

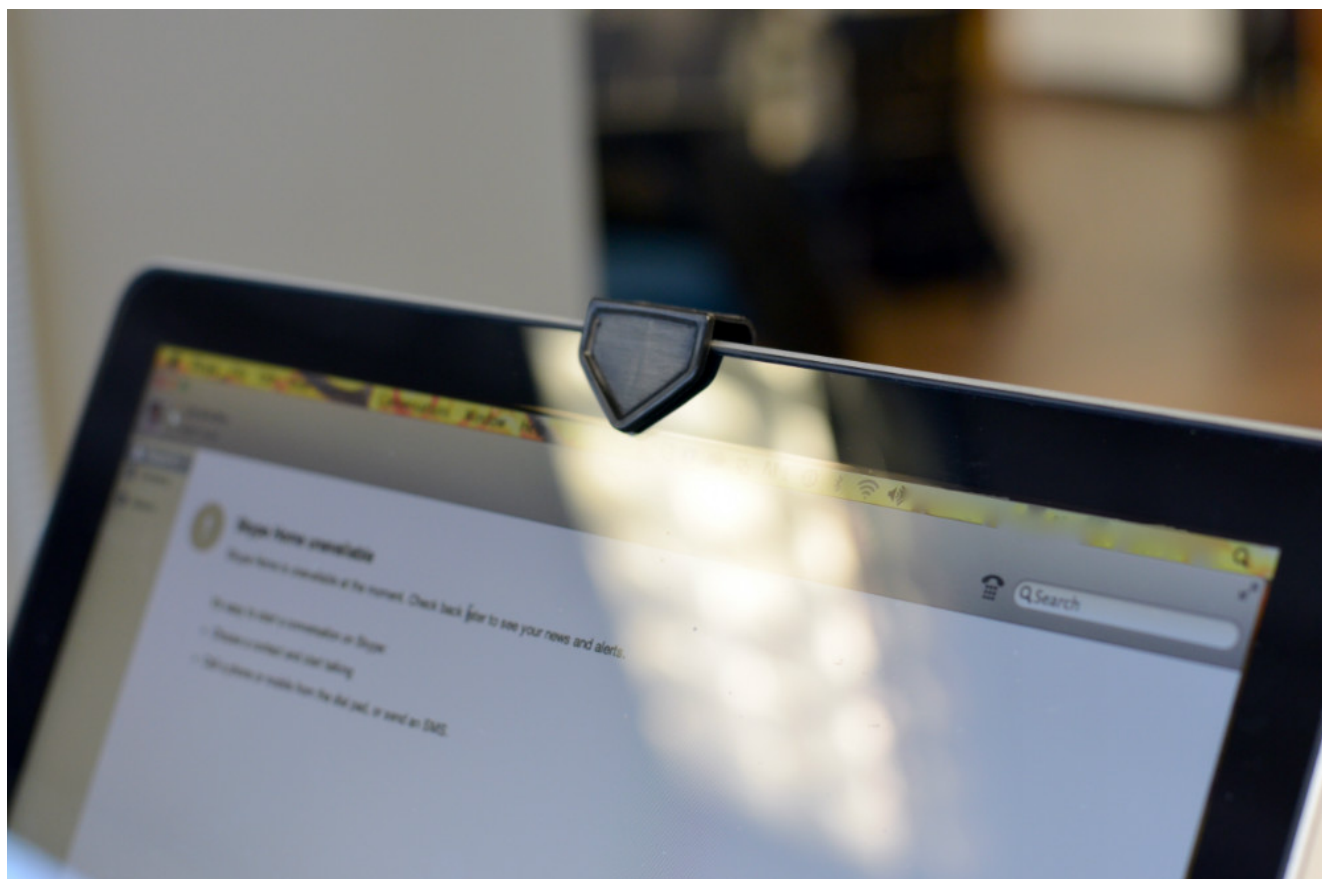
# چگونه متوجه استفاده نرم افزارهای ویندوز از وب کم شویم؟ - دیجیاتو

مانی میرجوادی | شنبه، ۰۶ بهمن ۱۳۹۷

جاسوسی از وب کم کاربران اینترنت موضوع تازه‌ای نیست. گاهی بدافزارها و تروجان‌ها عامل اصلی این اتفاق هستند و گاهی به دلیل آسیب پذیری روتر ممکن است دیگران به وب کم دستگاه شما دسترسی پیدا کنند. این حمله‌ها فقط در لپتاپ‌ها صورت نمی‌گیرد و ممکن است در تلفن‌های هوشمند و تبلت‌ها هم اتفاق بیفتد.

طبیعتاً هیچکس دوست ندارد ندانسته توسط دیگران دیده شود. در این مطلب قصد داریم به همین موضوع بپردازیم و راه‌های جلوگیری از جاسوسی وب کم لپتاپ را بررسی کنیم؛ این که متوجه شویم چه برنامه‌هایی از وب کم استفاده می‌کنند و چگونه جلوی دسترسی آن‌ها را بگیریم. با ما همراه باشید.

**راه حلی برای تمامی پلتفرم‌ها: وب کم را بپوشانید**



مهم نیست که از چه دستگاهی استفاده می‌کنید؛ یکی از روش‌های کاملاً عملی برای جلوگیری از دیده شدن توسط افراد سودجو و هکرها، پوشاندن لنز وب کم است. کاری بسیار ساده و صد در صد عملی.

شاید سریع‌ترین و هوشمندانه‌ترین راه این باشد که یک برچسب کاغذی روی سنسور بچسبانید. این کاغذ نیاز نیست خیلی بزرگ و چسبناک باشد. هر کاغذی که به طور کامل وب کم را بپوشاند کافیست.

اگر از وب کم می‌استفاده می‌کنید که از طریق USB به کامپیوتر متصل می‌شود می‌توانید به سادگی آن را از کامپیوتر جدا کنید و دیگر نگران جاسوسی از طریق وب کم نباشید. اما بعد از انجام این کار، باید متوجه شوید که چه برنامه‌هایی در حال استفاده از وب کم شما هستند و جلوی دسترسی غیر مجاز آن‌ها را بگیرید.

## استفاده از نرم افزار Process Explorer برای بررسی دسترسی‌ها به وب کم

عموماً کامپیوترهای ویندوزی به راحتی امکان دسترسی به وب کم‌ها را فراهم می‌کنند. خوشبختانه فهمیدن این موضوع که چه نرم افزارهایی به دوربین دسترسی دارند و همچنین جلوگیری از این دسترسی کار دشواری نیست. مایکروسافت نرم‌افزاری به نام Process Explorer تولید کرده که می‌توانید آن را برای ویندوز دانلود کنید. این نرم افزار **تنها 1.8 مگابایت حجم دارد** و رایگان است.

Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-5MTNQ77\atomi]

File Options View Process Find Users Help

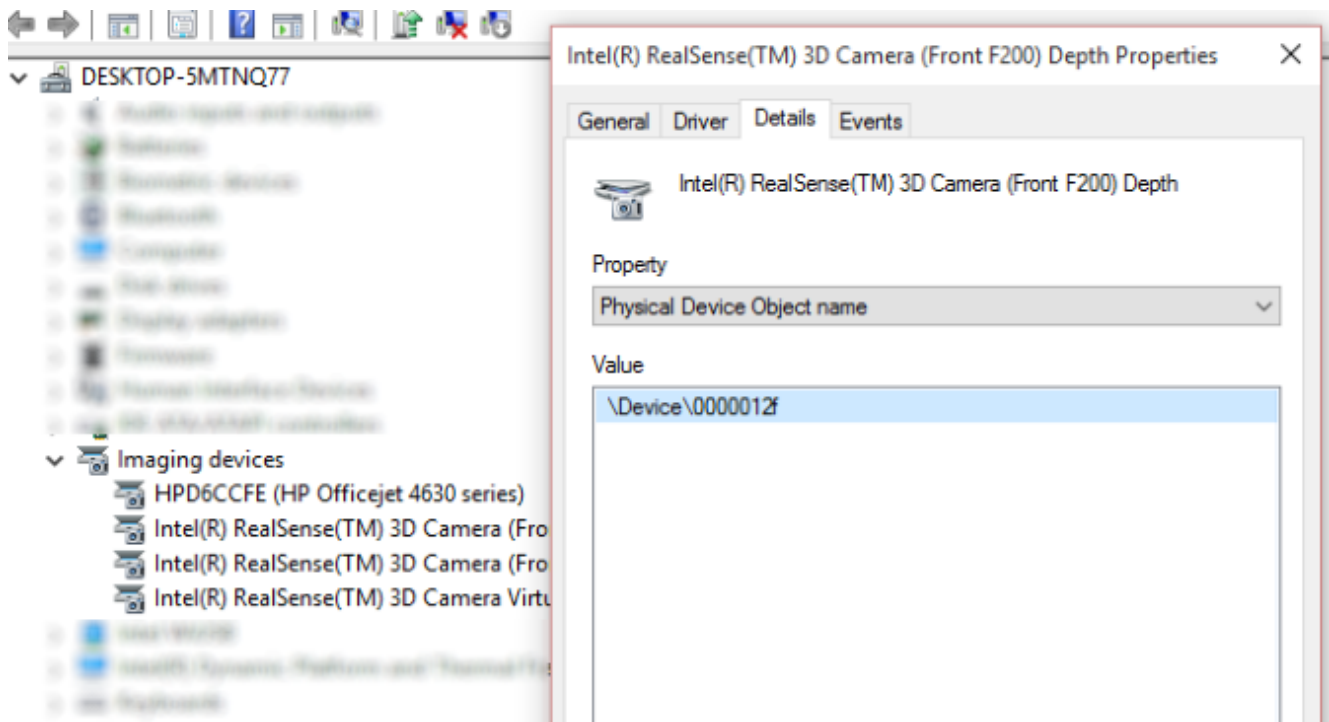
Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
System Idle Process	37.73	0 K	4 K	0		
System	19.87	4,516 K	1,849,120 K	4		
Interrupts	8.80	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		356 K	1,060 K	376	Windows Session Manager	Microsoft Corpor...
csrss.exe	< 0.01	1,624 K	5,512 K	660	Client Server Runtime Process	Microsoft Corpor...
csrss.exe	0.08	2,572 K	13,804 K	788	Client Server Runtime Process	Microsoft Corpor...
wininit.exe		932 K	4,420 K	788	Windows Start-Up Application	Microsoft Corpor...
services.exe		4,144 K	7,452 K	904	Services and Controller app	Microsoft Corpor...
svchost.exe	< 0.01	7,616 K	44,936 K	352	Host Process for Windows S...	Microsoft Corpor...
unsecapp.exe		1,532 K	6,792 K	4416	Sink to receive asynchronou...	Microsoft Corpor...
WmiPrvSE.exe		4,880 K	16,164 K	4580	WMI Provider Host	Microsoft Corpor...
WmiPrvSE.exe	2.65	10,064 K	18,092 K	5232	WMI Provider Host	Microsoft Corpor...
RuntimeBroker.exe	0.02	58,000 K	53,884 K	2224	Runtime Broker	Microsoft Corpor...
SettingSyncHost.exe		10,412 K	4,756 K	7724	Host Process for Setting Syn...	Microsoft Corpor...
unsecapp.exe	< 0.01	1,616 K	8,772 K	6284	Sink to receive asynchronou...	Microsoft Corpor...
InstallAgent.exe		34,072 K	20,416 K	11072	InstallAgent	Microsoft Corpor...
ApplicationFrameHost...		11,432 K	26,024 K	11048	Application Frame Host	Microsoft Corpor...
ALERTH~1.EXE		4,948 K	15,876 K	10280	McAfee Alert host	McAfee, Inc.
McVulAlert.exe		2,752 K	9,896 K	9636	McAfee Vulnerability Scanner	McAfee, Inc.
ShellExperienceHost	Susp	33,056 K	57,216 K	3180	Windows Shell Experience H	Microsoft Corpor...

وقتی دانلود به اتمام رسید، محتویات پوشه‌ی فایل ZIP را از حالت فشرده خارج کرده و سپس به فولدر ProcessExplorer بروید. روی نسخه‌ای که برای سیستم عامل شما مناسب است کلیک

راست کنید و سپس گزینه‌ی Run as Administrator را بزنید. در پنجره‌ی باز شده ابتدا روی Run کلیک کرده و سپس Agree را انتخاب نمایید.

## نام وب کم خود در ویندوز را بیابید

مرحله‌ی بعدی این است که بتوانید نام وب کم خود را بیابید و آن را شناسایی کنید. برای این کار باید به Device Manager بروید که می‌توانید با کلیک راست کردن روی منوی استارت به آن دسترسی داشته باشید. از لیست سمت راست روی فلش کوچک کنار Imaging Devices کلیک کرده و سپس از بین گزینه‌های اضافه شده روی گزینه‌ای که دارای Camera است کلیک راست کنید.



گزینه‌ی Properties را بزنید و در پنجره‌ی باز شده وارد تب Details شوید. از بخش Property گزینه‌ی Physical Device Object name را انتخاب کرده و روی رشته‌ی نوشته شده در زیر Value کلیک راست کرده و سپس آن را کپی نمایید.

## چه برنامه‌ای از وب کم شما استفاده می‌کند؟

برای پی بردن به این موضوع حالا کافیس‌ت نرم افزار Process Explorer را مجدداً باز کرده و سپس از منو گزینه‌ی Find (همچنین می‌توانید از کلیدهای ترکیبی Ctrl + F استفاده کنید) را انتخاب کرده و سپس محتویات کپی شده در مرحله‌ی قبل را در آن درج (Paste) کنید.

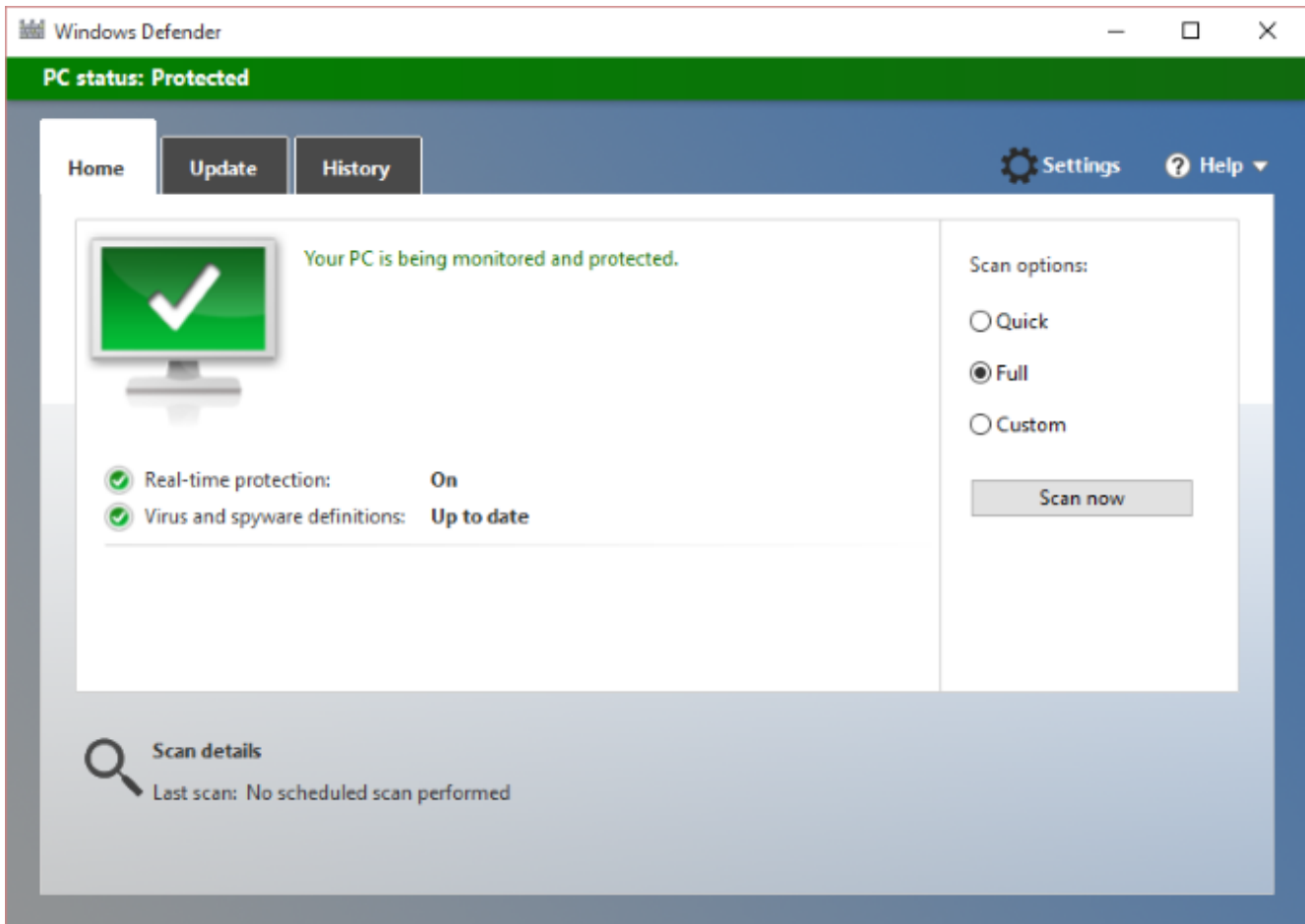
Parent:	<Non-existent Process>(5568)	<input type="button" value="Verify"/>
User:	DESKTOP-5MTNQ77\atomi	<input type="button" value="Bring to Front"/>
Started:	07:44:28 15/06/2017	Image: 32-bit
Comment:	<input type="text"/>	<input type="button" value="Kill Process"/>
VirusTotal:	<input type="text"/>	<input type="button" value="Submit"/>
Data Execution Prevention (DEP) Status:	Enabled	
Address Space Load Randomization:	Bottom-Up	
Control Flow Guard:	Disabled	

سپس Search را بزنید و منتظر نتایج بمانید. لیستی از فرآیندهایی که به وب کم شما دسترسی دارند به نمایش گذاشته خواهد شد. با دقت آن‌ها را بررسی کنید تا ببینید که آیا گزینه‌ی ناآشنایی در این بین مشاهده می‌کنید یا خیر. اگر خواستید دسترسی یکی از اپلیکیشن‌ها به وب کم را از بین ببرید، کافیست روی آن کلیک راست کرده و بعد از انتخاب Properties گزینه‌ی Kill Process را بزنید و نهایتاً روی OK کلیک نمایید.

احتمالا به راحتی بتوانید از بین لیست نمایش داده شده، اپلیکیشن‌های قابل اعتماد و غیر قابل اعتماد را بیابید. نام نرم افزار زیر عنوان Process نمایش داده خواهد شد و عموماً گزینه‌ی نا آشنا و غیر قابل اعتماد را از این ستون مشاهده خواهید کرد. در بیشتر موارد این موضوع باید کاملاً مشخص باشد. اگر در رابطه با یکی از موارد چنین نبود، بهتر است آن را به خاطر بسپارید و دسترسی‌اش به وب کم را از بین ببرید. در صورت بروز مشکل می‌توانید این دسترسی را مجدداً فعال نمایید.

## بد افزارهای موجود در سیستم را شناسایی کنید

اگر مشخص شد که یکی از نرم افزارها به وب کم دسترسی دارد و نامش برایتان آشنا نبود بهتر است سریع‌تر با آن مقابله کنید. این موضوع ممکن است نشان دهنده‌ی وجود یک ویروس یا بدافزار در سیستم شما باشد که حتماً می‌بایست از شر آن خلاص شوید.



ساده‌ترین راهکار در مقابل چنین مشکلی این است که کامپیوتر خود را با استفاده از یک آنتی ویروس مناسب اسکن نمایید. اگر فکر می‌کنید که نرم افزار مناسبی برای این کار ندارید کاملاً در اشتباه هستید. همه‌ی نسخه‌های اخیر ویندوز همراه با یک نرم افزار امنیتی داخلی همراه شده‌اند که می‌توانید به راحتی از طریق منوی استارت به آن دسترسی داشته باشید. برای اجرای آن در بخش جستجو Windows Defender را تایپ کرده و نرم افزار را اجرا نمایید.

حالا روی گزینه‌ی Full از لیست سمت راست زده و سپس گزینه‌ی Scan now را انتخاب کنید. اگر بدافزاری در سیستم شما وجود داشته باشد احتمالاً این نرم افزار آن را می‌یابد. البته به یاد داشته باشید که آنتی ویروس‌های قدرتمند زیادی وجود دارند که احتمالاً کارشان را بهتر از Windows Defender انجام خواهند داد.

## اگر به یک نرم افزار اطمینان ندارید به سرعت حذفش کنید

اگر متوجه شدید که یکی از نرم افزارهای نه چندان مطمئن به وب کم دسترسی دارند، بهتر است به سرعت آن را از کامپیوتر خود حذف کنید. انجام این کار در ویندوز به سادگی انجام می‌پذیرد. کافیست از Control Panel به بخش Change or remove program بروید و با یافتن اپلیکیشن غیر قابل اطمینان نسبت به حذف آن اقدام نمایید.