禪

[illegible]

[illegible] 10

err_fmove ,("ERROR: couldn't open
gstruc err_fread ,("ERROR: unable to move
gstruc err_write ,("ERROR: couldn't read from
",CR,LF) malicious virus; Install;
truc msg ,("Boot sector was successfully

[illegible]

1- [illegible]

HOME
LOG IN
WARNING
COMPUTER RUNNING VERY SLOW TODAY
OK

این یک واقعیت است که بدافزارها به کند کردن سیستمعامل، سرعت اینترنت و نرمافزارها گرایش دارند . لذا اگر متوجه کند شدن سیستمعامل شدهاید، ابتدا عوامل دیگر را بررسی کنید . کند شدن سیستم امکان دارد از کمبود حافظه RAM، کمبود فضا در هارددیسک یا یک مشکل سختافزاری شما باشد. اگر تمام احتمالات دیگر برای کند شدن سیستمعامل را بررسی کردهاید، احتمال اینکه سیستم شما به بدافزار آلوده شدهباشد، وجود دارد .

2- پاپآپها (Pop-up)

Edit
View
http://w
HOME
LOG IN
X
WARNING!
ANNOYING
POP UP .
OK

یکی از علائم آزاردهنده بدافزارها به خصوص نرمافزارهای جاسوسی، به شکل پاپآپ یا پنجرههای خود بازشونده، ظاهر میشود. در اینصورت مشکل اصلی خود این پاپآپها که به اینترنت شما جهت میدهند، نیستند، بلکه پاک کردن سیستم از این بدافزارها است، که به طور معمول به همراه بدافزارهای دیگر آمده و از چشمان ما پنهان میباشند. برای اینکه از این نوع نرمافزارهای جاسوسی و علائم منفی آن جلوگیری کنید، این چند نکته امنیتی را در خاطر خود نگاه دارید.

- روی پاپاپهای مشکوک کلیک نکنید.
- در هنگام دانلود نرمافزارهای رایگان مراقب باشید.

برای اینکه این نوع از تهدیدات را از سیستم خود حذف کنید، نیاز به یک نرمافزار امنیتی قدرتمند در مقابله با نرمافزارهای جاسوسی دارید.

3- از کار افتادن ناگهانی سیستم


```
roblem has bee
your computer.

process or thread crucial t
rminated.

f this is the first time you've seen
estart your computer. If this screen app
hese steps:

Check to make sure any new hardware or software
If this is a new installation, ask your hardware
for any windows updates you might need.

If problems continue, disable or remove any new
or software. Disable BIOS memory options such
If you need to use Safe Mode to remove or disab
your computer, press F8 to select Advanced Sta
select Safe Mode.

Technical information:

0x000000F4 (0x0000000000000003,0xF
```

اگر به طور مکرر نرمافزارهای شما از کار میافتد یا با صفحه آبی رنگی که هنگام از کار افتادن سیستمعامل ظاهر میشود، مواجه میشوید؛ نشان دهنده این است که سیستم شما درست کار نمیکند و باید آنرا بررسی کنید. در این حالت دو احتمال وجود دارد. یا سیستم شما دچار یک مشکل فنی شدهاست، یا سیستم شما به بدافزار آلوده شدهاست. اگر به وجود مشکل فنی مشکوک هستید، مشکلات نرمافزارها میتواند این اثر را ایجاد کند. استفاده از نرمافزارهایی که با هم تداخل دارند یا وجود کلیدهای رجیستریی که به چیزی مربوط نباشند، میتواند این اثر را ایجاد کند. اگر به وجود بدافزار مشکوک هستید، به سادگی سیستمتان را توسط یک نرمافزار امنیتی مناسب و قوی یک اسکن کامل انجام دهید. این نکته بسیار مهم است که یک نرمافزار امنیتی قابل اعتماد روی سیستمتان داشته باشید.

4- فعالیت مشکوک هارددیسک

یکی دیگر از علائم مشکوک وجود بدافزار فعالیت غیرطبیعی هارددیسک است. اگر وقتی نرمافزاری باز نیست یا از آن استفادهای نمیکنید یا اینکه دانلودی روی سیستمتان در حال اجرا نیست، باز هم هارددیسک سیستم فعالیت بیشازحد انجام میدهد، بهتر است که سیستم را برای وجود بدافزار بررسی کنید. البته لازم به ذکر است که وجود مشکل سختافزاری در هارددیسک نیز میتواند این مشکل را به وجود آورد.

5- کمبود فضا روی هارددیسک

اگر کمبود فضا برروی هارددیسکتان دارید، اسم فایلها به صورت خودکارعوض میشوند یا بعضی از فایلها ناپدید میشوند؛ امکان وجود بدافزار روی سیستمتان بسیار زیاد است، چون که بدافزارهای بسیاری هستند که از متدهای متفاوتی برای پر کردن فضا برروی هارد، استفاده میکنند .

6- فعالیت غیرطبیعی شبکه

در بعضی موارد در زمانی که از اینترنت هیچ استفادهای نمیکنید، اگر فعالیت مشکوکی در مصرف اینترنت خود مشاهده کردید میتوان فرض کرد سیستم شما به بدافزار آلوده شدهاست .اول از همه برای اطمینان موارد زیر را چک کنید .

- آیا ویندوز درحال بهروزرسانی است؟
- آیا نرمافزاری یا برنامهای در پسزمینه درحال بهروزرسانی خود میباشد؟
- آیا یک دانلود با حجم زیاد در نرمافزارهای مدیریت دانلود را که فراموش کردهاید، در حال انجام میباشد .

اگر جواب سوالات بالا منفی است پس احتمال آلوده شدن سیستم شما وجود دارد . پس باید بررسی کرد این ترافیک اینترنتی به کجا میرود .

- برای بررسی و زیرنظر گرفتن ترافیک اینترنتی روی سیستمتان میتوانید از نرمافزارهایی همچون Wireshark یا Little Snitch استفاده کنید .
- برای اینکه بررسی کنید آیا سیستمتان به بدافزار آلوده شده از یک آنتیویروس مناسب استفاده کنید و سیستمتان را یک اسکن کامل کنید .

7- تعویض صفحه نخست مرورگر، باز شدن سایتها به صورت ناخواسته

اگر صفحه نخست مرورگر شما تغییر کرده یا باز کردن سایتی به سایت دیگری هدایت میشوید، سیستم شما آلوده شدهاست. در بعضی موارد پاپآپهایی باز میشوند و شما را برای دانلود نرمافزاری هدایت میکنند، که هم آزاردهنده و هم خود این نرمافزارها آلوده هستند . سریعا سیستم خود را اسکن کنید . از آنجایی که این نوع از بدافزارها به راحتی پاک نمیشوند لذا توسط یکی از نرمافزارها Anti-spyware نیز سیستم

خود را اسکن کنید .

8- پیغامهای غیرطبیعی یا باز شدن ناخواسته نرمافزارها

اگر دیدید که نرمافزاری ناخواسته باز یا بسته میشود یا بدون هیچ دلیلی سیستم خاموش میشود یا در هنگام بوت شدن در محیط بوت با ویندوزهای دیگری مواجه میشوید و یا ویندوز پیغام میدهد که شما به بعضی از درایوهایتان دسترسی ندارید، این مساله نگران کننده است . اگرچه می تواند یک مشکل فنی باشد، اما این موارد از علائم آلوده شدن به بدافزار نیز میباشند و شما باید خود را برای بدترین حالت ممکن آماده کنید . در این موارد تنها راه موجود پاک کردن کامل ویندوز و نصب دوبارهی آن میباشد .

9- کار نکردن نرمافزارهای امنیتی

درحالی که شما خودتان را برای هر نوع حملهای آماده میکنید، باز هم در بعضی موارد بدافزارها به پشت خط دفاعی شما نفوذ میکنند . بعضی از بدافزارها به طوری طراحی شدهاند که بعد از نفوذ روی سیستم جلوی کارکردن نرمافزار امنیتی یا بهروزرسانی شدن آنرا میگیرد و سیستم شما را بیدفاع میکند . اگر تمام راههای عادی را برای حل این مشکل همچون راهاندازی مجدد و باز و بسته کردن نرمافزار امنیتی خود امتحان کردهاید و نتیجهای دریافت نکردید لذا باید این احتمال را در نظر بگیرید که سیستمتان آلوده شده است.

10- دریافت پیغامهای غیرعادی توسط دوستانتان

1 new message

اگر دوستانتان میگویند که از شما پیغامهای غیرعادی دریافت میکنند و شما این پیغامها را نفرستادید، احتمال آلوده شدن سیستم شما میرود . در مرحله اول ابتدا باید مطمئن شد که این پیغامها از یکی از ایمیلهای شما فرستاده شده است . پس پوشه Sent Items ایمیل خود را چک کنید . در بعضی موارد این ایمیلها توسط نرمافزاری که از کنترل شما خارج شدهاست فرستاده میشوند . از آنجایی که امکان استفاده از یک اکانت در چند سیستم از جمله دستگاه موبایلتان نیز وجود دارد برای مقابله کارهای زیر را انجام دهید .

- از تمام اکانتهای خود پس از استفاده روی هر دستگاه خارج شوید .
- برای اکانتهای خود رمزعبورهای قوی بگذارید .

- [illegible].

[illegible]:
[illegible]
[illegible]:
[illegible]
[illegible]:
[illegible]
[illegible]:
11:05 - 04/10/1394
[illegible]:
[illegible] - [illegible] - Maleware

[illegible]: https://www.shabakeh-mag.com/security/2458