ویروس کظم غیظ (kazm_gheyz)

ویروس کظم غیظ (kazm_gheyz) که مدتی است انتشار یافته است مشکلاتی را برای کامپیوترهای شخصی و دولتی ایجاد نموده است. بعضی از مشکلات ناشی شده از این ویروس عبارت اند از:

1) **قرار دادن** homepage **اکسپلورر به عنوان وبلاگ خودش به صورتی که هر موقع صفحه اکسپلورر را باز می کنیم به صورت اتوماتیک به وبلاگ مربوطه می رود و امکان حذف این حالت وجود ندارد.**

2) **غیر فعال کردن عنوان** manage **در منوی حاصل از راست کلیک بر روی** my computer

(یکی از کاربردهای گزینه manage **نصب نرم افزارهای مادر بورد و صدا و مودم و ... در ویندوزی که تازه نصب شده است می باشد.)**

3) **غیر فعال کردن گزینه** run **در منوی** start

4) **پنهان نمودن گزینه** folder options **در منوی** tools **در محیط** my computer

چگونگی انتقال این ویروس:

این ویروس در حالت عادی در هنگام اتصال از اینترنت به کامپوتر انتقال می یابد و با حضور در سایت و یا وبلاگ خاصی انتقال نمی یابد.

نحوه پاک کردن ویروس kazm_gheyz

مرحله 1 – ابتدا دو گزینه ی regedit.exe : و taskmgr.exe **را به کمک گزینه** search **در منوی** start **جستجو نمایید. بعد عنوان آنها را به صورت دلخواه تغییر دهید. (البته این کار موقعی لازم است که ویروس این دو گزینه را غیر فعال کرده باشد. اگر با زدن کلیدهای** ctrl + alt + delete **برنامه** task manager **اجرا شود یعنی هنوز ویروس این قسمت را فعال نکرده است. و یا اگر در گزینه** run **در منوی** start **کلمه** regedit **را تایپ نمایید و** ok **را بزنید و کادر مربوطه باز شود یعنی هنوز ویروس این گزینه را نیز غیرفعال نکرده ، پس می توانید به مرحله** 2 **بروید.**

مرحله 2 – **با زدن کلیدهای** ctrl + alt + delete **برنامه** task manager **را اجرا کنید و در** tab **با عنوان** processes **پروسه ها با عنوان** kazm_gheyz **و کلمات مشابه را انتخاب و** end process **را بزنید.**

مرحله 3 – **در گزینه** run **در منوی** start **کلمه** regedit **را تایپ نمایید و** ok **را بزنید تا کادر مربوطه باز شود در سمت راست کادر** my computer **را انتخاب نمایید و کلیدهای** ctrl + f **را بزنید کلمه** kazm **را وارد نمایید کلید** search **را بزنید و عبارات یافته شده تحت عنوان** kazm_gheyz **را** delete **نمایید و این کار را ادامه دهید. تا جستجو نتیجه ی دیگر نداشته باشد و جستجو پایان یابد.**

مرحله 4– **صفحه** my computer **را باز کنید و از منوی** tools **گزینه** folder options **را انتخاب کنید و به تب** view **بروید و تیک** show hidden files and folders **را بزنید و تیک دو تا گزینه زیدر آن که با** hide **شروع می شود را بردارید و کلید** apply **را بزنید.**

مرحله 5 – **هم با استفاده از گزینه** search **و هم به صورت جستجوی دستی از داخل همه درایوها دو فایل** kazm_gheyz.exe **و** autorun.info **را با زدن کلیدهای** shift + delete **پاک کنید** .

مرحله 6 – **یک نسخه از این ویروس در درایوهایی که ویندوز نصب کرده اید در شاخه** Windows/system۳۲ **نیز منتشر شده است که باید در این شاخه به دنبال عنوان** kazm_gheyz **بگیرید و آنها را نیز پاک کنید.**

مرحله 7– **به صفحه** internet explorer **بروید و از منوی** tools **گزینه** internet options **را انتخاب کنید و** home page **را روی** use blanked **قرار دهید.**

پس از انجام این کارها ویروس از بین می رود در هر صورت می توانید این مراحل را تکرار نمایید تا از بین رفتن آن اطمینان حاصل نمایید.

راه دیگر برای آگاهی از حضور این ویروس در کامپیوترتان نصب ویروس کش kaspersky **می باشد و اجرای آنها برای** scan **کامپیوتر می باشد.**

و یا نصب نرم افزار Trojan remover **می باشد.**