تحلیل تبلیغ افزار BitsAdmin

تحلیل تبلیغ افزار BitsAdmin

حدود یک هفته است که کاربران در فروم های سایت bleepingcomputer و Malwarebytes پست هایی در خصوص خط فرمان BITSADMIN 3.0 که به صورت خودکار و متناوب اجرا می شود و فایل دانلود می کند، می گذارند. چیزی که بین همه ی آن کاربران مشترک است، نصب نرم افزار های ناخواسته بروی رایانه ی آنها است.

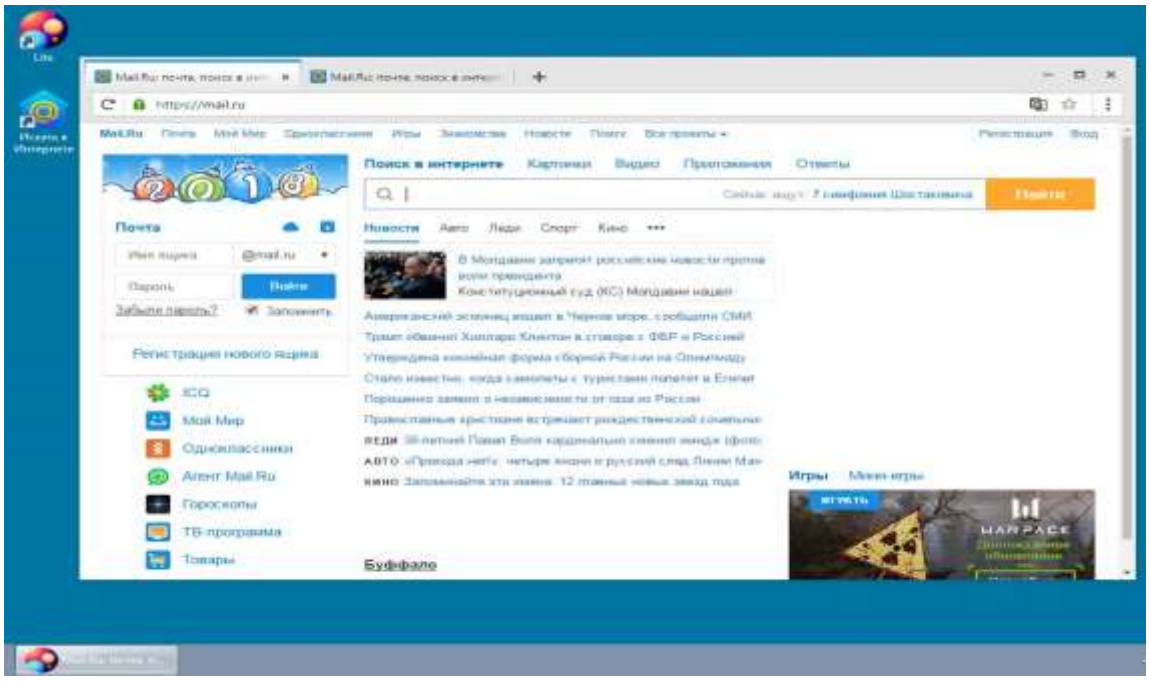
لازم به ذکر است که BitsAdmin مجموعه دستوراتی است که اجازه ی دانلود از طریق خط فرمان را به شما می دهد. کاربرد این دستور در ویندوز معادل دستور Wget در لینوکس است و در واقع یک برنامه ی مدیریت دانلود [۱] تحت داس می باشد.

پس از تحقیق و بررسی این موضوع ، محققان امنیتی کشف کردند که این رفتار به دلیل یک بسته ی تبلیغ افزار با نام FileTour میباشد.

نرم افزار FileTour یک بسته ی تبلیغ افزار است که تبلیغات، افزونه های ناخواسته ،PUP ها و استخراج کننده ها را بروی سیستم قربانی دانلود و اجرا می کند.

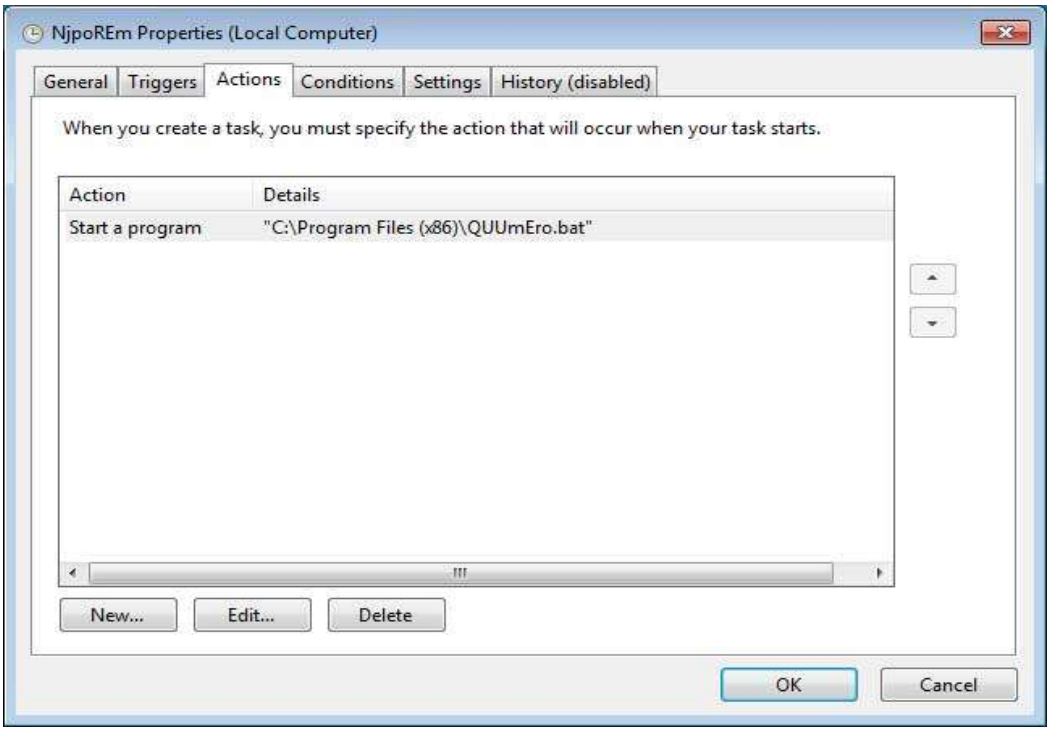
[۱] Download Manager

نکته ی جالب این تبلیغ افزار آن است که معمولاً PUP هایی را نصب می کند که مربوط به قربانیان روسی زبان بوده و این موضوع شامل نرم افزار هایی که به میل سرور mail.ru ارجاع می دهند نیز می شود .

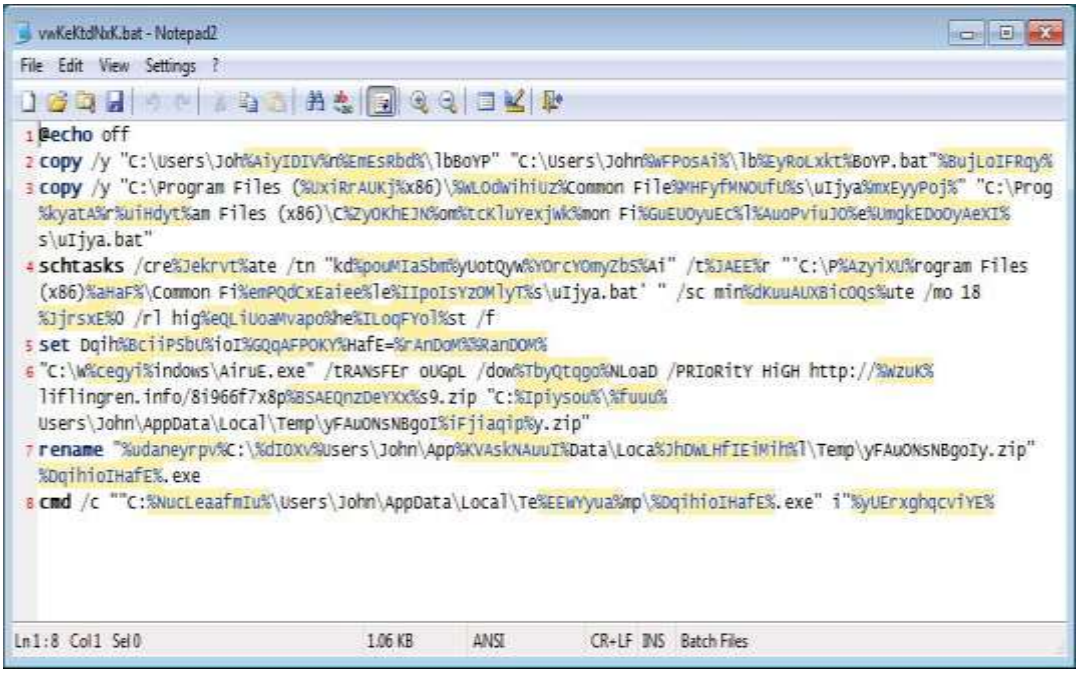


ظاهرا FileTour تصمیم گرفته که رفتاری متفاوت داشته باشد و شروع به دانلود و نصب نرم افزار های ناخواسته بروی سیستم قربانیان نموده است. این کار توسط ساخت یک بچ فایل[۲] (نوعی فایل اجرایی) و اجرای آن به صورت زمانبندی شده [۳] (هر ۳ ساعت یکبار) اتفاق می افتد.

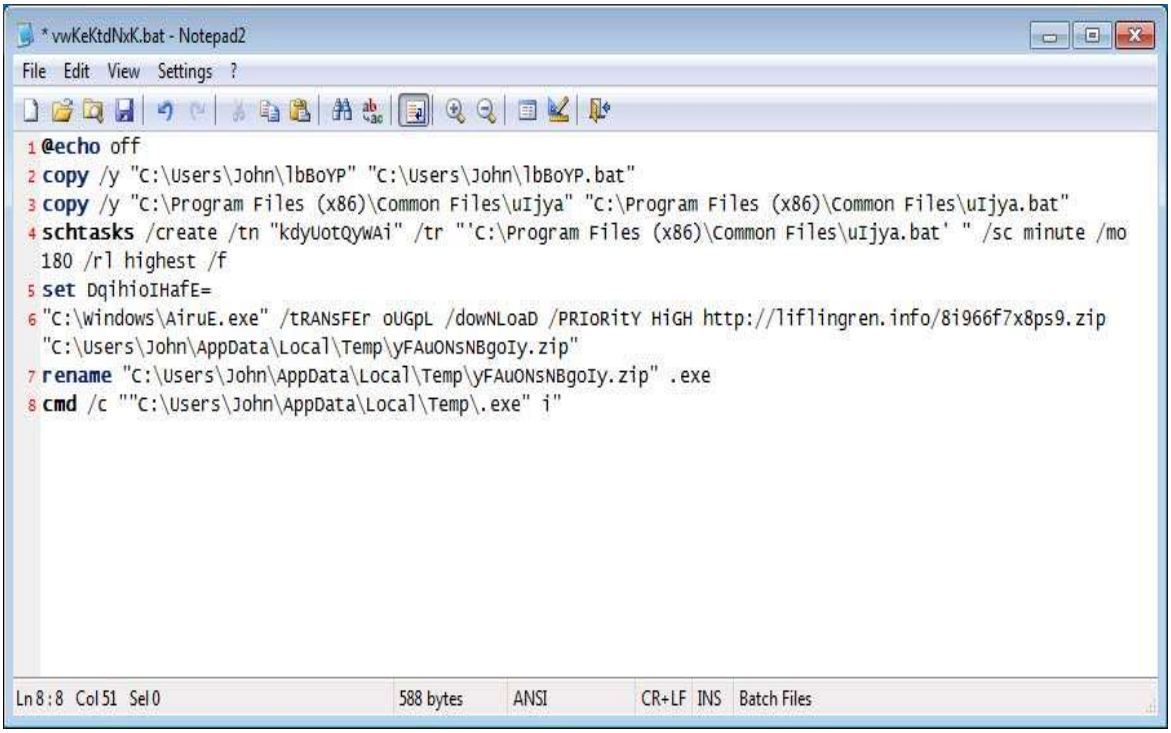
[۲] Batch file
[۳] scheduled tasks



بچ فایل ساخته شده حاوی کدی(که به صورت مبتدیانه سعی شده آن را مبهم سازند) است که کپی تغیر نام داده شده ای از BitsAdmin را که در مسیر C:\Windows قرار دارد، اجرا می کند تا دیگر ابزار های تبلیغ و برنامه های ناخواسته را بروی سیستم قربانی دانلود نماید.نمونه ایی از این بچ فایل را در تصویر زیر مشاهده می نمایید:



وقتی از کد بالا ابهام زدایی کنیم تصویر بهتری نسبت به کاری که بچ فایل قصد انجامش را دارد بدست می آید.
این بچ فایل یک Task جدید می سازد سپس از BitsAdmin تغییر نام داده شده استفاده می کند، آن را در مسیر C:\Windows\AireuE.exe قرار می دهد تا یک فایل را را از سایت مد نظر دانلود و اجرا نماید:



وقتی که طبق برنامه زمانبندی شده، بچ فایل اجرا می شود، یک پنجره ی command line که صفحه ی BitsAdmin را نمایش می دهد برای زمان کوتاهی نمایش داده می شود .

سپس BitsAdmin شروع به دانلود فایل از سایت های مورد نظر خود می کند که در این نمونه آدرس http://liflingren.info/8i966f7x8ps9.zip می باشد و آن را در مسیر %Temp% Folder در پوشه ی موقت ذخیره می کند .

پس از آن که دانلود فایل به اتمام رسید بچ فایل آن را اجرا می کند که باعث میشود پیغام UAC[۴] به شما نمایش داده شود .

[۴] User Account Control

اگر کاربر بروی گزینه ی بلی کلیک نماید ابزار تبلیغ دیگر یا برنامه ی ناخواسته ی دیگری بروی سیستم او نصب خواهد شد. این موضوع نشان می دهد که چگونه ابزار های تبلیغاتی از مرز ها عبور می کنند تا بتوانند یک بدافزار مخرب باشند که تنها هدف آنها انتشار نرم افزار های ناخواسته بروی رایانه قربانی است.

لازم به ذکر است که نرم افزار نصب شده میتواند یک باج افزار باشد.!

هش sha 256 :

۰۳f۸۷۹f۸۰۴۵۸a۰۵۳۱۱a۴۰dc۹۲۱c۳۶۵cc۳ac۹۱۳bec۹۳fd۳۵۴۲۵bbcf۲۳e۹ef۲b۳۰

آدرس ارتباطی سرور Adware :

http://liflingren.info

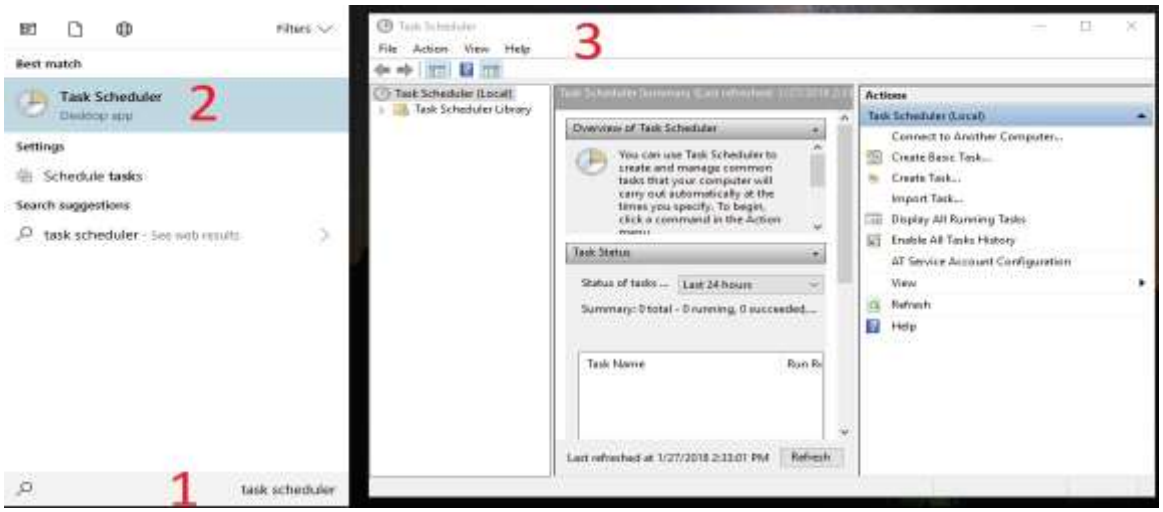
راهکار مقابله و پاکسازی BitsAdmin

برای مقابله با این تهدید، اقدامات زیر را در نظر بگیرید.

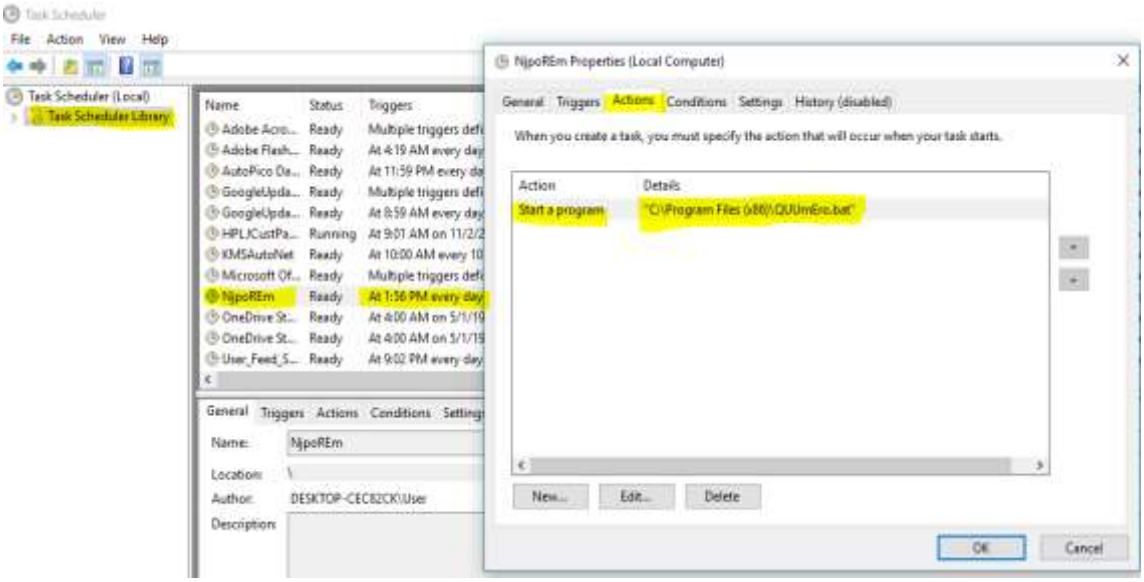
اقدام اول : حذف batch file و اجرای خودکار آن از Scheduled Tasks ویندوز

همان‌طور که قبلاً اعلام شد این تبلیغ‌افزار از طریق اجرای زمانبندی شده‌ی یک batch file اقدام به دانلود و نصب مکرر تبلیغ‌افزارها می‌نماید. بنابراین با حذف برنامه‌ی زمانبندی و batch file می‌توان به طور کامل فرایند این بدافزار را خاتمه داد.

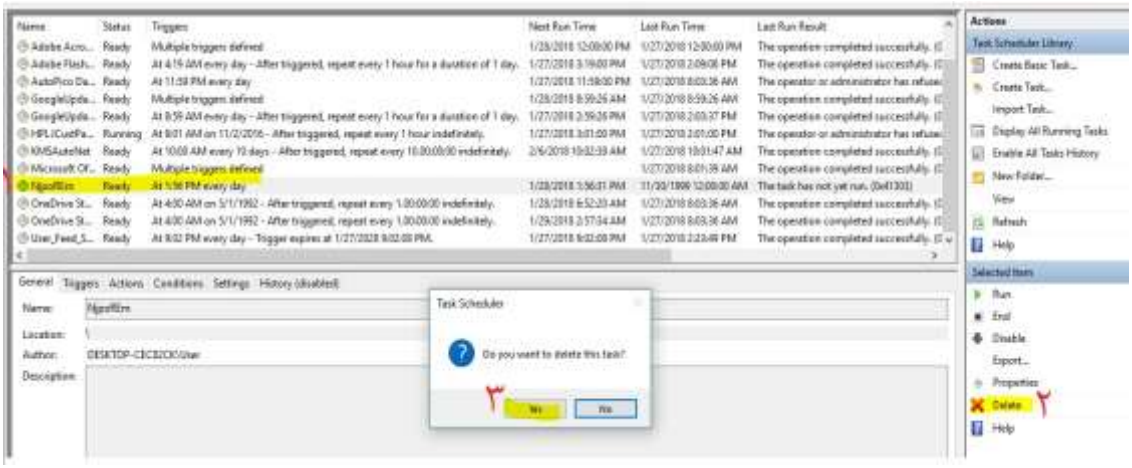
برای اینکار ابتدا باید برنامه زمانبندی ویندوز را اجرا نمایید. بدین منظور در نوار start کلمه‌ی task scheduler را جستجو و اجرا نمایید:



سپس بروی منوی Task Scheduler library کلیک نموده و از لیست وسط بروی زمانبند NjpoREm دوبار کلیک نمایید. در زبانه‌ی Actions می‌توان مسیر batch file را مشاهده نمود و با مراجعه به آن مسیر، آن batchfile را حذف نمود.



سپس برنامه‌ی زمانبندی را از لیست Task Scheduler library حذف تمایید.



لازم به ذکر است نام انتخاب شده برای batch file یا برنامه‌ی زمانبندی ممکن است در دیگر سیستم‌های آلوده متفاوت باشد. بنابراین در صورت آلودگی، لازم است تمامی Schedule Taskها برای یافتن وظیفه‌ی مدنظر بررسی شوند.

ضمناً در صورت وجود نرم‌افزار در لیست نرم‌افزارهای ویندوز باید آن را Uninstall نمود.

اقدام دوم: حذف کلیدهای رجیستری و فایل های Temp

در قسمت رجیستری ویندوز باید کلیدهای ساخته شده را حذف نمود. برای این کار باید در پنجره‌ی Run عبارت regedit را تایپ کرده (در ویندوزهای قدیمی تر regedit.msc) و کلید های زیر را جذف نمود.

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\A8CE93577A80
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{0F1F1FBC-1630-4656-A5D6-61C78F001A15}
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Plain\{0F1F1FBC-1630-4656-A5D6-61C78F001A15}
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{1618EB4E-B8DF-4D5A-BFB4-41EB85D6EBAD}

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Logon\{1618EB4E-B8DF-4D5A-BFB4-41EB85D6EBAD}

سپس به مسیر C:\USERS\THAIDUS\APPDATA\LOCAL\TEMP رفته و تمامی فایل‌های موجود در این پوشه را حذف نمایید.

در انتها با نصب ضدبدافزار معتبر و بروز می‌توان از اینگونه تهدیدات، پیشگیری کرد.

منابع:

- https://www.bleepingcomputer.com/news/security/adware-bundle-adds-persistence-to-download-more-malware-at-later-time/
- https://www.bleepingcomputer.com/forums/t/640953/cmd-windows-pop-bitsadmin/
  - https://forums.malwarebytes.com/topic/213937-bitsadmin-cmd-pop-up-constantly-downloading-unknown-publisher-software/