

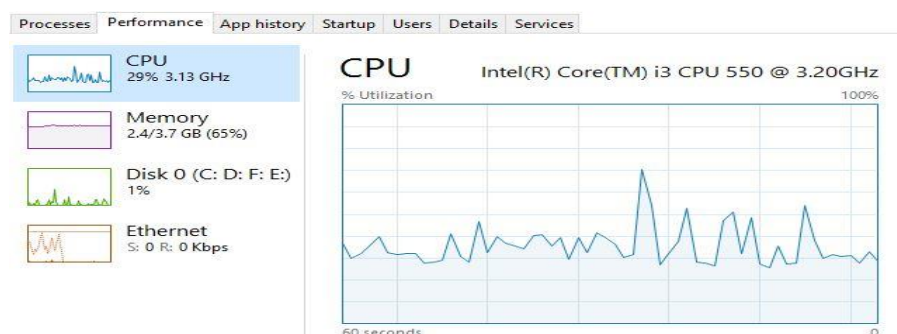
علائم ویروسی شدن کامپیوتر

ویروس های کامپیوتری انواع مختلفی دارند. اما به طور کلی همه آنها با یک هدف مشخص وارد کامپیوتر شما میشوند. تخریب سیستم عامل یا سرقت اطلاعات شخصی شما. هر ویروس روش خاصی را برای الوده کردن و آزار دادن شما دارند. در این آموزش قصد داریم علائم ویروسی شدن کامپیوتر را بگویم پس در ادامه تی ام ال منیجر را با نگاه گرمندان یاری کنید.

نکته: ممکن است بعضی از علامت های که گفته میشود منشأ سخت افزاری داشته باشند. و به ویروسی بودن سیستم عامل ربطی نداشته باشند.

بررسی وضعیت استفاده از سخت افزار سیستم

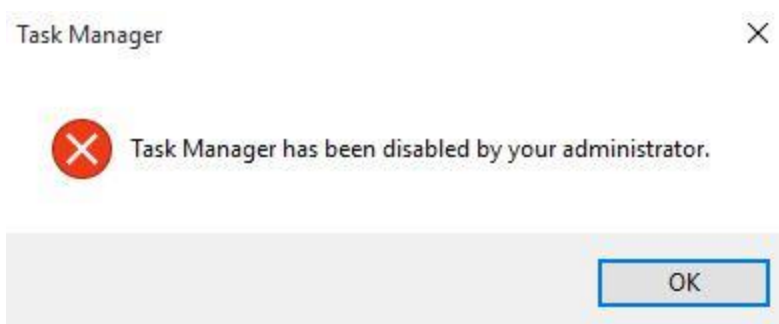
اولین گزینه ای که باید آن را بررسی کنید وضعیت کار کرد CPU و هارد دیسک شما میباشد به طور معمول همه ویروس ها باعث افزایش استفاده از منابع سخت افزار شما میشوند مثلا بدون اینکه هیچ برنامه ای را باز کرده باشید CPU سیستم شما روی ۷۰% به بالا کار کند یا مثلا Hard Disk سیستم شما روی وضعیت ۱۰۰% باشد. این بدان معناست که یک ویروس به صورت Background دارد فعالیت میکند.



برای بررسی این مورد بهتر است از ابزار Task Manager استفاده کنید و از قسمت Performance وضعیت استفاده از منابع سخت افزار را بررسی کنید. برای اجرای Task Manager روی نوار ابزار Taskbar کلیک راست نموده سپس Task Manager را اجرا کنید. ای میتوانید کلیدهای Ctrl + Shift + Esc را به طور همزمان نگاه داشته تا Task Manager اجرا شود.

مواجه شدن با خطای Program Has Bin Disable By your Administrator

یکی از کارهای که معمولا ویروس ها برای مخفی ماندن و بستن دست کاربر در اشکال زدایی انجام میدهند. غیر فعال نمودن ابزارهای ویندوز مثل Task Manager یا CMD یا Group Policy یا Regedit و یا ... میباشد. معمولا هنگامی که سعی میکنید این برنامه ها را اجرا کنید با خطای Program Has Bin Disabled By Your Administrator مواجه میشوید. که به معنی غیر فعال شده توسط مدیریت میباشد.



طول کشیدن Load Windows

اگر احساس میکنید Loading Windows تان زیاد شده مثلا بیش از یک دقیقه باید صبر کنید تا سیستم عامل به مرحله احراز هویت (Username And Password) برسد این بدین معنی میباشد که ممکن است سیستم شما به ویروس مبتلا شده باشد.

بررسی Startup ویندوز

یکی از مکانهای که ویروس ها در آنجا خیلی زیبا لم میدهند **Startup** ویندوز میباشد. به صورت عادی برنامه ها از محیط Startup برای اجرای هر چه سریعتر در هنگام بالا آمدن ویندوز استفاده میکنند. ولی ویروس ها هم از این ویژگی سوء استفاده نموده و خود را در Startup بارگذاری میکنند تا هنگام بالا آمدن ویندوز ویروس هم به صورت خود کار اجرا شود.

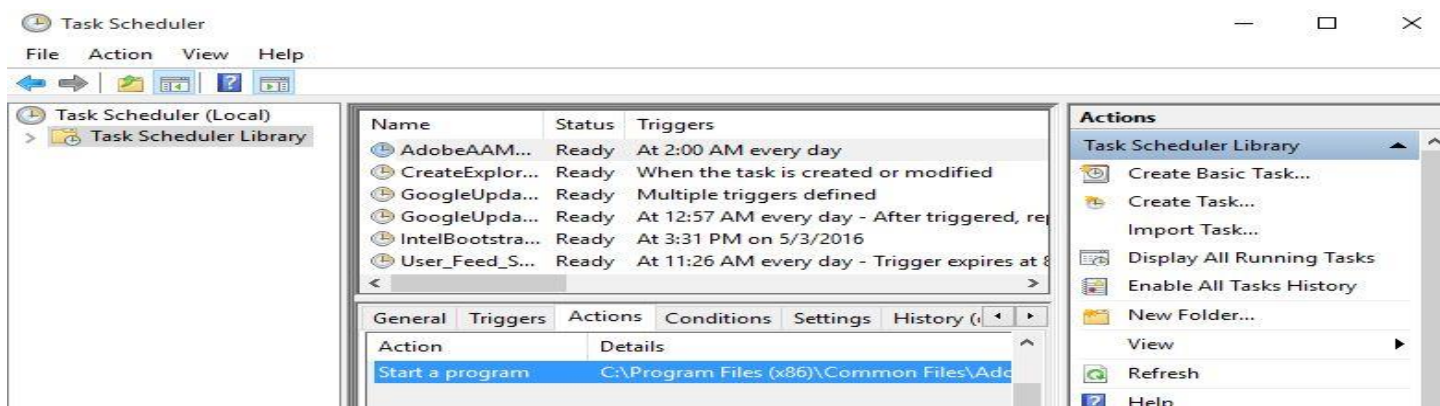
Name	Publisher	Status	Startup impact
DelayPluginl.exe		Disabled	None
Program		Disabled	None
Adobe CS6 Service Manager	Adobe Systems Incorpor...	Disabled	None
Program		Disabled	None
VMware Tray Process	VMware, Inc.	Disabled	None
Adobe Reader and Acrobat ...	Adobe Systems Incorpor...	Disabled	None
Skype	Skype Technologies S.A.	Disabled	None
Internet Download Manager...	Tonec Inc.	Disabled	None

برای بررسی Startup در ویندوز ۷ به قبل باید از دستور **MSCONFIG** در پنجره RUN استفاده کنید. پس از اجرای **MSCONFIG** وارد تب Startup شوید. برنامه های که در Startup هستند را بررسی کنید. اگر اسم های عجیب غریبی در Startup وجود دارد که آنها را میشناسید پس احتمالاً ویروس میباشد. برای بررسی دقیق تر کافیت تا نام آنها را در جستجوی گوگل جستجو کنید.

نکته: برای بررسی Startup در ویندوز 8 و 8.1 و 10 باید از همان ابزار Task Manager استفاده نموده و به تب Startup بروید.

بررسی محیط Task Schedules

یکی از برنامه های بسیار کاربردی در ویندوز Task Schedules میباشد که عموم کاربران از آن بی خبر هستند. این ابزار به شما اجازه میدهد تا یک برنامه یا یک کار را در تاریخ و زمان یا وضعیت مشخصی انجام دهید. درست است این برنامه توسط عموم کاربران ناشناخته باقی مانده اما توسط ویروس ها و بد افزار ها بسیار کاربردی و حیرت انگیز استفاده میشود. معمولاً بد افزارها از این برنامه برای زمان بندی نمودن کارهای خویش استفاده میکنند. تا مثلاً در ساعات بیکاری کامپیوتر شروع به انجام عملیات شیطانی خود کنند. مثلاً انتقال اطلاعات شما به سرور ویروس.



برای بررسی از وضعیت Task های موجود در ابزار Task Schedules کافیت تا کلمه Task Schedules را در Start جستجو کنید. یا `taskschd.msc` را در پنجره Run تایپ کنید. از قسمت Task Schedules Library کارهای زمانبندی شده را مشاهده خواهید نمود. به طور پیشفرض اگر همه آنها را هم حذف کنید اتفاق خاصی برای ویندوز نمی افتد. فقط ممکن است کرک های **AutoKMS Pico** (پیرد) پس آن موارد را هم بررسی نموده سپس مورد های مشکوک را حذف کنید از قسمت Action کار یا برنامه ای که توسط Task قرار است انجام شود را میتوانید مشاهده کنید.

خراب اجرا شدن برنامه ها

اگر برنامه های که تا حالا بدون مشکل اجرا میشدند حال با خطا مواجه شوند، یا هنگام کار به صورت خود کار بسته میشوند. پس احتمال دهید سیستم شما ویروسی شده است. چرا که یکی از کارهای که ویروسها انجام میدهند خراب نمودن سرویس های ویندوز و برنامه های کامپیوتری میباشد.

طبق تجربه شخصی معمولا برنامه ها با خطای Program Has Been Stopped Working بسته میشوند. و نصب دوباره نرم افزار فایده ای ندارد. چرا که خود سیستم عامل هم آغشته به ویروس شده است.

هنگ کردن یا Freeze شدن زیاد سیستم

هنگ نمودن سیستم یکی از علت های رایج در تشخیص ویروسی بودن سیستم میباشد اگر سیستم شما زیاد گیر میکند و مجبور به ریستارت نمودن دستی سیستم میشوید. پس احتمال دهید که سیستم شما ویروسی شده است.

پیدایش فایل های ناشناس در درایوها

کار اصلی ویروس تکثیر نمودن خود در سیستم میباشد. حال یا دیگر فایل ها را آلوده میکند، یا خود را در درایو ها کپی میکند. اگر در درایو های ویندوز به فایل های برخوردید که اسم های عجیب و غریب داشتند، پس احتمال دهید این فایلها ممکن است ویروس باشند. به صورت عادی در ویندوز یک سری فایل های مخفی سیستمی وجود دارد که آنها ویروس نیستند. بلکه فایل های مربوط به ویندوز میباشد. و برای کارکرد درست ویندوز حیاتی هستند. برای شناخت این فایلها به مقاله فایل های مخفی سیستمی مراجعه کنید.

ریستارت شدن یا خاموشی شدن خودکار سیستم

معمولا چون ویروس ها هسته ویندوز را خراب میکنند، سیستم عامل تا مرحله Login بالا می آید سپس به صورت خود کار ریستارت میشود. این مورد در اکثر موارد توسط ویروس های بازی گوش انجام میشود. این ویروس ها حرف حساب را همان اول میزنند و کلا به شما اجازه استفاده از ویندوز را نمیدهند. در بعضی از موارد به شخصه مشاهده نموده ام که ویروس ها حتی محیط Safe Mode را هم تخریب نموده اند. پس برای نصب ویندوز آماده شوید :

بهترین آنتی ویروسی که میتواند بهتون معرفی کنم [BitDifender](#) که واقعا طبق تجربه شخصی من عالی عمل کرده. هم از لحاظ سرعت هم از لحاظ تشخیص ویروس ها و افزایش امنیت ویندوز.