

**اگر اهل گشت و گذار در اینترنت مخصوصاً سایتهای امنیتی و یا هکری باشید حتماً با واژه تروجان آشنا هستید. شاید برداشت اکثریت ما از این واژه همان ویروس اینترنتی باشد. ولی تروجان چیست ؟**

اگر بخواهیم برای تروجان یک تعریف ساده بیان کنیم می توانیم بگوییم: تروجان یک فایل جاسوسی می باشد که توسط هکر با توجه به نیاز به اطلاعات قربانی آماده می شود و برای قربانی فرستاده می شود با کمی دقت در تعریف تروجان در می یابیم که تروجان هیچ وقت نمی تواند یک ویروس باشد.

هکر با توجه به نیازهای خود به اطلاعات قربانی که می تواند این اطلاعات: پسورد ایمیل یا ایدی قربانی، اشتراک اینترنت (اکانت)، نام و پسورد کامپیوتر قربانی و... است تنظیم کند.

**معمولاً تروجانها به دو قسمت تقسیم می شوند:**

- ۱- کلاینت: که تنظیمات را انجام داده و آن را با توجه به نیازهایی که بیان کردیم تنظیم می نمایند
- ۲- سرور: که بعد از تنظیمات باید این سرور برای قربانی فرستاده شود تا قربانی بعد از دریافت آن را اجرا کند. با توجه به تحقیقات می توانیم بگوییم هر هکری کار خود را با این نوع کارها شروع می کند. یعنی با تنظیم تروجان، فرستادن تروجان برای قربانی، هک کردن ایدی و اکانت اینترنت و... در اوایل ورود این نوع جاسوسها به اینترنت فقط کارایی محدودی داشتند.

همه کارایی آن نوع تروجانها به فرستادن پسورد یا هو ختم می شد. با گذشت زمان و علاقه برنامه نویسان به این نوع جاسوس ها کم کم امکانات آن را افزایش دادند تا به امروز.

**امکانات یک تروجان امروزی چیست ؟**

تروجانهای امروزی دیگر رشد کامل خود را تا حد زیادی طی نموده اند امکان دارد با ورود یک تروجان به کامپیوتر شما:

- ۱- فرستاده شدن پسورد ای دی مخصوصاً ایدی و پسورد مسنجر شما برای هکر (به ایمیل هکر یا ایدی یا یک اف تی پی مشخص شده توسط هکر)
- ۲- فرستاده شدن اکانت اینترنت شما برای هکر
- ۳- فرستاده شدن نام کامپیوتر شما همراه با پسورد ویندوز برای هکر
- ۴- محدود کردن کارهای شما با کامپیوتر (قفل شدن Task Manager یا Mscoing یا Registry و) کامپیوتر شما توسط هکر
- ۵- از کار انداختن ویروس کش و فایروال کامپیوتر شما
- ۶- در اختیار داشتن هارد شما توسط هکر (پاک کردن فایل از کامپیوتر شما و یا اضافه کردن فایل توسط هکر) بله همه اینها امکان دارد. فقط کافیست یک تروجان روی کامپیوتر شما توسط هکر فعال شود.

**چگونه امکان دارد که تروجان وارد کامپیوتر ما شود:**

- ۱- در حال چت کردن هستید فرد مقابل برایتان می خواهد عکس خودش یا نرم افزاری را سند کند. شما آن را می گیرید ولی

آیا این فایل سالم است. از کجا مطمئن هستید که حاوی تروجان نیست؟

۲- در حال گشت در یک سایت آموزش هک هستید می خواهید یک نرم افزار دانلود کنید از کجا مطمئن هستید که این نرم افزار سالم است؟

۳- برایتان یک ایمیل می آید. ایمی لی که فرستنده آن نامشخص است آیا ایمیل سالم است؟  
و تروجان ها بر خلاف ویروس ها که فقط شامل چند شکل محدود می شوند دارای اشکال خیلی زیادی هستند. یک تروجان می تواند خود را به شکلهای: عکس، یک فایل صوتی، یک فایل نقاشی، یک فایل Setup و... پس می بینید تروجان یک شکل مخصوص ندارد .

چگونه متوجه شویم که در کامپیوتر ما تروجان فعال است:

۱- در صورت از کار افتادن Task Manager و Msconfig

۲- از کار افتادن ویروس کش

۳- تغییر در شکل توپی پسورد در مسنجر و یا save نشدن آن

۴- در صورت دیدن علائم مشکوک در مسنجر (باز و بسته شدن یک پنجره پی ام)

۵- فعال بودن نرم افزار های مشکوک مثل Task Manager و Msconfig

۶- خوانده شدن ایمیل هایی که ما آنها را قبلا نخوانده ایم در ایمیلان

ما برای مقابله با این نوع جاسوسها چه کارهایی باید انجام دهیم؟

۱- داشتن یک ویروس کش قوی و به روز

۲- داشتن یک فایروال خوب یا فعال کردن فایروال خود ویندوز

۳- این را بدانید همیشه پسوند عکس ((.gif, .jpg))، می باشد و هیچ وقت یک عکس دارای پسوند exe نمی باشد و همیشه اگر

فایل (عکس، نوشته و) را گرفتید که دارای پسوند مشکوک بود هرگز باز نکنید

۴- همیشه Task Manager و Msconfig خود را چک کنید اگر چیزی مشکوک دیدید مثل sender.exe بروید و در

درایو ویندوز پوشه windows/system32 دنباله چنین فایل می باشید که مشکوک بود و آن را پاک کنید

۵- هرگز از کسی که شناخت کافی ندارید فایل دریافت نکنید

۶- سعی کنید اگر می خواهید نرم افزار دانلود کنید از سایتهای معتبر دانلود کنید.

۷- در صورت مشکوک شدن به وجود تروجان سریع اطلاعات خود را عوض کنید (پسورد ای دی، پسورد ویندوز و)

۸- سعی کنید ویندوز خود را عوض کنید و درایو ویندوز قبلی را فرمت کنید .

منبع : [www.iritn.com](http://www.iritn.com)

تنظیم و گردآوری : حکمت ، hgtoinfo@tabaar.com

This document was created with Win2PDF available at <http://www.daneprairie.com>.  
The unregistered version of Win2PDF is for evaluation or non-commercial use only.