Scam Email

دانشگاه فردوسی مشهد

مرکز فناوری اطلاعات و ارتباطات دانشگاه

بهار 1398

Scam چیست؟

Scam به فعالیت های غیرقانونی در سطح اینترنت گفته می‌شود که به منجر به کلاهبرداری از افراد و کاربران می‌شود. Scamها اشکال مختلفی در دنیای دیجیتال دارند و اگر کاربران به آنها توجه نکنند می‌تواند 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 می‌کنند.

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 می‌کند که از قربانی خود یک سری تصاویر ضبط شده تهیه کرده که در صورت عدم پرداخت مبلغ خاصی آنها را انتشار می‌دهند.

Move to...

hakles

To:

This account was recently infected! Renew the pswd right this moment!
You probably do not know me me and you really are most probably interested for what reason you are reading this particular email, right?
I am ahacker who exploitedyour emailand systemseveral months ago.
Do not waste your time and try out to msg me or alternatively seek for me, it is definitely not possible, because I forwarded you a letter using YOUR hacked account.
I have developed malware software on the adult vids (porno) site and guess you have enjoyed this website to enjoy it (you realize what I mean).
When you were keeping an eye on videos, your browser began operating as a RDP (Remote Control) that have a keylogger which provided me the ability to access your monitor and camera.
After that, my software programaquiredall data.
You entered passcodes on the web services you visited, I caught all of them.
Needless to say, you can change them, or already changed them.
Even so it doesn't matter, my program updates information regularly.
What actually I have done?
I compiled a reserve copy of the device. Of all files and contact lists.
I got a dual-screen movie. The 1st screen displays the film you were watching (you have an interesting preferences, wow...), the second part shows the tape from your webcam.
What do you have to do?
So, in my opinion, 1000 USD is a good amount of money for our little riddle. You will do the deposit by bitcoins (if you don't know this, go searching "how to buy bitcoin" in any search engine).
My bitcoin wallet address:

1K2ZKs6cjPmgkKhedazUezUrMg13ME2Kik

(It is cAsE sensitive, so just copy and paste it).
Attention:
You have only 48 hours to make the payment. (I have an exclusive pixel to this letter, and right now I know that you've read this email).
To monitorthe reading of a messageand the activityin it, I usea Facebook pixel. Thanks to them. (That whichis appliedfor the authorities can helpus.)
If I do not get bitcoins, I shall certainly send your recording to each of your contacts, along with family members, co-workers, etc?

همانطور که در متن این نامه ملاحظه می‌کنید، طراح این کلاهبرداری خود را به عنوان یک هکر معرفی می‌کند که ظاهرا ایمیل کاربر را هک کرده است. این کلاهبردار ادعا می‌کند 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 می‌تواند، 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 می‌دهد. کلاهبردار ادعا می‌کند که یک ویدیویی تهیه کرده است که فرد قربانی و ویدیویی که او تماشا می کند، به طور همزمان دیده شوند. این مهاجمان تهدید می‌کنند 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 کرده‌اند.

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 نرم‌افزار 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 می‌کنند. آنها معمولا ادعا می‌کنند که یک ویدیو را ضبط کرده‌اند و تهدید می‌کنند که آن را توزیع خواهند کرد. توجه داشته باشید که ایمیلهایی مانند "حساب کاربری شما هک شده است" فقط نمونه‌ای از ایمیل های Scam است. متاسفانه، مجرمان اینترنتی همچنین ایمیل هایی را ارسال می‌کنند که دارای پیوست‌های مخرب هستند. این گونه ایمیلها منجر به آلوده شدن کامپیوترها را با برنامه های مخرب مانند LokiBot ، TrickBot، Emotet، AZORult، Adwind و غیره می‌شوند. آنها ایمیلهایی را ارسال می‌کنند که حاوی لینک های وب یا فایل های پیوست مانند اسناد مایکروسافت آفیس یا PDF ، فایل های جاوا اسکریپت، بایگانی مانندZIP ، 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 می‌کنند. 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؟

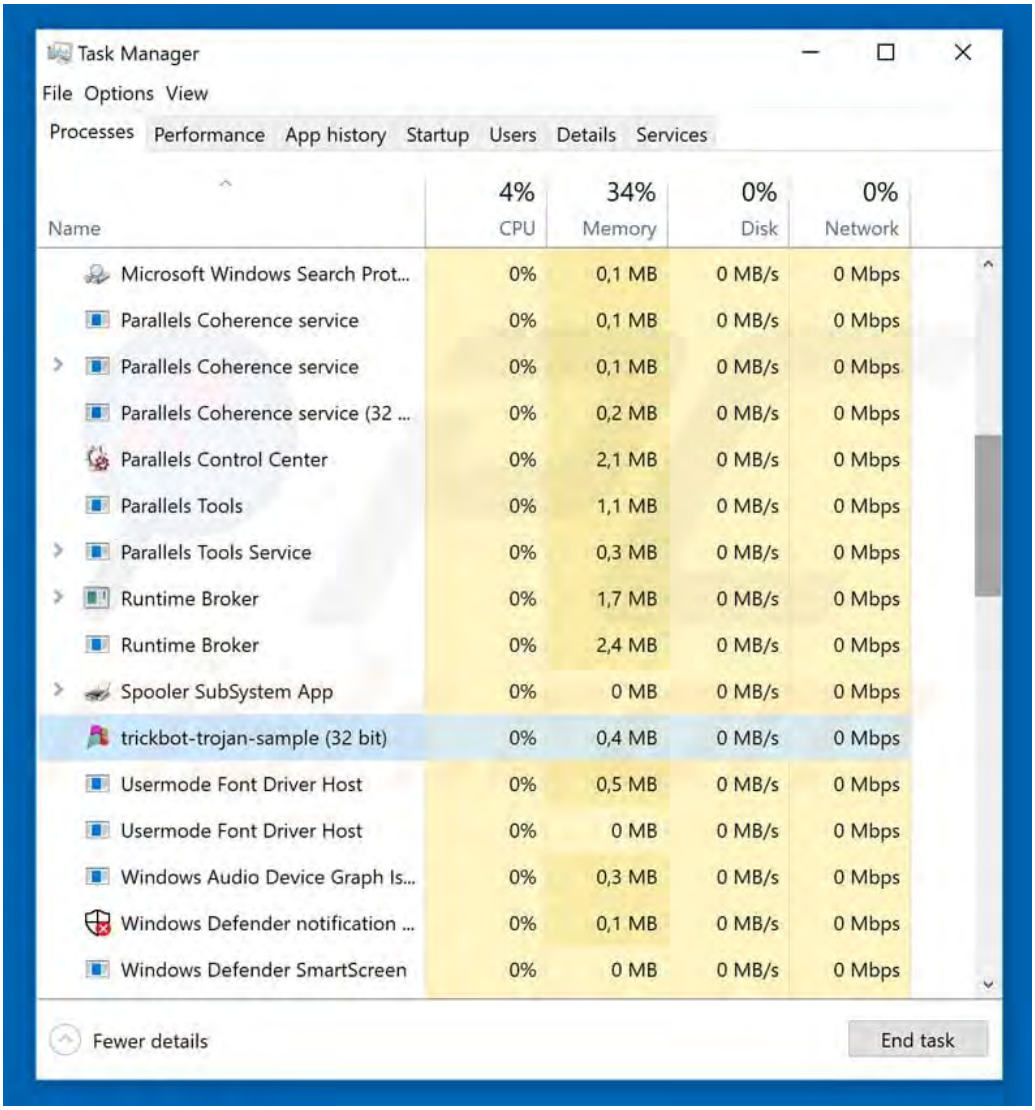
هر ایمیل را به دقت بررسی کنید، به خصوص اگر آن ایمیل حاوی پیوست یا لینک باشد. این ایمیل ها معمولا با عنوان رسمی و قانونی ارائه می شوند اما اغلب بی اهمیتند. اگر یک ایمیل به نظر مشکوک یا از یک آدرس ناشناس دریافت کردید، آن را باز نکنید. علاوه بر این، نرم افزارها را از منابع معتبر دانلود نمایید. برای حفظ 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 می‌شود. 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:

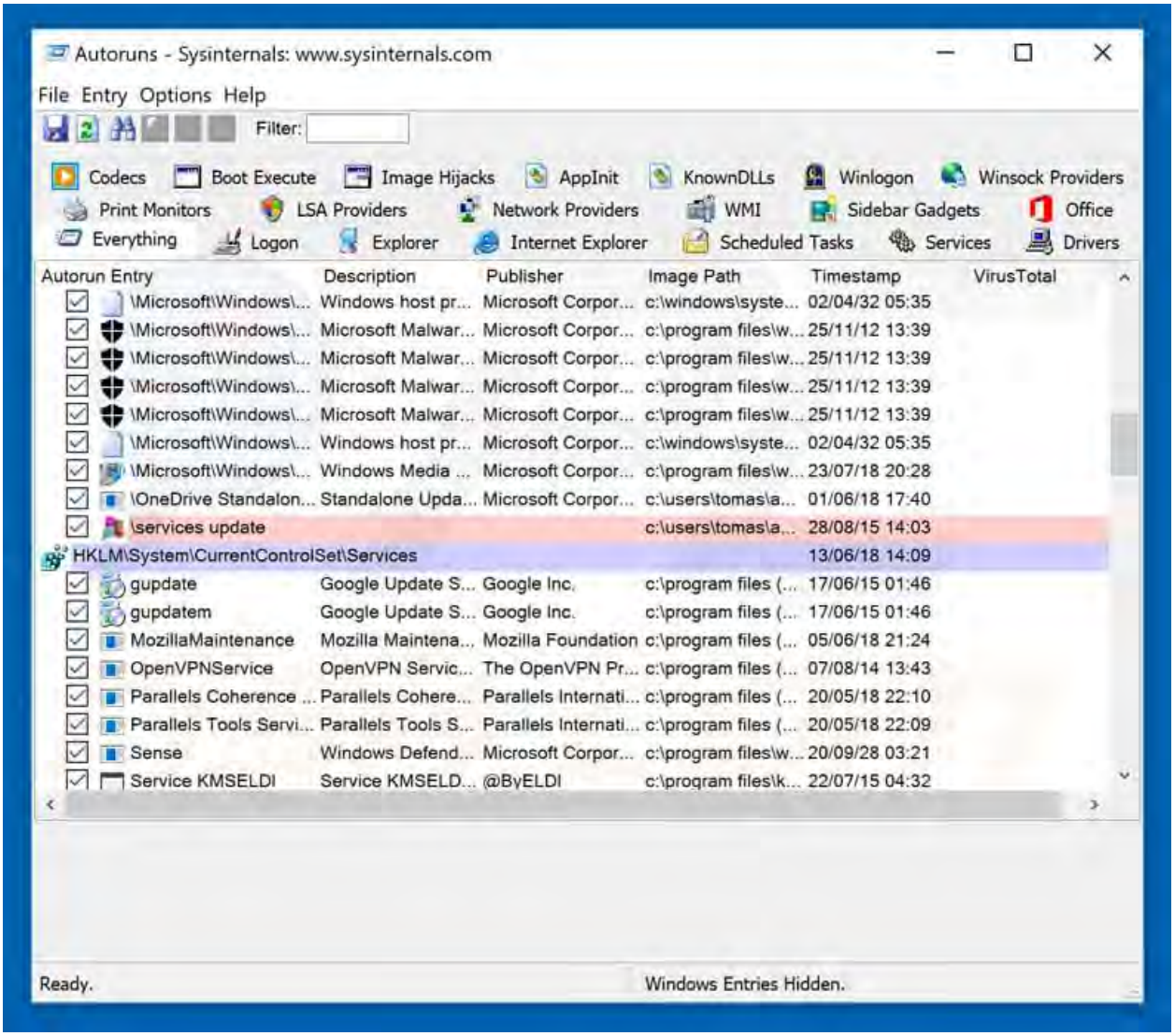


با استفاده از Task Manager لیست برنامه های در حال اجرا بر روی رایانه خود را چک کنید، سپس مراحل زیر را ادامه دهید:

مرحله 1:

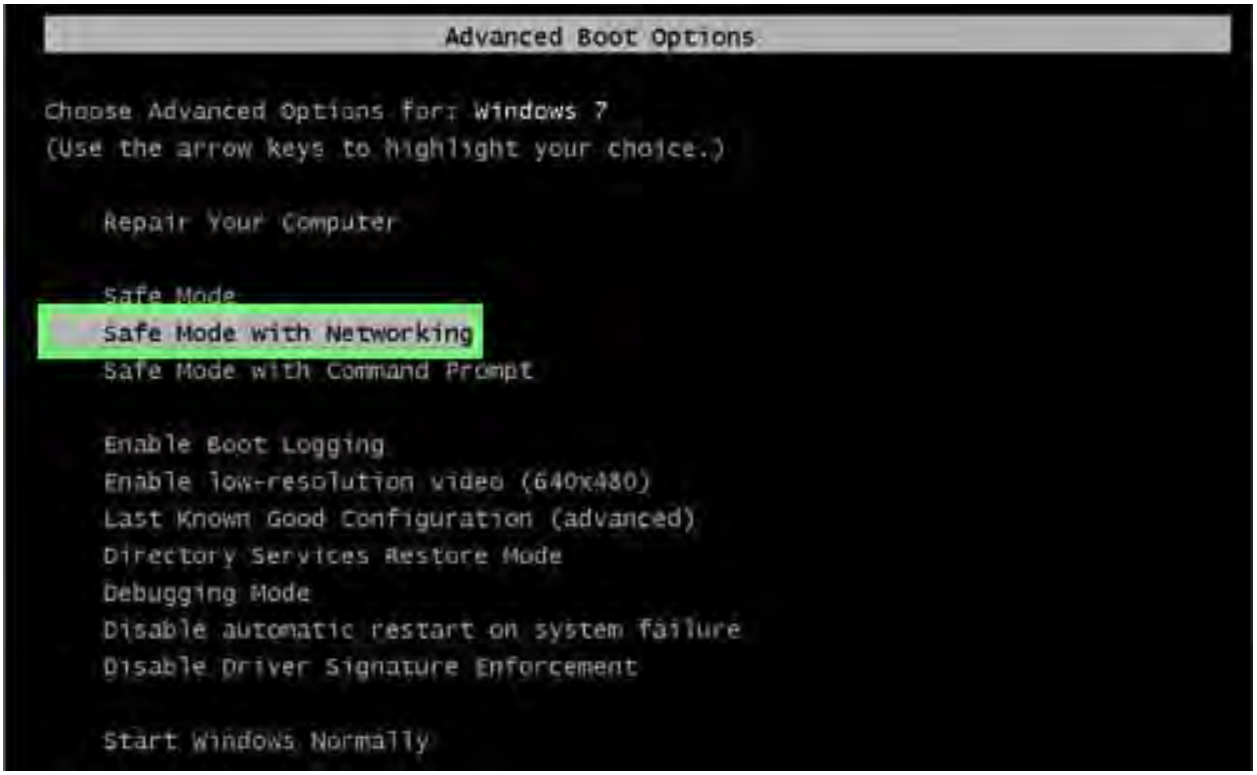
دانلود برنامه‌ای با نام Autoruns این برنامه، لیست تمام برنامه های نصب شده در سیستم و رجیستری را نشان می دهد :

(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.

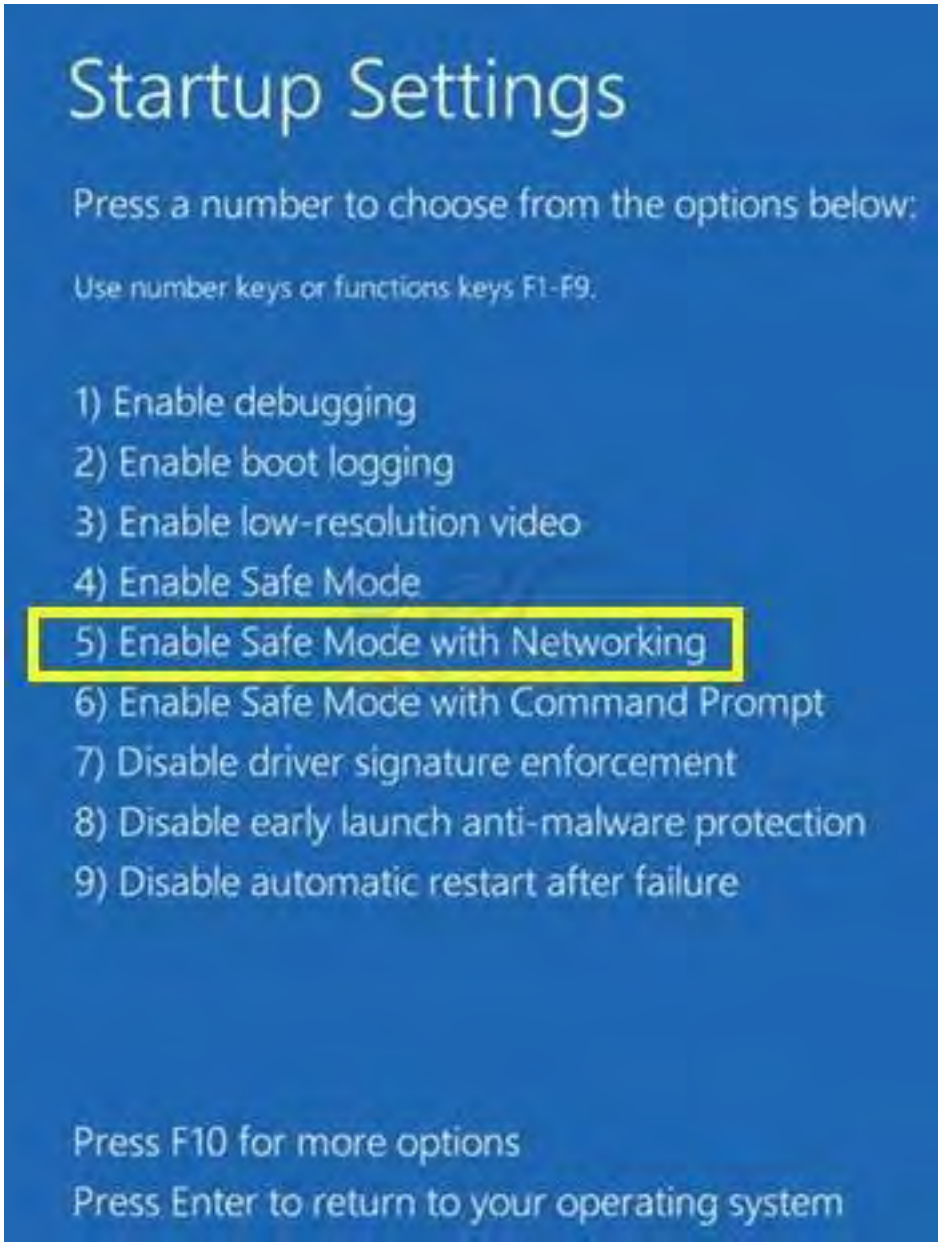


کاربران ویندوز XP و ویندوز 7:

کامپیوتر خود را در حالت Safe Mode راه‌اندازی 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 منویWindows Advanced Optionرا مشاهده کنید و در نهایت Safe Mode with Networkingرا از لیست انتخاب نمایید.

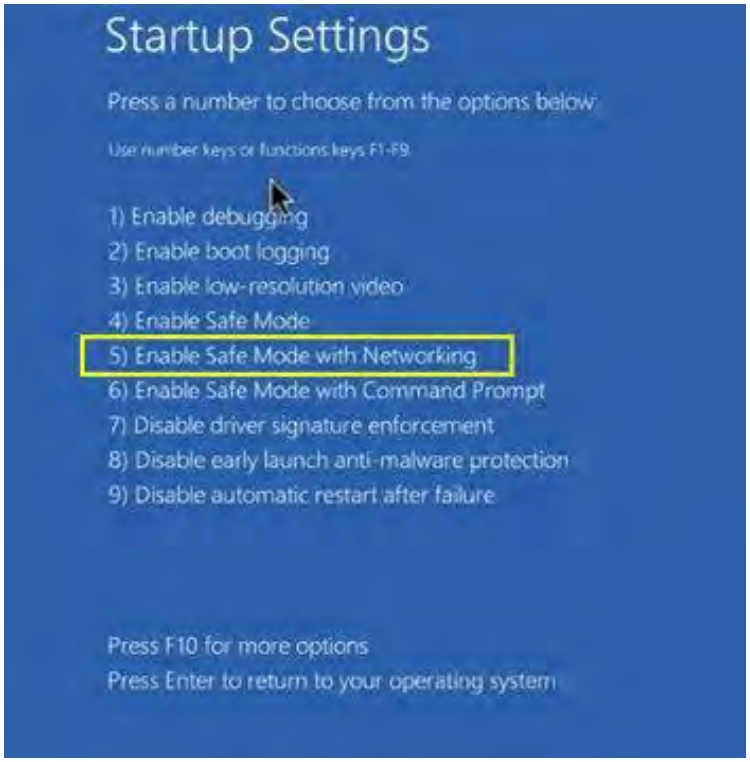
کاربران ویندوز 8:

سیستم را در حالت Safe Mode راه‌اندازی 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.



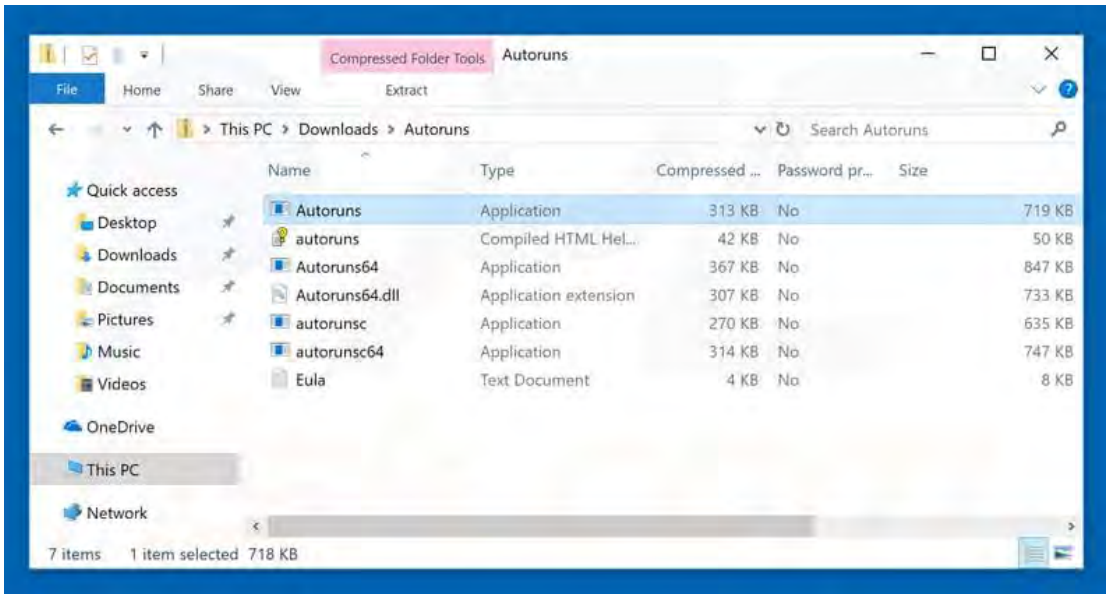
کاربران ویندوز 10:

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 وسیستم را Restart کنید. در نهایت مطابق شکل زیر سیستم خود را در حالت امن با شبکه راه اندازی کنید.



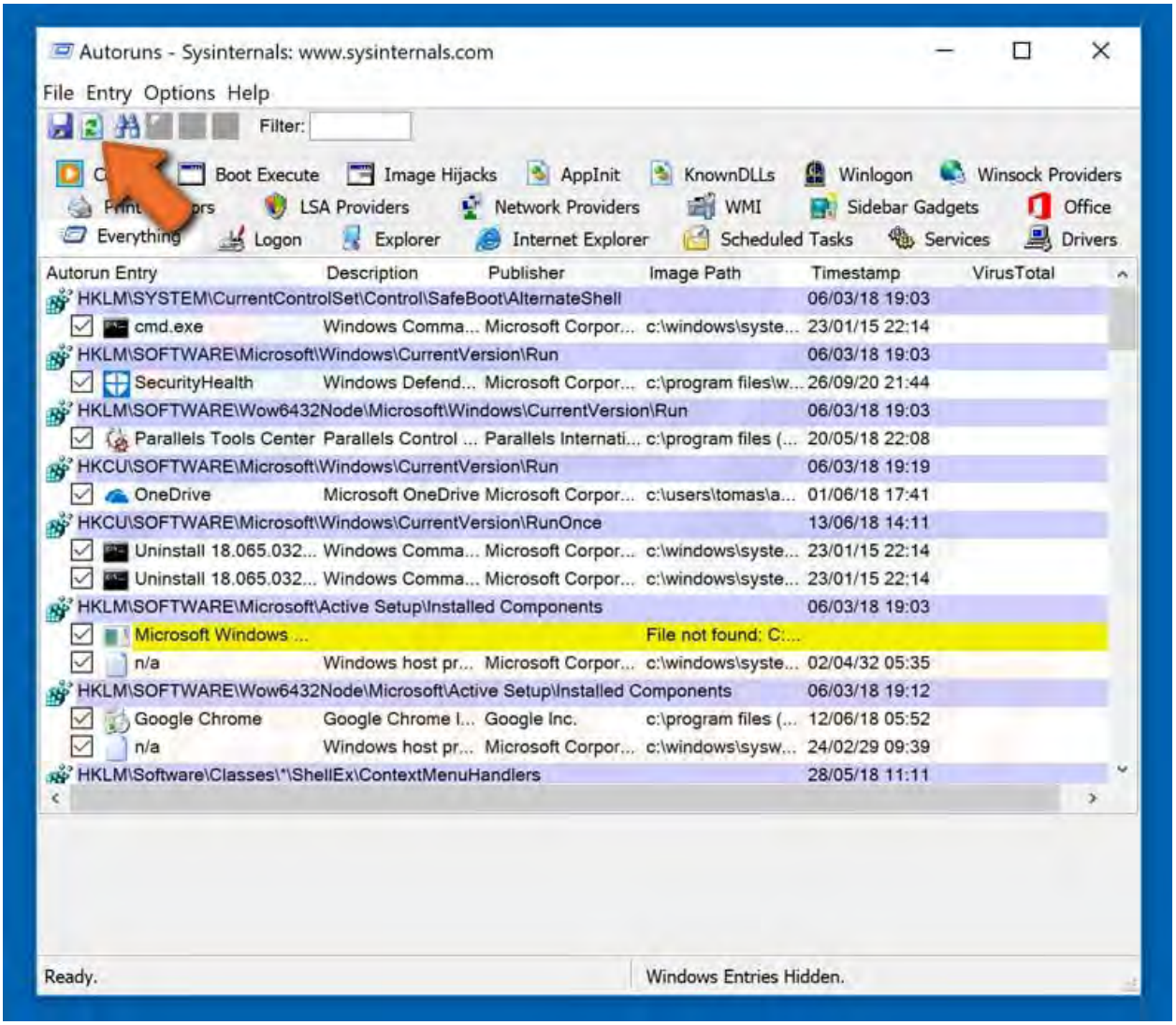
مرحله 3:

فایل Autoruns.exe را دانلود و اجرا کنید.



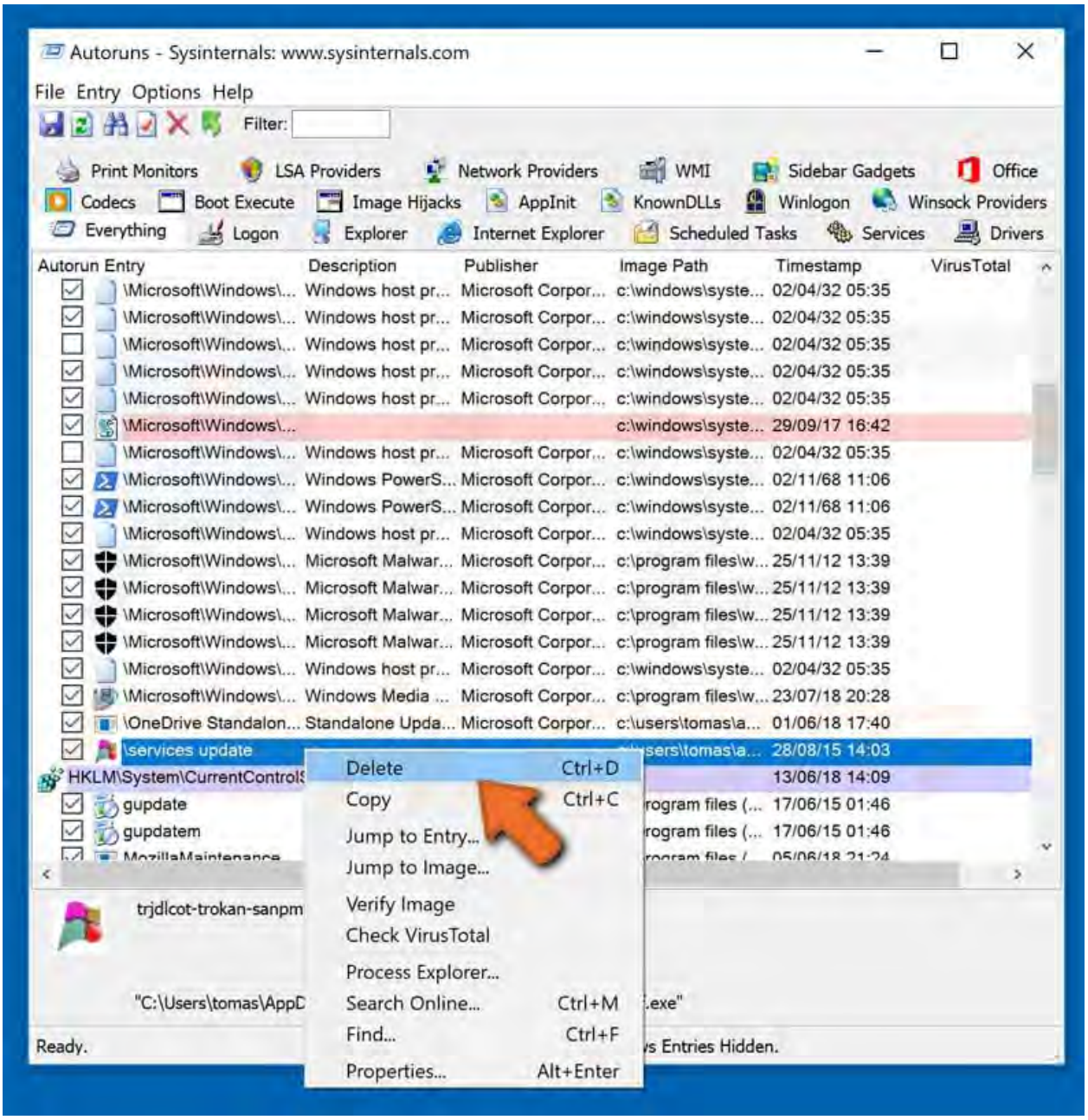
مرحله 4:

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.

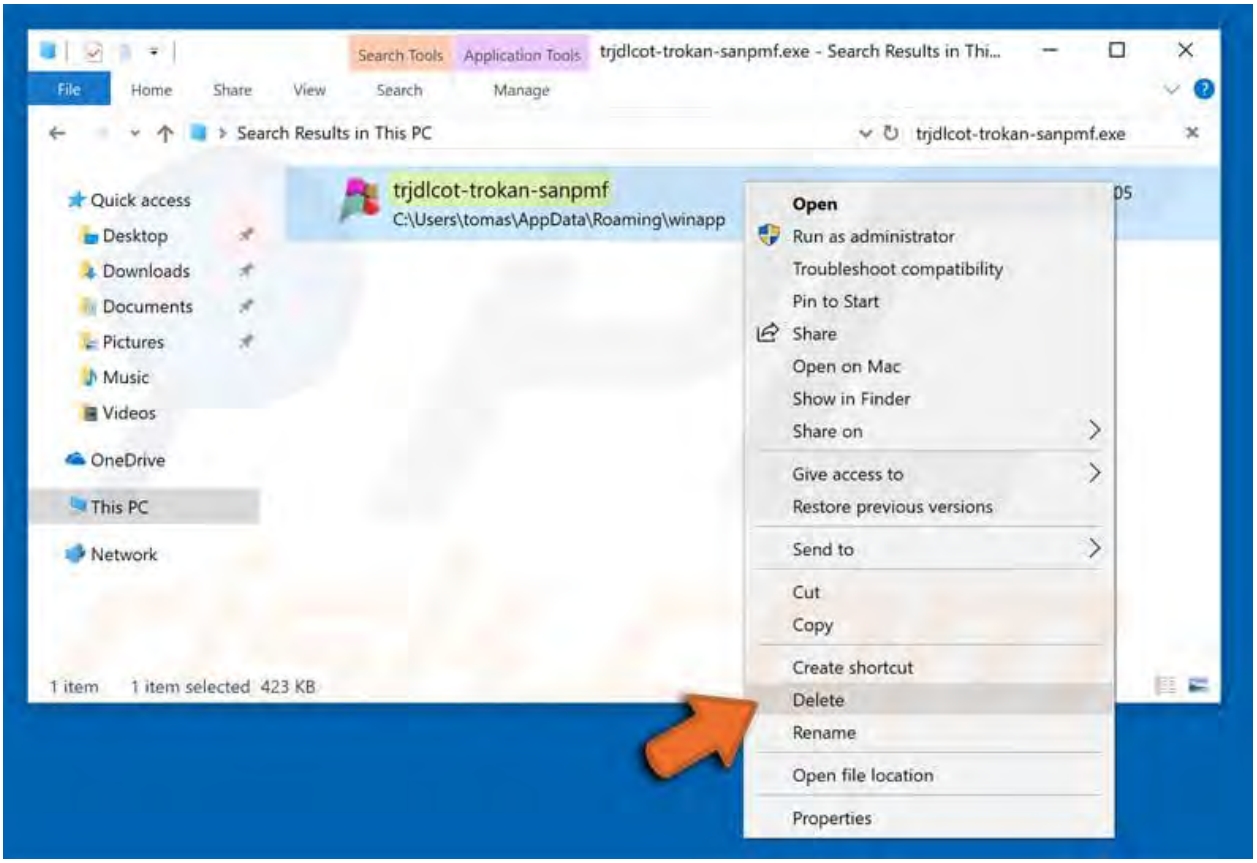

Autoruns - Sysinternals: www.sysinternals.com
File Entry Options Help
Filter:
Boot Execute
Image Hijacks
AppInit
KnownDLLs
Winlogon
Winsock Providers
LSA Providers
Network Providers
WMI
Sidebar Gadgets
Office
Everything
Logon
Explorer
Internet Explorer
Scheduled Tasks
Services
Drivers
Autorun Entry
Description
Publisher
Image Path
Timestamp
VirusTotal
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell 06/03/18 19:03
cmd.exe Windows Comma... Microsoft Corpor... c:\windows\syste... 23/01/15 22:14
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 06/03/18 19:03
SecurityHealth Windows Defend... Microsoft Corpor... c:\program files\w... 26/09/20 21:44
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run 06/03/18 19:03
Parallels Tools Center Parallels Control ... Parallels Internati... c:\program files (... 20/05/18 22:08
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 06/03/18 19:19
OneDrive Microsoft OneDrive Microsoft Corpor... c:\users\tomas\a... 01/06/18 17:41
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce 13/06/18 14:11
Uninstall 18.065.032... Windows Comma... Microsoft Corpor... c:\windows\syste... 23/01/15 22:14
Uninstall 18.065.032... Windows Comma... Microsoft Corpor... c:\windows\syste... 23/01/15 22:14
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components 06/03/18 19:03
Microsoft Windows ... File not found: C:...
n/a Windows host pr... Microsoft Corpor... c:\windows\syste... 02/04/32 05:35
HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components 06/03/18 19:12
Google Chrome Google Chrome I... Google Inc. c:\program files (... 12/06/18 05:52
n/a Windows host pr... Microsoft Corpor... c:\windows\sysw... 24/02/29 09:39
HKLM\Software\Classes*\ShellEx\ContextMenuHandlers 28/05/18 11:11
Ready.
Windows Entries Hidden.

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 نرم‌افزارهای مخرب است، مجدد سیستم را با Spyhunter اسکن نمایید.