Ange Albertini
corkami.com

PE 101 تجول خلال ملف ويندوز تنفيذي

ملف مفصل

تمثيل حرفي	تمثيل ست عشري	الحقول	القيم	الشرح
MZ.....@...	4D 5A 00 00-00 00 00 00-00 00 00 00-00 00 00 00 على بُعد:0x30 00 00 00 00-00 00 00 00-00 00 00 00-40 00 00 00	e_magic e_lfanew	'MZ' 0x40	بصمه ثابته بُعد ترويسة الـ PE ❶
PE..L.....a...	على بُعد:0x40 50 45 00 00-4C 01 03 00-00 00 00 00-00 00 00 00 00 00 00 00-E0 00 02 01...	Signature Machine NumberOfSections SizeOfOptionalHeader Characteristics	'PE', 0, 0 0x14c [intel 386] 3 0xe0 0x102 [32b EXE]	بصمه ثابته المعالج : ...../ARM/MIPS/Intel عدد الأقسام ❷ البُعد النسبي لجدول الأقسام ❷ EXE/DLL/...
....@..... ..... .@.....	على بُعد:0x58 ...0B 01 00 00-00 00 00 00 00 00 00 00-00 00 00 00-00 10 00 00-00 00 00 00 00 00 00 00-00 00 40 00-00 10 00 00-00 02 00 00 00 00 00 00-00 00 00 00-04 00 00 00-00 00 00 00 00 40 00 00-00 02 00 00-00 00 00 00-02 00 00 00 00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00 00 00 00 00-10 00 00 00...	Magic AddressOfEntryPoint ImageBase SectionAlignment FileAlignment MajorSubsystemVersion SizeOfImage SizeOfHeaders Subsystem NumberOfRvaAndSizes	0x10b [32b] 0x1000 0x400000 0x1000 0x200 4 [4 و ما يليه NT] 0x4000 0x200 2 [GUI] 16	32 bits/64 bits حيثما يبدأ التنفيذ ❺ العنوان المفترض عنده وضع الملف فى الذاكره حيثما تبدأ الأقسام فى الذاكره ❷ حيثما تبدأ الأقسام فى الملف ❷ إصدار الويندوز المطلوب المساحه الكليه للذاكره المطلوبه الحجم الكلى للترويسات ❸ ذو واجهة جرافيك / سطر أوامر / driver عدد مجلدات البيانات ❹
....	...00 00 00 00-00 00 00 00 00 20 00 00-00 00 00 00-00 00 00 00-00 00 00 00 00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00	ImportsVA	0x2000	العنوان النسبي* الأفتراضي للمُستوردّات ❹
.text... ..... .rdata..... ....@..@.data.. ....0..... .....@..+	على بُعد:0x138 2E 74 65 78-74 00 00 00 00 10 00 00-00 10 00 00-00 02 00 00-00 02 00 00 00 00 00 00-00 00 00 00-00 00 00 00-20 00 00 60 2E 72 64 61-74 61 00 00-00 10 00 00-00 20 00 00 00 02 00 00-00 04 00 00-00 00 00 00-00 00 00 00 00 00 00 00-40 00 00 40-2E 64 61 74-61 00 00 00 00 10 00 00-00 30 00 00-00 02 00 00-00 06 00 00 00 00 00 00-00 00 00 00-00 00 00 00-40 00 00 C0			

جدول الأقسام

Name	VirtualSize*	VirtualAddress*	SizeOfRawData (الحجم الفيزيائي)	PointerToRawData (الموقع الفيزيائي)	Characteristics
.text	0x1000	0x1000	0x200	0x200	CODE EXECUTE READ
.rdata	0x1000	0x2000	0x200	0x400	INITIALIZED READ
.data	0x1000	0x3000	0x200	0x600	DATA READ WRITE

لكل قسم تتم قراءة كتله بحجم SizeofRawData من الملف ابتداءاً من النقطه PointerToRawData
سيتم تحميلها فى الذاكره عند العنوان ImageBase + VirtualAddress فى كتله بحجم VirtualSize و تكون لهذا الكتله خصائص Characteristics محدده

الكود المكافيء بلغة الـ C	أسمبلي x86
MessageBox(0, "Hello World!","a simple PE executable", 0); ExitProcess(0);	push 0 push 0x403000 push 0x403017 push 0 call [0x402070] push 0 call [0x402068]

على بُعد:0x200
RVA:0x401000
6A 00 68 00-30 40 00 68-17 30 40 00-6A 00 FF 15 j.h.0@.h.0@.j. .
70 20 40 00-6A 00 FF 15-68 20 40 00 p.@.j. .h.@.

النتائج	هياكل المُستوردّات		
بعد التحميل، kernel32.dll فى ExitProcess سيشير إلى الداله 0x402068 user32.dll فى MessageBoxA سيشير إلى الداله 0x402070	*INT 0x204c, 0 اللمبحه الأسم 0,ExitProcess *IAT 0x204c, 0 *INT 0x205a, 0 اللمبحه الأسم 0,MessageBoxA *IAT 0x205a, 0 *العناوين هنا كلها عناوين نسبيه افتراضيه	موصّفات 0x203c kernel32.dll 0x2078 0x2068 0x2044 user32.dll 0x2085 0x2070 0 0 0 0 0	على بُعد:0x400 RVA:0x402000 3C 20 00 00-00 00 00 00-00 00 00 00-78 20 00 00 68 20 00 00-44 20 00 00-00 00 00 00-00 00 00 00 85 20 00 00-70 20 00 00-00 00 00 00-00 00 00 00 00 00 00 00-00 00 00 00-00 00 00 00-4C 20 00 00 00 00 00 00-5A 20 00 00-00 00 00 00-00 00 45 78 69 74 50 72-6F 63 65 73-73 00 00 00-4D 65 73 73 61 67 65 42-6F 78 41 00-4C 20 00 00-00 00 00 00 5A 20 00 00-00 00 00 00-6B 65 72 6E-65 6C 33 32 2E 64 6C 6C-00 75 73 65-72 33 32 2E-64 6C 6C 00 .....X.....x... h...D..... à...p..... .....L... ....Z.....Ex itProcess...Mess ageBoxA.L..... Z.....kernel32 .dll.user32.dll.

سلاسل حرفيه

a simple PE executable\0
Hello world!\0

على بُعد:0x600 RVA:0x403000
61 20 73 69-6D 70 6C 65-20 50 45 20-65 78 65 63 a.simple.PE.exec
75 74 61 62-6C 65 00 48-65 6C 6C 6F-20 77 6F 72 utable.Hello.wor
6C 64 21 00 ld!.

هذا هو الملف كاملاً مع ذلك معظم ملفات الـPE تحتوى على عناصر أكثر الشروع مبسطه للايجاز.

الاصدار رقم 1. 17 سبتمبر 2012

ترويسة الـ DOS

تُعين أنه ملف تنائي

ترويسة الـ PE

تُعين أنه ملف تنائي 'حديث'

الترويسه الأختياريه

معلومات عن الملف التنفيذي

مجلدات البيانات

مؤشرات تحو هياكل إضافيه (مُصدّرات، مستوردات، .....)

الترويسه

تفاصيل تقنيه عن الملف التنفيذي

جدول الأقسام

تحدد كيف يحمل الملف فى الذاكره

الكود

ما يتم تنفيذه

الأقسام

محتويات الملف التنفيذي

المُستوردّات

الربط بين الملف التنفيذي و مكتبات الويندوز

الداتا

معلومات يستخدمها الكود

SHA-1 b7af4cb51ce38e43e030656eb2698fab408cf9cb
download @ pe101.corkami.com

simple

simple.exe

ترجمة وليد عصر

عملية التحميل

❶ الترويسات

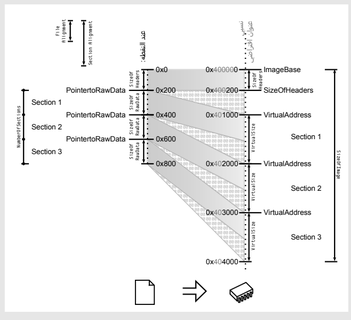
تتم قراءة ترويسة الـ DOS
تتم قراءة ترويسة الـ PE
قيمة الـe_lfanew فى ترويسة الـ DOS هى المسافه إلى ترويسة الـ PE
تتم قراءة الترويسه الاختياريه
(تتبع ترويسة الـ PE)

❷ جدول الأقسام

تتم قراءة جدول الأقسام
يوجد على بُعد: موقع (الترويسه الاختياريه) + SizeOfOptionalHeader
يحتوي على عدد NumberOfSections أقسام
يتم فحصه بمعية قيم المحاذاه للتأكد من صلاحيته
محاذاة الملف و محاذاة القسم

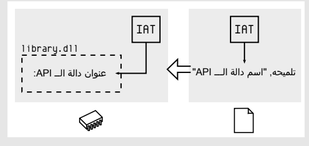
❸ الوضع

يوضع الملف فى الذاكره طبقًا لـ :
نقطة البدايه ImageBase
حجم الترويسات SizeOfHeaders
جدول الأقسام



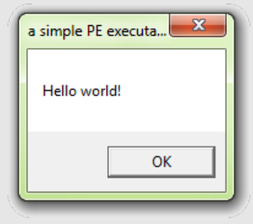
❹ المُستوردّات

تتم قراءة مجلدات البيانات
تتبع الترويسه الأختياريه
عدد المجلدات هو NumOfRVAAndSizes
المُستوردّات دائمًا هى المجلد رقم 2
تتم قراءة المُستوردّات
كل موصّف يحدد اسم ملف الـ DLL
تتم قراءة IAT و INT فى نفس الوقت
لكل دالة API فى INT
يكتب عنوانها فى مدخل IAT



❺ تنفيذ

يتم استدعاء الكود عند نقطة بداية التنفيذ EntryPoint
من خلال الـ IAT يتمكن الكود من الوصول لدوال الـ API



ملاحظات

ترويسة الـــ MZ هى نفسها ترويسة الـــ DOS
تبدأ بـــــ 'MZ' (الحروف الاولى من Mark Zbikowski مطور الـــ MS-DOS)
ترويسة الـــ PE هى نفسها IMAGE_FILE_HEADERS /COFF file header
تبدأ بـــــ 'PE' اى Portable Executable
الترويسه الاختياريه هى نفسها IMAGE_OPTIONAL_HEADER
اختياريه فقط للملفات غير التقليديه و لكنها مطلوبه للملفات التنفيذيه
عنوان نسبي افتراضي RVA
عنوان نسبي إلى نقطه البدايه ImageBase اى(عند نقطه البدايه ImageBase يكون الـــ RVA=0)
تقريبًا كل العناوين داخل الترويسات هى عناوين نسبيه افتراضيه RVAs
فى الكود, لا تكون العناوين نسبيه

جدول الأسماء المستورده INT
جدول من المؤشرات كل منها يشير الى التلميحه و هياكل الأسماء و ينتهى هذا الجدول بالصفر

جدول العناوين المستورده IAT
جدول من المؤشرات ينتهى بالصفر
داخل الملف ما هى إلا نسخه من الـــ INT
بعد التحميل تشير إلى دوال الـــ API المستورده

التلميحه
ترتيب الداله فى جدول مُصدّرات الـــ DLL الذي تقوم بالاستيراد منه
ليست بالضروريه و لكنها تسرع عملية البحث