



Scam Email

دانشگاه فردوسی مشهد

مرکز فناوری اطلاعات و ارتباطات دانشگاه

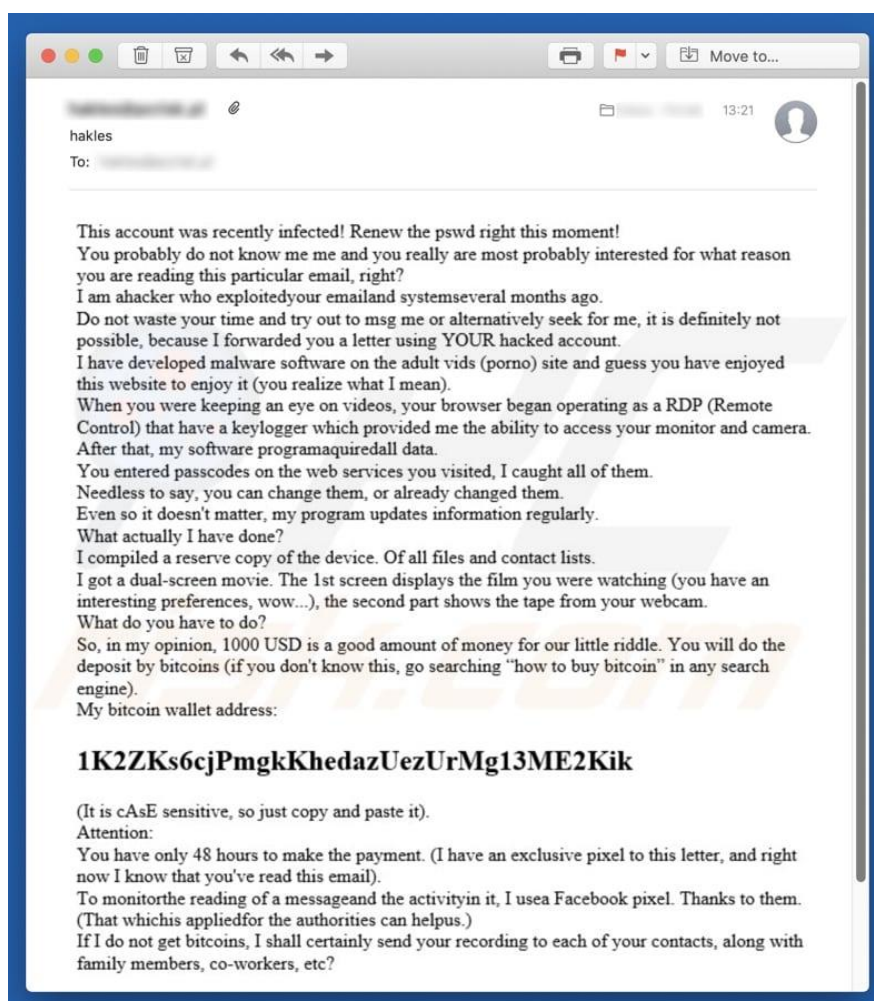
بهار 1398

Scam چیست؟

Scam به فعالیت های غیرقانونی در سطح اینترنت گفته می شود که به منجر به کلاهبرداری از افراد و کاربران می شود. Scam ها اشکال مختلفی در دنیای دیجیتال دارند و اگر کاربران به آنها توجه نکنند می تواند منجر به خساراتی مانند دزدیدن پول و یا از دست دادن اطلاعات شخصی افراد شود. فرستندگان Scam از تلفن، ایمیل، پیامک و خدمات پستی برای برای تماس با مردم استفاده می کنند.

نمونه ای از ایمیل Scam با موضوع "این حساب کاربری آلوده شده است."

این نمونه ای از ایمیل Scam است که با عنوان "آلوده شدن حساب کاربری" برای شناسه های مختلف ارسال می شود و Scammer ها امیدوارند که بتوانند از این طریق افراد را فریب دهند. این ایمیل در واقع ادعا می کند که از قربانی خود یک سری تصاویر ضبط شده تهیه کرده که در صورت عدم پرداخت مبلغ خاصی آنها را انتشار می دهند.



همانطور که در متن این نامه ملاحظه می کنید، طراح این کلاهبرداری خود را به عنوان یک هکر معرفی می کند که ظاهراً ایمیل کاربر را هک کرده است. این کلاهبردار ادعا می کند که او یک برنامه مخرب را در سیستم عامل نصب کرده است که وب کم هک شده و از صفحه اسکرین فرد قربانی در حال بازدید از یک وب سایت

پورنوگرافی فیلم گرفته است. این نرم افزار مخرب که یک Keylogger است قادر به نظارت بر فعالیت های کامپیوتری کاربران و ضبط فیلم ها با استفاده از وب کم کامپیوتر می باشد. این برنامه همچنین می تواند، رمزهای عبور مختلف را سرقت کند.

نکته اصلی این ایمیل این است با فریب دادن مردم به اعتقاد بر این که فیلمی از آنها ضبط شده است، مورد استفاده قرار می دهد. کلاهبردار ادعا می کند که یک ویدیویی تهیه کرده است که فرد قربانی و ویدیویی که او تماشا می کند، به طور همزمان دیده شوند. این مهاجمان تهدید می کنند که این فیلم را به تمام مخاطبین فرد قربانی ارسال خواهند کرد، مگر اینکه در عرض 48 ساعت (1000 دلار) در Bitcoins دریافت کنند و در نامه نیز یک آدرس پولی Bitcoin ارائه کرده اند.

نکته ای که باید مورد توجه قرار دهید این است که این گونه ایمیلها را نادیده بگیرید. هیچ یک از ادعاهایی که Scammer بیان کرده است، قابل اعتماد نیست. سیستم شما با نرم افزارهای مخرب آلوده نشده و شناسه ایمیل نیز هک نشده است.

خلاصه از تهدید	
نام یا عنوان	این شناسه ایمیل آلوده شده است
نوع تهدید	فیشینگ، کلاهبرداری، مهندسی اجتماعی، تقلب
علائم	خرید های آنلاین غیر مجاز، گذرواژه های حساب کاربری آنلاین، سرقت هویت، دسترسی غیر قانونی از رایانه شخصی
روش های توزیع	ایمیل های فریبنده، تبلیغات پاپ آپ آنلاین، موتورهای جستجوگر مسموم، دامنه های اشتباه گرفته شده
خسارت	از دست دادن اطلاعات خصوصی حساس، از دست دادن پول، سرقت هویت.
روش حذف	برای از بین بردن عواقب احتمالی نرم افزار مخرب، اسکن کردن سیستم با Spyhunter توصیه می شود.

به طور معمول، Scammer ها از این ایمیل ها برای تهیه تهدیدهای مختلف از مردم استفاده می کنند. آنها معمولاً ادعا می کنند که یک ویدیو را ضبط کرده اند و تهدید می کنند که آن را توزیع خواهند کرد. توجه داشته باشید که ایمیلهایی مانند "حساب کاربری شما هک شده است" فقط نمونه ای از ایمیل های Scam است. متأسفانه، مجرمان اینترنتی همچنین ایمیل هایی را ارسال می کنند که دارای پیوست های مخرب هستند. این گونه ایمیلها منجر به آلوده شدن کامپیوترها را با برنامه های مخرب مانند Emotet، TrickBot، LokiBot، AZORult، Adwind و غیره می شوند. آنها ایمیلهایی را ارسال می کنند که حاوی لینک های وب یا فایل های پیوست مانند اسناد مایکروسافت آفیس یا PDF، فایل های جاوا اسکریپت، بایگانی ZIP، RAR،

فایل های اجرا شده (.exe) و غیره هستند. هدف اصلی این ایمیل ها این است که افراد را فریب دهد تا فایل پیوست را باز کنند. هنگام باز شدن، برنامه های مخربی را دانلود و نصب می کنند. این برنامه های مخرب برای سرقت اطلاعات شخصی، اطلاعات مربوط به مرورگر، انتشار ویروس ها و انجام اقدامات دیگر است که می تواند منجر به از دست رفتن اطلاعات، مسائل مربوط به حریم خصوصی و سایر مشکلات شود.

جلوگیری از نصب نرم افزارهای مخرب یا malware چگونه است؟

هر ایمیل را به دقت بررسی کنید، به خصوص اگر آن ایمیل حاوی پیوست یا لینک باشد. این ایمیل ها معمولاً با عنوان رسمی و قانونی ارائه می شوند اما اغلب بی اهمیتند. اگر یک ایمیل به نظر مشکوک یا از یک آدرس ناشناس دریافت کردید، آن را باز نکنید. علاوه بر این، نرم افزارها را از منابع معتبر دانلود نمایید. برای حفظ امنیت رایانه، نرم افزار آنتی ویروس معتبر بر روی سیستم نصب شده و همیشه فعال باشد.

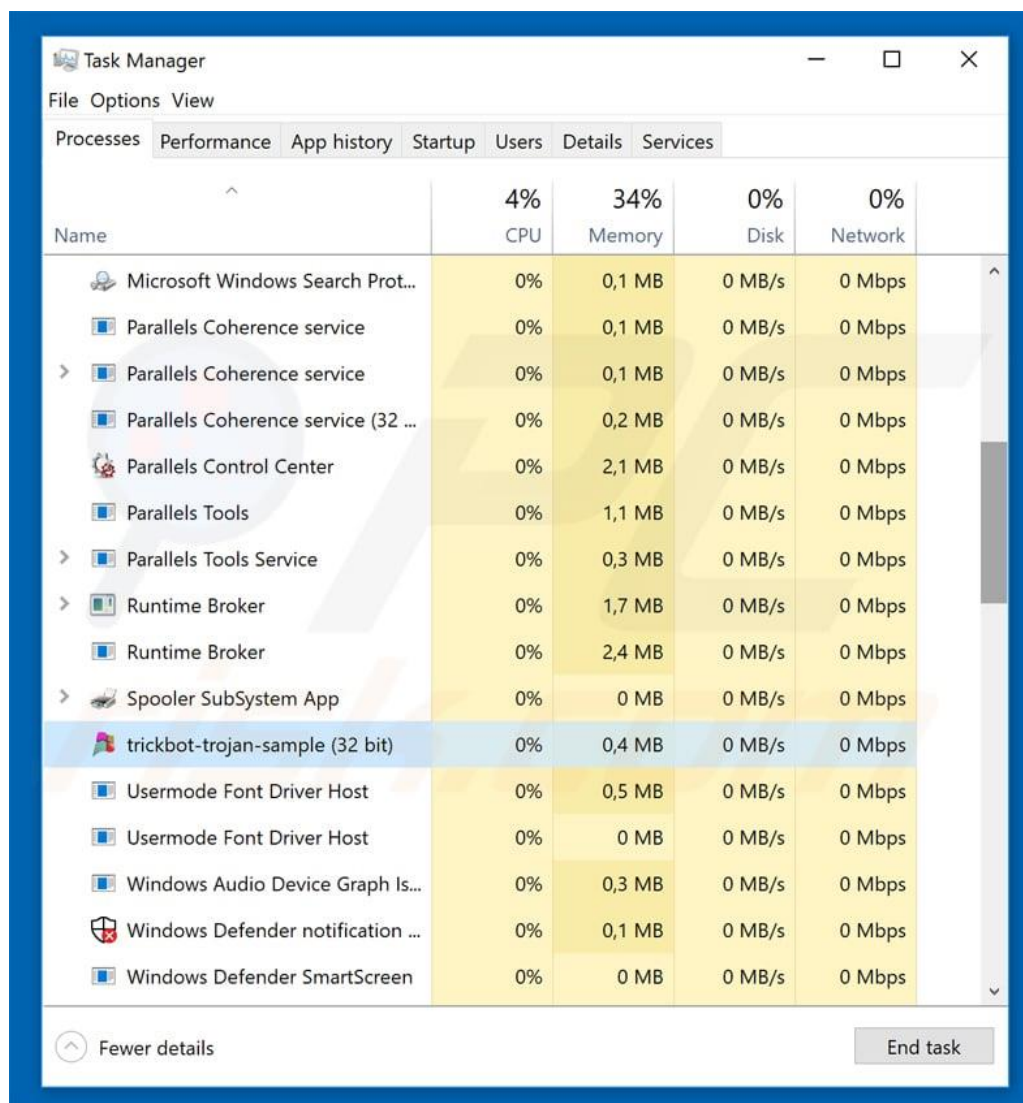
حذف برنامه های مخرب برای جلوگیری از عواقب احتمالی

حذف دستی بدافزارهای ممکن است یک روند طولانی و پیچیده باشد که نیاز به مهارت های پیشرفته کامپیوتری دارد. Spyhunter یک ابزار حرفه ای حذف نرم افزارهای مخرب است که برای از بین بردن برنامه های مخرب توصیه می شود و دانلود آن را از طریق لینک زیر امکان پذیر است:

<https://www.pcrisk.com/download-spyhunter-5>

نحوه حذف نرم افزارهای مخرب چگونه است؟

برای حذف بدافزارها استفاده از Spyhunter توصیه می شود. اگر می خواهید بدافزار را به صورت دستی حذف کنید، اولین گام این است که نام نرم افزارهای مخرب را که می خواهید حذف کنید شناسایی کنید. در ادامه یک مثال از یک برنامه مشکوک در حال اجرا بر روی یک کامپیوتر کاربر آمده است:

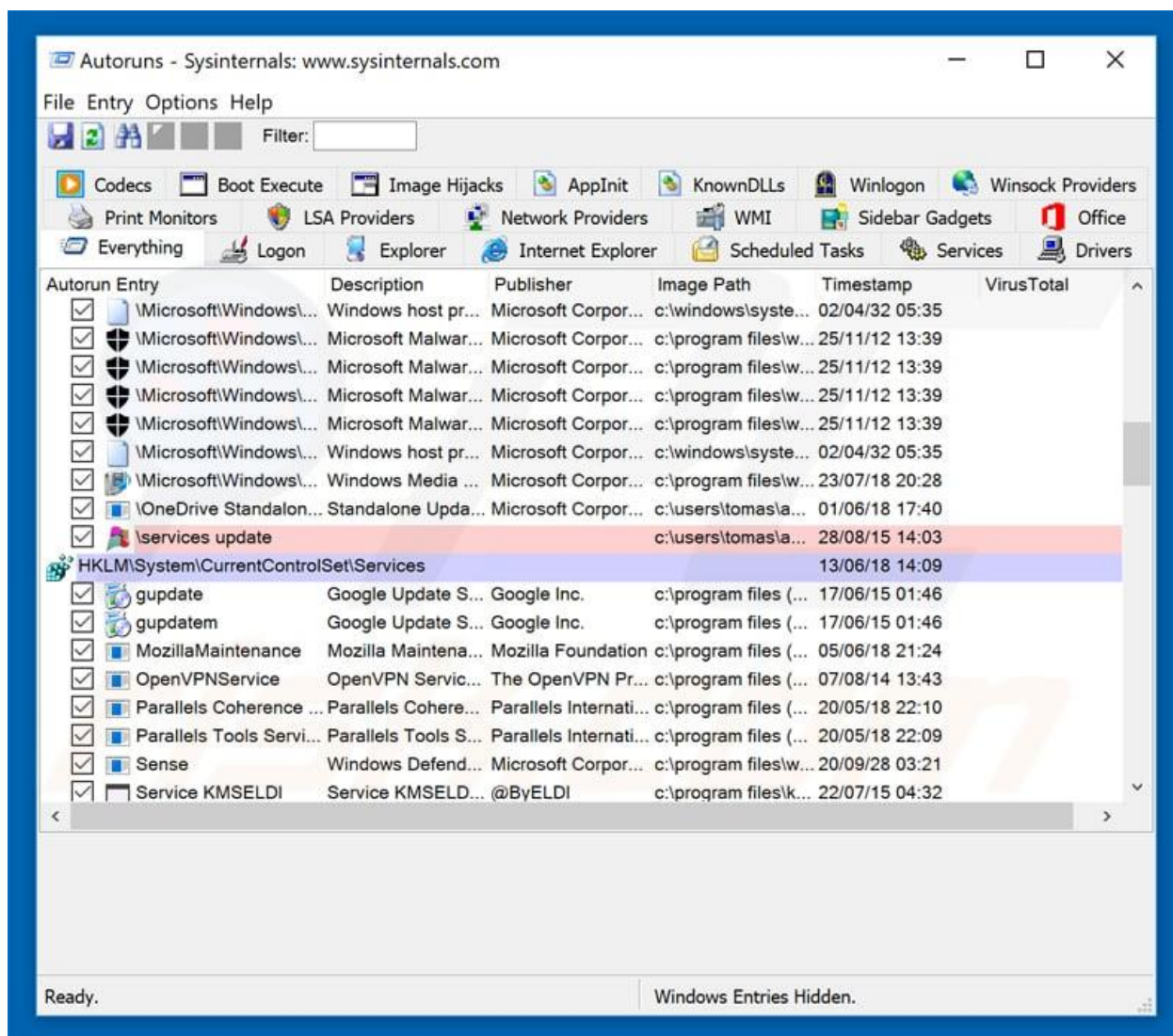


با استفاده از Task Manager لیست برنامه های در حال اجرا بر روی رایانه خود را چک کنید، سپس مراحل زیر را ادامه دهید:

مرحله 1:

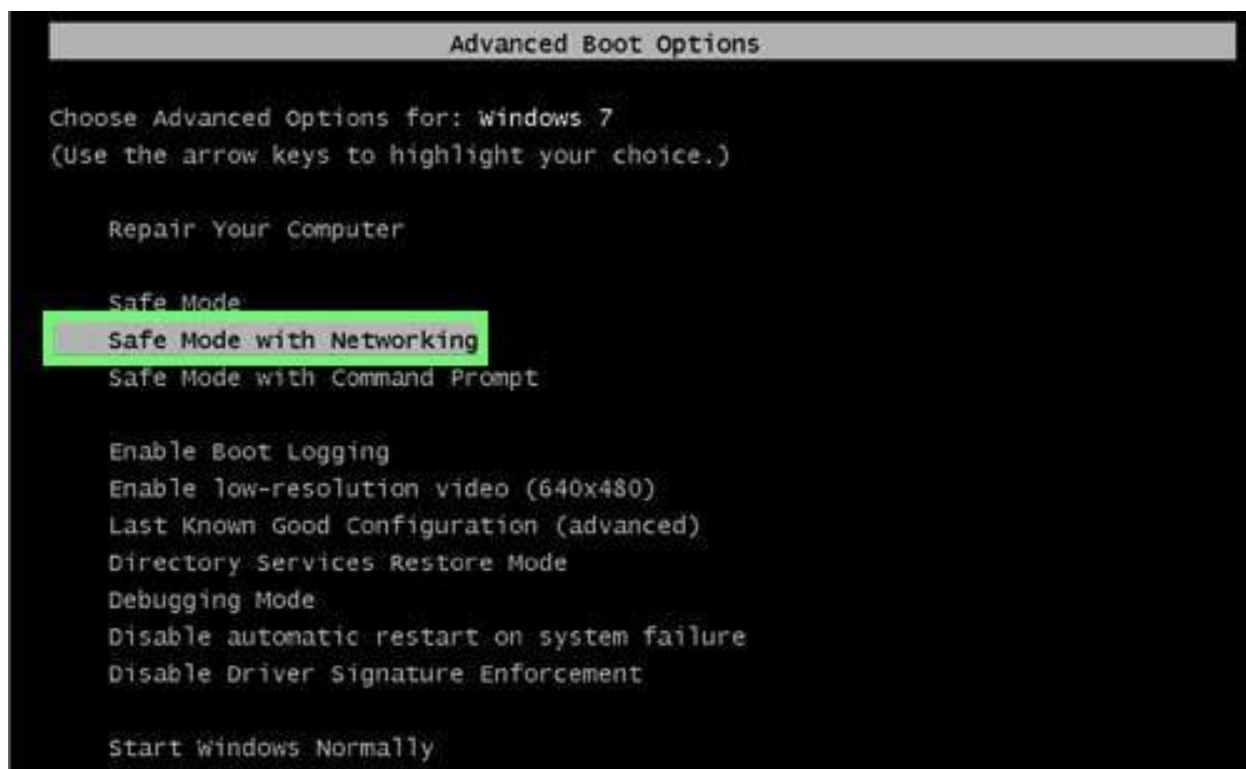
دانلود برنامه‌ای با نام Autoruns این برنامه، لیست تمام برنامه های نصب شده در سیستم و رجیستری را نشان می دهد :

(لینک نرم افزار <https://docs.microsoft.com/en-us/sysinternals/downloads/autoruns>)



مرحله 2:

کامپیوتر خود را در حالت Safe Mode راه اندازی مجدد کنید.



کاربران ویندوز XP و ویندوز 7:

کامپیوتر خود را در حالت Safe Mode راه اندازی کنید. سپس مجدد سیستم را Restart کنید. در طول فرایند شروع به کار کامپیوتر خود، کلید F8 را بر روی صفحه کلید خود چند بار فشار دهید تا منوی Windows Advanced Option را مشاهده کنید و در نهایت Safe Mode with Networking را از لیست انتخاب نمایید.

کاربران ویندوز 8:

سیستم را در حالت Safe Mode راه اندازی نمایید. از منوی Settings گزینه Advanced startup options را انتخاب نمایید. در پنجره "General PC Settings" باز شده، "Advanced startup" را انتخاب کنید. روی دکمه "Restart now" کلیک کنید. در حال حاضر رایانه شما به حالت "Advanced Startup options menu" راه اندازی مجدد خواهد شد. روی دکمه "Troubleshoot" کلیک کنید و سپس دکمه "Advanced options" را انتخاب کنید. در صفحه advanced option و تب «Startup settings» رفته و سیستم را Restart کنید. سیستم شما به صفحه تنظیمات راه اندازی مجدد خواهد رفت. دکمه F5 را بزنید تا سیستم در حالت امن با شبکه راه اندازی شود.

Startup Settings

Press a number to choose from the options below:

Use number keys or functions keys F1-F9.

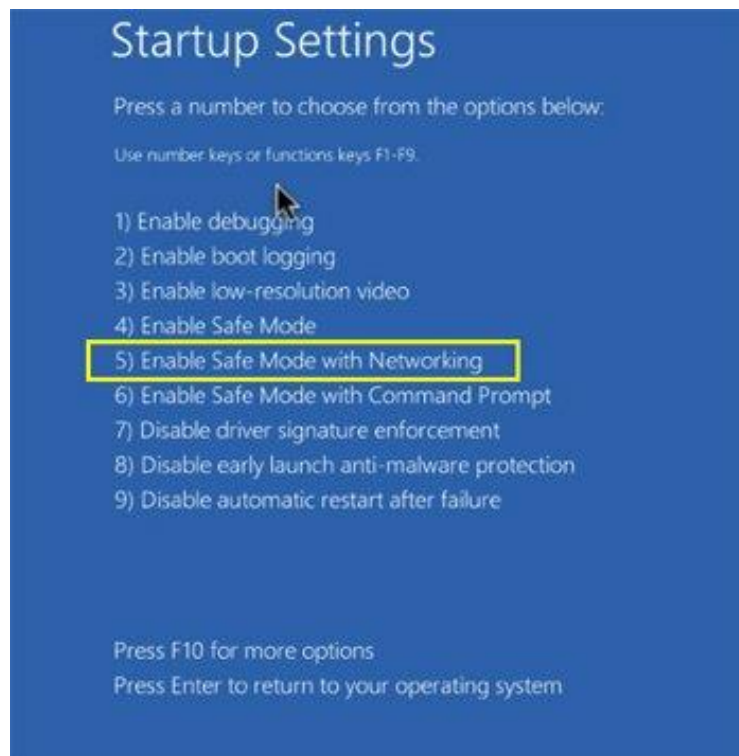
- 1) Enable debugging
- 2) Enable boot logging
- 3) Enable low-resolution video
- 4) Enable Safe Mode
- 5) Enable Safe Mode with Networking
- 6) Enable Safe Mode with Command Prompt
- 7) Disable driver signature enforcement
- 8) Disable early launch anti-malware protection
- 9) Disable automatic restart after failure

Press F10 for more options

Press Enter to return to your operating system

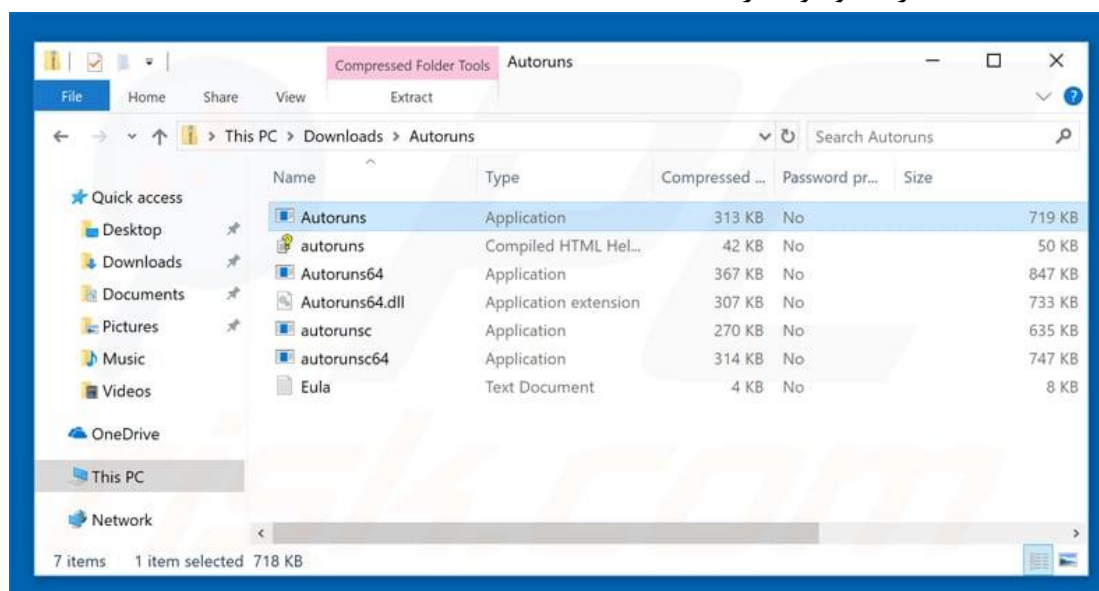
کاربران ویندوز 10:

سیستم را Restart کنید و دکمه Shift را روی صفحه کلید خود نگه دارید. در گزینه "choose an option" بر روی "Troubleshoot" کلیک کنید، بعد "Advanced options" را انتخاب نمایید. سپس "Startup Settings" را انتخاب کرده و سیستم را Restart کنید. در نهایت مطابق شکل زیر سیستم خود را در حالت امن با شبکه راه اندازی کنید.



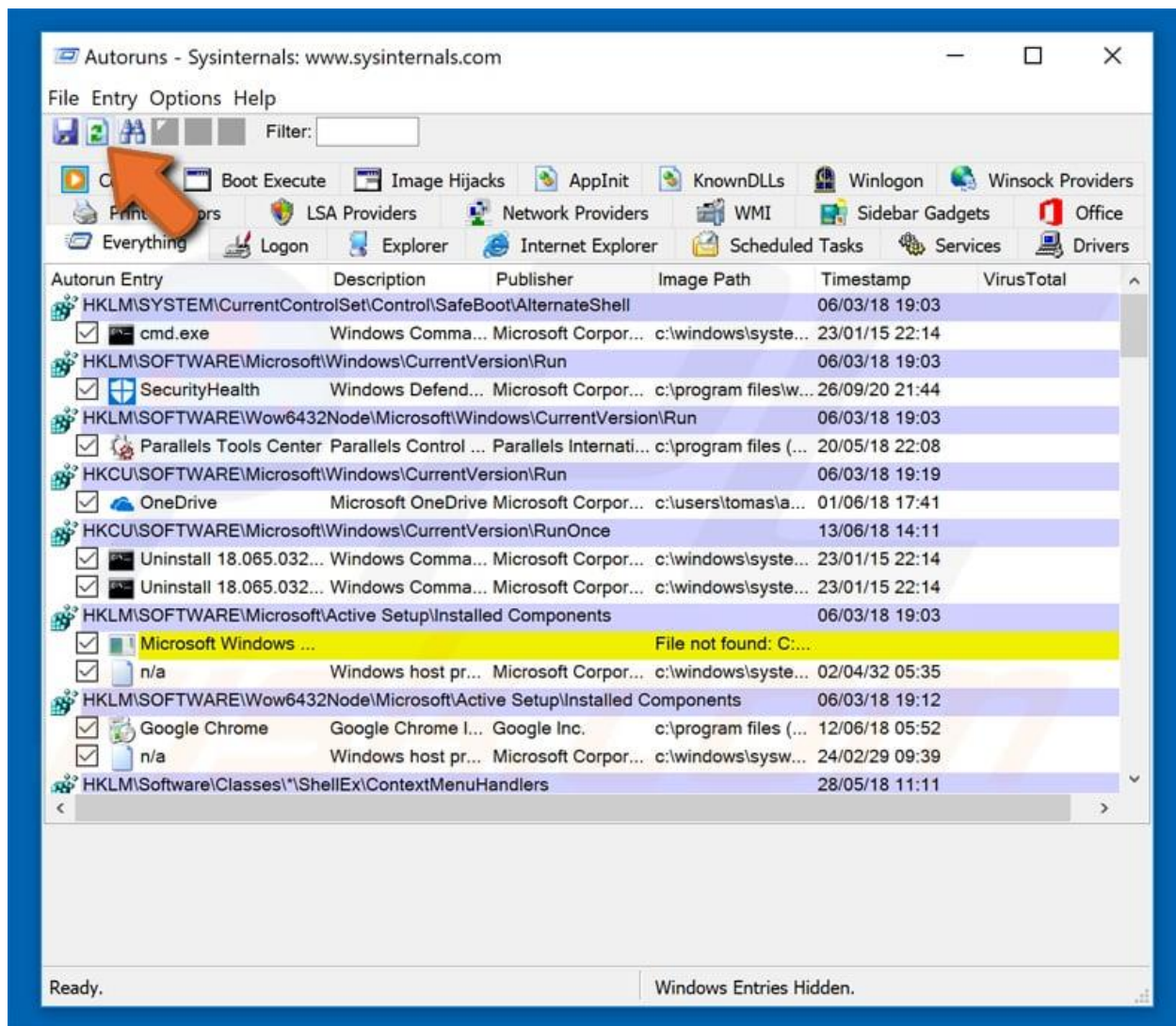
مرحله 3:

فایل Autoruns.exe را دانلود و اجرا کنید.



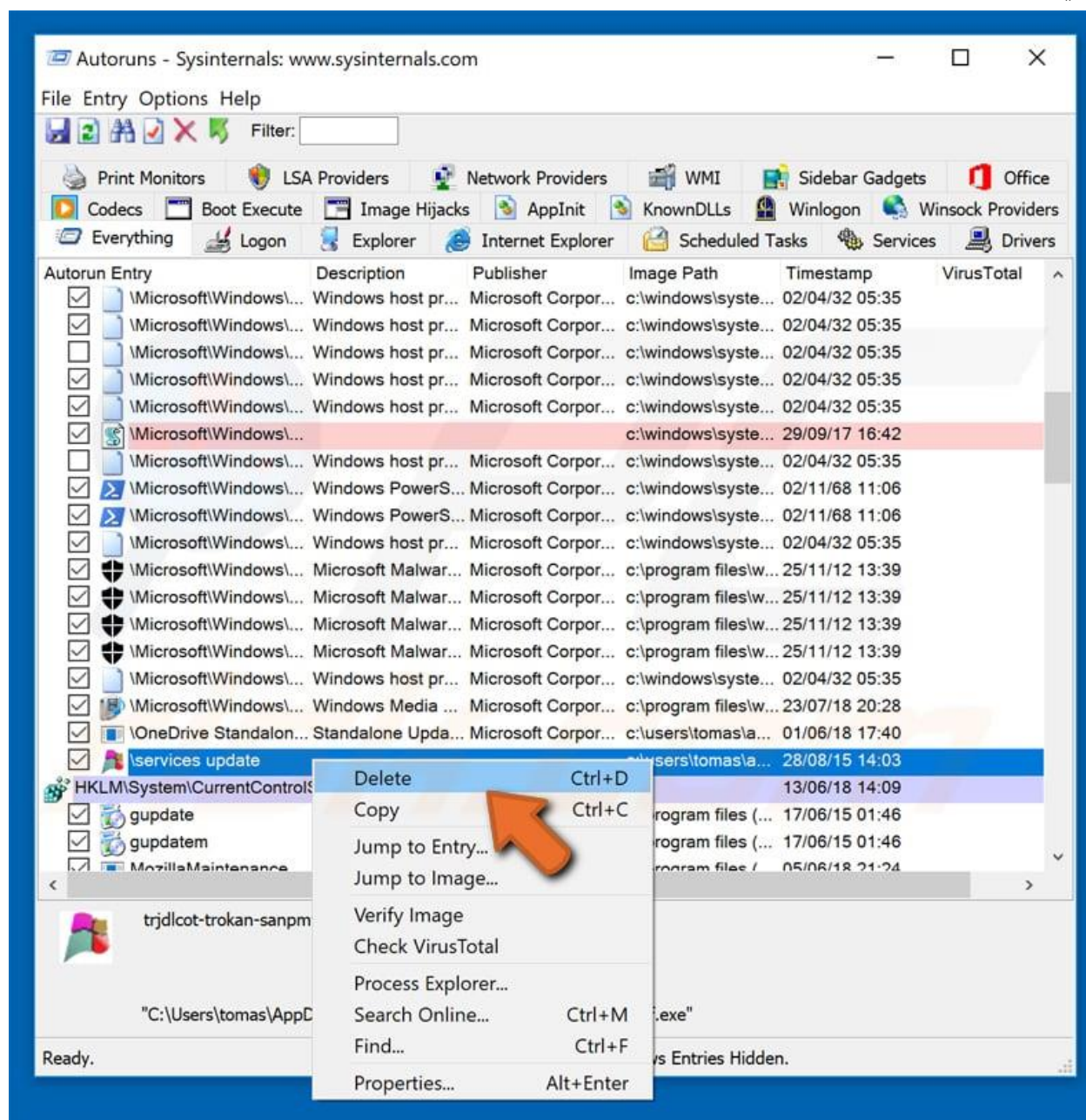
مرحله 4:

در برنامه Autoruns بر روی گزینه "Options" در بالای صفحه کلیک کنید و گزینه "Hide Empty Locations" و "Hide Windows Entries" را علامت بزنید. پس از این روش، روی "Refresh" کلیک کنید.

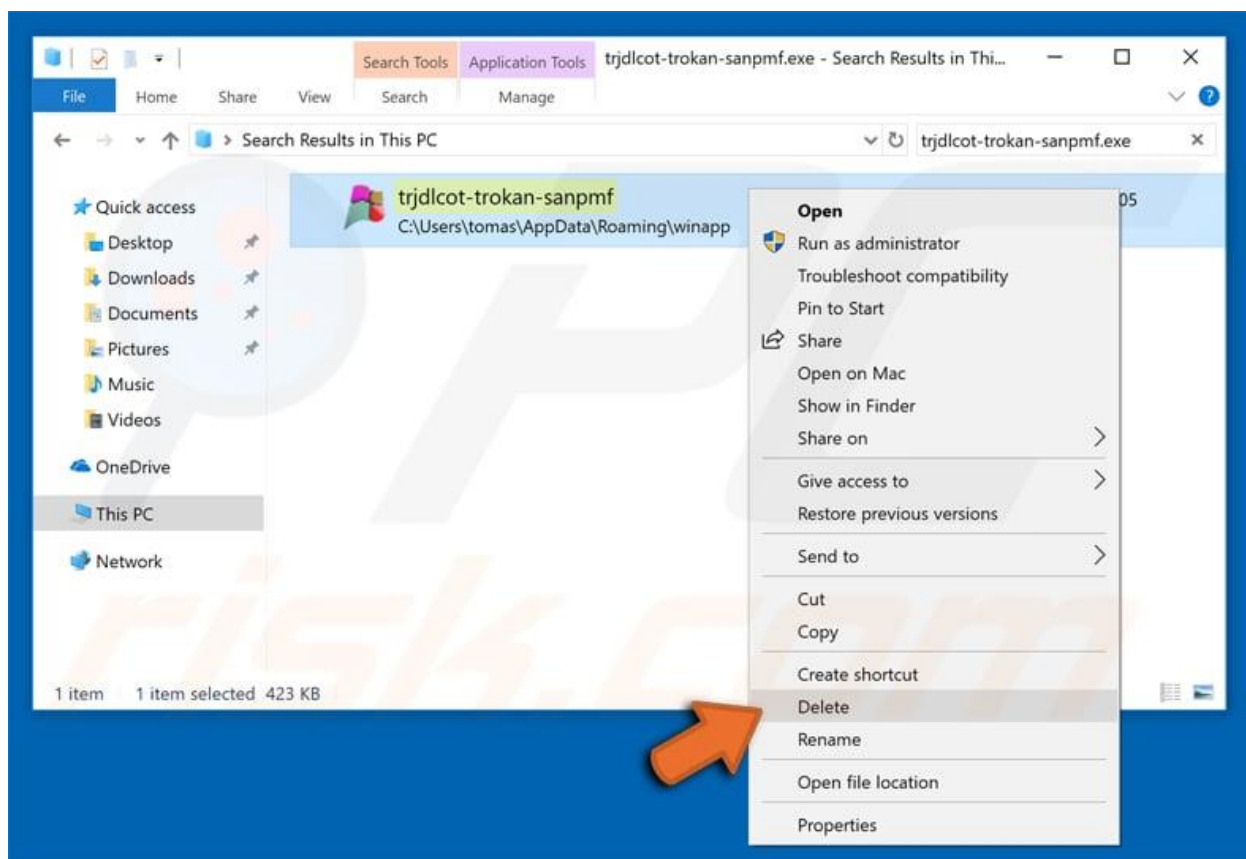


مرحله 5:

لیست ارائه شده توسط نرم افزار Autoruns را بررسی کنید و فایل بدافزاری را که می خواهید از بین ببرد پیدا کنید.



پس از حذف نرم افزارهای مخرب از طریق نرم افزار Autoruns (این امر تضمین می کند که نرم افزارهای مخرب در راه اندازی بعدی سیستم اجرا نمی شوند)، شما باید نام بدافزار را در رایانه خود جستجو کرده و آن را حذف کنید.



کامپیوتر خود را در حالت عادی راهاندازی کنید. برای اطمینان از اینکه کامپیوتر شما فاقد نرم افزارهای مخرب است، مجدد سیستم را با Spyhunter اسکن نمایید.