admin\desktop\sample_dump.exe	name (15)	hint (0)	thunk (0)	group (0)	type (1)
indicators (52) *		n/a	n/a	-	implicit
····> virustotal (error)		n/a	n/a		implicit
dos-header (64 bytes)		n/a	n/a	-	implicit
dos-stub (1/6 bytes)		n/a	n/a	4	împlicît
		n/a	n/a	12	implicit
<ul> <li>P file-neader (Oct.2013)</li> <li>S antianal hander (CUI)</li> </ul>		n/a	n/a	· · ·	implicit
directories (3)		n/a	n/a	4	implicit
b sections (file)		n/a	n/a	-	implicit
Ibraries (10) *		n/a	n/a	-	implicit
imports (count) *		n/a	n/a	12	implicit
→ exports (n/a)		n/a	n/a		implicit
🚽 exceptions (n/a)		n/a	n/a	4	implicit
→••••••••••••••••••••••••••••••••••••		n/a	n/a		implicit
ŷ relocations (n/a)		n/a	n/a	· · ·	implicit
		n/a	n/a	4	implicit
abc strings (4667)					
→ 🏠 debug (n/a)					
🗐 manifest (aslnvoker)					
<b>1.0</b> version (n/a)					
🗋 overlay (n/a)					

#### Figure 9: PeStudio Output For The Dumped File

Compare Figure 7 with Figure 9 to see how Scyllax86 helps with populating the imports. **We** have successfully extracted the UPX packed binary into a file

**"sample\_dump\_scy.exe"**. We can now continue analayzing this sample for identifying its functionality and purpose. Subsequent posts will be focused on this.

### References

Tags: <u>malware analysis upx unpacking</u> <u>Next Post →</u>