۳ روش برای دیدن وب سایت هایی که مخفیانه به کامپیوتر شما وصل هستند (نسخه PDF)

آیا سـرعت اینترنت شـما از آنچه که بایـد باشد کمتر شده است؟ آیا احساس میکنید کسـی به صورت مخفیانه شـما را کنترل میکند؟ صبر کنید!!! پاسخ شما را ما ITPro ها میـدهیم . کافی است تا اخر متن را بخوانید تا بفهمید در پس زمینه کامپیوتر شـما چه چیزهایی فضولی میکننـد؟ این احتمال وجود دارید که تعدادی ویروس و کرم و.. در پس زمینه کامپیوتر شـما بدون اطلاع شـما از اینترنت اسـتفاده کنند.در این جا ما به شما نشان میدهیم که اوضاع از چه قرار است!!

۱-با استفاده از CMD

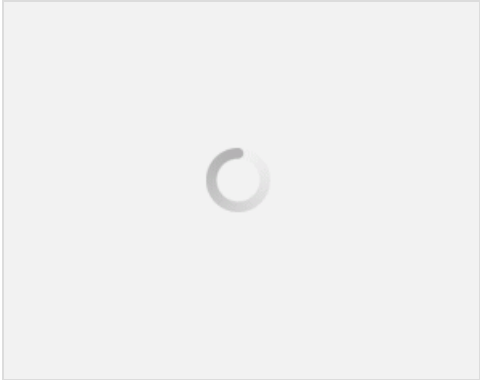
خوب چگونه میخواهید متوجه شوید که مشـکل از چیست؟ یک روش اسان به نام دستور Netstat با استفاده از CMDویندوز وجود دارد که میتوان از این روش در ویـنـدوز های Vista,XP,۸,۷ اسـتفاده کرد.درضمن اگر شما هنوز از ویندوز XP اسـتفاده میکنید خودتان را هک شده فرض کنید زیرا این سیسـتم عامل بسیار اسیب پذیر است.ما از دستور netstat استفاده میکنیم تا لیستی از همه چیزهایی که در یک زمان خـاص از اینترنت اسـتفاده میکننـد را درست کنیم.برای اسـتفاده از دسـتور Netstat شـما بایستی Command Prompt وینـدوز را در حالت Adminیا مدیر سیسـتم اجرا کنید.در ویندوز ۸ کافی است کلیـد های ترکیبی Windows+X را فشار داده و از لیست نمایش داده شـده گزینه Command Prompt (Admin) را انتخاب کنید.

اگر از ویندوز ۷ استفاده میکنید پس از باز کردن منوی Start در قسمت سرچ آن تایپ کنید "cmd.exe " وقتی که نتیجه نمایش داده شد با کلیک راست بر روی ان گزینه Run as Administrator را انتخاب کرده و در پنجره باز شده Yes بزنید.

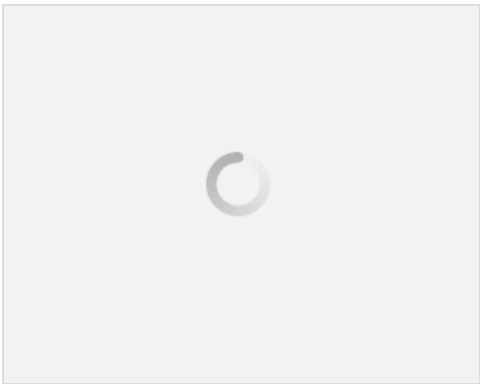
حال در CMD دستور زیر را تایپ کنید و کلید Enter را فشار دهید.

```
netstat -abf 5 > activity.txt
```

اپشن a- همه ی اتصالات و پورت آن ها را نشان میدهد. اپشن b- نشان میدهد که چه نرم افزار هایی کانکشن ایجاد کرده اند. اپشن f- نام کامل DNSهای هر اتصال را جهت سـهولت در فهمیـدن اینکه هر اتصال از کجا ساخته میشوند را نشان میدهد. اگر میخواهید فقط IP ان ها را نمایش دهد از اپشن h- استفاده کنید. آپشن ۵ هر اتصال را پنج ثانیه یک بار جهت ردیابی کردن مانیتور میکند .حدود ۲ دقیقه صبر کنید سپس کلیدهای ترکیبی Ctrl+C را فشار داده تا رکورد اطلاعات متوقف شود

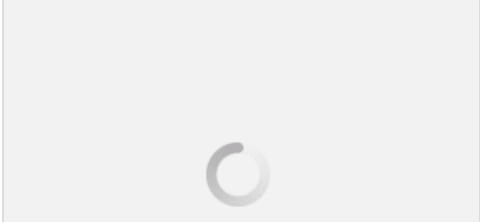


پس از توقف رکورد اطلاعات شما به سادگی میتوانید فایل activity.txt را در نرم افزار نرم افزارهای ویرایشگر متن(Notepad) جهت مشاهده نتیجه کار باز کنید.دراین لیست میتوانید همه ی پردازش های کامپیوتر خود را اعم از مرورگر وب , نرم افزار های پیام رسان و ارسال ایمیل و عیره که در دو دقیقه گذشـته اتصال اینترنتی ایجاد کرده اند را مشاهده کنید. و اگر شما زمان بیشتری جهت ثبت اطاعات منتظر بمانید به شـما نشان میدهد که کدام پردازش ها به کدام سایت ها متصل هسـتند. اگر نام پردازش مورد نظر یا ادرس وبسایت آن ها برای شـما اشـنا نبودند میتوانید نام آن پردازش مورد نظر را درگوگل سـرچ کنید و ببینید که آن چیست.؟میتواند پردازش سیستم شما باشد که از ان اطلاعاتی ندارید و یا پردازش یکی از نرم افزار های در حال اجرا باشد. با این حال اگر سایت مشکوکی به نظر میرسید باز میتوانید در گوگل سرچ کنید که چگونه از شر آن خلاص شوید(کلید حل کل مشکلات: گوگل) D:



۲-استفاده از نرم افزار TCP View

نرم افزار فوق العاده TCP View به شـما این امکان را میدهد که به سـرعت ببینید دقیقا چه پردازش های به چه منابعی در اینترنت متصل هسـتند و حتی به شـما اجازه میدهد که ان پردازش ها را ببنیدید و یا به سرعت عمل Whois Lookupبرای کسب اطلاعات بیشتری انجام دهید.بـدون شـک وقتی که بحث رفع مشـکلات پیش می ایـد و یا وقتی که میخواهیـد اطلاعات بیشتری از کامپیوتر خود به دست اورید TCP View اولین انتخاب ما میباشد.



توجه داشته باشید که وقتی این نرم افزار را اجرا میکنید ممکن است با انبوهی از اتصالات از نوع از ادرس های اینترنتی متونعی مواجه شوید ولی این بعضا مشکلی ندارد.اگر همه ی اتصالات در وضعیت Time-wait باشند به این معنی است که کانکشن ها در حال بسته شدن هستند و پردازشی برای اختصاص دادن به یک کانکشن وجود ندارد. این معمولا زمانی اتفاق می افتد که شما بعد از این که چند نرم افزار را اجرا کردید TCP View را اجرا میکنید در صورتی که شما باید وقتی که همه ی نرم افزار ها بسته هستند واتصالی ندارد ان را اجرا کنید.

۳- با استفاده از نرم افزار Currports

همچنین شما میتوانید از یک ابزار رایگان پرتابل(بدون نیاز به نصب) به نام Currports جهت نمایش تمامی پورت های باز شده از نوع TCP/IP و یا UDP کامپیوترتان استفاده کنید.برای هر پورتی که این نرم افزار لیست میکند اطلاعاتی در باره ی پردازش ان پورت به شما نمایش میدهد. شما میتوانید کانکشن های در حال اجرا را انتخاب و آن ها را ببینید یا اطلاعات پورت ها را در حافظه کلیپ بورد کپی کنید و در یک فایل HTML,XMLیا یک فایل متنی ذخیره کنید.شما میتواند اطلاعاتی مه در صفحه اصلی برنامه نشان داده شده است را به صورت ستونی ذخیره کنید.

برای چینش اطلاعات بر حسب یک ستون خاص فقط کافی است بر روی عنوان ان ستون کلیک کنید.این نرم افزار تحت ویندوز های ۷,۸ ,Server ۲۰۱۲ ,Server ۲۰۰۸,Server۲۰۰۳ ,NT,۲۰۰۰,XP واحتمالا ۱۰ کار میکند.و ورژن ۶۴بیت آن هم برای نسخه های ۶۴بیت موجود میباشد.جهت اطلاعات بیشتر و روش استفاده از ان میتوانید به وب سایت این نرم افزار مراجعه کنید.

نویسنده: M.Mehdi.SH

منبع: جزیره امنیت اطلاعات و ارتباطات وب سایت توسینسو

فرزانه

واااااای مرسی ممنون .

فرزانه

راستی چطوری ذخیرش کنیم تو ورد ؟

محمد مهدی نوری

بعد از این که در حافظه کلیپ بورد اون رو کپی کردید میتونید در یک فایل ورد اون رو Paste کنید.

مطلب اصلی