

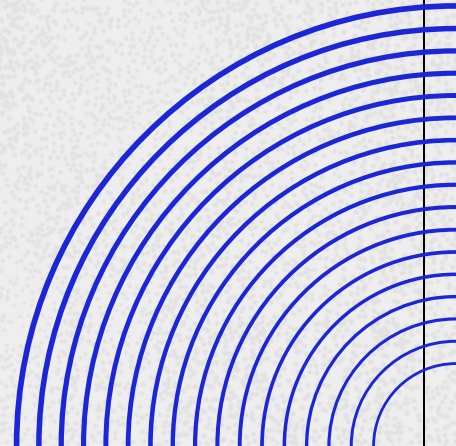


NT137.011.ATCL

Kỹ thuật — Packing

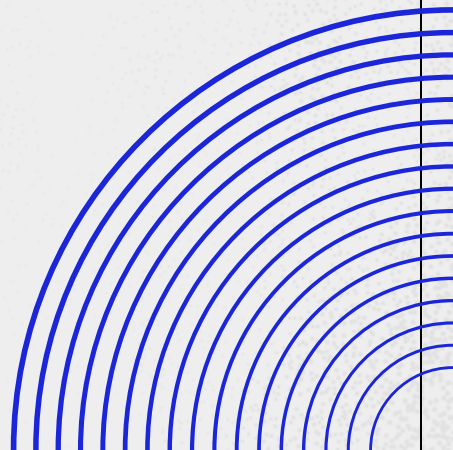
Nguyễn Mạnh Cường - 20520421

Nguyễn Trần Đức Anh - 20520392



01

Lý thuyết — Thống kê



Kỹ thuật Packing

Packing

Packing là một quá trình **biến đổi một tệp thực thi** thành một cấu trúc khác, sử dụng **nén và/hoặc mã hóa**, nhằm **bảo vệ/giấu đi nội dung gốc của tệp**.

Tốt và xấu

Packing được sinh ra với mục đích **giảm kích thước tệp và bảo vệ mã nguồn hợp pháp**. Nhưng lại được áp dụng rộng rãi trên mã độc, nhằm **tránh né quá trình phân tích**.

Cấp độ phức tạp

Packing 1 lớp

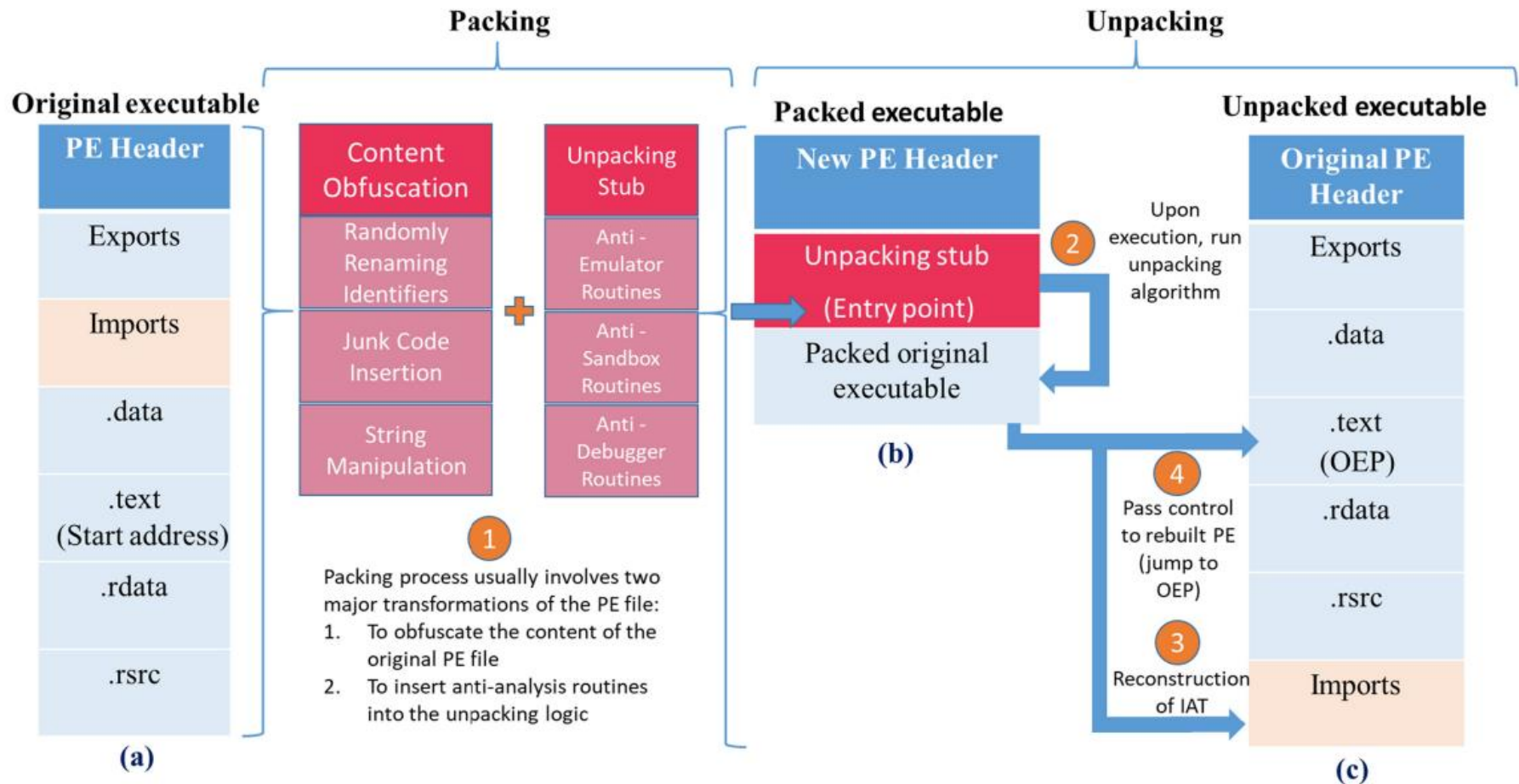
1 lớp thuật toán packing

Re-packing

Nhiều lớp với cũng 1 thuật toán

Packing đa lớp

Nhiều lớp với nhiều thuật toán



Unpacking phân tích

Unpacking tĩnh

Không cần thực thi. Chỉ hoạt động với các packer 1 lớp.

Unpacking động thủ công

Thực thi và xác định mã nguồn gốc sau khi được unpack, thủ công.

Unpacking động tự động

Tự động xác định OEP khi thực thi trong môi trường cách ly.

Phân loại Packer

Compressors

Chỉ nén. UPack, UPX và ASPack.

Protectors

Kết hợp nén, mã hóa và nhiều phương pháp khác. Armadillo và Themida.

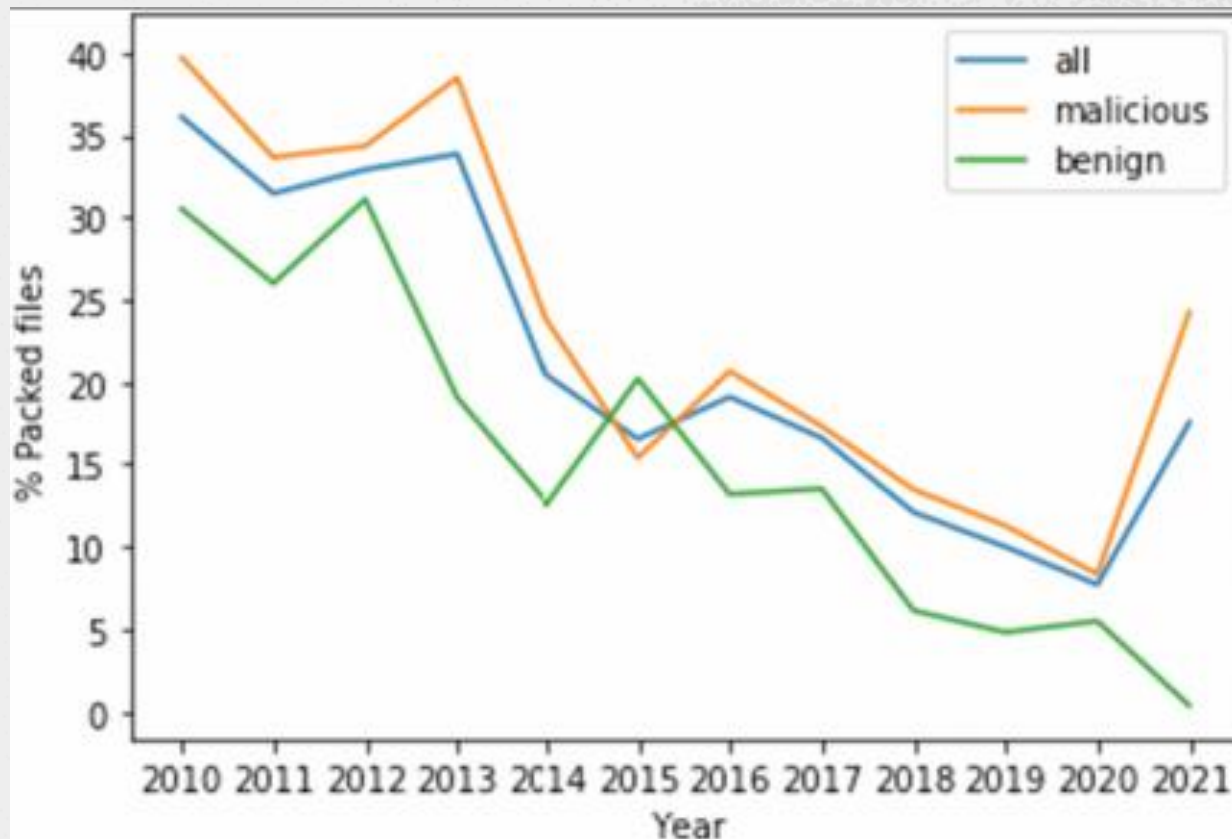
Crypters

Thêm mã hóa và chống phân tích. Yoda's Crypter và PolyCrypt PE.

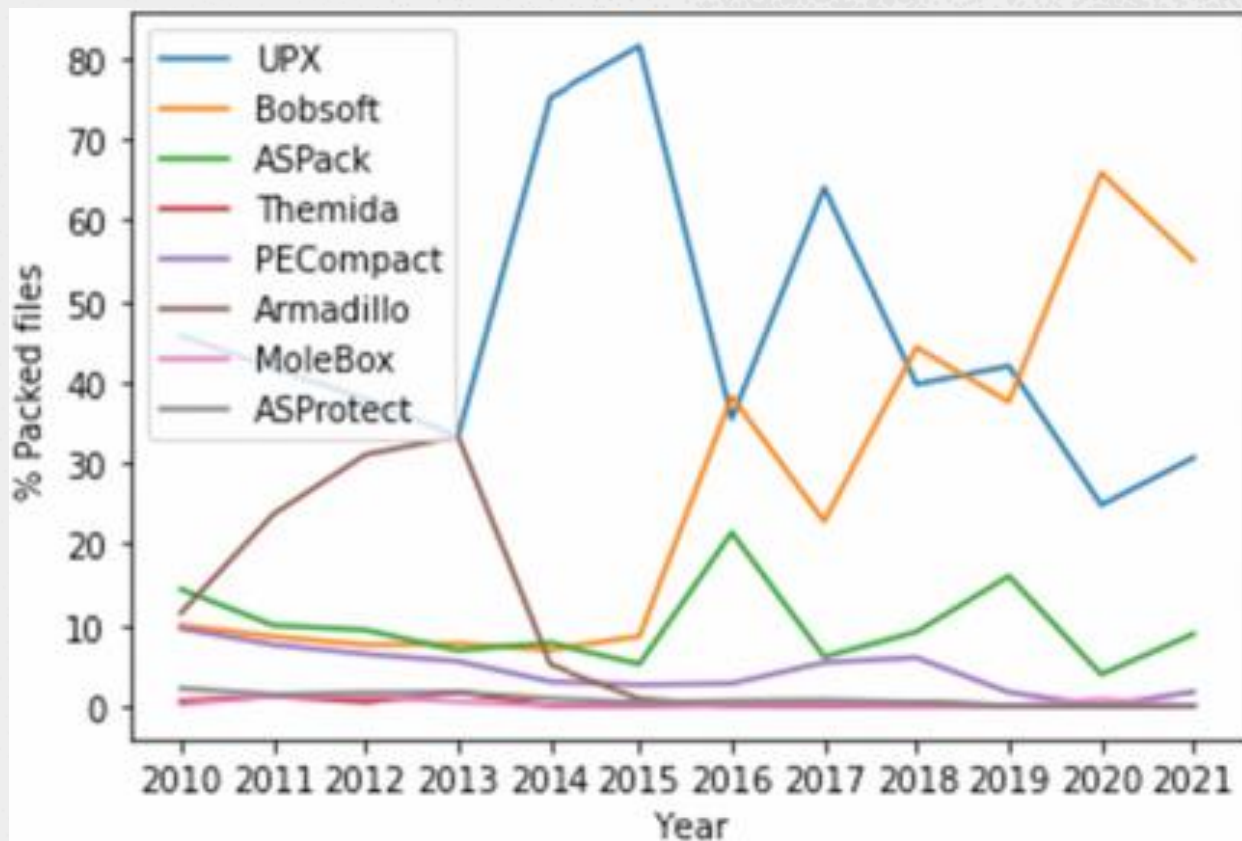
Bundlers

Pack nhiều tệp lại với nhau. PEBundle và MoleBox.

Biểu đồ thể hiện xu hướng packing từ 2010 đến 2021 của 24,000 tệp PE trên VirusTotal.

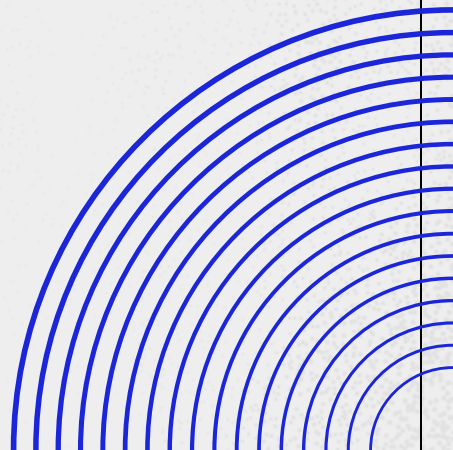


Biểu đồ thể hiện xu hướng các packer từ 2010 đến 2021 của 24,000 tệp PE trên VirusTotal.



02

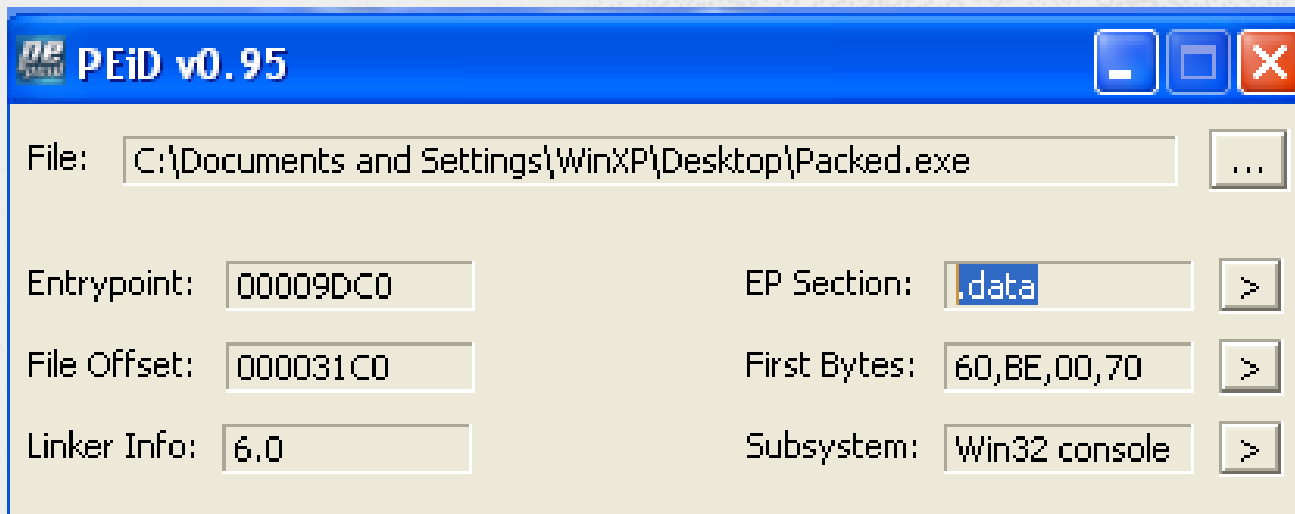
Triển khai —Thực nghiệm



Unpacking động thủ công


File **Packed.exe** được lấy từ Lab PracticalMalwareAnalysis.

Xem trên **PEiD** thấy **EP Section là .data** và không phát hiện packer, có vẻ là file bình thường (không được pack) ???












Xem file bằng **IDA pro**, khi mới mở thấy **warning một số imports segment đã bị hủy**, có thể là đã bị pack. **IDA pro** chỉ hiện hàm start và một số ít hàm được imports.

Warning

 The imports segment seems to be destroyed. This MAY mean that the file was packed or otherwise modified in order to make it more difficult to analyze. If you want to see the imports segment in the original form, please reload it with the 'make imports section' checkbox cleared.

OK

☐ Don't display this message again

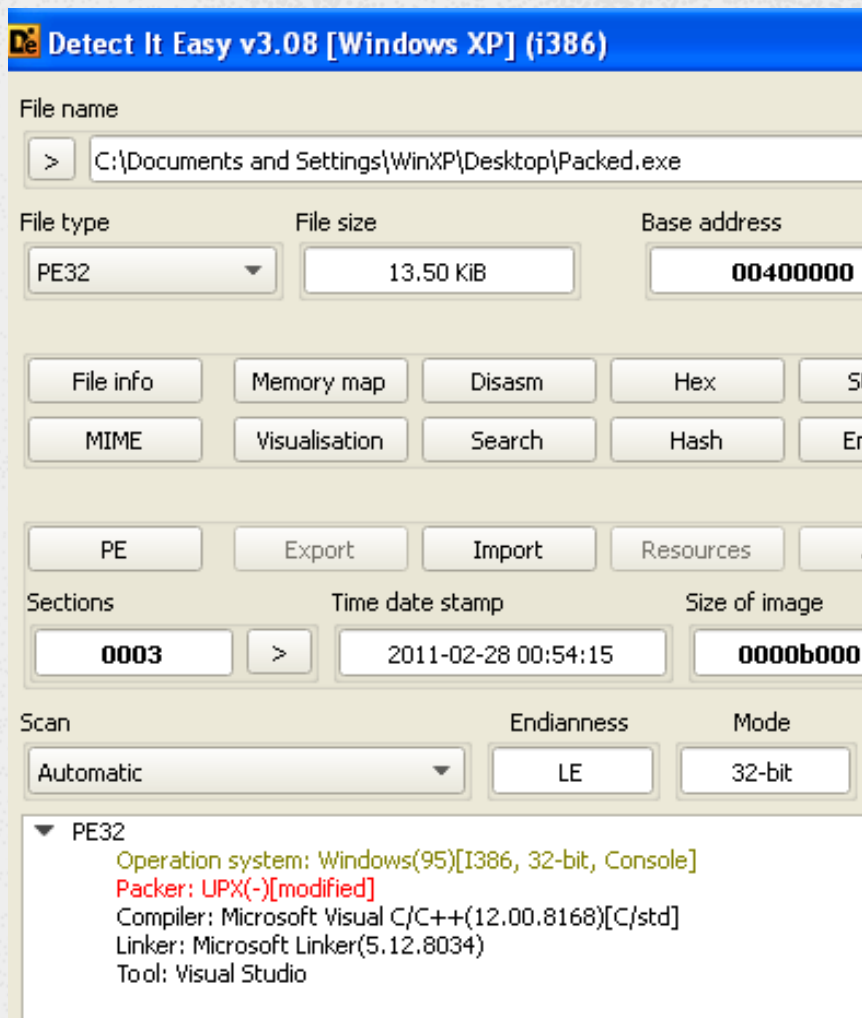
Function name	Segment	Address	Ordinal	Name	
 start	.data				
		 0040A050		LoadLibraryA	KERNEL32
		 0040A054		GetProcAddress	KERNEL32
		 0040A058		VirtualProtect	KERNEL32
		 0040A05C		VirtualAlloc	KERNEL32
		 0040A060		VirtualFree	KERNEL32
		 0040A064		ExitProcess	KERNEL32
		 0040A06C		GetUserNameA	ADVAPI32
		 0040A074		URLDownloadToCacheFileA	urlmon

Mở bằng **Pestudio** thấy signature là **UPX**, có section **UPX2**.

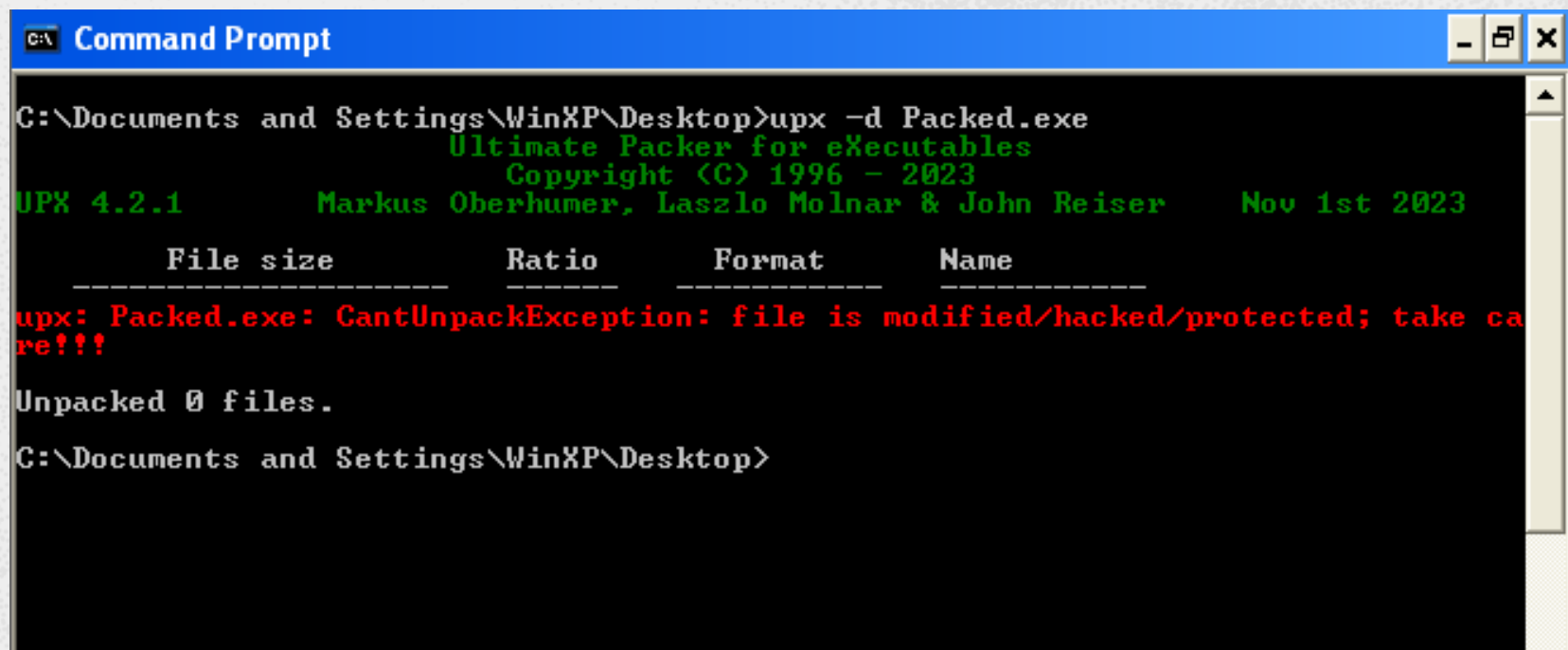
c:\documents and settings\winxp	property	value	value	value
indicators (6/16)	name	.text	.data	UPX2
virustotal (offline)	md5	n/a	532E5B5EE5D7161B86D9...	090CE89F259507897B11...
dos-stub (!This program cann	file-ratio (92.59 %)	0.00 %	88.89 %	3.70 %
file-header (Feb.2011□)	virtual-size (40960 bytes)	24576 bytes	12288 bytes	4096 bytes
optional-header (Console)	virtual-address	0x00001000	0x00007000	0x0000A000
directories (import-name)	raw-size (12800 bytes)	0 bytes	12288 bytes	512 bytes
sections (entry-point)	raw-address	0x00000400	0x00000400	0x00003400
libraries (3/3)	cave (0 bytes)	0 bytes	0 bytes	0 bytes
imports (8/8)	entropy	n/a	7.826	2.590
exports (n/a)	entry-point (0x00009DC0)	-	x	-
tls-callbacks (n/a)	blacklisted	-	-	x
resources (n/a)	writable	x	x	x
strings (11/207)	executable	x	x	-
	shareable	-	-	-

entropy	7.624
imphash	689DB29C407E9CA632770A9973BC254A
cpu	32-bit
signature	UPX -> www.upx.sourceforge.net
entry-point (hex)	60 BE 00 70 40 00 8D BE 00 A0 FF FF 57 EB 0B 90 8A
file-version	n/a
file-description	n/a
file-type	executable

Xem file bằng **DiE** thấy **có Packer**
và đã bị **modified**.



Sử dụng **upx** để unpack thử thì **không** được.



```
C:\> Command Prompt

C:\Documents and Settings\WinXP\Desktop>upx -d Packed.exe
                Ultimate Packer for eXecutables
                Copyright (C) 1996 - 2023
UPX 4.2.1      Markus Oberhumer, Laszlo Molnar & John Reiser   Nov 1st 2023

  File size      Ratio      Format      Name
  -----
upx: Packed.exe: CantUnpackException: file is modified/hacked/protected; take care!!!

Unpacked 0 files.

C:\Documents and Settings\WinXP\Desktop>
```

Xem luồng thực thi của chương trình bằng **IDA pro** thì thấy có đoạn **nhảy đến vị trí khá xa** với vị trí đang thực hiện và **OEP** của chương trình (Tail Jump).

```
00409F28 and     byte ptr [eax+28h], 7Fh
00409F2C pop     eax
00409F2D push    eax
00409F2E push    esp
00409F2F push    eax
00409F30 push    ebx
00409F31 push    edi
00409F32 call   ebp
00409F34 pop     eax
00409F35 popa
00409F36 lea     eax, [esp+2Ch+var_AC]
```

```
00409F3A
00409F3A loc_409F3A:
00409F3A push    0
00409F3C cmp     esp, eax
00409F3E jnz     short loc_409F3A
```

```
00409E51
00409E51 loc_409E51:
00409E51 add     ecx, 2
```

```
00409F40 sub     esp, 0FFFFFF80h
00409F43 jmp     near ptr byte 40154F
00409F43 start endp ; sp-analysis failed
00409F43
```

```
00409E54
00409E54 loc_409E54:
00409E54 cmp     ebp, 0FFFFFF300h
00409E5A adc     ecx, 1
00409E5D lea     edi+ebp]
00409E60 cmp     ebp, 0FFFFFFFCh
00409E63 jbe     short loc_409E74
```

```
00409E65
00409E65 loc_409E65:
00409E65 mov     al, [edx]
00409E67 inc     edx
00409E68 mov     [edi], al
00409E6A inc     edi
```

```
00409E74
00409E74 loc_409E74:
00409E74 mov     eax, [edx]
00409E76 add     edx, 4
00409E79 mov     [edi], eax
00409E7B add     edi, 4
```








Tại vị trí nhảy đến có nhiều dấu "?", có thể là phần đã được pack.

```
.text:00401000 ; Segment type: Pure code
.text:00401000 ; Segment permissions: Read/Write/Execute
.text:00401000 _text      segment para public 'CODE' use32
.text:00401000          assume cs:_text
.text:00401000          ;org 401000h
.text:00401000          assume es:nothing, ss:nothing, ds:_data, fs:nothing, gs:nothing
.text:00401000          dd 153h dup(?)
.text:0040154C          db 3 dup(?)
.text:0040154F byte_40154F db ? ; CODE XREF: start+183↓j
.text:00401550          dd 0EDCh dup(?)
.text:004050C0 byte_4050C0 db ? ; DATA XREF: .data:00407017↓r
.text:004050C1          db 3 dup(?)
.text:004050C4          dd 7CFh dup(?)
.text:004050C4 _text      ends
.text:004050C4
```

Sử dụng **x32dbg** để thực hiện debug, đặt **breakpoint** tại vị trí sẽ thực hiện **lệnh nhảy**.

Log	Notes	Breakpoints	Memory Map	Call Stack	SEH	Script
Address	Module/Label/Exception	State	Disassembly			
00409DC0	<packed.exe.OptionalHeader.Address0	One-time	pushad			
00409F43	packed.exe	Enabled	jmp packed.40154F			

Tại vị trí sẽ nhảy trước khi thực thi chương trình chỉ là **những bytes rỗng**.

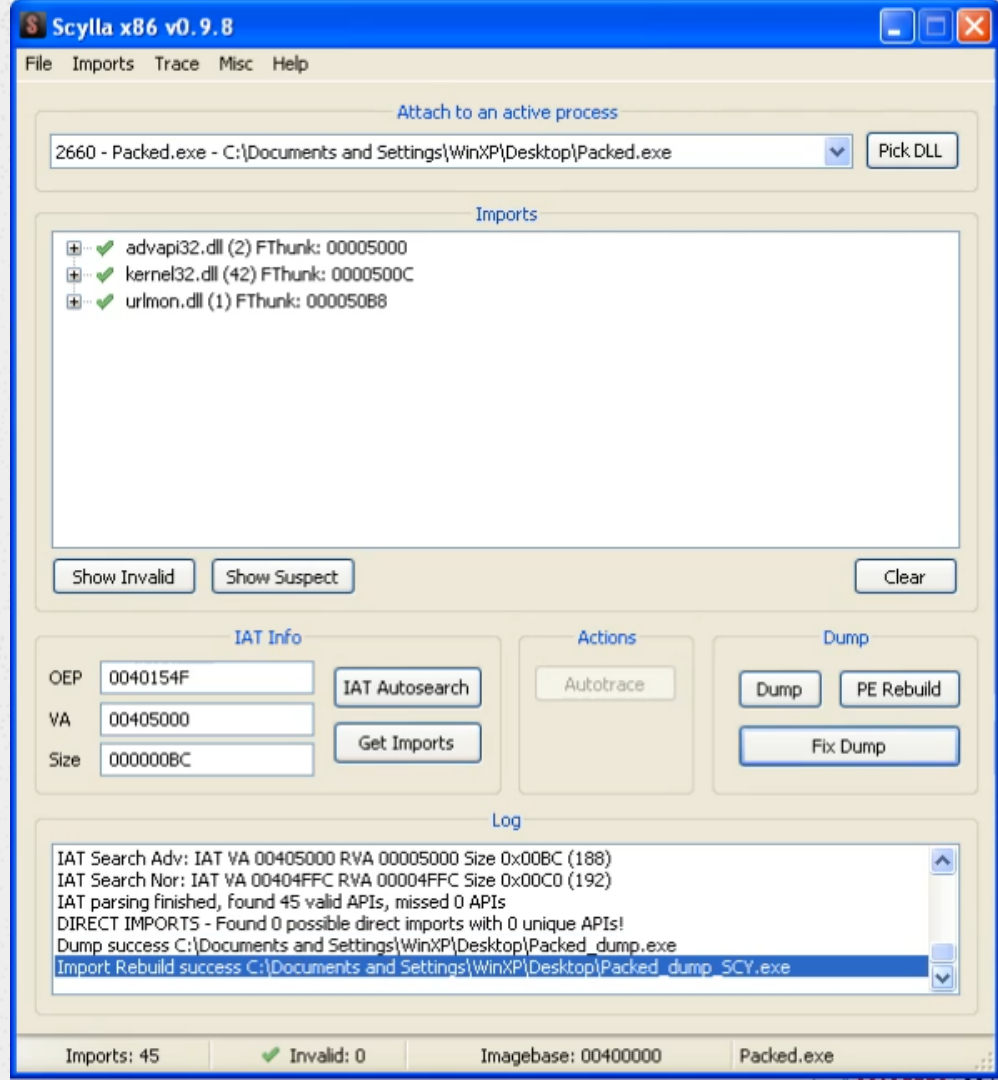
	 Breakpoints	 Memory Map	 Call Stack	 SEH	 Script	 Symbols
●	0040154F	0000	add byte ptr ds:[eax], al			
●	00401551	0000	add byte ptr ds:[eax], al			
●	00401553	0000	add byte ptr ds:[eax], al			
●	00401555	0000	add byte ptr ds:[eax], al			
●	00401557	0000	add byte ptr ds:[eax], al			
●	00401559	0000	add byte ptr ds:[eax], al			
●	0040155B	0000	add byte ptr ds:[eax], al			
●	0040155D	0000	add byte ptr ds:[eax], al			
●	0040155F	0000	add byte ptr ds:[eax], al			
●	00401561	0000	add byte ptr ds:[eax], al			
●	00401563	0000	add byte ptr ds:[eax], al			
●	00401565	0000	add byte ptr ds:[eax], al			
●	00401567	0000	add byte ptr ds:[eax], al			
●	00401569	0000	add byte ptr ds:[eax], al			
●	0040156B	0000	add byte ptr ds:[eax], al			

Sau khi thực hiện đến breakpoint, vị trí nhảy đến **có các lệnh**.

Breakpoints	Memory Map	Call Stack	SEH	Script	Symbols
0040154F	55	push ebp			
00401550	8BEC	mov ebp,esp			
00401552	6A FF	push FFFFFFFF			
00401554	68 08514000	push packed.405108			
00401559	68 34294000	push packed.402934			
0040155E	64:A1 00000000	mov eax,dword ptr fs:[0]			
00401564	50	push eax			
00401565	64:8925 00000000	mov dword ptr fs:[0],esp			
0040156C	83EC 10	sub esp,10			
0040156F	53	push ebx			
00401570	56	push esi			
00401571	57	push edi			
00401572	8965 E8	mov dword ptr ss:[ebp-18],esp			
00401575	FF15 20504000	call dword ptr ds:[<&GetVersion>]			
0040157B	33D2	xor edx,edx			
0040157D	8AD4	mov dl,ah			
0040157F	8915 34694000	mov dword ptr ds:[406934],edx			
00401585	8BC8	mov ecx,eax			
00401587	81E1 FF000000	and ecx,FF			
0040158D	89D0 30694000	mov dword ptr ds:[406930],ecx			
00401593	C1E1 08	shl ecx,8			
00401596	03CA	add ecx,edx			
00401598	89D0 2C694000	mov dword ptr ds:[40692C],ecx			
0040159E	C1E8 10	shr eax,10			
004015A1	A3 28694000	mov dword ptr ds:[406928],eax			
004015A6	6A 00	push 0			
004015A8	E8 52120000	call packed.4027FF			
004015AD	59	pop ecx			
004015AE	85C0	test eax,eax			
004015B0	75 08	jne packed.4015BA			
004015B2	6A 1C	push 1C			
004015B4	E8 9A000000	call packed.401653			
004015B9	59	pop ecx			
004015BA	8365 FC 00	and dword ptr ss:[ebp-4],0			
004015BE	E8 91100000	call packed.402654			
004015C3	FF15 1C504000	call dword ptr ds:[<&GetCommandLineA>]			
004015C9	A3 587E4000	mov dword ptr ds:[407E58],eax			
004015CE	E8 4F0F0000	call packed.402522			
004015D3	A3 10694000	mov dword ptr ds:[406910],eax			
004015D8	E8 F80C0000	call packed.4022D5			

Sử dụng **plugin Scylla** để thực hiện **kết xuất đoạn mã** sau khi **được unpack** vào chương trình ban đầu và thay đổi **OEP** mới đến nơi thực hiện đoạn code của mã độc.

(Dump để thêm code vào chương trình mới, Fix Dump để thực hiện liên kết các lời gọi hàm, thư viện)



Sau khi thực hiện xong, mở file **Packed_dump_SCY.exe** vừa được tạo ra bằng **IDA pro**. Lúc này các hàm, các imports đã được thêm vào.

The screenshot displays the IDA Pro interface with two main windows open: the Functions window on the left and the Imports list on the right.

Functions window: This window lists all functions found in the binary. The function `URLDownloadToCacheFileA` is highlighted in pink. Other functions include `sub_401000`, `sub_4010BB`, `sub_4011A3`, `_main`, `_strlen`, `_memset`, `_sprintf`, `__alloca_probe`, `start`, `__amsg_exit`, `_fast_error_exit`, `_flsbuf`, `__output`, `_write_char`, `_write_multi_char`, `_write_string`, `_get_int_arg`, `_get_int64_arg`, `_get_short_arg`, `_cinit`, `_exit`, `__exit`, and `_doexit`.

Imports list: This window shows the list of imported functions. The first function, `GetCurrentHwProfileA`, is highlighted in blue. The list includes various Windows API functions from `advapi32` and `kernel32`.

Address	Ordinal	Name	Library
00405000		GetCurrentHwProfileA	advapi32
00405004		GetUserNameA	advapi32
0040500C		Sleep	kernel32
00405010		CreateProcessA	kernel32
00405014		FlushFileBuffers	kernel32
00405018		GetStringTypeW	kernel32
0040501C		GetCommandLineA	kernel32
00405020		GetVersion	kernel32
00405024		ExitProcess	kernel32
00405028		TerminateProcess	kernel32
0040502C		GetCurrentProcess	kernel32
00405030		UnhandledExceptionFilter	kernel32
00405034		GetModuleFileNameA	kernel32
00405038		FreeEnvironmentStringsA	kernel32
0040503C		FreeEnvironmentStringsW	kernel32
00405040		WideCharToMultiByte	kernel32
00405044		GetEnvironmentStringsA	kernel32
00405048		GetEnvironmentStringsW	kernel32
0040504C		LockResource	kernel32
00405050		GetStdHandle	kernel32
00405054		GetFileType	kernel32
00405058		GetStartupInfoA	kernel32
0040505C		HeapDestroy	kernel32
00405060		HeapCreate	kernel32
00405064		VirtualFree	kernel32

Mô hình phân loại mã độc

Wild dataset: các mẫu tệp thực thi PE (Windows x86).

- 50,724 mẫu (*bao gồm 4,396 unpacked benign, 12,647 packed benign và 33,681 packed malicious*).
- 9 nhóm với tổng cộng 56,543 thuộc tính.

PE headers	28	Byte n-grams	13,000
PE sections	570	Opcode n-grams	2,500
DLL imports	4,305	Strings	16,900
API imports	19,168	File generic	2
Rich Header	66		

Mô hình phân loại mã độc

Mô hình được xây dựng với **4 thuật toán**. Thực nghiệm **Google Colaboratory**.

Kết quả Accuracy:

- DecisionTree: 92.5% RandomForest: 94.5%
- GradientBoosting: 95.2% AdaBoost: 94.9%

	precision	recall	f1-score	support
False	0.95	0.95	0.95	669
True	0.95	0.96	0.95	669
accuracy			0.95	1338
macro avg	0.95	0.95	0.95	1338
weighted avg	0.95	0.95	0.95	1338



Cảm ơn!

**Cảm ơn sự theo dõi của thầy
và các bạn.**

CREDITS: This presentation template was
created by **Slidesgo**, and includes icons by
Flaticon and infographics & images by **Freepik**