1- روش های تحلیل بدافزار را نام برده و مختصرا شرح دهید.

1) Static Analysis

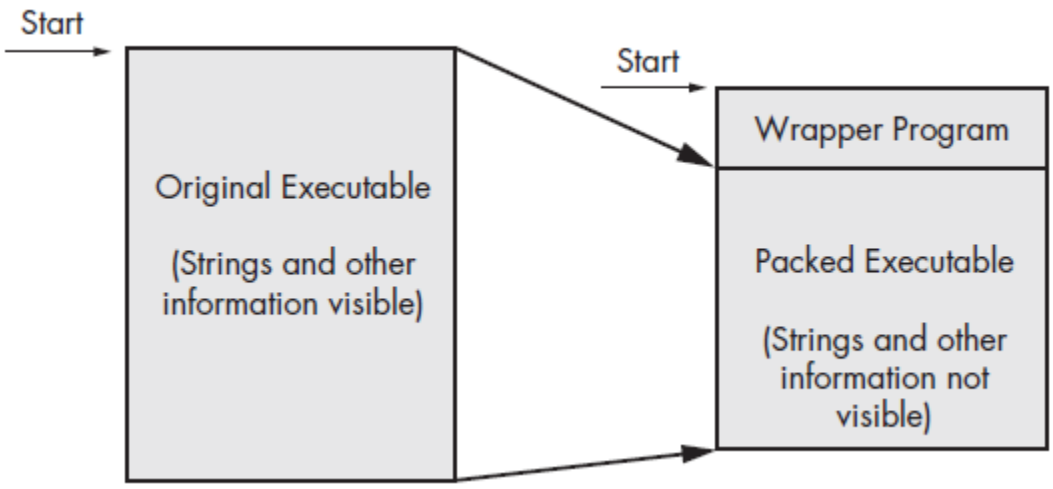
در این روش سعی می شود بدون اجرا کردن بدافزار و با disassemble کردن بد افزارآن را تحلیل کرد. در این روش میتوان از ابزار های Disassembler و نرم افزار های بررسی فرمت هدر فایل های اجرایی اطلاعات خوبی از بدافزار بدست آورد.

2) Dynamic Analysis

در این روش با اجرای بدافزار روی سیستم سعی می شود با بررسی رفتار آن بدافزار اطلاعاتی از نحوه ی اجرا شدن و همچنین تاثیران آن بر روی سیستم اطلاعاتی بدست آورد. این روش موثر تر از روش Static است.

2- Obfuscation یا packingچیست و چه تاثیری بر فرایند تحلیل بدافزار دارد.

در این حالت ها بدافزار فشرده یا رمز شده است .درحالت packed بدافزار ابتدا با قطعه کدی سعی میکند که خود را از حالت فشرده خارج کند و در رم جای دهد سپس به صورت عادی اجرا می شود. بنابر این در این حالت نمی توان بدون اجرا یا خارج کردن بد افزار از حالت obfuscated با روش های تحلیل استاتیک آن را مورد بررسی قرار داد.



3- چگونه متوجه شویم بدافزار pack شده است؟

ابتدا می توان با استفاده از نرم افزار های WSUnpacker یا PEiD بدافزار را مورد بررسی قرار داد درصورتی که از packer های معرف استفاده نشده باشد می توان با بررسی سایز قسمت های کد برنامه در حالت مجازی و حقیقی به بدافزار مشکوک شد.

4- چگونه می توان اطلاعاتی از قسمت های برنامه بدست آورد؟

می توان با استفاده از نرم افزار های تحلیل هدر فایل های اجرایی که به فرمت PE (Portable Executable) هستند اطلاعاتی از این قسمت ها بدست آورد. کی از این نرم افزار ها PEview است همچنین می توان از سایت virusTotal.com برای مشاهده این اطلاعات برای بدافزار های شناخته شده استفاده کرد.

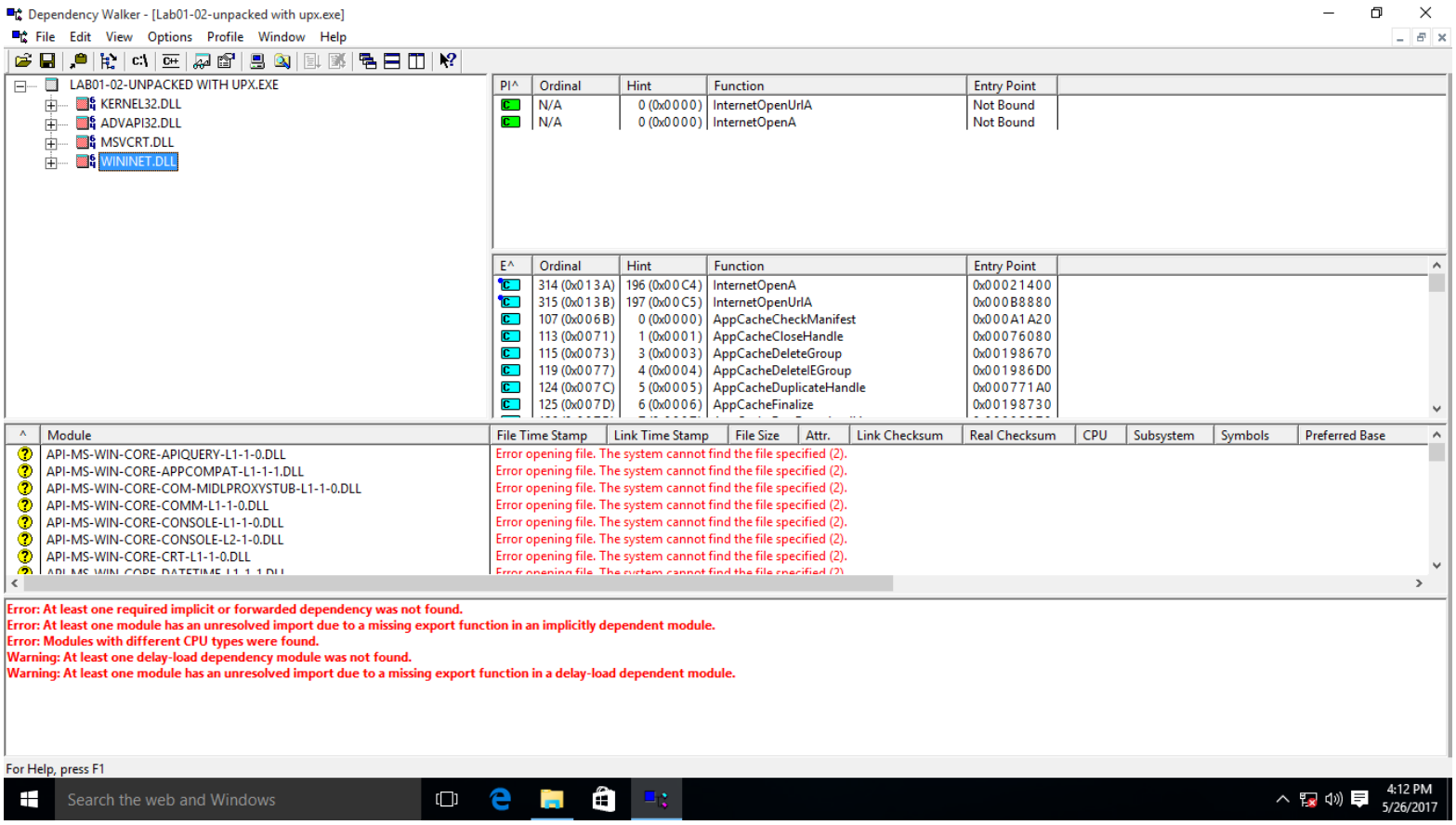
PE sections

Name	Virtual address	Virtual size	Raw size	Entropy	MD5
UPX0	4096	16384	0	0.00	d41d8cd98f00b204e9800998ecf8427e
UPX1	20480	4096	1536	7.07	ad0f236c2b34f1031486c8cc4803a908
UPX2	24576	4096	512	2.80	f998d25f473e69cc89bf43af3102beea

سایز قسمت اول که همان قسمت کد است در حالت مجازی 16384 ولی در حالت خام 0 پس نتیجه میگیرم این بدافزار pack شده است که در این مورد با نرم افزار UPX فشرده شده است.

5- چگونه متوجه شویم بدافزار از چه کتابخانه های از سیستم استفاده میکند.

می توان از روی هدر PE بدافزار کتابخانه های import و export شده را به همراه توابع مورد استفاده بدست اورد. Dependency walker از نرم افزار هایی است که این کار را برای ما انجام میدهد.



همان گونه که مشاهده میکند این بدافزار کتابخه ی WININET.dll و توابع InternetOpenUrlA و InternetOpenA از این کتابخه را استفاده می کند.

6- SandBox چیست و چند نمونه از آن را نام ببرید.

SandBox یه محیط امن است که می توان روی آن بدافزار مورد نظر خورد را اجرا کنیم و یک تحلیل جامع درباره ی عملکرد آن بد افزار داشته باشیم.

CW SandBox ، cuckoo

7- ProcMon چیست؟

Procmon ابزاری برای مشاهده ی رویداد های انتفاق افتاده درسیستم است. این رویداد ها میتوانندتغییرات ودسترسی های registry، دسترسی های شبکه، file system و رویداد های مربوط به process و thread باشند.

8- با چه ابرازی می توان dll ها را بدون اجرا executable مرتبط به اجرا کرد؟

به وسیله ی نرم افزار rundll32 می توان توابع export شده ی dll را اجرا کرد.

9- Disassembler چیست و تفاوت آن با Decompiler چیست؟ یک disassembler را نام ببرید.

Disassembler نرم افزرای است که زبان ماشین را به زبان اسمبلی ترجمه میکند که این کار عکس کار assembler است در حالی که Decompiler سعی می کند به جای تبدیل assemble به زبان سطح بالا این کار را انجام دهد.

10- Resource hacker چیست؟

Resource Hacker ابزاری برای مشاهده ی resource های که در یک فایل اجرایی وجود دارند است. از جمله این resource ها میتوان به رشته ها، آیکون نرم افزار و ... اشاره کرد. شکل زیر مواردی است که resource hacker برای یک نرم افزار نمایش داده است.