دانشکده مهندسی کامپیوتر

عنوان:

گزارش بررسی سیستم های ۳۲ بیتی و ٦٤ بیتی و ساختار فایل PE در آن ها

استاد:

دکتر سعید پارسا

دانشجو:

محسن امیریان

۹۵۷۲۳۰۳٤

پائیز ۹۵

فهرست مطالب

۱- مقدمه..... ٤

۲- سیستم عامل های ۳۲ بیتی و ٦٤ بیتی..... ٥

۳- پردازنده های ۳۲ بیتی و ٦٤ بیتی..... ٦

٤- تشخیص فایل **PE** ۳۲ بیتی و ٦٤ بیتی از ساختار آن..... ۷

٤-۱- ویرایشگر متن..... ۷

٤-۲- ابزار PE Studio..... ۹

٤-۳- ابزار MiTeC EXE Explorer..... ۱۰

٥- فهرست منابع..... ۱۱

فهرست شکل‌ها

شکل ۱ – ساختار یک فایل PE ۳۲ بیتی در Notepad ۸
شکل ۲ – ساختار یک فایل PE ٦٤ بیتی در Notepad ۸
شکل ۳ – خروجی ابزار PE Studio بر روی فایل firefox.exe ۹
شکل ٤ – خروجی ابزار MiTeC EXE Explorer بر روی فایل chrome.exe ۱۰

۱- مقدمه

در این گزارش، ابتدا سیستم عامل های ۳۲ بیتی و ٦٤ بیتی مورد بررسی قرار گرفته و تفاوت مهم آنها ذکر شده است.

سپس در مورد پردازنده های ۳۲ بیتی و ٦٤ بیتی بحث شده و به تفاوت های آن ها در نحوه ی اجرای برنامه ها و همچنین سرعت اجرای برنامه ها اشاره شده است.

در نهایت فایل های اجرایی در این دو نوع معماری را بررسی کرده ایم و روش هایی ارائه کردیم که به کمک آن ها می توان ساختار این فایل ها (فایل های PE) را مطالعه نمود و ۳۲ یا ٦٤ بیتی بودن آن را تشخیص داد.

۲- سیستم عامل های ۳۲ بیتی و ٦٤ بیتی

پردازنده های ٦٤ بیتی می توانند در هر سیکل زمانی داده های بیشتری را پردازش کنند، از این رو نرم افزارهای شـــما نیز بر روی این پـــرازنده ها با سرعـت بیشتر اجرا و کار می کنند. طبیعی است که شما صرفا با نصب ویندوز ٦٤ بیتی نمی توانید از این قابلیت استفاده کنید و قطعا سخت افزار پردازنده شما نیز بایستی دارای ساختار ٦٤ بیتی باشد.

سیستم عامل ٦٤ بیتی می تواند نسبت به سیستم عامل ۳۲ بیتی از حافظه RAM بیشتری استفاده کند و در واقع دسترسی بیشتری به منابع موجود بر روی سخت افزار سیستم داشته باشد. برای سیستم عامل های ۳۲ بیتی سقف استفاده از حافظه RAM سیستم به اندازه ٤ گیگابایت تعیین شده است که شامل حافظه ی موجود بر روی کارت گرافیک شما نیز می شود. بنابراین شما هر چقدر هم بر روی سیستم خود RAM اضافه کنید اما سیستم عامل شما ۳۲ بیتی باشد در نهایت فقط ٤ گیگابایت آن قابل استفاده است که در بیشتر مواقع به دلیل محدویت های سیستم عامل ۳۲ بیتی صرفا ۳ و نیم گیگابایت آن به شما نمایش داده می شود.

یک سیستم عامل نسخه ٦٤ بیتی صرفا بر روی سخت افزاری می تواند نصب شود که دارای معماری ٦٤ بیتی باشد اما یک سیستم عامل ۳۲ بیتی می تواند بر روی سخت افزارهای ٦٤ بیتی نصب و راه ندازی شود و معماری ٦٤ بیتی را پشتیبانی می کند ، نکته در اینجاست که شما نباید از پورشه برای مسافرکشی استفاده کنید! دقیقا یعنی اینکه زمانیکه سخت افزار شما ٦٤ بیتی است ، سیستم عاملی را در آن نصب کنید که بتواند به بهترین شکل از منابع آن استفاده کند.

۳- پردازنده های ۳۲ بیتی و ٦٤ بیتی

اولین پردازنده‌ی ٦٤ بیتی دنیا در سال ۱۹٦۱ توسط IBM و در سوپر کامپیوتر Stretch 7030 طراحی و استفاده شد. اما تا دهه‌ی ۲۰۰۰ از این پردازنده‌ها در کامپیوترهای خانگی استفاده نشد. پردازنده‌های ٦٤ بیتی با عرضه‌ی ویندوز اکس‌پی رایج شدند. پس از آن تمام نسخه‌های ویندوز از پردازش ٦٤ بیتی پشتیبانی کردند. کامپیوترهای که به پردازنده‌ی ٦٤ بیتی مجهز می‌شوند قادرند نسخه‌ی ۳۲ بیتی از سیستم‌عامل‌ها و اپلیکیشن‌ها را اجرا کنند، اما برعکس این موضوع صادق نیست. علاوه بر این برای اینکه از تمام توان پردازنده‌ی ٦٤ بیتی دستگاه خود استفاده کنید، باید نسخه‌ی ٦٤ بیتی سیستم‌عامل و نرم‌افزارهای مورد نظر خود را داشته باشید.

یکی از مهم‌ترین تفاوت‌های بین پردازش ۳۲ بیتی و ٦٤ بیتی در تعداد محاسباتی است که هر کدام در هر ثانیه انجام می‌دهند. در واقع به بیان ساده، در برخی از شرایط پردازنده‌های ٦٤ بیتی سریع‌تر از ۳۲ بیتی‌ها عمل می‌کنند.

و اما نکته مهم این است که تفاوت تنها در پشتیبانی بیشتر از حافظه‌ی RAM نیست. عبارت "اگر حافظه‌ی رم دستگاه بیشتر از ٤ گیگابایت نباشد، تفاوتی بین پردازنده‌ی ۳۲ بیتی و ٦٤ بیتی نیست" که به آن اشاره شد، همیشه درست نیست! در این شکی نیست که مهم‌ترین تفاوت بین پردازنده‌های ٦٤ بیتی با ۳۲ بیتی در پشتیبانی از حافظه‌ی رم بالاتر است. اما تفاوت‌های دیگری نیز وجود دارد:

- مدیریت حافظه در پردازنده‌های ٦٤ بیتی بهتر از ۳۲ بیتی است. پردازنده‌های ۳۲ بیتی قادر نیستند فایل‌های حجیم و بزرگ‌تر از ٤ گیگابایت را به سادگی آدرس دهی کنند و تنها بخشی از فایل را به اصطلاح در حافظه «مپ» می‌کنند.

- نرم‌افزارهای خاص مانند آن‌هایی که به رمزگذاری یا رمزگشایی محتوا می‌پردازند می‌توانند از آدرس دهی بهتر پردازنده‌ی ٦٤ بیتی بهره برده و با سرعت بیشتری امور مورد نظر خود را انجام دهند. مثلا برنامه‌های رندر سه بعدی یا ویرایش ویدیو می‌تواند بازده به مراتب بالاتری را در پردازنده‌های ٦٤ بیتی داشته باشند.
- در برخی از امور پردازنده مجبور است مرتبا مقادیر مورد نظر خود را از حافظه خوانده و رجیستر کند، به همین دلیل شاید انجام یک کار مشخص در پردازنده‌ی ٣٢ بیتی به چند سیکل در CPU نیاز داشته باشد، اما همان تسک در یک پردازنده‌ی ٦٤ بیتی به دلیل دسترسی وسیع‌تر به حافظه در سیکل‌های کمتری انجام شود. در واقع پردازنده‌های ٦٤ بیتی قادر هستند تا آدرس دهی وسیع‌تری را در حافظه داشته باشند و با حجم به مراتب بالاتری از اطلاعات در اپلیکیشن‌ها کار کنند. این موضوع در نرم‌افزارهایی همچون ویرایش ویدیو، محاسبات سنگین ریاضی، دیتابیس‌های بزرگ و مواردی از این دست به خوبی خود را نشان می‌دهد.

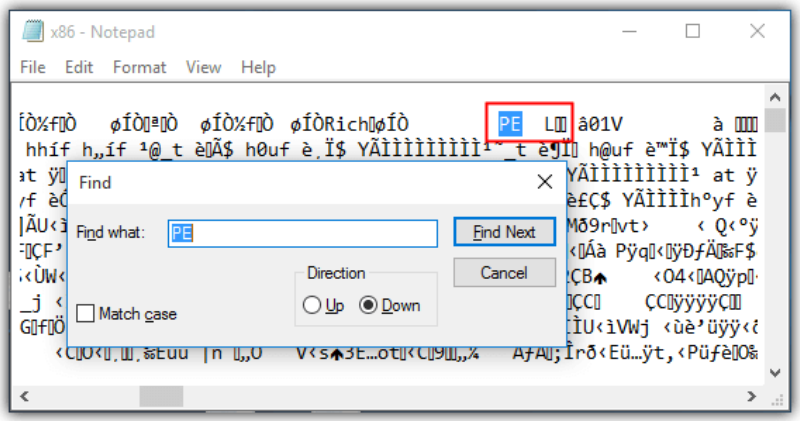
٤- تشخیص فایل PE ٣٢ بیتی و ٦٤ بیتی از ساختار آن

برای تشخیص اینکه یک نرم افزار کاربردی و یا یک فایل با فرمت exe. برای اجرا بر روی سیستم های ٣٢ بیتی ساخته شده است و یا ٦٤ بیتی، روش های گوناگونی وجود دارد. این مسئله با توجه با ساختار فایل PE قابل شناسایی خواهد بود. سه روش مختلف برای این تشخیص این فایل ها را شرح می دهیم:

٤-١- ویرایشگر متن

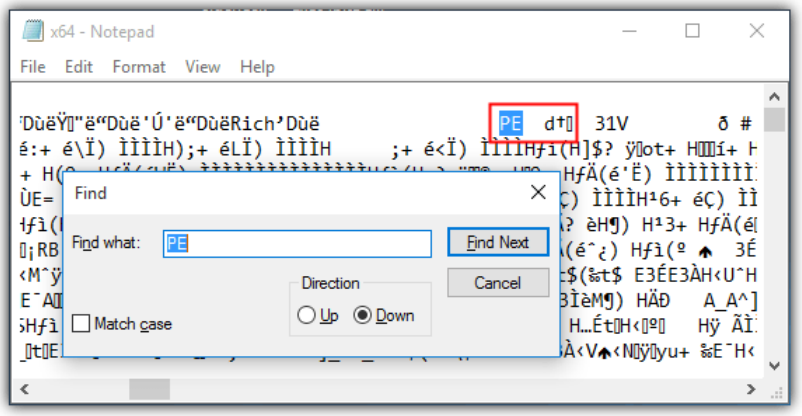
در صورتی که یک فایل با فرمت exe. را در یک ویرایشگر متن مانند notepad یا notepad++ باز کنیم، با تعداد بسیار زیادی از کاراکترهای ناشناخته و در هم ریخته مواجه خواهیم شد که معنی خاصی نیز ندارند. در این متن کلمه "PE" را جستجو خواهیم کرد.

بعد از یافتن آن، به کاراکتر های بعدی دقت می کنیم. اگر اولین کاراکتر قابل تشخیص بعد از کلمه ی "PE" ، کاراکتر "L" باشد می توان گفت که فایل مورد نظر دارای ساختار ۳۲ بیتی است.



شکل ۱ – ساختار یک فایل *PE* ۳۲ بیتی در *Notepad*

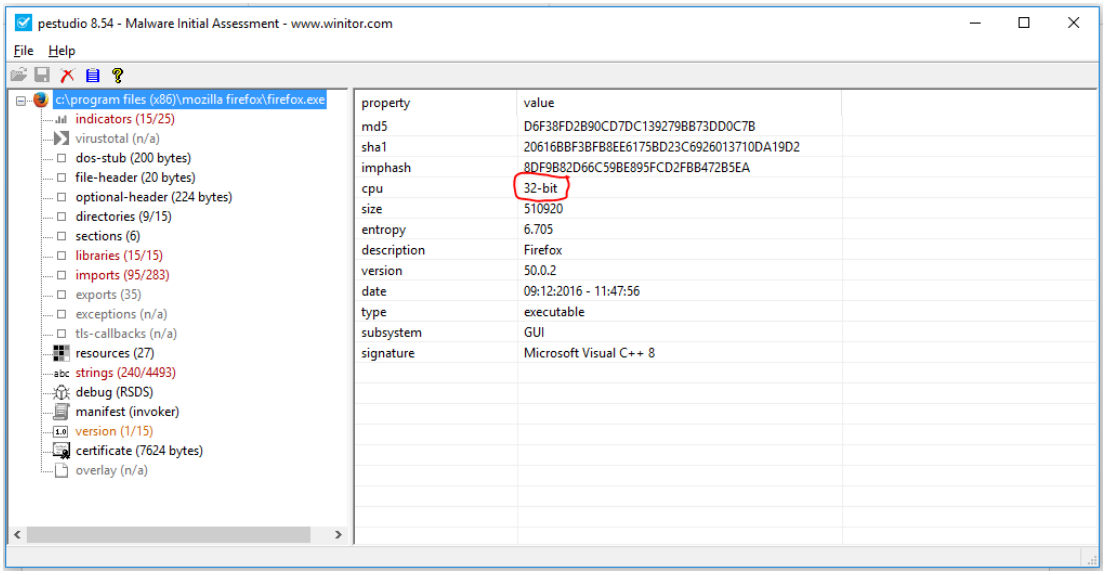
حال اگر اولین کاراکتر قابل تشخیص بعد از کلمه ی "PE" ، کاراکتر "d" و پس از آن نماد "†" باشد می توان گفت که فایل مورد نظر دارای ساختار ٦٤ بیتی است.



شکل ۲ – ساختار یک فایل *PE* ٦٤ بیتی در *Notepad*

٤-٢- ابزار PE Studio

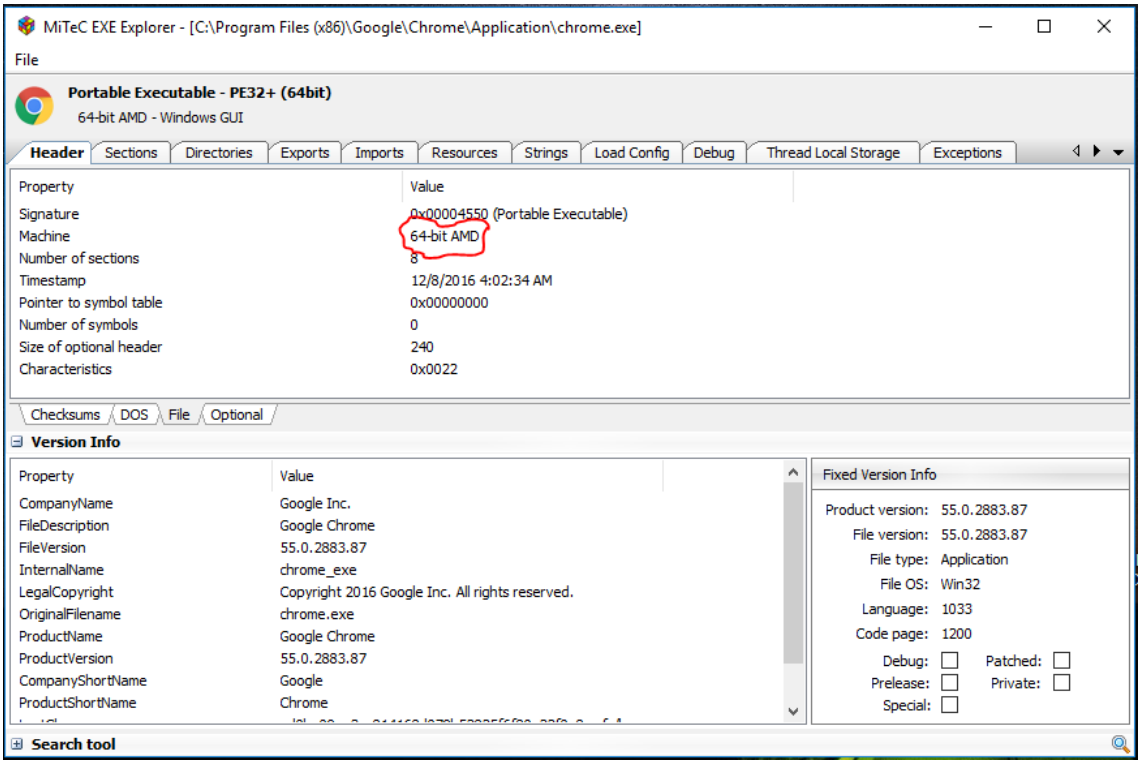
این نرم افزار برای شناسـایی و ارزیابی اولیه تروجان ها طراحی شده است. به کمک آن می توان ساختار برخی از فایل های exe. (نه همه) را مورد بررسی قرار داد. به کمک این ابزار به راحتی می توان ٣٢ و یا ٦٤ بیتی بودن فایل را تشخیص داد. در شکل زیر خروجی این ابزار را بر روی مرورگر FireFox (firefox.exe) مشاهده می کنید.



شکل ٣ – خروجی ابزار *PE Studio* بر روی فایل *firefox.exe*

٤-٣- ابزار MiTeC EXE Explorer

این ابزار نیز همانند ابزار PE Studio، یک فایل اجرایی را به عنوان ورودی دریافت کرده و اطلاعات زیادی در مورد ساختار و ویژگی های آن در اختیار می گذارد. خروجی این ابزار بر روی فایل chrome.exe را مشاهده می کنیم:



شکل ٤ – خروجی ابزار *MiTeC EXE Explorer* بر روی فایل *chrome.exe*

۵- فهرست منابع

www.zoomit.ir

www.computerhope.com

www.en.wikipedia.org

www.raymond.cc