

قسمت ۴ – تجزیہ و تحلیل کاربردی بدافزارها

راهنمای جامع مهندسی معکوس، تجزیہ و تحلیل بدافزارها،
باچافزارها، جاسوس افزارها، روت کیت‌ها و بوتکیت‌های رایانه‌ای

آزمایشگاه امنیت کی‌پاد

نویسنده: میلاد کھساری الہادی

تجزیه و تحلیل دینامیک ساده بدافزار^۱

هر بررسی که پس از اجرای فایل بدافزار صورت گیرد، تجزیه و تحلیل دینامیک خوانده می‌شود. تکنیک‌های تجزیه و تحلیل دینامیک ساده دومین گامی هستند که در پروسه تحلیل بدافزار صورت می‌گیرند. معمولاً روش تجزیه و تحلیل دینامیک ساده بدافزار پس از تجزیه و تحلیل ایستای ساده^۲ که به بن‌بست رسیده است، توسط متخصصین صورت می‌گیرد.

تجزیه و تحلیل ایستای ساده ممکن است به دلیل مبهم‌سازی^۳ یا بسته‌بندی^۴ فایل اجرایی بدافزار به بن‌بست برسد یا شخص تحلیلگر از روش‌های موجود در تجزیه و تحلیل ایستا خسته شده باشد. این روش شامل نظارت فعالیت‌های بدافزار هنگام اجرا و بررسی سیستم پس از اجرای بدافزار می‌شود.

بر خلاف تجزیه و تحلیل ایستای ساده بدافزار، تجزیه و تحلیل دینامیک ساده به شما این امکان را می‌دهد که ویژگی‌های واقعی بدافزار را مشاهده کنید. به عنوان مثال، اگر بدافزار مورد تحلیل شما یک کیلاگر است، تجزیه و تحلیل دینامیک به شما اجازه می‌دهد محل فایل ذخیره‌سازی داده‌های بدافزار را شناسایی کنید، انواع اسنادی را که ذخیره کرده است، کشف کنید، مقصد ارسال اطلاعات بدافزار را رمزگشایی کنید و غیره. به دست آوردن این اطلاعات با روش تجزیه و تحلیل ایستای ساده بسیار مشکل است.

گرچه روش تجزیه و تحلیل دینامیک ساده بدافزار بسیار قدرتمند است، با این حال همواره این روش باید پس از اتمام روش تجزیه و تحلیل ایستای ساده بدافزار صورت گیرد، زیرا تجزیه و تحلیل دینامیک بدافزار، ممکن است سیستم و شبکه شخص تحلیلگر را در خطر قرار دهد.

روش‌های دینامیک محدودیت‌های خاص خودشان را دارند، زیرا هنگامی که یک قسمت خاص برنامه در حال فعالیت است، تمامی کدهای بدافزار در این روش ممکن است، اجرا نشوند. به عنوان مثال، بدافزارها در حالت خط فرمان نیاز به پارامترهای ورودی دارند، هر یک از پارامترها می‌تواند ویژگی‌های برنامه را به گونه مختلفی اجرا کند، بدون دانستن این پارامترها مطمئناً شما نخواهید توانست با استفاده از روش تجزیه و تحلیل دینامیک

¹ Basic Dynamic Malware Analysis

² Basic Static Malware Analysis

³ Obfuscation

⁴ Packaging

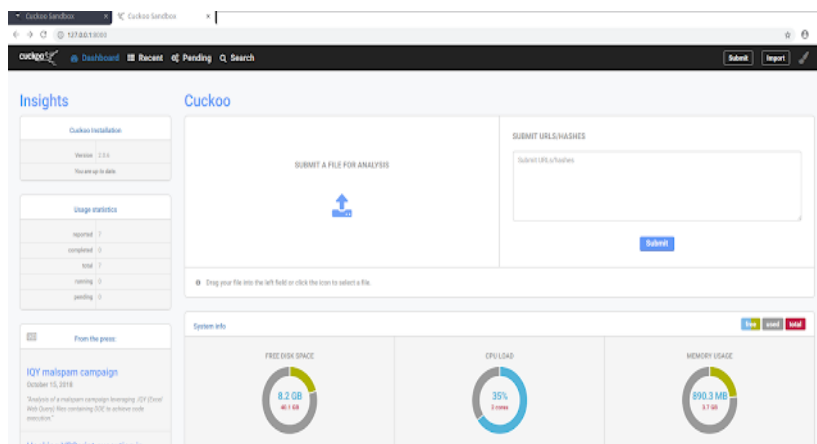
ساده همه ویژگی‌های برنامه را تحلیل کنید. به شما توصیه می‌کنیم از روش‌های تجزیه و تحلیل دینامیک یا تجزیه و تحلیل ایستای پیشرفته به منظور بررسی تمامی ویژگی‌های بدافزار استفاده کنید. در این فصل روش‌های تجزیه و تحلیل دینامیک ساده را تشریح خواهیم کرد و در ادامه به روش‌های پیشرفته تجزیه و تحلیل ایستا و دینامیک بدافزارها خواهیم پرداخت.

جعبه‌های شنی: رویکردی کثیف و سریع¹

برنامه‌های مختلفی به منظور تجزیه و تحلیل دینامیک ساده بدافزارها تولید شده‌اند که می‌توانند به سادگی روی بدافزارها تجزیه و تحلیل دینامیک انجام دهند، مشهورترین آن‌ها از تکنولوژی جعبه‌شنی استفاده می‌کنند که در مقاله قبلی یک نمونه از آن‌ها را مورد بررسی قرار دادیم.

جعبه‌شنی یک مکانیزم امنیتی است که برای اجرای برنامه‌های مخرب و مشکوک در یک محیط ایمن مورد استفاده قرار می‌گیرد، بدون آن که ترس آسیب رسیدن به سیستم و شبکه وجود داشته باشد.

در فصل گذشته نحوه راه‌اندازی و استفاده از جعبه‌شنی کوکو را آموختیم. جعبه‌شنی کوکو یکی از معروف‌ترین جعبه‌شنی‌های جهان است که به منظور تجزیه و تحلیل بدافزارها مورد استفاده قرار می‌گیرد.



تصویر ۱: محیط جعبه‌شنی کوکو

شایان ذکر است، جعبه‌های شنی شامل یک محیط مجازی هستند که در آن اغلب سرویس‌های شبکه‌ای را به منظور اجرای عادی بدافزار شبیه‌سازی می‌کنند.

¹ Sandboxes: The Quick-and-Dirty Approach

بیشتر جعبه‌های شنی، از قبیل جعبه‌شنی Cuckoo، جعبه‌شنی hybrid-analysis، جعبه‌شنی Joesandbox، جعبه‌شنی ThreatExpert، جعبه‌شنی BitBlaze، جعبه‌شنی Run و تحلیلگر بدافزار Valkyrie Comodo به رایگان بدافزار را تحلیل خواهند کرد.

در حال حاضر جعبه‌شنی Intezer و جعبه‌شنی Cuckoo و جعبه‌شنی Run.any میان متخصصین کامپیوتر جزو مشهورترین جعبه‌شنی‌ها هستند. این جعبه‌های شنی یک خروجی قابل درک و واضح از تحلیل بدافزار ارائه می‌دهند و برای ارزیابی اولیه بسیار عالی هستند.

نکته: شما می‌توانید ابزارهای جعبه‌شنی را به منظور استفاده در خانه خریداری کنید، اما آن‌ها گران قیمت هستند. با این حال به جای خریداری آن‌ها، می‌توانید با روش‌های تجزیه و تحلیل اساسی که در این فصل تشریح می‌شوند، تمام چیزهایی را که جعبه‌های شنی شناسایی می‌کنند، خود به صورت دستی کشف کنید.

البته، اگر شما تعداد زیادی بدافزار برای تحلیل دارید، در این شرایط بهتر است به منظور افزایش سرعت راندمان تحلیل بدافزارهای خود یکی از این نرم‌افزارهای جعبه‌شنی را خریداری کنید.

البته جعبه‌های شنی رایگانی هم مانند Cuckoo وجود دارند که قدرت تحلیل آن‌ها نسبتاً خوب است. البته تنها مشکلی که جعبه‌های شنی دارند، این است که آن‌ها قادر به تحلیل کدهای دیزاسمبلی یک بدافزار نیستند، این جعبه‌های شنی فقط صرفاً می‌توانند رفتار یک بدافزار را تحلیل کنند که آن هم متأسفانه با یک سری رویکردهای خاص مانند استفاده از توابع Sleep یا نحوه شناسایی محیط جعبه‌شنی به سادگی قابل دور زدن است.

بیشتر جعبه‌های شنی مشابه یکدیگر کار می‌کنند، بنابراین ما فقط به تشریح یکی از آن‌ها خواهیم پرداخت. در این قسمت ما روی جعبه‌شنی GFI متمرکز خواهیم شد، زیرا این جعبه‌شنی جزو مشهورترین جعبه‌های شنی موجود برای متخصصین تحلیل بدافزار است.

تصویر ۲ محتوای یک فایل PDF گزارش شده را نمایش می‌دهد که با اجرا شدن یک فایل در تحلیلگر خودکار جعبه‌شنی GFI تولید شده است. این گزارش شامل جزئیات مختلف بدافزار از قبیل فعالیت‌های شبکه‌ای که انجام داده است، فایل‌هایی که ایجاد کرده است، نتیجه پویش فایل در سایت VirusTotal و غیره می‌باشد.

GFI SandBox™ Analysis # 2307	
Sample: win32XYZ.exe (56476e02c29e5dbb9286b5f7b9e708f5)	
Table of Contents	
Analysis Summary	3
Analysis Summary	3
Digital Behavior Traits	3
File Activity	4
Stored Modified Files	4
Created Mutexes	5
Created Mutexes	5
Registry Activity	6
Set Values	6
Network Activity	7
Network Events	7
Network Traffic	8
DNS Requests	9
VirusTotal Results	10

شکل ۲: نمونه نتیجه جعبه‌شنی GFI برای فایل win32XYZ.exe

گزارش‌های تولید شده توسط جعبه‌شنی GFI در هر بخش شامل یک سری اطلاعات در مورد فایل win32XYZ.exe می‌باشد. گزارش تولید شده توسط GFI شامل شش بخش کلی است که در زیر هر بخش به صورت مجزا و ساده تشریح شده است.

۱. بخش Summary اطلاعات تجزیه و تحلیل ایستا به همراه نتایج تحلیل پویا را نمایش می‌دهد.
۲. بخش Activity لیست فایل‌هایی که توسط بدافزار باز، ایجاد یا حذف شده‌اند، نمایش می‌دهد.
۳. بخش Created Mutexes لیست Mutex‌های ایجاد شده توسط بدافزار را نمایش می‌دهد.
۴. بخش Registry Activity اطلاعات فعالیت‌های شبکه‌ای بدافزار را نمایش می‌شود.

۵. بخش VirusTotal نتایج بررسی فایل توسط VirusTotal را برای شما نمایش خواهد داد.

نکته: به منظور مطالعه بیشتر در مورد نحوه عملکرد جعبه‌های شنی و همچنین آشنایی با جعبه‌شنی Cuckoo می‌توانید کتاب راهنمای استفاده از جعبه‌شنی Cuckoo نوشته میلاد کهساری الهادی را مورد مطالعه قرار بدهید. این کتاب به صورت رایگان از آدرس (<http://aiooo.ir/>) قابل دریافت است.

معایب جعبه‌شنی

جعبه‌های شنی دارای معایب بزرگی هستند. به عنوان مثال، جعبه‌های شنی به سادگی فایل اجرایی بدافزار را بدون توجه به ساختار و جریان اجرای بدافزار اجرا می‌کنند. مثلاً اگر بدافزار نیاز به پارامترهای تحت خط فرمان داشته باشد و به آن از طریق خط فرمان پارامتر مورد نیاز ارائه نشود، بدافزار هیچگونه کدی از خود را اجرا نمی‌کند. در نتیجه جعبه‌شنی بعد از اجرای بدافزار، با رفتار اصلی باینری رو به رو نخواهد شد و ممکن است بدافزار را به عنوان یک نرم‌افزار مشروع شناسایی کند.

علاوه بر این، بدافزار اگر قبل از اجرای درپشتی منتظر یک بسته شبکه‌ای از سرور کنترل و فرماندهی خود باشد، درپشتی هیچ‌گاه در جعبه‌شنی اجرا نخواهد شد. همچنین جعبه‌شنی ممکن است تمامی رویدادهای اتفاق افتاده بعد از اجرای بدافزار را نتواند ضبط کند، زیرا یا شما یا بدافزار نمی‌تواند مدت زمان طولانی به منظور تحلیل رویدادهای بدافزار منتظر بماند. به عنوان مثال، فرض کنید اگر یک بدافزار بگونه‌ای تنظیم شده باشد که به منظور انجام عملیات مخرب خود باید به مدت زمان یک روز متوقف (Sleep) شود.

در این حالت، شما ممکن است آن رویداد را از دست بدهید. (در بیشتر جعبه‌های شنی، به منظور جلوگیری از انجام این مکانیزم، تابع Sleep را هوک می‌کنند و مقدار زمان توقف یا Sleep را با یک مقدار محدود تنظیم می‌کنند، اما باز هم راه‌های بسیاری به منظور متوقف سازی انجام عملیات جعبه‌شنی توسط بدافزار وجود دارد که جعبه‌شنی نمی‌تواند تمامی آن‌ها را رسیدگی کند.) مابقی معایب جعبه‌های شنی در زیر آورده شده است :

۱. اگر بدافزار در یک ماشین مجازی اجرا شود، می‌تواند این موضوع را شناسایی کند. اگر بدافزار بتواند یک ماشین مجازی را شناسایی کند از اجرای خود جلوگیری خواهد کرد و یا یک رفتار نامتعارف از

خود به منظور انحراف تحلیلگر بروز خواهد داد. بیشتر جعبه‌های شنی نمی‌توانند این مسئله را کنترل کنند.

۲. برخی از بدافزارها نیاز به بعضی از کلیدهای رجیستری ویندوز یا فایل‌های روی سیستم دارند که ممکن است در جعبه‌شنی آن‌ها پیدا نشوند. این فایل‌ها و یا رجیسترها می‌توانند داده‌های مجازی از قبیل برخی فرمان‌ها یا کلیدهای رمزنگاری باشند.

۳. اگر بدافزار یک Dll باشد، برخی از توابع صادراتی (Exported) آن نمی‌توانند به صورت مناسبی اجرا شوند، زیرا یک Dll به آسانی یک فایل exe اجرا نمی‌شود.

۴. سامانه‌عامل محیط جعبه‌شنی ممکن است برای بدافزار صحیح نباشد. به عنوان مثال، بدافزار ممکن است روی ویندوز XP اجرا نشود اما روی ویندوز هفت به خوبی راه‌اندازی و اجرا شود.

۵. یک جعبه‌شنی نمی‌تواند به شما بگوید یک بدافزار چه کاری انجام می‌دهد. جعبه‌های شنی می‌توانند فقط عملکردهای ساده بدافزار را گزارش دهند اما نمی‌توانند به شما بگویند که بدافزار یک ابزار نمونه‌بردار هش^۱ از مدیریت امن حساب‌های کاربری (SAM) سامانه‌عامل ویندوز یا یک درپشتی سرقت‌کننده کلیدهای فشرده رمزنگاری شده است.

اجرای بدافزار

اگر ما نتوانیم بدافزارها را اجرا کنیم، روش تجزیه و تحلیل دینامیک بی‌فایده می‌شود. در این قسمت روی قالب‌های EXE و DLL بدافزارها تمرکز خواهیم کرد که با آن‌ها بسیار مواجه خواهید شد. گرچه اجرای فایل‌های EXE با دو بار کلیک یا اجرای آن از طریق خط فرمان بسیار ساده است اما اجرای فایل‌های DLL مخرب اینطور نیست، زیرا ویندوز نمی‌داند آن‌ها را چگونه به صورت خودکار اجرا کند (در فصل ۸ با جزئیات بیشتری، ساختار درونی فایل‌های DLL را بررسی خواهیم کرد).

حال بگذارید به نحوه اجرای فایل‌های کتابخانه‌ای پیوندی پویا (DLL) به منظور اعمال موفقیت‌آمیز تجزیه و تحلیل روی بدافزار نگاهی بیندازیم. تمامی سامانه‌عامل‌های مدرن ویندوز شامل برنامه rundll32.exe

¹ Hash Dump

می‌باشند. این برنامه امکان اجرای فایل‌های DLL را به ما ارائه می‌کند. با دستورالعمل زیر می‌توانید DLLها را با این برنامه اجرا کنید.

```
C:\Users\clightning> rundll32.exe DLLname, Export arguments
```

مقدار پارامتر **Export** باید نام یک تابع یا یک عدد ترتیبی¹ از جدول توابع صادراتی فایل DLL باشد. همان‌طور که در قسمت ۲ این سلسله مقالات یاد گرفتید، می‌توانید از برنامه‌های **PEview** یا **PEexplorer** یا **CFFExplorer** یا **Dependency Walker** یا حتی پنجره **Exports** درون **IDA Pro**، **Hopper**، **Ghidra** و ... برای دیدن جداول توابع صادراتی (**Exports**) و وارداتی (**Imports**) استفاده کنید. به عنوان مثال فایل **rip.dll** توابع صادراتی زیر را دارد.

```
Install  
Uninstall
```

تابع صادراتی **Install** به نظر می‌رسد راهی برای اجرای **rip.dll** باشد، به هر حال بگذارید بدافزار را با فرمان زیر اجرا کنیم.

```
C:\Users\clightning> rundll32.exe rip.dll, Install
```

همچنین بدافزارها می‌توانند توابعی داشته باشند که به صورت عدد ترتیبی صادر شده باشند، بدین معنی که به جای نام تابع در خروجی از یک عدد ترتیبی استفاده شود، در این مورد در قسمت اول این سلسله مقالات بحث کردیم. با این حال در کتابخانه‌ها، هر تابع یک شماره دارد که به ترتیب به آن شماره‌ها اضافه می‌شود (بدین دلیل عدد ترتیبی خوانده می‌شوند).

به هر صورت، مسئله‌ای که در مورد **Import Name Table**، **Import Ordinal Table** و **Import Address Table** پیش از این در قسمت‌های گذشته توضیح دادم، مفاهیم پایه در بارگزاری و مدیریت فایل‌های اجرایی قابل حمل (فایل‌های **EXE** و **DLL** و **LIB** و ...) ویندوز هستند.

¹ Ordinal

وقتی شما در دیزاسمبلری مانند IDA یا یک دیباگری مانند LLDB یک دستورالعمل مانند call ds:20304050 مشاهده می کنید، این آدرس 20304050 به سادگی توسط دینامیک لودر سامانه عامل تولید نشده است. در پس زمینه سامانه عامل کلی اتفاق رخ می دهد که وقتی شما تابعی را فراخوانی می کنید، سامانه عامل بتواند جایگاه بلاک کد تابع را در فضای آدرس پروسه¹ پیدا کند و دستورات تابع را یک به یک اجرا و در نهایت به مسیر تابع فراخواننده تابع اصلی (تابع Caller) بازگشت کند. اما شناسایی آدرس توابع به چه صورت رخ می دهد؟

پیش از اینکه، به این مبحث بپردازیم، باید در گام اول در محیط ویندوز با دو مفهوم آدرس مجازی نسبی (RVA) و آدرس مجازی (VA) یا همان Relative Virtual Address و Virtual Address آشنا شوید. این دو مفهوم در محیط ویندوز با هم تفاوت دارند و رویکرد ویندوز استفاده از RVA است.

در این رویکرد، ویندوز همواره یک آدرس را به عنوان آدرس پایه (Base Address) انتخاب می کند که در فایل فرمت PE فیلد ImageBase حاوی این آدرس پایه است و مابقی چیزها مانند سکشن ها، دیرکتوری ها، جدول ها و مسائل دیگر را به نسبت این آدرس معرفی می کند.

به عنوان مثال، وقتی شما مشاهده می کنید آدرس پایه یک ایمج 10000000 است و آدرس نسبی سکشن RDATA به عنوان مثال 2030 است، در اصل سکشن RDATA در هنگام ترسیم (Map) به درون حافظه در آدرس 10002030 قرار دارد که در نهایت به آدرس 10002030 آدرس مجازی یا همان Virtual Address سکشن RDATA در حافظه گویند.

دومین مسئله که فهم آن برای ما اهمیت دارد این است که چطور دینامیک لودر ویندوز می تواند آدرس توابع را در حالت زمان اجرا یا همان Runtime به صورت بلادرنگ یا همان Real-Time محاسبه کند؟ ما در فایل فرمت PE سامانه عامل ویندوز چندین دیرکتوری بسیار مهم داریم که اطلاعات بسیار مهمی را در بر می گیرند، یکی از این دیرکتوری ها در حقیقت دیرکتوری Import Directory است که یک بازتعریف از استراکچر Image_Import_Descriptor است که به صورت آراییه برای هر DLL تعریف می شود.

این استراکچر چندین مولفه مهم دارد که به عنوان Original First Thunk, First Thunk و Name شناسایی می شوند (مهم ترین اعضا این سه تا هستند) که در حقیقت عضو Original First Thunk به

¹ Process Address Space

جدول Import Name Table و عضو First Thunk به جدول Import Address Table، و مولفه Name هم به نام کتابخانه DLL که توابع در آن قرار دارند، اشاره می‌کنند.

جدول Import Name Table حاوی نام توابعی می‌شود که از یک DLL به برنامه فراخوانی شده‌اند و جدول Import Address Table هم حاوی آدرس متناظر با نام توابع در جدول INT است. مثلاً اگر تابع MiladKahsariAlhadi در جدول INT در اندیس ۵ شناسایی شود، لودر به اندیس شماره ۵ جدول ENT یا همان Export Name Table کتابخانه DLL می‌رود که در آنجا آدرس اصلی تابع MiladKahsariAlhadi قرار دارد. آن آدرس را بر می‌دارد و در جدول IAT پروسه قرار می‌دهد. با این روند برنامه می‌تواند آدرس تابع MiladKahsariAlhadi را با رجوع به جدول IAT شناسایی و آن را فراخوانی کند.

Member	Offset	Size	Value	Meaning
Magic	00000120	Word	010B	PE32
MajorLinkerVersion	00000122	Byte	0E	
MinorLinkerVersion	00000123	Byte	0A	
SizeOfCode	00000124	Dword	00001200	
SizeOfInitializedData	00000128	Dword	00001800	
SizeOfUninitializedD...	0000012C	Dword	00000000	
AddressOfEntryPoint	00000130	Dword	0000163C	.text
BaseOfCode	00000134	Dword	00001000	
BaseOfData	00000138	Dword	00003000	
ImageBase	0000013C	Dword	00400000	
SectionAlignment	00000140	Dword	00001000	
FileAlignment	00000144	Dword	00000200	

تصویر ۳: آدرس ImageBase فایل MathClient

به عنوان مثال در تصویر ۳ مشاهده می‌کنید، مقدار فیلد ImageBase پروسه MathClient ما برابر با 00400000 است و آدرس نسبی جدول IAT ما (تصویر ۴) در آدرس 3000 است که اگر آن را با آدرس ImageBase جمع کنیم، مقدار آن برابر با 00403000 می‌شود.

CFF Explorer VIII - [MathClient.exe]

File Settings ?

MathClient.exe

Member	Offset	Size	Value	Section
Security Directory RVA	000001A0	Dword	00000000	
Security Directory Size	000001A4	Dword	00000000	
Relocation Directory RVA	000001A8	Dword	00006000	.reloc
Relocation Directory Size	000001AC	Dword	000001B8	
Debug Directory RVA	000001B0	Dword	00003170	.rdata
Debug Directory Size	000001B4	Dword	00000070	
Architecture Directory RVA	000001B8	Dword	00000000	
Architecture Directory Size	000001BC	Dword	00000000	
Reserved	000001C0	Dword	00000000	
Reserved	000001C4	Dword	00000000	
TLS Directory RVA	000001C8	Dword	00000000	
TLS Directory Size	000001CC	Dword	00000000	
Configuration Directory RVA	000001D0	Dword	000031E0	.rdata
Configuration Directory Size	000001D4	Dword	00000040	
Bound Import Directory RVA	000001D8	Dword	00000000	
Bound Import Directory Size	000001DC	Dword	00000000	
Import Address Table Directory RVA	000001E0	Dword	00003000	.rdata
Import Address Table Directory Size	000001E4	Dword	000000FC	
Delay Import Directory RVA	000001E8	Dword	00000000	
Delay Import Directory Size	000001EC	Dword	00000000	
.NET Metadata Directory RVA	000001F0	Dword	00000000	
.NET Metadata Directory Size	000001F4	Dword	00000000	

تصویر ۴: آدرس جدول IAT

اگر هم قصد داشته باشیم به قسمت جدول IAT توابع وارد شده از کتابخانه MathLibrary برویم، باید مقدار فیلد FT را بررسی کنیم که این کتابخانه در دیرکتوری Import پروسه ما شامل چه RVA می‌شود. در نتیجه می‌توانیم آن مقدار را با ImageBase جمع کنیم و سپس مستقیم وارد جدول این کتابخانه شویم. همانطور که در ۵ مشاهده می‌کنید، مقدار آدرس نسبی این جدول ۳۰۶۴ است.

Microsoft (R) Windows Debugger Version 6.12.0002.633 AMD64
Copyright (c) Microsoft Corporation. All rights reserved.

CommandLine: C:\Users\IEUser\Desktop\MathClient.exe
Symbol search path is: *** Invalid ***

a symbol search path.
symbol path.
ad to refresh symbol locations.

```

MathClient.exe
ntdll.dll
ntdll32.dll
C:\Windows\SYSTEM32\wow64.dll
C:\Windows\SYSTEM32\wow64win.dll
C:\Windows\SYSTEM32\wow64cpu.dll
ode 80000003 (first chance)
Defaulted to export symbols for ntdll.dll -

MathClient.exe
s could not be loaded for MathClient.exe
Defaulted to export symbols for C:\Windows\SYSTEM32\wow64win
Defaulted to export symbols for C:\Windows\SYSTEM32\wow64.dl
Defaulted to export symbols for C:\Windows\SYSTEM32\wow64cpu
Defaulted to export symbols for ntdll32.dll -

```

Module Name	Imports	OFts	TimeDateSt...	ForwarderC...	Name RVA	FTs (IAT)
00001E94	N/A	00001C74	00001C78	00001C7C	00001C80	00001C84
szAnsi	(nfunctions)	Dword	Dword	Dword	Dword	Dword
MathLibrary.dll	3	000037A0	00000000	00000000	00003894	00003064
MSVCP140.dll	11	00003770	00000000	00000000	00003854	00003034
VCRUNTIME14...	4	00003780	00000000	00000000	000038AE	00003074

OFts	FTs (IAT)	Hint	Name
Dword	Dword	Word	szAnsi
00003852	00003852	0002	?Multiply@Functions@SA...
00003872	00003872	0001	?AddMultiply@Functions@...
00003838	00003838	0000	?Add@Functions@@SANN...

public static double __cdecl Functions::Multiply(double, double)

تصویر ۵: آدرس جدول FT

حال اگر برنامه را در دیباگر WinDBG بارگزاری کنیم و در پنجره مموری به آدرس (MathClient+3064) برویم مقادیر موجود در این جدول را مشاهده خواهیم کرد که قبل از اجرای برنامه در این فیلدها مقادیر هینت‌های توابع وجود دارد (تصویر ۶).

```

Virtual: MathClient+3064
00000000 01343064 74ea1020 74ea1030 74ea1010 00000000 746ae780
00000000 01343078 746af150 746ab950 746a2d80 00000000 734077c0
00000000 0134308c 00000000 73407350 00000000 73479710 00000000
00000000 013430a0 73402fd0 733fdec0 73454830 73406eb0 73454100
00000000 013430b4 73456230 73454820 73456270 73406f00 73403060
00000000 013430c8 73485ae0 734059c0 733f5670 73456210 73407940
00000000 013430dc 734531a0 73456250 73403120 734562b0 00000000
00000000 013430f0 73407790 73407960 00000000 01341f39 00000000
00000000 01343104 013414bc 00000000 00000000 01341410 013414b4
00000000 01343118 00000000 00000000 00000000 00000000 00000000
00000000 0134312c 00000000 01344020 01344070 202b2061 203d2062
00000000 01343140 00000000 202a2061 203d2062 00000000 202b2061
00000000 01343154 2a206128 20296220 0000203d 9999999a 401d9999
00000000 01343168 00000000 4058c000 00000000 5b1aa074 00000000
00000000 0134317c 00000002 00000082 00003260 00018600 00000000
00000000 01343190 5b1aa074 00000000 0000000c 00000014 000032e4
00000000 013431a4 000018e4 00000000 5b1aa074 00000000 0000000d
00000000 013431b8 00000264 000032f8 000018f8 00000000 5b1aa074
00000000 013431cc 00000000 0000000e 00000000 00000000 00000000
00000000 013431e0 00000068 00000000 00000000 00000000 00000000
00000000 013431f4 00000000 00000000 00000000 00000000 00000000
00000000 01343208 00000000 00000000 00000000 00000000 00000000
00000000 0134321c 01344004 01343250 00000004 013430fc 00000000
00000000 01343230 00000000 00000000 00000100 00000000 00000000
00000000 01343244 00000000 00000000 00000000 00001d6b 00001ff0
00000000 01343258 00002010 00002040 53445352 81c96a19 41fe3f61
00000000 0134326c 290e9988 309653f5 00000001 555c3a43 73726573
00000000 01343280 6563725c 6f5c696d 7264656e 5c657669 75636f64
00000000 01343294 746e656d 69765c73 6c617573 75747320 206f6964
    
```

تصویر ۶: نمایش جدول IAT در WinDBG

بعد که برنامه را اجرا کنیم، مشاهده خواهیم کرد که به جای مقادیر هینت‌ها، لودر آدرس توابع فراخوانی شده از کتابخانه MathLibrary را در این جدول قرار می‌دهد (تصویر ۷) که حال شما می‌توانید با دستور In و آدرس فیلدهای درون جدول IAT سیگنچر یا نام توابع را مشاهده کنید.

```

Virtual: MathClient+3064
00000000 01343064 74ea1020 74ea1030 74ea1010 00000000 746ae780
00000000 01343078 746af150 746ab950 746a2d80 00000000 734077c0
00000000 0134308c 00000000 73407350 00000000 73479710 00000000
00000000 013430a0 73402fd0 733fdec0 73454830 73406eb0 73454100
00000000 013430b4 73456230 73454820 73456270 73406f00 73403060
00000000 013430c8 73485ae0 734059c0 733f5670 73456210 73407940
00000000 013430dc 734531a0 73456250 73403120 734562b0 00000000
00000000 013430f0 73407790 73407960 00000000 01341f39 00000000
00000000 01343104 013414bc 00000000 00000000 01341410 013414b4
00000000 01343118 00000000 00000000 00000000 00000000 00000000
00000000 0134312c 00000000 01344020 01344070 202b2061 203d2062
00000000 01343140 00000000 202a2061 203d2062 00000000 202b2061
00000000 01343154 2a206128 20296220 0000203d 9999999a 401d9999
00000000 01343168 00000000 4058c000 00000000 5b1aa074 00000000
00000000 0134317c 00000002 00000082 00003260 00018600 00000000
00000000 01343190 5b1aa074 00000000 0000000c 00000014 000032e4
00000000 013431a4 000018e4 00000000 5b1aa074 00000000 0000000d
00000000 013431b8 00000264 000032f8 000018f8 00000000 5b1aa074
00000000 013431cc 00000000 0000000e 00000000 00000000 00000000
00000000 013431e0 00000068 00000000 00000000 00000000 00000000
00000000 013431f4 00000000 00000000 00000000 00000000 00000000
00000000 01343208 00000000 00000000 00000000 00000000 00000000
00000000 0134321c 01344004 01343250 00000004 013430fc 00000000
00000000 01343230 00000000 00000000 00000100 00000000 00000000
00000000 01343244 00000000 00000000 00000000 00001d6b 00001ff0
00000000 01343258 00002010 00002040 53445352 81c96a19 41fe3f61
00000000 0134326c 290e9988 309653f5 00000001 555c3a43 73726573
00000000 01343280 6563725c 6f5c696d 7264656e 5c657669 75636f64
00000000 01343294 746e656d 69765c73 6c617573 75747320 206f6964
    
```

تصویر ۷: نمایش نام توابع با دستور In در محیط WinDBG

نکته : همانطور که پیش از این ذکر شد، با ابزاری مانند PEexplorer، CFFExplorer و Dependency Walker می‌توانید لیست توابع صادراتی (Exported Functions) و توابع وارداتی (Imported Functions) یک فایل اجرای قابل حمل (PE) را مشاهده کنید. شایان ذکر است، ابزارهایی مانند IDA Pro و Ghidra و Hopper علاوه بر نمایش توابع صادراتی و وارداتی فایل اجرایی PE، توانایی نمایش توابع وارداتی و صادراتی فایل اجرایی ELF برای لینوکس و فایل اجرایی Mach-o برای مکینتاش را دارند. شایان ذکر است، در این برنامه‌ها علاوه بر نام تابع، یک عدد هم در کنار نام توابع نوشته شده است که به آن عدد ترتیبی (Ordinal Numbers) توابع می‌گویند. در حالت کلی می‌شود گفت به جای استفاده از نام تابع، می‌توان از آن عدد ترتیبی استفاده کرد و آن تابع را فراخوانی کرد.

هنگامیکه فقط عدد ترتیبی تابع صادراتی وجود دارد، هنوز می‌توانید با استفاده از rundll32.exe (سامانه‌های ۳۲ بیتی) و rundll64.exe (سامانه‌های ۶۴ بیتی) آن توابع را از فایل DLL با استفاده از فرمان زیر فراخوانی کنید. در فرمان نمایش داده شده در قسمت زیر، عدد ۵، شماره ترتیبی مختص تابع است که باید آن را فراخوانی کنید. شایان ذکر است، پیش از فراخوانی اعداد ترتیبی قبل از آن‌ها باید یک علامت (#) بگذارید. به شکل زیر:

```
C:\Users\clightning> rundll32.exe xyzzy.dll, #5
```

از آنجاییکه کتابخانه‌های پیوندی پویا مخرب، بیشتر کدهای خودشان را پیوسته درون DllMain اجرا می‌کنند (نقطه ورود به کتابخانه پیوندی پویا^۱ خوانده می‌شود) و چونکه DllMain هرگاه که کتابخانه‌ای بارگذاری

¹ DLL entry point

می‌شود، اجرا می‌گردد، شما اغلب می‌توانید با اجرای DLL با استفاده از rundll32.exe به صورت پویا از آن اطلاعات دریافت کنید.

حتی بجای این روش می‌توانید یک DLL را به حالت اجرایی درآورید، بدین منظور باید هدر فایل PE آن را به همراه نام قالب (.dll) تعویض کنید تا ویندوز بتواند آن را اجرا کند. به منظور تعویض قالب اجرایی فایل DLL به یک فایل اجرایی، باید فلگ (0x2000) IMAGE_FILE_DLL را از IMAGE_FILE_HEADER در فیلد خصوصیات (Characteristics) فایل DLL پاک کنید.

این تغییر باعث اجرای متد DLLMain می‌شود، در حالی که هیچ تابع صادراتی اجرا نخواهد شد و البته ممکن است باعث خرابی و توقف غیر منتظره فایل DLL شود. به هر حال، اگر این اعمال تغییرات باعث اجرای پیلود مخرب بدافزار شود و بتوانید به منظور جمع‌آوری اطلاعات آن را مورد تحلیل قرار بدهید، مابقی موارد دیگر مهم نیستند. همچنین قابل ذکر است، گاهی اوقات ممکن است Dll بدافزار نیاز داشته باشد با یک خروجی مناسب از قبیل InstallService به عنوان یک سرویس نصب شود.

```
C:\Users\clightning> rundll32 ipr32x.dll, InstallService ServiceName  
C:\Users\clightning> net start ServiceName
```

پارامتر ServiceName باید به بدافزار ارائه شود تا بتواند نصب و اجرا گردد. همچنین قابل ذکر است، دستور net start برای اجرای یک سرویس در سامانه‌عامل ویندوز مورد استفاده قرار می‌گیرد و همچنین از آن می‌توان برای مشاهده سرویس‌های در حال اجرا روی سامانه‌عامل استفاده کرد.

نکته : هنگامی که یک تابع ServiceMain را بدون یک تابع خروجی مناسب از قبیل Install یا InstallService مشاهده کردید، ممکن است نیاز داشته باشید سرویس را به صورت دستی نصب کنید. بدین منظور می‌توانید با استفاده از فرمان SC ویندوز یا با تغییر در رجیستری برای یک سرویس استفاده نشده و سپس اجرای دستور net start روی آن سرویس این کار را انجام بدهید. عناصر سرویس در قسمت HKLM\SYSTEM\CurrentControlSet\Services قرار دارند.

برنامه Process Monitor یک ابزار پیشرفته نظارتی برای ویندوز است که این امکان را به شما می‌دهد، تعاملات مرتبط با رجیستری، فایل سیستم، شبکه، پروسه‌ها و ... در سامانه‌عامل ویندوز را مشاهده و کنترل کنید. این برنامه ترکیب شده از دو برنامه قدیمی RegMon و FileMon است که عملکرد آن‌ها افزایش داده شده است.

Time	Process Name	PID	Operation	Path	Result	Detail
11:38:08	Explorer.EXE	4116	ReadFile	C:\Windows\System32\SHCore.dll	SUCCESS	Offset 581.632 Len...
11:38:08	sppsvc.exe	1932	CreateFile	C:\Windows\System32\spplstore2.0\dat...	NAME NOT FOUND	Desired Access: R...
11:38:08	sppsvc.exe	1932	CreateFile	C:\Windows\System32\spplstore2.0\dat...	NAME NOT FOUND	Desired Access: R...
11:38:08	sppsvc.exe	1932	CreateFile	C:\Windows\System32\spplstore2.0\dat...	SUCCESS	Desired Access: G...
11:38:08	sppsvc.exe	1932	WriteFile	C:\Windows\System32\spplstore2.0\dat...	SUCCESS	Offset 0. Length: 5.9...
11:38:08	sppsvc.exe	1932	WriteFile	C:\Windows\System32\spplstore2.0\dat...	SUCCESS	Offset 0. Length: 8.1...
11:38:08	vmtoolsd.exe	412	ReadFile	C:\Windows\System32\ucrbase.dll	SUCCESS	Offset 900.460. Len...
11:38:08	vmtoolsd.exe	412	ReadFile	C:\Windows\System32\ucrbase.dll	SUCCESS	Offset 872.448. Len...
11:38:08	vmtoolsd.exe	412	ReadFile	C:\Program Files\VMware\VMware Tool...	SUCCESS	Offset 1.153.536 Le...
11:38:08	vmtoolsd.exe	412	ReadFile	C:\Program Files\VMware\VMware Tool...	SUCCESS	Offset 1.014.784 Le...
11:38:08	sppsvc.exe	1932	CloseFile	C:\Windows\System32\spplstore2.0\dat...	SUCCESS	
11:38:08	sppsvc.exe	1932	ReadFile	C:\Windows\System32\kernelbase.dll	SUCCESS	Offset 2.404.352 Le...
11:38:08	Explorer.EXE	4116	ReadFile	C:\Windows\System32\shlwapi.dll	SUCCESS	Offset: 300.032 Len...
11:38:08	Explorer.EXE	4116	ReadFile	C:\Windows\System32\shlwapi.dll	SUCCESS	Offset 239.616 Len...
11:38:08	Explorer.EXE	4116	ReadFile	C:\Windows\System32\windows.storage...	SUCCESS	Offset 6.731.264 Le...
11:38:08	Explorer.EXE	4116	ReadFile	C:\Windows\System32\windows.storage...	SUCCESS	Offset 6.714.800 Le...
11:38:08	Explorer.EXE	4116	ReadFile	C:\Windows\explorer.exe	SUCCESS	Offset 3.282.944 Le...
11:38:08	vmtoolsd.exe	412	CreateFile	C:\ProgramData\VMware\VMware Tools...	NAME NOT FOUND	Desired Access: R...
11:38:08	sppsvc.exe	1932	CreateFile	C:\Windows\System32\spplstore2.0\dat...	SUCCESS	Desired Access: R...
11:38:08	sppsvc.exe	1932	QueryAttributeT...	C:\Windows\System32\spplstore2.0\dat...	SUCCESS	Attributes: HA, Rep...
11:38:08	sppsvc.exe	1932	QueryBasicInfo...	C:\Windows\System32\spplstore2.0\dat...	SUCCESS	CreationTime: 5/29/...
11:38:08	sppsvc.exe	1932	CreateFile	C:\Windows\System32\spplstore2.0	SUCCESS	Desired Access: W...
11:38:08	sppsvc.exe	1932	SetRenameInfo...	C:\Windows\System32\spplstore2.0\dat...	SUCCESS	ReplaceIfExists: Tr...
11:38:08	sppsvc.exe	1932	CloseFile	C:\Windows\System32\spplstore2.0	SUCCESS	
11:38:08	sppsvc.exe	1932	CloseFile	C:\Windows\System32\spplstore2.0\dat...	SUCCESS	
11:38:08	sppsvc.exe	1932	CloseFile	C:\Windows\System32\spplstore2.0\dat...	SUCCESS	Desired Access: R...
11:38:08	sppsvc.exe	1932	QueryAttributeT...	C:\Windows\System32\spplstore2.0\dat...	SUCCESS	Attributes: HA, Rep...
11:38:08	sppsvc.exe	1932	QueryBasicInfo...	C:\Windows\System32\spplstore2.0\dat...	SUCCESS	CreationTime: 5/29/...
11:38:08	sppsvc.exe	1932	CreateFile	C:\Windows\System32\spplstore2.0	SUCCESS	Desired Access: W...
11:38:08	sppsvc.exe	1932	SetRenameInfo...	C:\Windows\System32\spplstore2.0\dat...	SUCCESS	ReplaceIfExists: Tr...
11:38:08	sppsvc.exe	1932	CloseFile	C:\Windows\System32\spplstore2.0	SUCCESS	
11:38:08	sppsvc.exe	1932	CloseFile	C:\Windows\System32\spplstore2.0\dat...	SUCCESS	
11:38:08	slui.exe	956	ReadFile	C:\Windows\System32\spcpeet.dll	SUCCESS	Offset 507.392 Len...
11:38:08	slui.exe	956	ReadFile	C:\Windows\System32\spcpeet.dll	SUCCESS	Offset 515.554 Len...
11:38:08	slui.exe	956	ReadFile	C:\Windows\System32\spcpeet.dll	SUCCESS	Offset 470.528 Len...
11:38:08	slui.exe	956	ReadFile	C:\Windows\System32\spcpeet.dll	SUCCESS	Offset 470.528 Len...
11:38:08	slui.exe	956	ReadFile	C:\Windows\System32\spcpcomapi.dll	SUCCESS	Offset 272.364 Len...
11:38:08	slui.exe	956	ReadFile	C:\Windows\System32\spcpcomapi.dll	SUCCESS	Offset 272.364 Len...
11:38:08	slui.exe	956	ReadFile	C:\Windows\System32\slui.exe	SUCCESS	Offset 223.744 Len...
11:38:08	slui.exe	956	ReadFile	C:\Windows\System32\slui.exe	SUCCESS	Offset 227.840 Len...
11:38:08	Explorer.EXE	4116	ReadFile	C:\Windows\explorer.exe	SUCCESS	Offset 3.237.888 Le...
11:38:08	slui.exe	956	ReadFile	C:\Windows\System32\oleaut32.dll	SUCCESS	Offset 731.648 Len...
11:38:08	slui.exe	956	ReadFile	C:\Windows\System32\oleaut32.dll	SUCCESS	Offset 731.648 Len...
11:38:08	slui.exe	956	ReadFile	C:\Windows\System32\oleaut32.dll	SUCCESS	Offset 689.152 Len...
11:38:08	slui.exe	956	ReadFile	C:\Windows\System32\oleaut32.dll	SUCCESS	Offset 689.152 Len...
11:38:08	slui.exe	956	RegOpenKey	HKLM\System\CurrentControlSet\Control...	REPARSE	Desired Access: R...
11:38:08	slui.exe	956	RegOpenKey	HKLM\System\CurrentControlSet\Control...	REPARSE	Desired Access: R...
11:38:08	slui.exe	956	RegOpenKey	HKLM\System\CurrentControlSet\Control...	SUCCESS	Desired Access: R...
11:38:08	slui.exe	956	RegOpenKey	HKLM\System\CurrentControlSet\Control...	SUCCESS	Desired Access: R...

تصویر ۸: محیط Process Monitor در حال ارائه گزارش از رویدادهای سامانه‌عامل

اگرچه برنامه Process Monitor توانایی دریافت مقدار زیادی اطلاعات از تعاملات سطح سامانه‌عامل را دارد، اما با این حال این برنامه نمی‌تواند تمامی موارد موجود را دریافت کند. به عنوان مثال، این برنامه می‌تواند فعالیت درایور دستگاه یک مولفه سطح کاربر در حال تعامل با یک روت‌کیت از طریق کنترل‌های ورودی و خروجی دستگاه را از دست بدهد، همچنین این برنامه ممکن است برخی از فراخوانی‌ها از قبیل SetWindowsHookEx را هم از دست بدهد. گرچه برنامه Process Monitor می‌تواند مفید باشد، اما از آن نباید برای ثبت فعالیت‌های شبکه استفاده کرد، زیرا این برنامه برای چنین کاری مناسب نیست.

نکته : در طول این قسمت از سلسله مقالات تجزیه و تحلیل بدافزار کی پاد، از ابزارهای متنوعی برای بررسی بدافزارها به صورت پویا استفاده خواهیم کرد. شایان ذکر است، هنگامی که یک بدافزار را تحلیل می کنید با استفاده از ماشین های مجازی اطمینان حاصل کنید که به سیستم و شبکه شما آسیب نمی رسد. مطابق با آنچه که در فصول قبل در راه اندازی آزمایشگاه مجازی آموختید.

برنامه **Process Monitor** تمامی فراخوانی های سیستمی را نظارت می کند، اما از آنجاییکه فراخوانی های سیستمی در سامانه عامل ویندوز بسیار زیاد هستند (گاهی اوقات بیش از ۵۰۰۰ فراخوانی در دقیقه صورت می گیرد)، معمولاً غیر ممکن است که بتوان همه این فراخوانی ها را ثبت کرد، چون برنامه **Process Monitor** از حافظه **RAM** کامپیوتر برای ذخیره سازی داده های ثبتی استفاده می کند که ممکن است با اتمام این حافظه موجب خرابی سامانه عامل شود.

به منظور جلوگیری از خرابی سامانه عامل توسط **Process Monitor** شما باید برای یک دوره زمانی محدودی از **Process Monitor** برای ثبت فعالیت های سیستمی استفاده کنید. بدین منظور کافی است که به منوی فایل رفته و گزینه **Capture Events** را انتخاب کنید یا کلید ترکیبی **Ctrl + E** را بفشارید تا فعالیت **Process Monitor** به اتمام برسد.

توجه کنید، قبل استفاده از **Process Monitor** برای تجزیه و تحلیل، ابتدا تمامی رویدادهای ثبت شده توسط برنامه را پاک کنید. بدین منظور کافی است به منوی فایل بروید و روی گزینه **Clear Display** کلیک کنید یا کلید ترکیبی **Ctrl+X** را بفشارید تا تمامی رویدادها حذف شوند.

سپس فایل اجرایی بدافزار را اجرا کنید و **Process Monitor** را در حالت نظارت بر روی فایل اجرایی بدافزار (از منوی فیلتر برنامه و مشخص کردن نام فایل اجرایی بدافزار) قرار دهید تا تمامی رویدادهای ایجاد شده توسط بدافزار را دریافت و ذخیره سازی کند و بعد از مدتی دوباره می توانید پروسه **Process Monitor** را متوقف سازید.

باعث خرسندی است که صفحه نمایش برنامه Process Monitor قابل پیکربندی است. هر جدول در این برنامه شامل اطلاعات مجزای رویدادهای سیستمی است. به عنوان مثال همان طور که در تصویر ۹ مشاهده می کنید، این برنامه شامل جداول شماره سلسله مراتبی رویدادها^۱، برچسب زمان^۲، نام پروسه^۳ مولد رویداد، عملیات رویداد^۴، مسیر^۵ استفاده رویداد و نتیجه^۶ عملیات رویداد شده است. تصویر ۹ یک مجموعه از رویدادها را نمایش می دهد که پس از اجرای بدافزار mm32.exe رخ داده اند.

متخصصین می توانند با خواندن جزئیات رویدادهای مرتبط با بدافزار به راحتی دریابند این برنامه چه عملیاتی در سامانه عامل انجام می دهد. به عنوان مثال همان طور که در تصویر مشاهده می کنید، در شماره ۲۱۲ (به عبارت دیگر، رویداد ۲۱۲) یکی از رویدادهای این برنامه مشخص شده است که از تابع CreateFile استفاده می کند و یک فایل متنی در مسیر C:\Documents and Settings\All Users\Application Data mw2mmgr.txt ایجاد می کند و همان طور که در تصویر ۹ مشاهده می کنید، محتوای جدول Result برای این رویداد با SUCCESS مقداردهی شده است که گواهِ موفقیت انجام این عملیات است.

Seq. Time	Process Name	Operation	Path	Result	Detail
200 1:55:31	mm32.exe	CloseFile	Z:\Malware\mw2mmgr32.dll	SUCCESS	
201 1:55:31	mm32.exe	ReadFile	Z:\Malware\mw2mmgr32.dll	SUCCESS	Offset: 11,776, Length: 1,024, I/O Flag
202 1:55:31	mm32.exe	ReadFile	Z:\Malware\mw2mmgr32.dll	SUCCESS	Offset: 12,800, Length: 32,768, I/O Fla
203 1:55:31	mm32.exe	ReadFile	Z:\Malware\mw2mmgr32.dll	SUCCESS	Offset: 1,024, Length: 9,216, I/O Fla
204 1:55:31	mm32.exe	ReqOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Exec	NAME NOT	Desired Access: Read
205 1:55:31	mm32.exe	ReadFile	Z:\Malware\mw2mmgr32.dll	SUCCESS	Offset: 45,568, Length: 25,088, I/O Fla
206 1:55:31	mm32.exe	QueryOpen	Z:\Malware\imagehlp.dll	NAME NOT	
207 1:55:31	mm32.exe	QueryOpen	C:\WINDOWS\system32\imagehlp.dll	SUCCESS	CreationTime: 2/28/2006 8:00:00 AM,
208 1:55:31	mm32.exe	CreateFile	C:\WINDOWS\system32\imagehlp.dll	SUCCESS	Desired Access: Execute/Traverse, S
209 1:55:31	mm32.exe	CloseFile	C:\WINDOWS\system32\imagehlp.dll	SUCCESS	
210 1:55:31	mm32.exe	ReqOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Exec	NAME NOT	Desired Access: Read
211 1:55:31	mm32.exe	ReadFile	Z:\Malware\mw2mmgr32.dll	SUCCESS	Offset: 10,240, Length: 1,536, I/O Fla
212 1:55:31	mm32.exe	CreateFile	C:\Documents and Settings\All Users\Application Data\mw2mmgr.txt	SUCCESS	Desired Access: Generic Write, Read
213 1:55:31	mm32.exe	ReadFile	C:\\$Directory	SUCCESS	Offset: 12,288, Length: 4,096, I/O Fla
214 1:55:31	mm32.exe	CreateFile	Z:\Malware\mm32.exe	SUCCESS	Desired Access: Generic Read, Disc
215 1:55:31	mm32.exe	ReadFile	Z:\Malware\mm32.exe	SUCCESS	Offset: 0, Length: 64

تصویر ۹: نمایش رویدادهای mm32.exe در برنامه Procmon

¹ Sequence number

² Timestamp

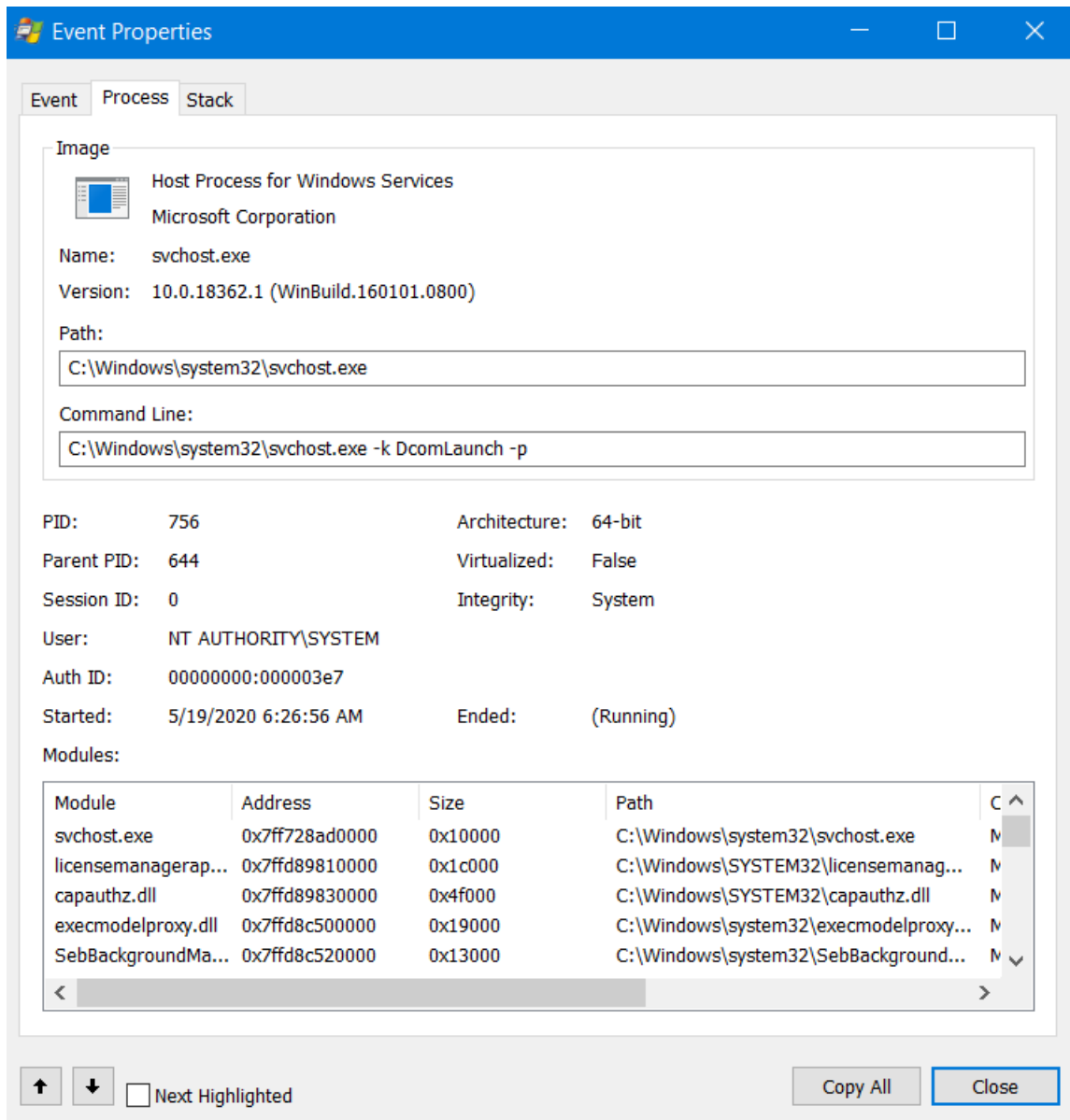
³ Process name

⁴ Event operation

⁵ Path

⁶ Result

شایان ذکر است، جزئیات این اطلاعات می‌توانند بیش از حد طولانی بوده و مناسب نمایش در صفحه برنامه Process Monitor نباشند یا خواندن جزئیات آن‌ها بسیار دشوار باشد. بدین منظور برای خواندن اطلاعات دقیق رویدادها در یک پنل واضح‌تر کافی است، روی رویداد مد نظر خود دوبار کلیک کنید تا مشخصات آن رویداد در صفحه‌ای جداگانه به صورت دقیق نمایش داده شود. تصویر ۱۰ پنجره مشخصات یک رویداد را نمایش می‌دهد.



تصویر ۱۰: محیط جزئیات اطلاعات یک رویداد

پیدا کردن اطلاعات رویدادهای خاص مرتبط با یک فایل اجرایی از طریق Process Monitor هنگامی که هزاران رویداد وجود دارد، کار بسیار دشواری است. در این حالت است که قابلیت کلیدی فیلتر برنامه Process Monitor به کار متخصصین می‌آید.

شما می‌توانید با قابلیت فیلتر یک فایل اجرایی خاص را در حالت ثبت رویداد با Process Monitor قرار بدهید. این قابلیت خصوصا برای تجزیه و تحلیل بدافزار بسیار مفید است، زیرا می‌توانید برنامه Process Monitor را در حالت ثبت رویداد یک بدافزار خاص تنظیم کنید. همچنین متخصصین می‌توانند برای برخی از فراخوانی‌های سیستمی مانند CreateFile، ReadFile و RegSetValue هم فیلتر گذاری کنند.

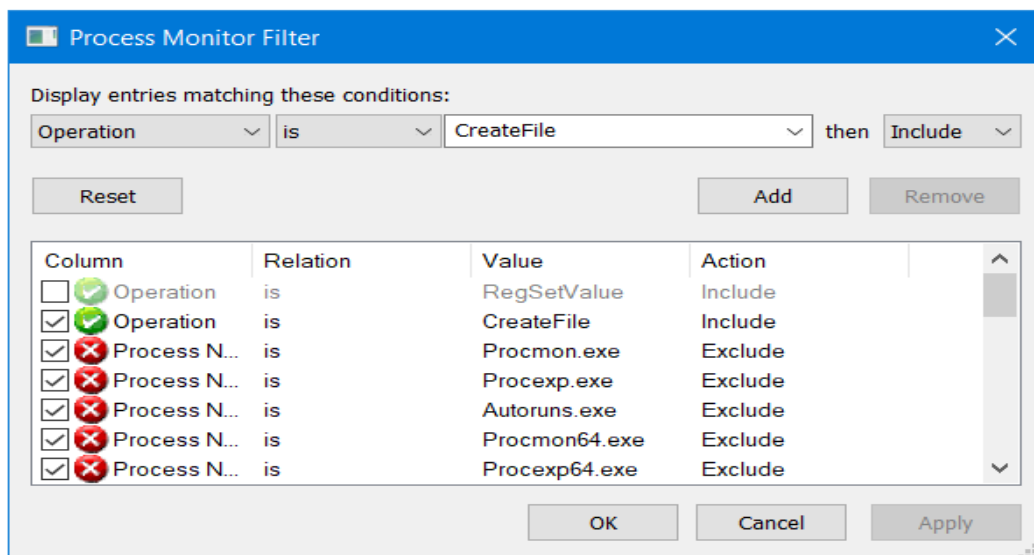
هنگامی که فیلتر برنامه Process Monitor را فعال می‌کنید، این ابزار فقط رویدادهای منطبق با فیلتری تنظیم کردید، نمایش خواهد داد اما با این حال هنوز تمامی رویدادهای ایجاد شده در سطح سیستم توسط Process Monitor در دسترس متخصص خواهند بود، در این شرایط کافی است فیلتر را غیرفعال کنید تا مجدد به تمامی رویدادهای ایجاد شده در سطح سیستم دسترسی بگیرید. به هر صورت، حتی اگر اعمال فیلتر باعث شود گروه محدودی از رویدادها نمایش داده شوند، باز هم شما به دیگر رویدادها دسترسی خواهید داشت. در ضمن اعمال فیلترینگ روی خروجی Process Monitor باعث ممانعت از اتلاف حافظه توسط این برنامه نمی‌شود.

حال به منظور اعمال فیلتر روی نمایش خروجی برنامه Process Monitor به منوی Filter رفته و سپس گزینه Filter را انتخاب کنید، تا منوی اعمال فیلتر در خروجی Process Monitor ظاهر شود. همان‌طور که در تصویر ۱۱ مشاهده می‌کنید، هنگام اعمال یک فیلتر روی خروجی، از قسمت بالای دکمه Reset یک منوی باز شو به شما ارائه می‌شود که باید یکی از جداول برنامه را به منظور اعمال فیلتر انتخاب کنید.

در این قسمت با ارزش‌ترین جداول برای ما نام پروسه (Process Name)، عملیات (Operation) و جزئیات (Detail) رویداد است، در این مرحله ما جدول Operation را به منظور اعمال فیلتر انتخاب کردیم. سپس باید یک مقایسه کننده از منوی باز شو سمت راست آن انتخاب کنید، که یکی از مقادیر Is، Contains و یا Less Than باشد.

در پایان، از منوی باز شوی سمت راست عبارت **Then**، باید مشخص سازید فیلتر کننده برنامه **Process Monitor** تمامی رویدادهایی که با مشخصات فیلتر شما مطابقت دارند را برای نمایش در خروجی مانع (**Exclude**) شود یا تمامی رویدادهایی که با فیلتر شما مطابقت دارد را در خروجی به نمایش (**Include**) بگذارد.

به زبانی ساده‌تر می‌توان گفت که دو عبارت **Include** و **Exclude** باعث می‌شوند، فیلتری که شما اعمال کرده‌اید، تمامی رویدادهایی که با فیلتر شما مطابقت دارند در خروجی حذف شوند یا نمایش داده شوند. به عنوان مثال؛ همان‌طور که در تصویر ۱۱ مشاهده می‌کنید، در پنجره اعمال فیلتر، ما برای **Process Monitor** تعریف کرده‌ایم، تمامی رویدادهایی که در جدول **Operation** خود از تابع **CreateFile** استفاده کرده‌اند را در خروجی برنامه **Process Monitor** به ما نمایش بدهد. سپس به منظور اعمال فیلتر کافی است روی دکمه **Add** سپس روی دکمه **Ok** کلیک کنید تا خروجی رویدادهای برنامه **Process Monitor** برای شما ویرایش شود.



تصویر ۱۱: نمایش محیط فیلترینگ خروجی Process Monitor

در تصویر ۱۲ مشاهده می‌کنید که خروجی برنامه مورد اصلاح قرار گرفته است و تمامی رویدادهایی که در جدول **Operation** خود از تابع **CreateFile** استفاده کرده‌اند و جدول **Process Name** شامل نام **Explorer.exe** و **ctfmon.exe** بوده، به معرض نمایش گذاشته شده است. این قابلیت می‌تواند کمک‌های شایانی به ما در هنگام تحلیل عملیات بدافزارها و حتی دیگر برنامه‌های اجرایی در محیط ویندوز کند.

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time o...	Process Name	PID	Operation	Path	Result	Detail
12:08:56...	Explorer.EXE	4116	CreateFile	C:\Users\mkahs\AppData\Local\Temp...	SUCCESS	Desired Access: R...
12:08:56...	Explorer.EXE	4116	CreateFile	C:\	SUCCESS	Desired Access: R...
12:08:56...	Explorer.EXE	4116	CreateFile	C:\Users	SUCCESS	Desired Access: R...
12:08:56...	Explorer.EXE	4116	CreateFile	C:\Users\mkahs	SUCCESS	Desired Access: R...
12:08:56...	Explorer.EXE	4116	CreateFile	C:\Users\mkahs\AppData	SUCCESS	Desired Access: R...
12:08:56...	ctfmon.exe	2076	CreateFile	C:\Windows\System32\en-US\mssp7en...	NAME NOT FOUND	Desired Access: R...
12:08:56...	ctfmon.exe	2076	CreateFile	C:\Windows\Globalization\ELS\SpellDict...	SUCCESS	Desired Access: R...
12:08:56...	ctfmon.exe	2076	CreateFile	C:\Windows\System32\en-US\mssp7en...	NAME NOT FOUND	Desired Access: R...
12:08:56...	ctfmon.exe	2076	CreateFile	C:\Windows\Globalization\ELS\SpellDict...	SUCCESS	Desired Access: R...
12:08:56...	ctfmon.exe	2076	CreateFile	C:\Windows\system32\Fluency\en-US\c...	PATH NOT FOUND	Desired Access: R...
12:08:56...	ctfmon.exe	2076	CreateFile	C:\Windows\Globalization\ELS\SpellDict...	SUCCESS	Desired Access: R...
12:08:56...	ctfmon.exe	2076	CreateFile	C:\Windows\System32\en-US\mssp7en...	NAME NOT FOUND	Desired Access: R...
12:08:56...	ctfmon.exe	2076	CreateFile	C:\Windows\Globalization\ELS\SpellDict...	SUCCESS	Desired Access: R...
12:08:56...	ctfmon.exe	2076	CreateFile	C:\Windows\system32\Fluency\en-US\c...	PATH NOT FOUND	Desired Access: R...
12:08:56...	ctfmon.exe	2076	CreateFile	C:\Windows\Globalization\ELS\SpellDict...	SUCCESS	Desired Access: R...
12:08:56...	ctfmon.exe	2076	CreateFile	C:\Windows\System32\en-US\mssp7en...	NAME NOT FOUND	Desired Access: R...
12:08:56...	Explorer.EXE	4116	CreateFile	C:\Users\mkahs\AppData\Local	SUCCESS	Desired Access: R...
12:08:56...	ctfmon.exe	2076	CreateFile	C:\Windows\Globalization\ELS\SpellDict...	SUCCESS	Desired Access: R...

تصویر ۱۲: نمایش فیلتر اعمال شده در خروجی Procmon

به این نکته توجه داشته باشید، اگر بدافزار مد نظر شما یک فایل اجرایی دیگری را استخراج و اجرا کرد، اطلاعات آن هنوز برای شما وجود خواهد داشت. یادتان باشد، اعمال فیلترینگ، فقط روی نمایش نتایج رویدادهای ثبت شده در خروجی صورت می‌گیرد.

با این حال برنامه Process Monitor تمامی فراخوانی‌های سیستمی که هنگام اجرای بدافزار رخ می‌دهد را دریافت می‌کند، این رویدادها شامل فراخوانی‌های سیستمی بدافزاری که از برنامه مخرب اصلی استخراج شده بود، شامل می‌شود.

در حالت کلی اگر مشاهده کردید که بدافزار فایل اجرایی دیگری را استخراج و اجرا کرد، فیلتر را به‌روزرسانی کنید تا آن پروسه هم در خروجی به نمایش گذاشته شود. زیرا آن دو با هم‌دیگر در ارتباط خواهند بود. قابل ذکر است، برنامه Process Monitor فیلترهای خودکار سودمندی را در نوار ابزار خود ارائه می‌دهد. همان‌طور که در تصویر ۱۳ مشاهده می‌کنید دور پنج فیلتر خط کشیده شده است که پنج گروه اطلاعات مرتبط زیر را فیلتر می‌کنند.

۱. **رجیستری (Registry):** این فیلتر موجب نمایش تعاملات سطح رجیستری ویندوز می‌شود.

تحلیلگر بدافزار با بررسی عملیات‌های صورت گرفته روی رجیستری سامانه‌عامل ویندوز می‌تواند بگوید چگونه یک قسمت از بدافزار خودش را در رجیستری نصب می‌کند.

۲. **سیستم‌فایل (File System):** این فیلتر تعاملات بدافزار یا یک فایل اجرایی با سیستم‌فایل

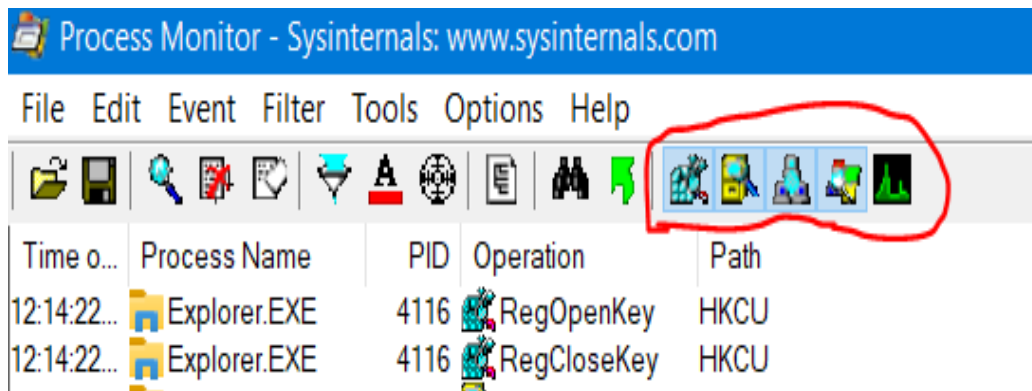
را نمایش می‌دهد. کاوش تعاملات سیستم‌فایل می‌تواند همه فایل‌هایی را که توسط بدافزار ایجاد یا برای استفاده خود مورد پیکربندی قرار گرفته‌اند، نمایش دهد.

۳. **فعالیت پروسه (Process Activity):** این فیلتر تعاملات سطح پروسه یک فایل اجرایی را نمایش می‌دهد. با فعال‌سازی این فیلتر می‌توانید بررسی کنید که آیا بدافزار تحت نظر پروسه‌های اضافی دیگر ایجاد می‌کند یا خیر.

۴. **شبکه (Network):** این فیلتر تعاملات سطح شبکه یک فایل اجرایی را نمایش می‌دهد. با فعال‌سازی این فیلتر می‌توانید لیست تمامی پورت‌هایی که بدافزار در سامانه‌عامل روی شنود قرار می‌دهد، به دست آورید.

۵. **پروفایلینگ (Profiling):** در حقیقت این فیلتر یک نمونه پروفایلر ساده است که به شما توسط Process Monitor ارائه شده است. با فعال‌سازی این فیلتر می‌توانید نحوه استفاده از پردازنده توسط پروسه‌ها یا یک فایل اجرایی مشخص را متوجه شوید.

این پنج فیلتر به صورت پیش‌فرض انتخاب شده‌اند. برای غیرفعال‌سازی آن‌ها مطابق با موضوع مدنظرتان، کافی است به راحتی روی آن‌ها کلیک کنید. هنگامیکه یک فیلتر پیش‌فرض Process Monitor را فعال‌سازی می‌کنید، رنگ پس‌زمینه آن آبی رنگ خواهد شد، تا مشخص شود که فعال است.



تصویر ۱۳: فیلترهای Process Monitor

نکته : اگر بدافزار شما در هنگام راه‌اندازی (Boot) سیستم‌عامل اجرا می‌شود، گزینه Boot Logging را از منوی Options فعال کنید. تا برنامه Process Monitor در زمان اجرای سیستم‌عامل بارگذاری شود و تمامی رویدادها را ثبت کند.

به هر صورت تحلیل رویدادهای ثبت شده توسط Process Monitor نیاز به تمرین و صبر فراوان دارد. هر چه بیشتر از Process Monitor استفاده کنید، راحت تر می توانید رویدادهای یک برنامه را مورد تحلیل قرار دهید. شایان ذکر است، با تحلیل تعاملات متنوع یک بدافزار توسط Process Monitor خیلی راحت می توانید تشخیص بدهید که بدافزار مذکور از چه خانواده ای است. بدافزارها از قبیل جاسوس افزارها، باج افزارها، کیلاگرها و ... الگوری رفتاری متعلق به خود را دارند.

مشاهده پروسه ها با Process Explorer

برنامه Process Explorer یک برنامه رایگان از شرکت مایکروسافت است. این برنامه یک Task Manager قدرتمند می باشد که در هنگام تجزیه و تحلیل بدافزار بهتر است مورد استفاده قرار گیرد. این برنامه می تواند اطلاعات دقیقی از یک پروسه در حال اجرا روی سیستم به ما ارائه دهد.

به عنوان مثال، شما می توانید از این برنامه برای لیست کردن پروسه های در حال اجرا روی سیستم، کتابخانه های پیوندی پویا (DLL) بارگذاری شده توسط پروسه ها، خصوصیات گوناگون پروسه ها و تمامی اطلاعات سیستم استفاده کنید. همچنین می توانید از این برنامه برای از بین بردن یک پروسه، خارج سازی یک کاربر از سیستم و اجرای یک پروسه تأیید اعتبار شده استفاده کنید.

صفحه نمایش برنامه Process Explorer

برنامه Process Explorer پروسه های در حال اجرا روی سامانه عامل را نظارت کرده و آنها را در یک ساختار درختی نمایش می دهد و در این ساختار درختی پروسه فرزند و پروسه مولد را مشخص می سازد. به عنوان مثال، در تصویر ۱۴ مشاهده می کنید که پروسه Services.exe پروسه فرزند Wininit.exe است. این موضوع در شکل با یک براکت در سمت چپ نمایش داده شده است.

همچنین می توانید برای دیدن ساختار درختی پروسه های در حال اجرا روی سیستم از برنامه Plist هم استفاده کنید. اما این ابزار یک برنامه تحت خط فرمان می باشد و قابلیت های کلیدی برنامه Process Explorer را ندارد. در ادامه ابزار Plist را مورد بررسی قرار خواهیم داد.

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	Path
System Idle Process	54.63	0 K	24 K	0			
System	0.20	48 K	580 K	4			
csrss.exe	< 0.01	1,416 K	1,664 K	392			[Error opening process]
wininit.exe		1,128 K	1,012 K	460			[Error opening process]
services.exe		5,636 K	4,404 K	608			[Error opening process]
svchost.exe		3,112 K	4,160 K	692	Host Process for Windows Services	Microsoft Corporation	C:\Windows\System32\svchost.exe
wmplayer.exe	4.64	33,820 K	44,912 K	7676	Windows Media Player	Microsoft Corporation	C:\Program Files\Windows Media Pla
svchost.exe		3,916 K	4,924 K	768	Host Process for Windows Services	Microsoft Corporation	C:\Windows\System32\svchost.exe
atiesrxx.exe		880 K	680 K	816	AMD External Events Service Module	AMD	C:\Windows\System32\atiesrxx.exe
atiesclxx.exe		1,692 K	1,080 K	1332			[Error opening process]
svchost.exe		17,104 K	11,040 K	900	Host Process for Windows Services	Microsoft Corporation	C:\Windows\System32\svchost.exe
audiodg.exe	0.61	15,828 K	10,336 K	6256			[Error opening process]
svchost.exe	< 0.01	5,328 K	7,184 K	932	Host Process for Windows Services	Microsoft Corporation	C:\Windows\System32\svchost.exe
svchost.exe	0.02	9,884 K	15,344 K	968	Host Process for Windows Services	Microsoft Corporation	C:\Windows\System32\svchost.exe
svchost.exe	0.05	28,432 K	21,524 K	996	Host Process for Windows Services	Microsoft Corporation	C:\Windows\System32\svchost.exe
svchost.exe		2,292 K	3,184 K	1128	Host Process for Windows Services	Microsoft Corporation	C:\Windows\System32\svchost.exe
vpnagent.exe		5,960 K	6,840 K	1288	VPN Agent Service	Cisco Systems, Inc.	C:\Program Files\Cisco\Cisco AnyCon
svchost.exe	0.02	10,092 K	8,740 K	1408	Host Process for Windows Services	Microsoft Corporation	C:\Windows\System32\svchost.exe
spoolsv.exe		4,776 K	3,396 K	1520	Spooler SubSystem App	Microsoft Corporation	C:\Program Files\Microsoft SQL Serv
svchost.exe		15,876 K	12,752 K	1556	Host Process for Windows Services	Microsoft Corporation	C:\Windows\System32\svchost.exe
armsvc.exe		836 K	836 K	1656	Adobe Acrobat Update Service	Adobe Systems In corpora...	C:\Program Files\Common Files\Adob
SkypeC2CAutoUpd...		1,004 K	752 K	1688	Updates Skype Click to Call	Microsoft Corporation	C:\Program Files\Skype\Toolbars\Aut
SkypeC2CPNRSvc...		42,340 K	16,656 K	1720	Phone Number Recognition (PNR) mo...	Microsoft Corporation	C:\Program Files\Skype\Toolbars\PNF
svchost.exe		4,812 K	5,496 K	1760	Host Process for Windows Services	Microsoft Corporation	C:\Windows\System32\svchost.exe
service-install.exe	< 0.01	1,352 K	996 K	1828	ServiceEx Console Application	ServiceEx	C:\Program Files\EasyPHP-Webserve
ews-dashboard.exe	< 0.01	3,736 K	4,628 K	1864			[Error opening process]
svchost.exe	0.01	5,616 K	6,980 K	1872	Host Process for Windows Services	Microsoft Corporation	C:\Windows\System32\svchost.exe
kvpnccsv.exe	0.02	7,060 K	6,840 K	1992	Kerio VPN Client Service	Kerio Technologies Inc.	C:\Program Files\Kerio\VPN Client\kv
MsDtsSrvr.exe		14,360 K	2,300 K	396		Microsoft Corporation	
sqlservr.exe	0.16	108,788 K	49,120 K	1444	SQL Server Windows NT	Microsoft Corporation	C:\Program Files\Microsoft SQL Servi
msmdsrvr.exe	0.03	36,492 K	6,712 K	1912	Microsoft SQL Server Analysis Services	Microsoft Corporation	C:\Program Files\Microsoft SQL Servi
ReportingServicesS...	0.06	71,416 K	17,674 K	348	Reporting Services Service	Microsoft Corporation	C:\Program Files\Microsoft SQL Servi
taskhost.exe							

تصویر ۱۴: برنامه Process Explorer در حال بررسی بدافزار svchost.exe

برنامه Process Explorer به شما پنج ستون ارائه می‌دهد که آن پنج ستون شامل نام پروسه‌ها (Process)، شناسه عددی پروسه‌ها (PID)، مقدار استفاده پروسه از پردازنده (CPU)، شرح جزئیات پروسه (Description)، نام شرکت (Company Name) می‌شود.

تمامی مقادیر موجود در این ستون‌ها لحظه به لحظه به‌روز می‌شوند. در حالت پیش‌فرض، در این برنامه سرویس‌ها با رنگ صورتی، پروسه‌ها با رنگ آبی، پروسه‌های تازه ایجاد شده با رنگ سبز و پروسه‌های از بین رفته (Killed) با رنگ قرمز نمایش داده می‌شوند.

قابل ذکر است، رنگ سبز و قرمز به صورت لحظه‌ای ظاهر می‌شوند و گواه آغاز به کار و پایان کار یک پروسه هستند. متخصصین هنگام تجزیه و تحلیل یک بدافزار باید به پنجره Process Explorer توجه کامل کنند تا بتوانند تغییرات و پروسه‌های ایجاد شده توسط بدافزار را مورد بررسی قرار دهند.

برنامه Process Explorer می‌تواند اطلاعات کاملی برای هر پروسه ارائه دهد. هنگامی که پنجره View DIIs در پایین برنامه فعال باشد، شما می‌توانید با کلیک روی هر پروسه تمامی کتابخانه‌های پیوندی پویا را که آن پروسه در حافظه بارگذاری کرده است، مشاهده کنید. در تصویر ۱۵ تمامی کتابخانه‌های پیوندی پویایی (DIIs) را مشاهده می‌کنید که پروسه explorer.exe در حافظه بارگذاری کرده است.

Name	Description	Company Name	Path
explorer.exe		Microsoft Corporation	C:\Users\mkahs\AppData\Local\Microsoft\Windows\Caches\{3DA71D5A-20CC-432F-A115-DFE92379E91F}.3.ver0d000000000000016d.db
dmw.exe			C:\ProgramData\Microsoft\Windows\Caches\{6AF0698E-D558-4F6E-9B3C-3716689AF493}.2.ver0d0000000000000001.db
dlhost.exe		Microsoft Corporation	C:\Users\mkahs\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0d000000000000000e.db
dlhost.exe		Microsoft Corporation	C:\ProgramData\Microsoft\Windows\Caches\{D0F571F2-BE38-426D-8288-1A9A39C3FDA2}.2.ver0d0000000000000001.db
dlmngmr.exe			C:\Windows\ServiceProfiles\LocalService\AppData\Local\FontCache\FontCache-FontFace.dat
dlmngmr.exe			C:\Windows\ServiceProfiles\LocalService\AppData\Local\FontCache\FontCache-s-1-5-21-3538707957-2260588633-2711446803-1001
dlmngmr.exe			C:\Windows\ServiceProfiles\LocalService\AppData\Local\FontCache\FontCache-System.dat
dlmngmr.exe			C:\Windows\rescache_merged\11590964771434633187.pri
dlmngmr.exe			C:\Windows\rescache_merged\118001884\3561925437.pri
dlmngmr.exe			C:\Program Files\7-zip\7-zip.dll
dlmngmr.exe			C:\Windows\System32\AboveLockAppHost.dll
dlmngmr.exe			C:\Windows\System32\ActionCenter.dll
dlmngmr.exe			C:\Windows\System32\en-US\ActionCenter.dll.mui
dlmngmr.exe			C:\Windows\System32\actprny.dll
dlmngmr.exe			C:\Windows\System32\advapi32.dll
dlmngmr.exe			C:\Windows\System32\apphelp.dll
dlmngmr.exe			C:\Windows\System32\ApplicationFrame.dll
dlmngmr.exe			C:\Windows\System32\en-US\ApplicationFrame.dll.mui
dlmngmr.exe			C:\Windows\System32\AppResolver.dll
dlmngmr.exe			C:\Windows\System32\AppDeploymentClient.dll
dlmngmr.exe			C:\Windows\System32\atitunk.dll
dlmngmr.exe			C:\Windows\System32\AudioSes.dll
dlmngmr.exe			C:\Windows\System32\avrt.dll

تصویر ۱۵: پانل View Dlls در برنامه Process Explorer

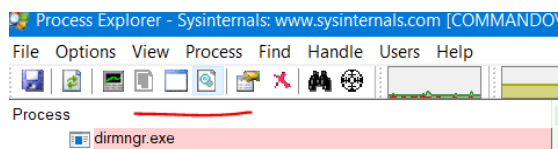
حتی می‌توانید پنجره View Dlls را به View Handles عوض کنید که تمامی هندل‌ها مرتبط با منابع ایجاد شده توسط یک پروسه در سامانه‌عامل نمایش داده شود. شایان ذکر است، برای کسب اطلاعات بیشتر در مورد مفاهیم و برنامه‌نویسی سیستمی ویندوز می‌توانید به وبسایت (www.ai000.ir) رجوع کنید. تصویر ۱۶ تمامی هندل‌های پروسه explorer.exe را به نمایش گذاشته است.

Type	Name
ALPC Port	{RPC Control\OLE57FBAE24F2063F118478C988BFA8}
ALPC Port	{BaseNamedObjects}[CoreUI]-PID(4116)-TID(4368) 6ee8637a-c539-43b1-8ffc-4649bdbb309f
ALPC Port	{BaseNamedObjects}[CoreUI]-PID(4116)-TID(4356) 5d8edbd6-6559-429d-901e-539468cefd4
ALPC Port	{BaseNamedObjects}[CoreUI]-PID(4116)-TID(4356) 378eebed-6cb2-44aa-8a04-3d9e974580d
ALPC Port	{BaseNamedObjects}[CoreUI]-PID(4116)-TID(4356) 5d299ced-f81-459b-8137-4d37e4ae1cb0
ALPC Port	{BaseNamedObjects}[CoreUI]-PID(4116)-TID(4120) cbb2e967-d71a-41ef-9d7d-aca3b28d454f
ALPC Port	{RPC Control\LRPC-69dc5fa127b30668d2}
ALPC Port	{BaseNamedObjects}[CoreUI]-PID(4116)-TID(4280) d6525e33-c66d-404f-a699-b0a2ab59b0be
ALPC Port	{BaseNamedObjects}[CoreUI]-PID(4116)-TID(3964) 0a619e02-760e-405f-872a-b08b81174e0c
ALPC Port	{BaseNamedObjects}[CoreUI]-PID(4116)-TID(3964) 46cb285-b50c-4125-96bb-995182b13e64
ALPC Port	{BaseNamedObjects}[CoreUI]-PID(4116)-TID(668) 458f999-3e0a-43da-980e-adedad88b40f
Directory	{KnownDlls}
Directory	{Sessions}\BaseNamedObjects
Event	{KernelObjects}\MaximumCommitCondition
Event	{BaseNamedObjects}\StateRepository\SecondaryTileUserNotificationChannel {B2C8ED9A-...
Event	{BaseNamedObjects}\TermSrvReadyEvent
Event	{BaseNamedObjects}\CPProgressEvent
Event	{BaseNamedObjects}\{c245290c-497c-4811-9aba-7eb0ddc882a2}
Event	{BaseNamedObjects}\{7FE2FCEE-B914-4AAF-A10F-93532FBA52C3}
Event	{BaseNamedObjects}\{44ea083b-899c-4440-8338-2469f4681cf}
Event	{Sessions}\BaseNamedObjects\ShellReadyEvent
Event	{Sessions}\BaseNamedObjects\PRS_EXTERNAL_CHECK_CHANGED_NOTIFY
Event	{Sessions}\BaseNamedObjects\TortoiseSVNCacheInvalidationEvent
Event	{Sessions}\BaseNamedObjects\TortoiseSVNCacheInvalidationEvent

تصویر ۱۶: پانل View Handles در برنامه Process Explorer

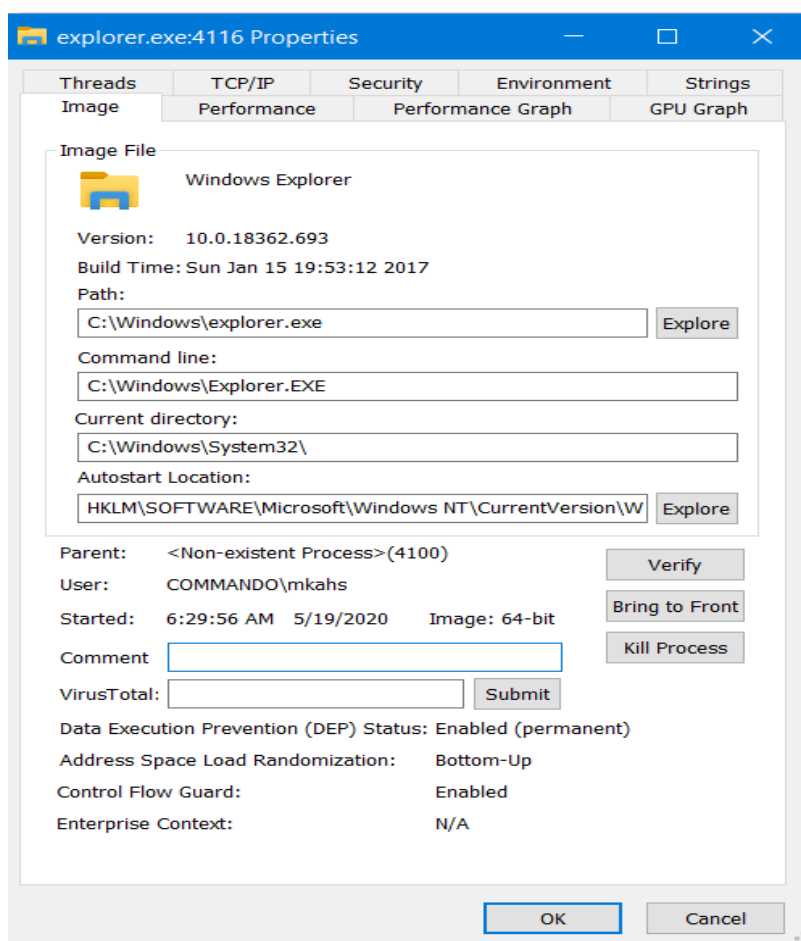
به منظور فعال‌سازی این پانل‌ها در پایین محیط Process Explorer کافی است از قسمت نوار ابزار روی آیکون مشخص شده در تصویر ۱۷ کلیک کنید. توجه کنید، ابتدا وقتی روی آیکون مذکور می‌روید یک راهنما ظاهر می‌گردد که به شما فعال‌سازی پانل View Handles یا View Dlls را معرفی می‌کند. در ابتدا

وقتی روی این آیکون کلیک می‌کنید پانل View Dlls ظاهر می‌شود و اگر دوباره روی همان آیکون کلیک کنید پانل View Handles ظاهر می‌شود.



تصویر ۱۷: فعال‌سازی پانل View Dlls و View Handles در Process Explorer

پنجره خصوصیات پروسه‌ها^۱ که در تصویر ۱۸ به نمایش گذاشته شده است، با دوبار کلیک روی پروسه‌ها در برنامه Process Explorer ظاهر می‌شود. این پنجره می‌تواند اطلاعات بسیار مفیدی درباره پروسه بدافزار به شما ارائه کند.



تصویر ۱۸: پنجره خصوصیات پروسه‌ها

¹ Properties Process

در پنجره خصوصیت‌های پروسه در Process Explorer اطلاعات زیر ارائه می‌شوند:

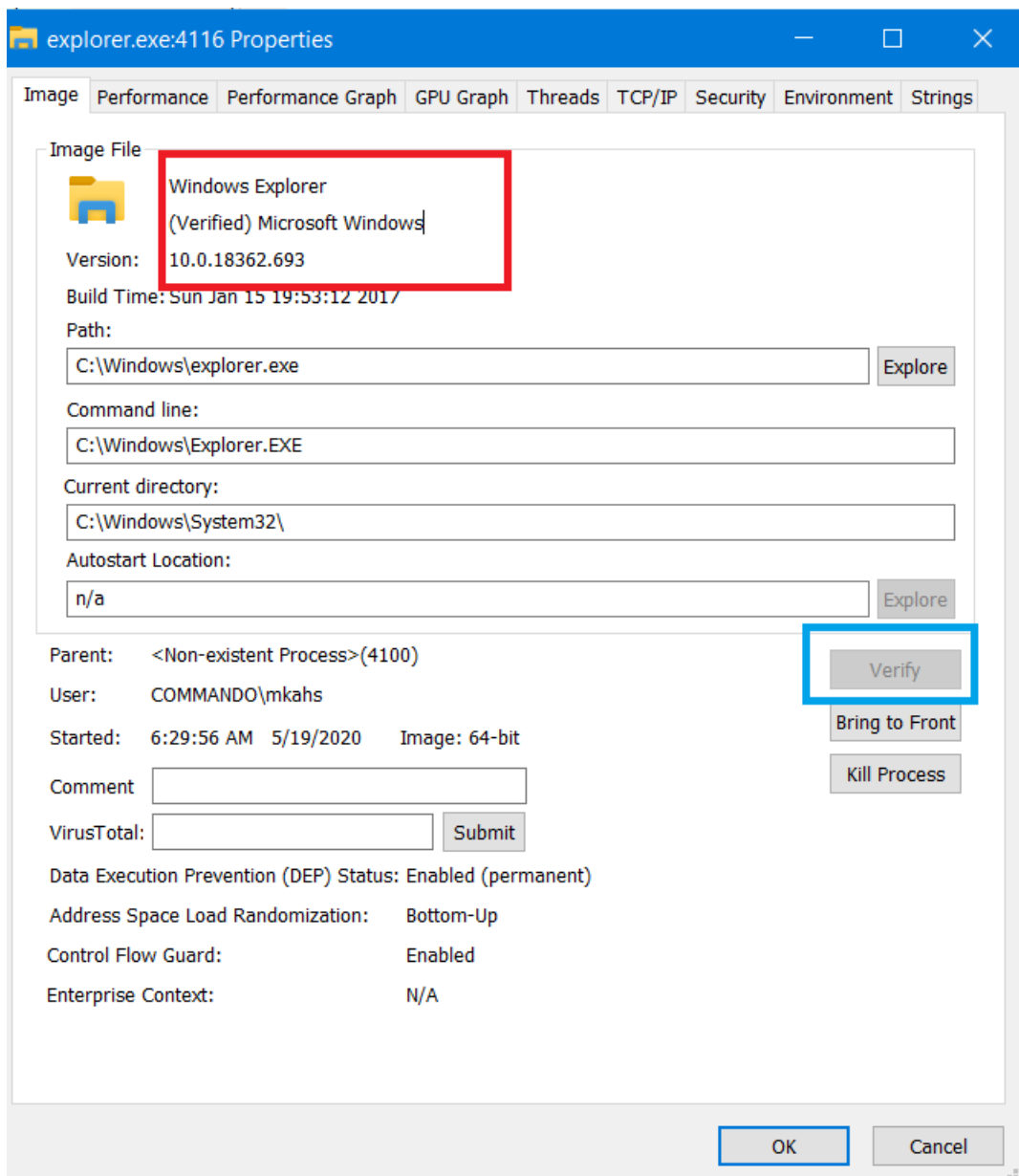
۱. تب Threads تمامی تردهای فعال پروسه را نمایش می‌دهد.
۲. تب TCP/IP تمامی ارتباط‌های فعال و یا پورت‌هایی باز پروسه را نمایش می‌دهد.
۳. تب Image مسیر فایل اجرایی را نمایش می‌دهد.
۴. تب Performance اطلاعات آماری فایل اجرایی را نمایش می‌دهد.
۵. تب Environment اطلاعات مرتبط با متغیرهای محیطی پروسه را نمایش می‌دهد.
۶. تب Security اطلاعات مرتبط با حساب کاربری و سطح دسترسی امنیتی پروسه را نمایش می‌دهد.
۷. تب Strings اطلاعات مرتبط با رشته‌هایی که در فایل اجرایی نهفته‌سازی شدند، نمایش می‌دهد.

این دست اطلاعات برای تحلیل یک فایل اجرایی و ماهیت آن بسیار مفید است. این اطلاعات می‌توانند به شخص تحلیلگر کمک کنند تا بهتر و عمیق‌تر اطلاعات و نوع رفتار فایل اجرایی (بدافزار) را مشخص کنند.

استفاده از گزینه Verify

یکی از مزیت‌های بسیار مفید در برنامه Process Explorer دکمه Verify در تب Image است. روی این گزینه کلیک کنید تا مشخص شود ایمیج موجود برنامه روی دیسک، واقعا یک باینری امضاء شده مایکروسافت است. از آنجاییکه مایکروسافت از امضاءهای دیجیتالی برای بیشتر فایل‌های اجرایی اصلی خودش استفاده می‌کند، هنگامی که برنامه Process Explorer امضاء دیجیتالی یک برنامه را تأیید می‌کند، می‌توان اطمینان حاصل کرد که آن یک فایل اجرایی معتبر برای مایکروسافت است. این ویژگی مخصوصا برای تأیید خراب نبودن یک فایل ویندوزی روی دیسک بسیار مفید است، چون اغلب بدافزارها خودشان را با فایل‌های معتبر ویندوزی جایگزین می‌کنند تا عملیات خود را مخفی به پایان برسانند.

به عنوان مثال، هنگامیکه در قالب حمله فیشینگ بدافزاری بر روی سیستم شما بارگزاری شد، برای اینکه بدافزار خود را به عنوان یک نرم‌افزار مشروع جای بزند، ممکن است از نام یکی از برنامه‌های اصلی مایکروسافت استفاده کند. مثلا نام بدافزار ممکن است، چیزی مانند explorer.exe باشد که یکی از برنامه‌های مشروع سامانه‌عامل به حساب می‌آید. از همین روی، شما به راحتی می‌توانید با کلیک بر روی دکمه Verify بررسی کنید (کادر آبی رنگ در تصویر ۱۹) که آیا هویت این نرم‌افزار قابل تصدیق است یا خیر. اگر برنامه واقعا توسط مایکروسافت امضاء شده باشد، در کادر قرمز رنگ تصویر ۱۹ با پیام (Verified) اعلام خواهد شد.



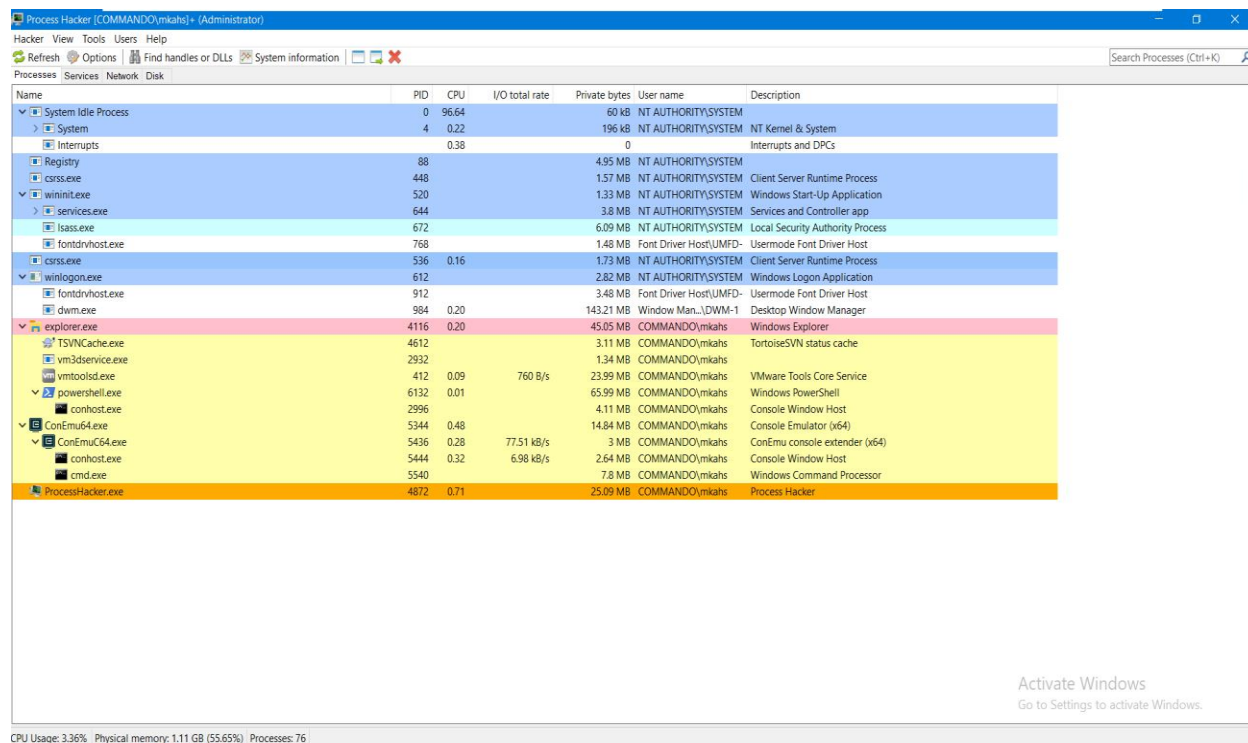
تصویر ۱۹: محیط تب Image در Process Explorer

به هر صورت، دکمه Verify می‌تواند ایمج فایل‌های اجرایی^۱ را بجای روی حافظه، بر روی دیسک سخت تأیید کند. ولی این نکته را باید به یاد داشته باشید، مهاجم اگر از روش‌هایی مانند Module Stomping یا جایگزینی پروسه^۲ استفاده کند که در آن یک پروسه در حال اجرا روی سیستم فضای آدرس مشخصی را

¹ Image of Executable File

² Process Replacement

درون حافظه هیپ با یک فایل اجرایی مخرب بازنویسی و در نهایت اجرا می کند، این موضوع بی فایده خواهد بود.

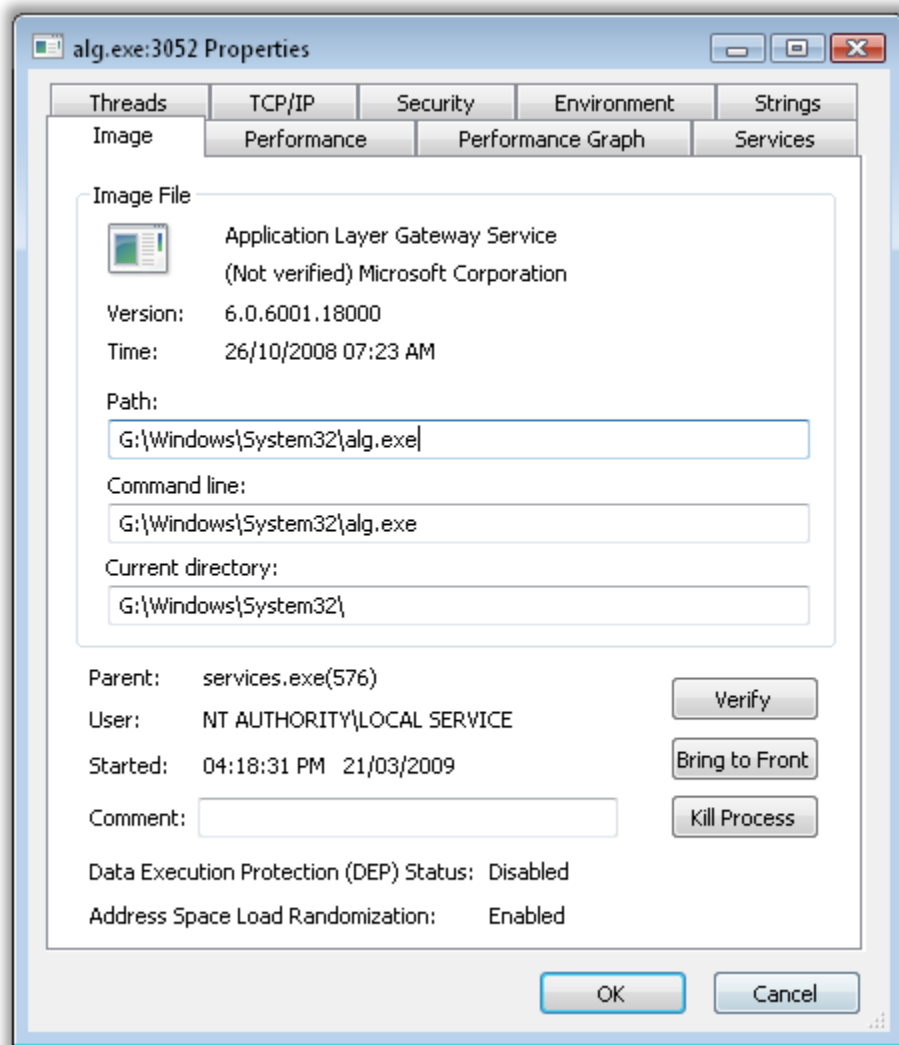


Name	PID	CPU	I/O total rate	Private bytes	User name	Description
System Idle Process	0	96.64		60 kB	NT AUTHORITY\SYSTEM	
System	4	0.22		196 kB	NT AUTHORITY\SYSTEM	NT Kernel & System
Interrupts		0.38		0		Interrupts and DPCs
Registry	88			4.95 MB	NT AUTHORITY\SYSTEM	
csrss.exe	448			1.57 MB	NT AUTHORITY\SYSTEM	Client Server Runtime Process
wininit.exe	520			1.33 MB	NT AUTHORITY\SYSTEM	Windows Start-Up Application
services.exe	644			3.8 MB	NT AUTHORITY\SYSTEM	Services and Controller app
lsass.exe	672			6.09 MB	NT AUTHORITY\SYSTEM	Local Security Authority Process
fontdrvhost.exe	768			1.48 MB	Font Driver Host\UMFD-	Usermode Font Driver Host
csrss.exe	536	0.16		1.73 MB	NT AUTHORITY\SYSTEM	Client Server Runtime Process
winlogon.exe	612			2.82 MB	NT AUTHORITY\SYSTEM	Windows Logon Application
fontdrvhost.exe	912			3.48 MB	Font Driver Host\UMFD-	Usermode Font Driver Host
dwm.exe	984	0.20		143.21 MB	Window Man...DWM-1	Desktop Window Manager
explorer.exe	4116	0.20		45.05 MB	COMMANDO\mkahs	Windows Explorer
TSVNCache.exe	4612			3.11 MB	COMMANDO\mkahs	TortoiseSVN status cache
vm3dservice.exe	2932			1.34 MB	COMMANDO\mkahs	
vmtoolsd.exe	412	0.09	760 B/s	23.99 MB	COMMANDO\mkahs	VMware Tools Core Service
powershell.exe	6132	0.01		65.99 MB	COMMANDO\mkahs	Windows PowerShell
conhost.exe	2996			4.11 MB	COMMANDO\mkahs	Console Window Host
ConEmu64.exe	5344	0.48		14.84 MB	COMMANDO\mkahs	ConEmu Emulator (x64)
ConEmu64.exe	5436	0.28	77.51 kB/s	3 MB	COMMANDO\mkahs	ConEmu console extender (x64)
conhost.exe	5444	0.32	6.98 kB/s	2.64 MB	COMMANDO\mkahs	Console Window Host
cmd.exe	5540			7.8 MB	COMMANDO\mkahs	Windows Command Processor
ProcessHacker.exe	4872	0.71		25.09 MB	COMMANDO\mkahs	Process Hacker

تصویر ۲۰: محیط Process Hacker

نکته: یکی از ابزارهای دیگر که مانند Process Explorer عمل می کند و شهرت زیادی در بین تحلیلگران بدافزار دارد، ابزار Process Hacker است. این ابزار هم مانند Process Explorer کاربران زیادی اکنون دارد و اطلاعات زیادی درباره پروسه های در حال اجرا، تعاملات سطح شبکه و فایل سیستم، نحوه استفاده از CPU یا GPU و ... به کاربر یا مدیر سامانه عامل ارائه می دهد. همچنین کاربر می تواند به رجوع به منوی Options رنگ بندی نرم افزار را مجدد بازتعریف کند، و حتی اطلاعات مرتبط با Dllها و Handleها را مشاهده کند. در تصویر ۲۰، محیط این برنامه نمایش داده شده است.

شایان ذکر است، در روش Module Stomping که نوعی از رویکرد جایگزینی پروسه به حساب می آید، پروسه مخربی که با پروسه تأیید شده جایگزین می شود، دارای یک سطح دسترسی مشابه روی سامانه عامل خواهند بود. بنابراین برنامه می تواند در قالب یک برنامه قانونی پروسه خود را اجرا کرده و به کار خود ادامه دهد.



تصویر ۲۱: عدم تأیید ایمج فایل اجرایی توسط Process Explorer

با این حال بدافزار باز هم از خود اثراتی باقی می گذارد. قابل ذکر است، فایل های اجرایی در حافظه از فایل های اجرایی روی دیسک سخت خیلی متفاوت هستند. به عنوان مثال، در تصویر ۲۱ پروسه alg.exe به نظر می رسد یک پروسه تأیید شده باشد، در حالی که یک بدافزار است و ایمج آن توسط Process Explorer

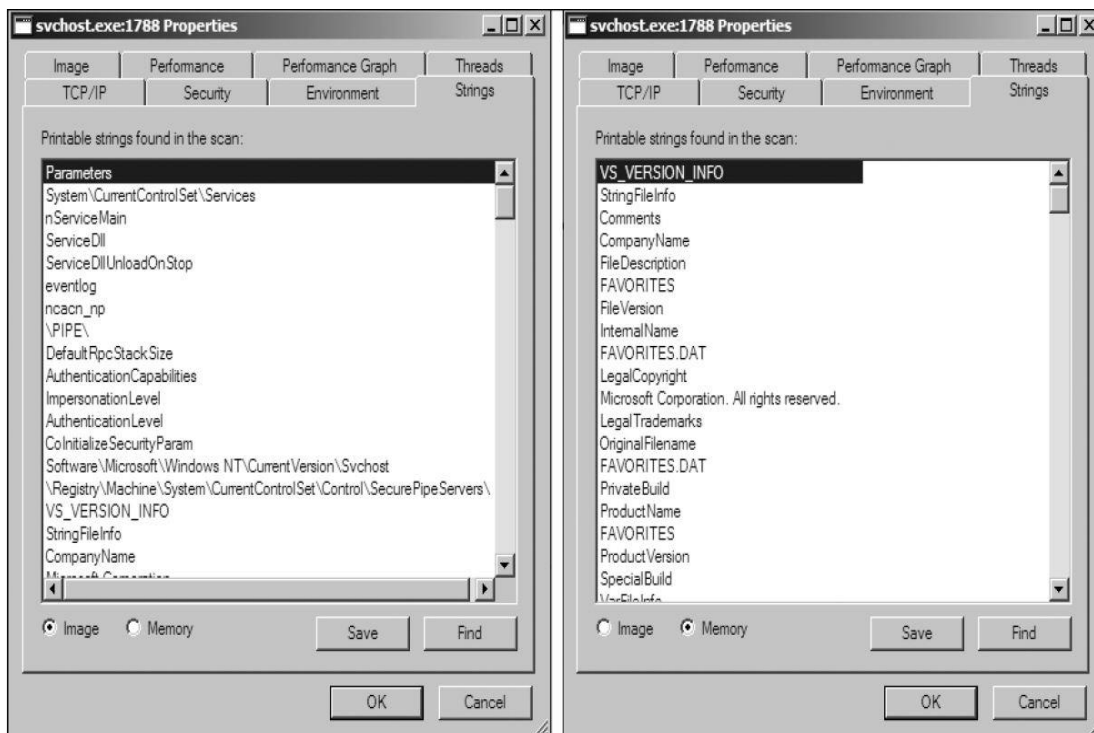
به عنوان **Not Verified** مشخص شده است. (در مورد روش جایگزینی پروسه در قسمت‌های بعدی بیشتر بحث خواهیم کرد).

مقایسه رشته‌ها

یکی از موثرترین راه‌ها برای شناسایی روش جایگزینی پروسه استفاده از زبانه **Strings** موجود در پنجره **Properties** برنامه **Process Explorer** است. شما می‌توانید با قابلیت ارائه شده در این زبانه، رشته‌های موجود پروسه اجرایی روی دیسک سخت (ایمج برنامه) را با پروسه اجرا شده در حافظه بررسی کنید.

همان‌طور که در تصویر ۲۲ مشاهده می‌کنید، می‌توانید به راحتی با دکمه‌های رادیویی سمت چپ نمایش رشته‌ها را تغییر بدهید. اگر رشته‌های نمایش داده شده در دیسک سخت با رشته‌های نمایش داده شده در حافظه متفاوت بود، می‌توان نتیجه گرفت که جایگزینی پروسه رخ داده است.

به عنوان مثال مشاهده می‌کنید که در تصویر ۲۲ جایگزینی پروسه رخ داده است. در این مثال، رشته **FAVORITES.DAT** چندین بار در پانل سمت راست تصویر (svchost.exe در حافظه) نمایش داده شده است، اما این رشته در پانل سمت چپ تصویر (svchost.exe روی دیسک) وجود ندارد.



تصویر ۲۲: نمایش رشته‌های پروسه **svchost** روی دیسک سخت و روی حافظه

تحلیل مستندات مخرب

خوشبختانه متخصصین تجزیه و تحلیل بدافزار می‌توانند از برنامه Process Explorer به منظور یک راه ساده و سریع برای تحلیل فایل‌های گوناگون، از قبیل فایل‌های قابل حمل متنی (PDF) و فایل‌های متنی Word استفاده کنند.

سریع‌ترین راه برای این که مشخص سازید یک فایل مستند مخرب است یا خیر، این است که ابتدا برنامه Process Explorer را اجرا کرده و سپس روی فایل مستند مشکوک خود کلیک کنید تا اجرا شود، اگر فایل مستند یک پروسه دیگر روی سامانه‌عامل را اجرا کرد و شما آن را در برنامه Process Explorer مشاهده کردید، می‌توانید به راحتی با رجوع به زبانه Image از منوی Properties پروسه محل آن بدافزار را روی دیسک سخت پیدا کنید.

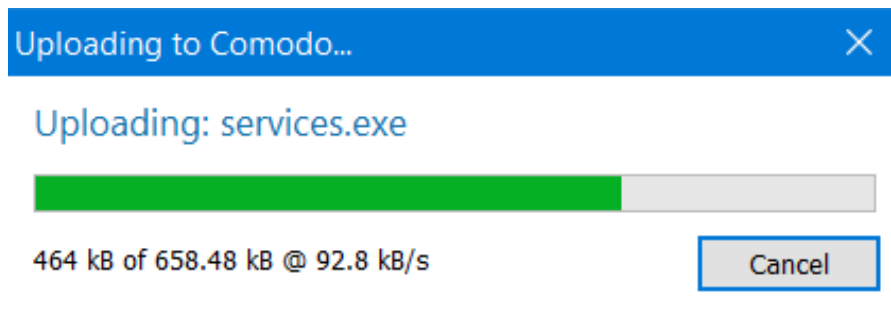
نکته : باز کردن یک فایل مستند مخرب هنگام استفاده از برنامه‌های نظارتی سریع‌ترین راه برای تشخیص هویت یک فایل است. شما می‌توانید با این روش به سرعت مشخص کنید که فایل مخرب است یا خیر. با این حال، هنگامی بدافزار به صورت موفقیت‌آمیز در سیستم شما اجرا خواهد شد که از یک برنامه آسیب‌پذیر مانند نسخه‌های قدیمی Adobe Reader و Microsoft Word برای مشاهده فایل مخرب استفاده کرده باشید تا فایل مخرب بتواند آن‌ها را اکسپلویت کند و در پایان بدافزار تعبیه شده درون خود را اجرا کند. برای تحلیل این نوع بدافزارها، راحت‌ترین راه این است که از حالات ماشین مجازی چندین Snapshot بگیرید، سپس آن‌ها را مورد تحلیل قرار بدهید.

علاوه بر این، ابزارهای Process Explorer و حتی Process Hacker به شما اجازه می‌دهند، در صورت مشاهده یک پروسه مشکوک در حال اجرا بر روی سامانه‌عامل، هویت آن را با استفاده از سرویس‌های امنیتی مانند VirusTotal یا Comodo مورد ارزیابی و تحلیل عمیق قرار بدهید.

Registry		4,256 K	17,824 K	88	
System Idle Process	96.74	60 K	8 K	0	
System	0.20	196 K	112 K	4	
Interrupts	0.34	0 K	0 K	n/a	Hardware Interrupts and DPCs
smss.exe		1,184 K	964 K	360	
Memory Compression		160 K	12,668 K	1264	
csrss.exe		1,592 K	4,576 K	448	
wininit.exe		1,360 K	6,028 K	520	
services.exe		3,452 K	7,044 K	644	
lsass.exe		6,096 K	16,404 K	672	Local Security Authority Process Microsoft Corporation
fontdrvhost.exe		1,516 K	2,304 K	768	
csrss.exe	0.15	1,644 K	4,688 K	536	
winlogon.exe		2,808 K	8,796 K	612	
explorer.exe	0.31	42,600 K	108,800 K	4116	Windows Explorer Microsoft Corporation
ConEmu64.exe	0.45	15,092 K	36,012 K	4832	Console Emulator (x64) ConEmu-Maximus5
ConEmu64.exe	0.17	3,044 K	7,808 K	3960	ConEmu console extender (x64) ConEmu-Maximus5
procexp64.exe	1.10	32,144 K	62,280 K	1700	Sysinternals Process Explorer Sysinternals - www.sysinternals.com

تصویر ۲۳: ارزیابی پروسه توسط Virustotal

کافی است، روی پروسه مشکوک کلیک راست کنید و سپس گزینه Check Virustotal را انتخاب کنید تا مشخص شود پروسه مورد نظر مخرب است یا خیر. اگر پروسه مخرب باشد، در قسمت Description (کادر قرمز در تصویر ۲۳) مشخص خواهد شد که چند موتور ضدویروس این پروسه را به عنوان یک پروسه مخرب شناسایی کرده‌اند.


















تصویر ۲۴: بارگزاری پروسه در سرویس Comodo توسط Process Hacker

شایان ذکر است، ابزار Process Hacker، علاوه بر Virustotal از سرویس‌های دیگر مانند سرویس Comodo و ... پشتیبانی می‌کند. هنگامیکه در حال استفاده از Process Hacker هستید، با رجوع به منوی Send to می‌توانید پروسه را بر روی سرویس‌های ضدویروس آنلاینی مانند Virustotal یا Comodo یا Jotti بارگزاری و بررسی کنید. تصویر ۲۴ نحوه بارگزاری یک پروسه در سرویس Comodo را نمایش می‌دهد، اگرچه تحلیلگر می‌تواند پروسه را برای بررسی بر روی سرویس‌های دیگر مانند Jotti بارگزاری کند.

Dropper.exe

Name:	Dropper.exe	Status:	Scan finished. 14/15 scanners reported malware.
Size:	709KB (726,016 bytes)	Scan taken on:	May 30, 2020 at 10:11:45 PM GMT+2
Type:	PE32 executable (GUI) Intel 80386, for MS Windows		
First seen:	May 30, 2020 at 10:11:40 PM GMT+2		
MD5:	e93a3705fdd01cf942e4830e148f0b66		
SHA1:	4f640da558a758dd5d58483c150e6d41a05f3766		

 May 30, 2020	Win32.CoinminerX-gen	 May 30, 2020	Trojan.GenericKD.33566550	 May 30, 2020	Win.Trojan.Gamarue-7673992-0
 May 30, 2020	Trojan.DownLoader33.21716	 May 30, 2020	Trojan.GenericKD.33566550	 May 30, 2020	Win32/Kryptik.HCGQ
 May 30, 2020	W32/Kryptik.HCGQ/tr	 May 30, 2020	Found nothing	 May 30, 2020	Heuristic.HEUR/AGEN.1133046
 May 30, 2020	Trojan.GenericKD.33566550	 May 29, 2020	Trojan.Win32.Racealer	 May 29, 2020	Riskware (0040eff71)
 May 30, 2020	Mal/RyPack-A	 May 29, 2020	Trojan.Win32.GLUPTeBA.AFLH	 May 29, 2020	Trojan.Wacatac

تصویر ۲۵: گزارش Jotti از تحلیل بدافزار

به عنوان مثال در تصویر ۲۵، گزارش Jotti آورده شده است که بعد از بارگزاری یک پروسه بر روی آن تولید شده است. در این گزارش، مشخص شده است که پروسه بارگزاری شده توسط ضدویروس‌های گوناگون مانند Bitdefender یا Avast یا SOPHOS به عنوان یک بدافزار شناخته شده است.

مشاهده ساختار درختی پروسه‌ها با Plist

همانطور که تا به الان متوجه شدید، یک خاصیت منحصر بفرد درباره یک پروسه که بیشتر ابزارها آن را نشان نمی‌دهند، شناسه یا ID پروسه والد یک پروسه است. اما با این حال، شما می‌توانید با استفاده از Process Monitor (یا از راه برنامه‌نویسی) با پرس‌وجوی شناسه پروسه خالق این اطلاعات را به دست آورید. همچنین ابزار Pslist.exe (در ابزارهای دیباگ سامانه‌عامل ویندوز) می‌تواند ساختار درختی پروسه‌ها را با استفاده از سوئیچ /t نمایش دهد. در تصویر ۲۶ یک نمونه مثال از این ابزار آورده شده است.

```

C:\Users\mkahs
λ pslist /t

PsList v1.4 - Process information lister
Copyright (C) 2000-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

Process information for COMMANDO:

Name                Pid Pri Thd  Hnd    VM      WS  Priv
Idle                 0   0   2    0     8       8    60
System              4   8  117 2129   3840    112   196
  smss               360  11   2   53 4194303  884  1184
  Memory Compression 1264  8   14   0   38016 10880  152
  Registry           88   8   4   0  102912 15872  4872
  csrss              448  13  10  391 4194303  4536  1584
  wininit            520  13   1  156 4194303  6028  1360
  services           644   9   6  373 4194303  7108  3636
  svchost            512   8  14  710 4194303 26200 18500
  svchost            716   8  17  724 4194303 64500 52388
  ctfmon             2076 13   8  373 4194303 12780  3304
  svchost            756   8  13  791 4194303 24092  7556
  SearchUI           2124  8  29  949 4194303 60988 57492
  WmiPrvSE           3448  8   7  304 4194303 14260 14972
  WmiPrvSE           3456  8  11  356 4194303 16568  8752
  RuntimeBroker      3696  8   1  241 4194303 13460  2796
  StartMenuExperienceHost 4472  8   7  579 4194303 56264 28368
  RuntimeBroker      4552  8   3  220 4194303 17008  3076
  RuntimeBroker      4892  8   1  283 4194303 15288  4812
  SettingSyncHost    5012  6   9  714 4194303 10532 12884

```

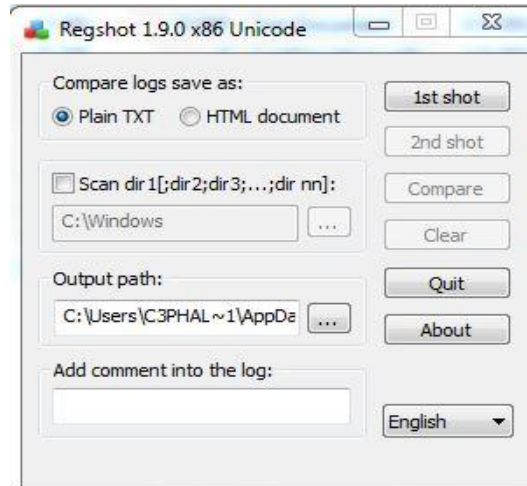
تصویر ۲۶: اجرای فرمان pslist برای نمایش پروسه‌ها

در خروجی برنامه pslist.exe که در تصویر ۲۶ مشاهده می‌کنید، هر یک از پروسه‌ها دندان‌گذاری شده است تا ارتباط خودش با والد و فرزند مشخص باشد. شایان ذکر است، پروسه‌هایی که والدشان وجود ندارد، به سمت چپ دندان‌گذاری شده‌اند (مانند پروسه wininit که در لیست بالا برجسته شده است) چون حتی اگر یک والد بزرگ^۱ پروسه برای آنها وجود داشته باشد، هیچ راهی به منظور شناسایی ارتباط بین آنها وجود ندارد.

مقایسه رجیستری Snapshotها با Regshot

برنامه Regshot را در تصویر ۲۷ مشاهده می‌کنید. Regshot یک برنامه متن باز برای مقایسه تغییرات اعمال شده روی رجیستری است که به شما اجازه می‌دهد دو حالت متفاوت رجیستری را با هم مقایسه کنید. به منظور استفاده از Regshot برای تجزیه و تحلیل بدافزار، به سادگی از حالت رجیستری قبل از اجرای بدافزار با کلیک روی دکمه 1st Shot یک نمونه‌برداری کنید و پس از آن بدافزار را اجرا کنید، سپس چند لحظه صبر کنید تا بدافزار تغییراتی روی رجیستری اعمال کند.

¹ Grandparent



تصویر ۲۷: برنامه RegShot

بعد از آن، برای دومین بار با کلیک روی دکمه **2st shot** از رجیستری یک نمونه برداری دوباره کنید. در پایان روی دکمه **Compare** کلیک کنید تا دو نمونه رجیستری را با هم مقایسه کند. لیست ۱، یک زیر مجموعه از نتایج تولید شده توسط **Regshot** در طی تجزیه و تحلیل جاسوس افزار **ckr.exe** را نمایش می‌دهد.

```

Regshot
Comments:
Datetime: <date>
Computer: MALWAREANALYSIS
Username: username

-----
Keys added: 0
-----
Values added:3
-----
❶ HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\ckr:C:\WINDOWS\system32\
ckr.exe
...
-----
Values modified:2
-----
❷ HKLM\SOFTWARE\Microsoft\Cryptography\ RNG\Seed: 00 43 7C 25 9C 68 DE 59 C6 C8
9D C3 1D E6 DC 87 1C 3A C4 E4 D9 0A B1 BA C1 FB 80 EB 83 25 74 C4 C5 E2 2F CE
4E E8 AC C8 49 E8 E8 10 3F 13 F6 A1 72 92 28 8A 01 3A 16 52 86 36 12 3C C7 EB
5F 99 19 1D 80 8C 8E BD 58 3A DB 18 06 3D 14 8F 22 A4
...
-----
Total changes:5
-----

```

لیست ۱: نتایج مقایسه برنامه Regshot

جاسوس افزار ckr.exe پس از اجرا یک مقدار در HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run مکانیزم پایداری ایجاد کرده است (شماره ۱). مقداری معینی نویز (شماره ۲) در این نتایج معمولی است، زیرا تولید کننده اعداد تصادفی seed بطور مرتب در رجیستری به روزرسانی می شود. شایان ذکر است، همانند ابزار Procmon به منظور به دست آوردن اطلاعات جالب با استفاده از Regshot نیاز به تجربه و تمرین دارید و باید در این راه حوصله به خرج دهید.

راه اندازی یک شبکه جعلی^۱

بدافزارها اغلب یک سیگنال هشداردهنده ارسال می کنند و در نهایت با سرور کنترل و فرماندهی خود ارتباط برقرار می کنند، در این باره در قسمت های بعدی با جزئیات بیشتر بحث خواهیم کرد. با این حال، شما می توانید با ایجاد یک شبکه جعلی بدون این که به اینترنت متصل شوید، به سرعت تمامی نشانه های شبکه ای بدافزار را جمع آوری کنید.

این نشانه ها شامل سرویس نام دامنه^۲، آدرس های IP و نشانه های دیجیتالی بسته های شبکه می شود. شایان ذکر است، به منظور جعل موفقیت آمیز یک شبکه، باید کاری کنید تا بدافزار نتواند تشخیص دهد که در یک محیط مجازی اجرا شده است (در قسمت ۳ این سلسله مقالات در مورد راه اندازی ماشین های مجازی بحث شده است).

با ترکیب ابزارهایی که در این قسمت مورد بحث قرار می گیرند، به همراه راه اندازی شبکه ماشین مجازی، شانس شما به منظور جعل موفقیت آمیز یک شبکه فوق العاده بالا می رود.

استفاده از ApateDNS

ApateDNS ابزاری رایگان از شرکت Mandiant است که سریع ترین راه برای مشاهده درخواست های DNS ارسالی است که توسط بدافزار ارسال می شوند. این ابزار با شنود روی پورت 53 پروتکل UDP روی ماشین محلی، جواب های DNS را جعل کرده تا به آدرس IP تعیین شده توسط کاربر هدایت شوند.

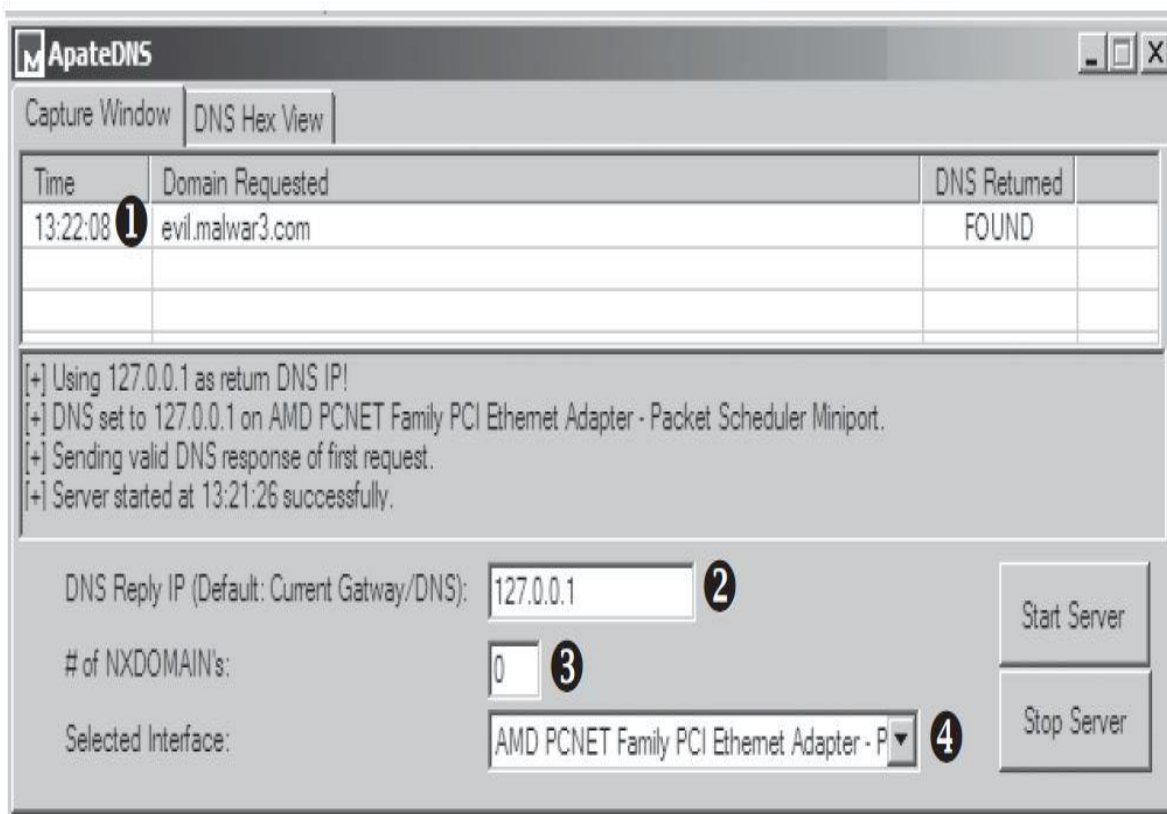
¹ Faking a network

² DNS names

برنامه ApateDNS به درخواست‌های DNS با آدرس IP که شما مشخص کرده‌اید پاسخ می‌دهد. همچنین ApateDNS می‌تواند نتایج تمامی درخواست‌های DNS دریافتی را با اسکی (ASCII) و هگزادسیمال (Hexadecimal) نمایش دهد.

برای استفاده از برنامه ApateDNS، آدرس IP که قصد دارید با آن درخواست‌های DNS را ارسال کنید، ابتدا مشخص سازید (شماره ۲ در تصویر ۲۸) و رابط شبکه را از قسمت مشخص شده توسط (شماره ۳ در تصویر ۲۸) انتخاب کرده و سپس روی دکمه Start کلیک کنید، تا به صورت خودکار سرور DNS اجرا شده و برنامه تنظیمات شبکه را به میزبان محلی (Localhost) تعویض کند.

سپس، بدافزار را اجرا کنید تا در پنجره ApateDNS درخواست‌های ارسالی DNS توسط بدافزار را مشاهده کنید. به عنوان مثال، در تصویر ۲۸ ما درخواست‌های ایجاد شده توسط بدافزار Rshell را تغییر مسیر داده‌ایم. در تصویر ۲۸ مشاهده می‌کنید که این بدافزار برای دامنه <http://evil.malwar3.com> در زمان ۱۳:۲۲:۰۸ (شماره ۱) یک درخواست ارسال کرده است.



تصویر ۲۸: پاسخگویی ApateDNS به یک درخواست برای evil.malwar3.com

در مثال نمایش داده شده در تصویر ۲۸، ما درخواست‌های DNS ارسالی بدافزار را به ۱۲۷.۰.۰.۱ (میزبان محلی یا Localhost) تغییر مسیر داده‌ایم، اما احتمال دارد شما بخواهید این آدرس را با یک آدرس خارجی تعویض کنید، مانند یک وب سرور که روی یک ماشین مجازی لینوکس در حال خدمات‌دهی است.

زیرا آدرس IP ماشین مجازی تجزیه و تحلیل بدافزار ویندوز با آدرس IP ماشین مجازی لینوکس متفاوت خواهد بود، اطمینان حاصل کنید که آدرس IP درستی را قبل از اجرای سرور (Start Server) وارد کرده باشید. در حالت پیش فرض برنامه ApateDNS از دروازه^۱ پیش فرض یا تنظیمات جاری DNS برای پاسخگویی به درخواست‌های DNS استفاده می‌کند.

نظارت با Netcat^۲

حتما می‌دانید در دنیا چاقوهای همه‌کاره سویی بسیار معروف هستند، ابزار Netcat هم مانند چاقو همه‌کاره سویی می‌باشد و قادر است برای پوشش اتصالات ورودی و خروجی، تونل زدن^۳، سرویس‌های پراکسی^۴، جابه‌جایی پورت^۵ و... مورد استفاده قرار گیرد.

حال اجازه دهید نگاهی بیندازیم به این که چگونه می‌توانیم از Netcat برای تحلیل بدافزار Rshell استفاده کنیم. با استفاده از ApateDNS در مرحله قبل، ما در خواست‌های DNS ارسالی بدافزار به evil.malwar3.com را به ماشین محلی تغییر مسیر دادیم.

فرض کنید که بدافزار از پورت ۸۰ (رایج‌ترین پورت مورد استفاده توسط بدافزارها) برای برقراری ارتباط خارجی استفاده می‌کند. در این هنگام، ما می‌توانیم از Netcat برای شنود این ارتباط استفاده کنیم. بدافزارها پیوسته از پورت‌های ۸۰ و ۴۴۳ (به ترتیب پورت‌های Http و Https) استفاده می‌کنند، زیرا این پورت‌ها در حالت معمول مسدود نشده‌اند. لیست ۲ یک مثال را نمایش می‌دهد.

¹ Gateway

² Monitoring with Netcat

³ Tunneling

⁴ Proxying

⁵ Port forwarding

```
C:\> nc -l -p 80 ❶
POST /cq/frame.htm HTTP/1.1
Host: www.google.com ❷
User-Agent: Mozilla/5.0 (Windows; Windows NT 5.1; TWfSd2FyZUh1bnRlcmg==;
rv:1.38)
Accept: text/html, application
Accept-Language: en-US, en;q=
Accept-Encoding: gzip, deflate
Keep-Alive: 300
Content-Type: application/x-form-urlencoded
Content-Length

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

Z:\Malware> ❸
```

لیست ۲: خروجی برنامه Netcat

دستور NC و دیگر گزینه‌های نمایش داده شده در لیست ۲ (شماره ۱)، پارامترهای مورد نیاز برای شنود یک پورت را نمایش می‌دهد. در این دستور ما از پارامتر `-l` برای شنود و از پارامتر `-p` برای تشخیص یک پورت به منظور شنود، استفاده کرده‌ایم.

بدافزار پس از اجرا به شنونده Netcat ما متصل می‌شود، زیرا ما از قبل با استفاده از ApateDNS درخواست‌های ارسالی به DNS را به ماشین محلی خود تغییر مسیر داده‌ایم. همان‌طور که مشاهده می‌کنید، Rshell یک بدافزار از نوع پوسته معکوس^۱ است که پس از اجرا، خط فرمان سیستم قربانی را به مهاجم ارائه می‌کند (شماره ۳ در لیست ۲ نمایشگر خط فرمان قربانی به مهاجم است).

اما همان‌طور که در خروجی مشاهده می‌کنید، بدافزار ابتدا یک درخواست POST به گوگل ارسال کرده است (شماره ۲)، احتمالاً بدافزار این کار را برای مبهم‌سازی عملیات پوسته معکوس خود انجام داده است.

¹ Reverse Shell

شنود بسته‌های شبکه با Wireshark

این ابزار یکی از بهترین تحلیل‌گرهای بسته‌های شبکه‌ای با کد منبع باز است که امروزه وجود دارد و در سطح گسترده‌ای از آن استفاده می‌شود. نسخه‌ی اصلی این ابزار با نام **Ethereal** وجود داشت که از سال ۲۰۰۶ میلادی به بعد این پروژه به **Wireshark** تغییر نام یافت.

نرم‌افزار **Wireshark** بسیار شبیه ابزار **tcpdump** است، با این تفاوت که ابزار **Wireshark** واسط گرافیکی بسیار قوی داشته و اطلاعات خیلی بیشتری در زمینه‌ی مرتب‌سازی و فیلتر بسته‌های شبکه در اختیار کاربر قرار می‌دهد. علاوه بر این‌ها، **Wireshark** ابزاری مفید و رایگان برای شنود و تحلیل ترافیک شبکه در سیستم‌های ویندوزی و لینوکسی است. این ابزار توانایی بررسی داده‌ها را به صورت زنده و یا از روی فایل ذخیره شده ارائه می‌دهد.

نرم‌افزار **Wireshark** همچنین صدها پروتکل را پشتیبانی می‌کند و ابزاری بسیار قوی در زمینه شنود ارتباطات شبکه‌ای می‌باشد. این برنامه امکان تجزیه و تحلیل یک جریان شبکه‌ای از بسته‌ها و تجزیه و تحلیل بسته‌های شبکه به صورت مجزا را ارائه می‌دهد. با این حال، همانند بسیاری از ابزارها که در این کتاب مورد بحث قرار گرفت، **Wireshark** می‌تواند برای اهداف مخربانه و یا اهداف پاک مورد استفاده قرار گیرد. از این برنامه می‌توانید برای تحلیل ویژگی‌های شبکه، خطایابی مسائل برنامه‌های کاربردی و مطالعه روی پروتکل‌ها استفاده کنید.

علاوه بر این‌ها، شما می‌توانید به منظور اهداف مخرب، مانند شنود کلمه‌های عبور، مهندسی معکوس پروتکل‌های شبکه، دزدی اطلاعات حساس و... همچنین از این برنامه سوءاستفاده کنید. صفحه نمایش **Wireshark** شامل سه بخش کلی است که در زیر تشریح شده‌اند:

۱. **پانل ثبت بسته‌ها^۱ (شماره ۱ در تصویر ۲۹):** در این قسمت تمامی پکت‌های ارسالی و

دریافتی شبکه در یک صف سلسله مراتبی نمایش داده می‌شوند. هر خط در این لیست یک بسته

ثبت شده را انعکاس می‌دهد. صفحه نمایش این پانل به سطرها و ستون‌ها مختلفی تقسیم شده

¹ Capture panel

است که هر یک از ردیف‌ها داده‌های یک بسته و هر ستون اطلاعات اضافی درباره یک بسته را نمایش می‌دهد.

۲. پانل مشخصات بسته^۱ (قسمت ۳ و ۲ در تصویر ۲۹): هنگامی که یک بسته داده را از

پانل ثبت بسته‌ها انتخاب می‌کنید، جزئیات اطلاعات آن بسته در این پانل نمایش داده می‌شود.

۳. پانل بایت‌های بسته^۲ (قسمت ۴ در تصویر ۲۹): این قسمت محتویات بسته جاری را به

هگزادسیمال نمایش می‌دهد.

The screenshot shows the Wireshark interface with the following details:

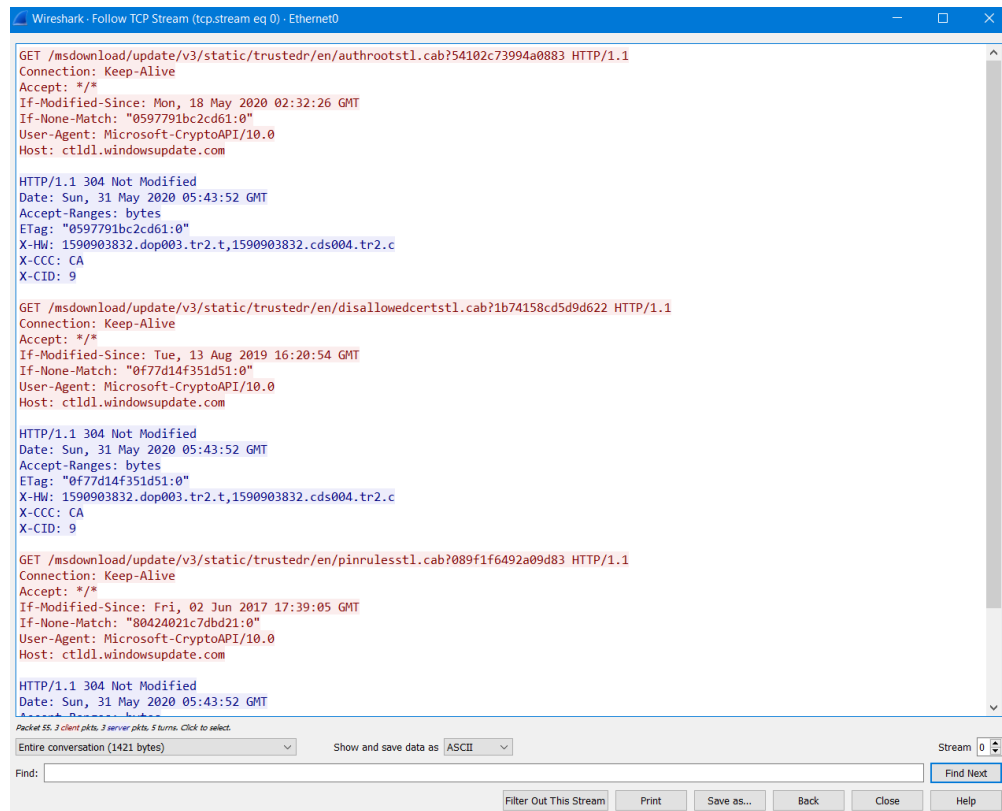
- Packet List:** A table with columns for No., Time, Source, Destination, Protocol, and Info. Packet 47 is highlighted, showing a GET request for / HTTP/1.1.
- Packet Details:**
 - Frame 47 (347 bytes on wire, 347 bytes captured)
 - Ethernet II, Src: vmware_ae:96:3a (00:0c:29:ae:96:3a), Dst: vmware_fc:bf:0d (00:50:56:fc:bf:0d)
 - Internet Protocol, Src: 192.168.159.129 (192.168.159.129), Dst: 67.228.110.120 (67.228.110.120)
 - Transmission Control Protocol, Src Port: dfn (1133), Dst Port: http (80), Seq: 1, Ack: 1, Len: 293
 - Hypertext Transfer Protocol
 - GET / HTTP/1.1\r\n
 - Accept: image/gif, image/jpeg, image/pjpeg, image/pjpeg, application/x-shockwave-flash, */*\r\n
 - Accept-Language: en-us\r\n
 - User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; windows NT 5.1; Trident/4.0)\r\n
 - Accept-Encoding: gzip, deflate\r\n
- Packet Bytes:** A hex dump of the packet data, with the ASCII column showing the beginning of the GET request: "...v..GE T / HTTP /1.1..Ac cept: im age/gif, image/j ppeg, ima ge/pjpeg, ima ge/pjpeg, a plication/x sho".

شکل ۱۴-۳: مثال DNS و Http در برنامه Wireshark

¹ Packet details panel

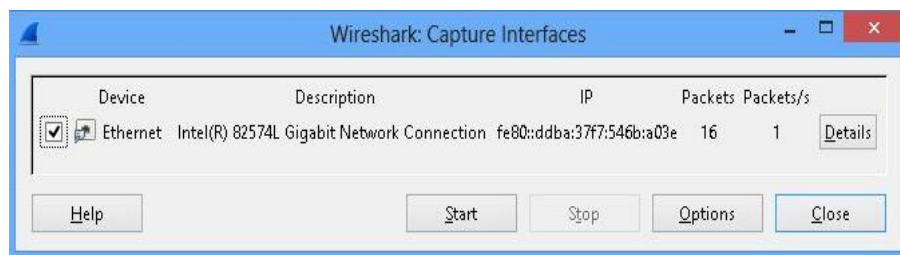
² Packet bytes panel

برای استفاده از Wireshark به منظور مشاهده محتویات یک جلسه TCP، کافی است روی یک بسته از نوع TCP کلیک راست کرده و گزینه Follow TCP Stream را انتخاب کنید. همان طور که در تصویر ۳۰ مشاهده می کنید. گفتگو در یک جلسه با دو رنگ مجزا نمایش داده شده است.



تصویر ۳۰: پنجره Follow TCP Stream برنامه Wireshark

به منظور دریافت بسته‌های شبکه با برنامه Wireshark کافی است ابتدا به منوی Capture بروید و روی گزینه Interfaces کلیک کنید، سپس در پنجره‌ای که باز می‌شود مانند تصویر ۳۱ ÷ رابط شبکه‌ای که قصد دارید مورد شنود قرار بدهید را انتخاب کرده و روی دکمه Start کلیک کنید.



تصویر ۳۱: رابط‌های شبکه در Wireshark

برنامه Wireshark با شنود بسته‌های ارتباطی بدافزار، می‌تواند به شما کمک کند تا بفهمید بدافزار چگونه ارتباطات شبکه خود را انجام می‌دهد. برای استفاده از Wireshark بدین منظور آن را در حالت گرفتن بسته‌های شبکه (Capture Packet) قرار بدهید و سپس بدافزار را اجرا کنید. (می‌توانید از برنامه Netcat برای شبیه‌سازی یک اتصال شبکه استفاده کنید) در قسمت‌های آینده بیشتر درباره این برنامه بحث خواهیم کرد.

استفاده از InetSim

برنامه INetSim یک برنامه رایگان و مبتنی بر لینوکس است که به منظور شبیه‌سازی سرویس‌های رایج اینترنت می‌تواند مورد استفاده قرار گیرد. راحت‌ترین راه برای اجرای INetSim اگر از یک سامانه‌عامل بر پایه میکروسافت استفاده می‌کنید، این است که آن را در یک سامانه‌عامل لینوکس مجازی که در شبکه مشابه سامانه‌عامل ویندوز شما قرار دارد، آن را راه‌اندازی کرده و مورد استفاده قرار بدهید.

با این حال، برنامه INetSim بهترین ابزار برای ارائه سرویس‌های جعلی است. این برنامه به شما اجازه می‌دهد، رفتارهای یک بدافزار ناشناس را با شبیه‌سازی سرویس‌های Http، Https، Ftp، Dns، Smtپ و دیگر سرویس‌های رایج اینترنت مورد تحلیل قرار بدهید. لیست ۳ تمامی سرویس‌هایی که برنامه INetSim در حالت پیش‌فرض شبیه‌سازی می‌کند را شامل می‌شود.

- * dns 53/udp/tcp - started (PID 9992)
- * http 80/tcp - started (PID 9993)
- * https 443/tcp - started (PID 9994)
- * smtp 25/tcp - started (PID 9995)
- * irc 6667/tcp - started (PID 10002)
- * https 465/tcp - started (PID 9996)
- * ntp 123/udp - started (PID 10003)
- * pop3 110/tcp - started (PID 9997)
- * finger 79/tcp - started (PID 10004)
- * syslog 514/udp - started (PID 10006)
- * tftp 69/udp - started (PID 10001)
- * pop3s 995/tcp - started (PID 9998)

-
- * time 37/tcp - started (PID 10007)
 - * ftp 21/tcp - started (PID 9999)
 - * ident 113/tcp - started (PID 10005)
 - * time 37/udp - started (PID 10008)
 - * ftps 990/tcp - started (PID 10000)
 - * daytime 13/tcp - started (PID 10009)
 - * daytime 13/udp - started (PID 10010)
 - * echo 7/tcp - started (PID 10011)
 - * echo 7/udp - started (PID 10012)
 - * discard 9/udp - started (PID 10014)
 - * discard 9/tcp - started (PID 10013)
 - * quotd 17/tcp - started (PID 10015)
 - * quotd 17/udp - started (PID 10016)
 - * chargen 19/tcp - started (PID 10017)
 - * dummy 1/udp - started (PID 10020)
 - * chargen 19/udp - started (PID 10018)
 - * dummy 1/tcp - started (PID 10019)
-

لیست ۳: سرویس‌های شبیه‌سازی شده پیش‌فرض برنامه InetSim

برنامه InetSim تمام تلاش خود را می‌کند که مانند یک وب سرور واقعی باشد. بدین منظور برنامه InetSim ویژگی‌های قابل پیکربندی دارد، که برنامه می‌تواند با استناد به آن‌ها با موفقیت به مقصود خود برسد. برخی از بهترین ویژگی‌های InetSim شبیه‌سازی سرویس‌های Http و Https می‌باشد.

همچنین برنامه InetSim می‌تواند تقریباً هر نوع فایل درخواستی را سرویس‌دهی کند. به عنوان مثال، اگر یک قسمت از بدافزار یک فایل JPEG از یک سرور برای ادامه فعالیت خود درخواست دهد، برنامه InetSim می‌تواند به آن با یک قالب JPEG مناسب پاسخ دهد. اگرچه آن عکس ممکن است چیزی نباشد که بدافزار به دنبال آن بوده است، اما با این حال دیگر سرور به درخواست بدافزار خطای ۴۰۴ یا یک خطای دیگر نمی‌دهد و بدافزار می‌تواند به کار خود ادامه دهد.

برنامه InetSim می‌تواند همه درخواست‌های ورودی و ارتباطات را ذخیره‌سازی کند. این مزیت می‌تواند به ویژه برای پیدا کردن این که آیا بدافزار به یک سرویس استاندارد متصل شده است یا خیر بسیار مفید واقع شود.

همچنین برنامه InetSim فوق‌العاده قابل پیکربندی است، به عنوان مثال، اگر در حین تحلیل بدافزار متوجه شدید، بدافزار به دنبال یک صفحه خاص است، قبل از اجرا آن می‌توانید آن صفحه را به بدافزار ارائه دهید. شما می‌توانید پورت‌هایی که سرویس‌ها روی آن‌ها روی شنود قرار گرفته اند را تغییر دهید. این مزیت هنگامی که بدافزار از یک مجموع پورت غیراستاندارد استفاده می‌کند، بسیار مناسب است. همچنین از آنجای که برنامه InetSim با عقیده تحلیل بدافزار ایجاد شده است، یک مجموعه منحصر بفرد از ویژگی‌ها را برای تحلیل بدافزارها ارائه می‌دهد، از قبیل سرویس‌های مصنوعی که یک ویژگی برای ثبت تمامی درخواست‌های ارسالی با صرف نظر از پورت سمت کلاینت است. سرویس‌های مصنوعی به ویژه برای دریافت ترافیک ارسالی از کلاینت به هر پورت و سرویسی بسیار مفید است. شما می‌توانید از آن برای ذخیره‌سازی همه داده‌های ارسالی از بدافزار به پورت‌ها بهره‌مند شوید.

ابزارهای تجزیه و تحلیل دینامیک در عمل¹

تمامی ابزارهای بحث شده در این فصل می‌توانند در ارتباط با جمع‌آوری اطلاعات در حین تجزیه و تحلیل دینامیک بدافزار مورد استفاده قرار گیرند. پروسه ساده آماده‌سازی محیط برای تحلیل بدافزار به ترتیب زیر است:

۱. ابتدا برنامه Procmon را اجرا کرده و یک فیلتر برای نام فایل اجرایی بدافزار (بدافزار مورد تحلیل، مثال clightning.exe) تنظیم کنید. همچنین کلیه رویدادهای قبلی در برنامه ثبت شده برنامه Procmon را هم قبل از اجرای بدافزار پاک سازی کنید.
۲. در گام دوم برنامه Process Explorer را برای نظارت پروسه اجرا کنید.
۳. سپس از حالت رجیستری اولیه سیستم (قبل از اجرای بدافزار) با برنامه Regshot یک Snapshot بگیرید.
۴. در گام بعدی، باید شبکه مجازی خودتان را به منظور مرتبط ساختن ماشین تحلیلگر به سرور InetSim پیکربندی کنید.
۵. در گام آخر برای تحلیل رویدادهای شبکه باید برنامه Wireshark را راه‌اندازی کنید.

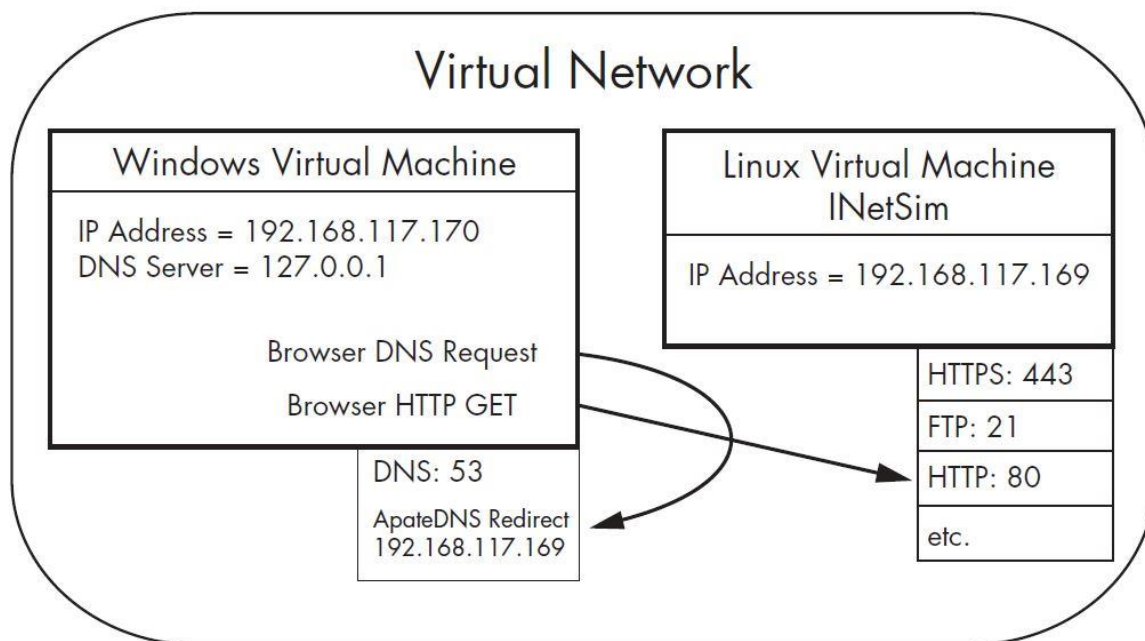
¹ Basic Dynamic Tools in Practice

تصویر ۳۲ دیاگرام یک شبکه مجازی که برای تحلیل بدافزار طراحی شده است را نمایش می‌دهد. این شبکه مجازی دارای دو میزبان می‌باشد: یک میزبان که ماشین مجازی ویندوز است که از آن به منظور تحلیل بدافزار استفاده می‌شود و دیگری ماشین مجازی لینوکس است که روی آن InetSim در حال اجرا است.

ماشین مجازی لینوکس در حین استفاده از InetSim روی خیلی از پورت‌ها از قبیل Https، Ftp و Http در حال شنود قرار می‌گیرد و ماشین مجازی ویندوز روی پورت ۵۳ به منظور درخواست‌های DNS از طریق برنامه ApateDNS در حال شنود قرار خواهد گرفت.

در حالت پیش‌فرض سرور DNS برای ماشین مجازی ویندوز با میزبان محلی پیکربندی شده است. اما اکنون ApateDNS باید دوباره پیکربندی شود، تا درخواست‌های DNS را به ماشین مجازی لینوکس (۱۹۲.۱۶۸.۱۱۷.۱۶۹) تغییر مسیر دهد. (آی‌پی 127.0.0.1 را به آی‌پی ماشین مجازی لینوکس تغییر بدهید).

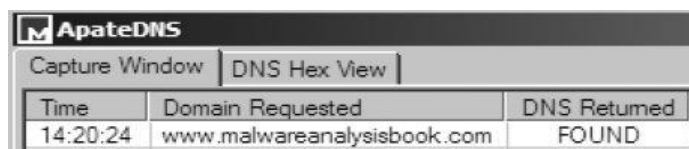
پس از اعمال این تغییرات اگر شما در ماشین مجازی وارد یک وب‌سایت شوید درخواست‌های DNS تجزیه شده توسط ApateDNS به ماشین مجازی لینوکس تغییر مسیر داده می‌شوند. پس از آن، مرورگر از پورت ۸۰ به سرور INetSim که در حال گوش دادن به آن پورت بر روی ماشین مجازی لینوکس است، یک درخواست Get می‌دهد.



تصویر ۳۲: مثال شبکه مجازی

حال به صورت عملی با بررسی بدافزار msts.exe نحوه عملکرد این تنظیمات را مشاهده و تحلیل خواهیم کرد. ابتدا تنظیمات مراحل آماده‌سازی که در قسمت قبل ذکر شد را کامل کرده و سپس بدافزار msts.exe را در ماشین مجازی تحلیل بدافزار خود اجرا می‌کنیم. بعد از چند لحظه، ثبت رویدادها توسط Procmon را متوقف می‌سازیم و برای دومین بار از رجیستری توسط Regshot یک Snapshot می‌گیریم. در این قسمت ما تحلیل خود را به شکل زیر پیش می‌بریم:

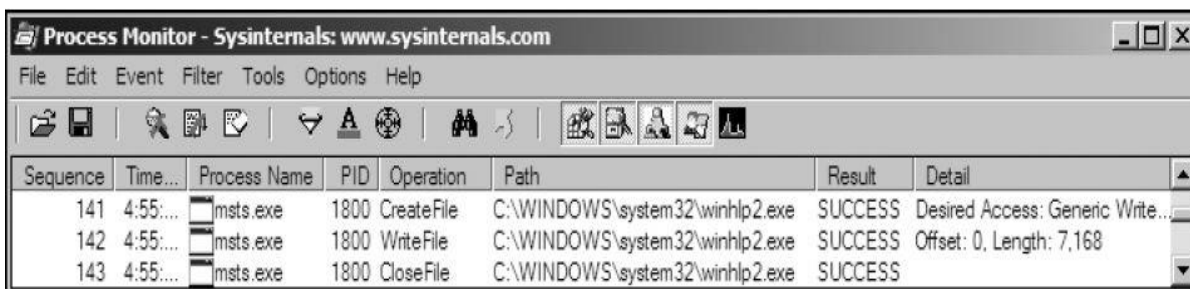
۱. برنامه ApatDNS را باز کنید تا درخواست‌های DNS صادر شده را بتوانید مشاهده کنید. همان‌طور که در شکل ۱۸-۳ مشاهده می‌کنید، بدافزار یک درخواست DNS برای www.malwareanalysisbook.com ارسال کرده است.



ApatDNS		
Capture Window		DNS Hex View
Time	Domain Requested	DNS Returned
14:20:24	www.malwareanalysisbook.com	FOUND

تصویر ۳۳: درخواست DNS برای www.malwareanalysisbook.com در برنامه ApatDNS را نمایش می‌دهد.

۲. نتایج برنامه Procmon برای تغییرات سیستمی اعمال شده را بررسی کنید. در نتایج Procmon نمایش داده شده در تصویر ۳۴، مشاهده می‌کنید عملیات‌های CreateFile و WriteFile (شماره‌های ۱۴۱ و ۱۴۲) در جدول Operation برای C:\WINDOWS\system32\winhlp2.exe رخ داده است. با تحقیقات بیشتر، و مقایسه winhlp2.exe و msts.exe مشاهده خواهیم کرد که آن‌ها با هم مشابه هستند. از این موضوع نتیجه می‌گیریم، بدافزار خودش را در آن محل کپی می‌کند.



Sequence	Time...	Process Name	PID	Operation	Path	Result	Detail
141	4:55:...	msts.exe	1800	CreateFile	C:\WINDOWS\system32\winhlp2.exe	SUCCESS	Desired Access: Generic Write...
142	4:55:...	msts.exe	1800	WriteFile	C:\WINDOWS\system32\winhlp2.exe	SUCCESS	Offset: 0, Length: 7,168
143	4:55:...	msts.exe	1800	CloseFile	C:\WINDOWS\system32\winhlp2.exe	SUCCESS	

شکل ۱۹-۳: نتیجه‌های Procmon برای فیلتر msts.exe

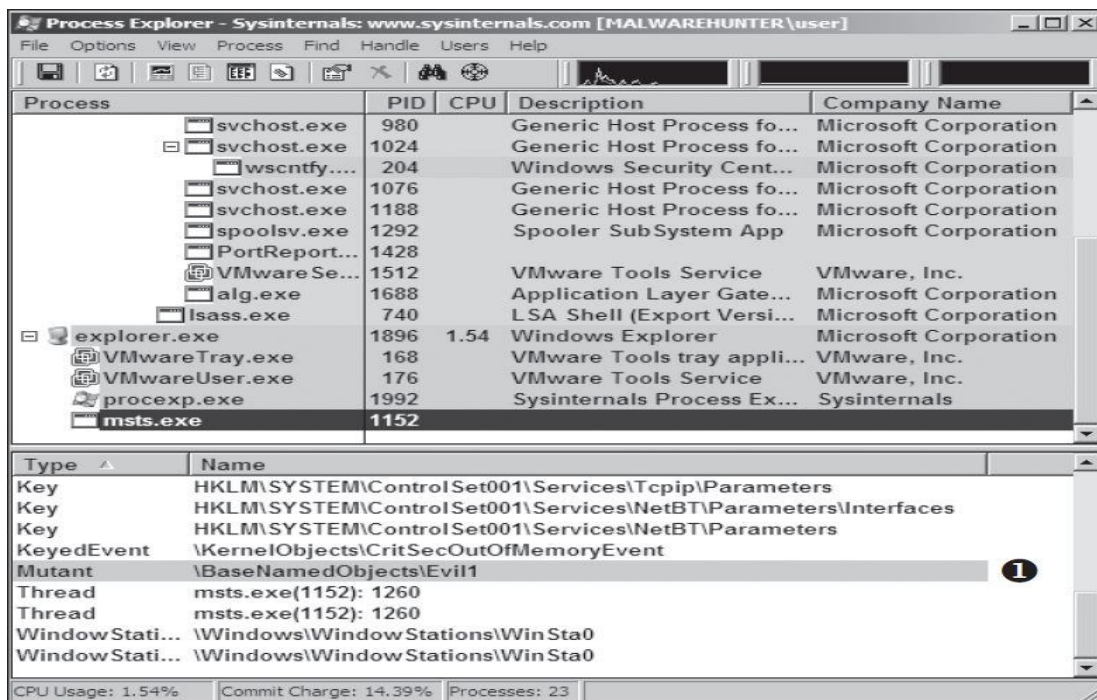
۳. در گام سوم دو Snapshot گرفته شده از رجیستری توسط Regshot را بررسی کنید. مشاهده خواهید کرد (لیست ۴) بدافزار مقدار اجرای خودکار winhlp را در محل HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run افزوده است. مقدار نوشته شده برای آن (C:\WINDOWS\system32\winhlp2.exe) جایی است که بدافزار خود را در آنجا کپی می‌کند. و پس از این موضوع، بدافزار کپی شده پس از هر بار راه‌اندازی مجدد سیستم اجرا می‌شود.

Values added:3

**HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\winhlp
: C:\WINDOWS\system32\winhlp2.exe**

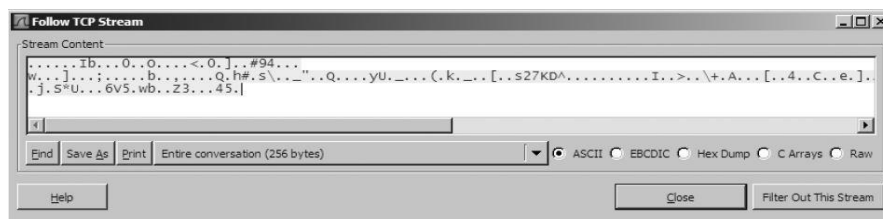
لیست ۴: مقدار رجیستری افزوده شده توسط بدافزار

۴. از برنامه Process Explorer برای مشخص کردن پروسه‌ای که Mutex یا شنونده به منظور برقراری ارتباط در سیستم ایجاد کرده استفاده کنید. همان‌طور که در خروجی Process Explorer که در تصویر ۳۴ نمایش داده شده است، مشاهده می‌کنید بدافزار یک Mutex با نام Evil ایجاد کرده است (شماره ۱ در تصویر ۳۴)، در مورد Mutexها در قسمت هفتم سلسله مقالات تجزیه و تحلیل بدافزار کی‌پاد بیشتر بحث خواهیم کرد. اما بهتر است بدانید، بدافزار msts.exe یک Mutex ایجاد کرده تا اطمینان حاصل کند در هر زمان یک نسخه از بدافزار روی سیستم در حال اجرا خواهد بود. Mutexها اگر به قدر کافی منحصر به فرد باشند، می‌تواند یک رد پای بسیار عالی از بدافزار به ما ارائه دهند.



تصویر ۳۴: بررسی پروسه فعال msts.exe در Process Explorer

۵. ترافیک ضبط شده بدافزار توسط Wireshark را بازبینی مجدد کنید. با استفاده از INetSim هنگام ضبط بسته‌ها با استفاده از Wireshark می‌توانیم عملیات‌های TCP Hand Shaking و بسته‌های اولیه ارسالی بدافزار را ضبط کنیم. محتویات جریان TCP ارسال شده از پورت ۴۴۳ در تصویر ۳۵ نمایش داده شده است. در این شکل داده‌ها با کد اسکی تصادفی نمایش داده شده‌اند که اغلب بیانگر یک پروتکل سفارشی است. وقتی این اتفاق می‌افتد، بهتر است چندین بار بدافزار را اجرا کرده و بسته‌های اولیه ارسالی برای ارتباط آن را مشاهده کنید. (نتیجه این اطلاعات می‌تواند در تهیه یک امضاء دیجیتالی مبتنی بر شبکه استفاده شود، این موضوع را در قسمت پانزدهم مورد بررسی قرار خواهیم داد).



تصویر ۳۵: برنامه Wireshark یک پروتکل سفارشی را نمایش می‌دهد

نتیجه گیری

تجزیه و تحلیل دینامیک ساده بدافزار می تواند نتایج به دست آمده از تجزیه و تحلیل ایستا ساده بدافزار را تأیید کند. بیشتر ابزارهای مورد بررسی قرار گرفته در این بخش رایگان و برای استفاده بسیار ساده هستند و اطلاعات قابل توجهی ارائه می دهند.

با این حال، روش های تجزیه و تحلیل دینامیک ساده بدافزار معایب خود را دارند. بنابراین نمی توانیم اینجا توقف کنیم. به عنوان مثال، برای درک مولفه های شبکه تعبیه شده در برنامه `msts.exe` شما نیاز به اعمال مهندسی معکوس روی پروتکل آن دارید تا مشخص کنید چگونه به بهترین شکل می توان تحلیل بدافزار را ادامه داد.

گام بعدی انجام روش های تحلیل ایستا پیشرفته با دیزاسمبلی یا کالبدشکافی در سطح باینری بدافزار است که در قسمت بعد مورد بررسی قرار خواهد گرفت.