

اگر اهل گشت و گذار در اینترنت مخصوصاً سایتهای امنیتی و یا هکری باشید حتمی 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 میتوانیم بگوییم: **"تروجان یک فایل جاسوسی میباشد که توسط هکر با توجه به نیاز به اطلاعاته قربانی آماده میشود و برای قربانی فرستاده میشود"**

با کمی دقت در تعریف تروجان در می یابیم که تروجان هیچ وقت نمیتواند یک ویروس باشد. هکر با توجه به نیازهای خود به اطلاعات قربانی که میتواند این اطلاعات: پسورد ایمیل یا ایدی قربانی، اشتراک اینترنت (اکانت)، نام و پسورد کامپیوتر قربانی و ... میباشد تنظیم میکند. معمولاً تروجانها به دو قسمت تقسیم میشوند:

- 1- کلاینت: که تنظیمات را انجام داده و آن را با توجه به نیازهایی که بیان کردیم تنظیم مینماید
 - 2- سرور: که بعد از تنظیمات باید این سرور برای قربانی فرستاده شود تا قربانی بعد از دریافت آن را اجرا کند. با توجه به تحقیقاتی که داشتیم میتوانیم بگوییم هر هکری کار خود را با این نوع کارها شروع میکند. 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 پاهو ختم میشد.
- با گذشت زمان و علاقه برنامه نویسان به این نوع جاسوسها کم کم امکانات آن را افزایش دادند تا به امروز.

ولی امکانات یک تروجان امروزی چیست؟

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

- 1- 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)
- 2- فرستاده شدن اکانت اینترنت شما برای هکر
- 3- فرستاده شدن نام کامپیوتر شما همراه با پسورد ویندوز برای هکر
- 4- محدود کردن کارهای شما با کامپیوتر (قفل شدن Task Manager یا Mscoing یا Rigistry و...) کامپیوتر شما توسط هکر

5- از کار انداختن ویروس کش و فایروال کامپیوتر شما

6- در اختیار داشتن هارد شما توسط هکر (پاک کردن فایل از کامپیوتر شما و یا اضافه کردن فایل توسط هکر) بله همه اینها که خوندید امکان دارد. فقط کافیست یک تروجان روی کامپیوتر شما توسط هکر فعال شود. ولی چگونه امکان دارد که تروجان وارد کامپیوتر ما شود:

- 1- در حال چت کردن هستید فرد مقابل برایتان میخواهد عکس خودش یا نرم افزاری را سند کند. شما آن را میگیرید ولی آیا این فایل سالم است. از کجا مطمئن هستید که حاوی تروجان نیست؟
 - 2- در حال گشت در یک سایت آموزش هک هستید میخواهید یک نرم افزار دانلود کنید از کجا مطمئن هستید که این نرم افزار سالم است؟
 - 3- برایتان یک ایمیل میاید. ایمیلی که فرستنده آن نامشخص است آیا ایمیل سالم است؟
- و...

تروجانها بر خلاف ویروسها که فقط شامل چند شکل محدود میشوند دارای اشکال خیلی زیادی هستند.

یک تروجان میتواند خود را به شکلهای: عکس، یک فایل صوتی، یک فایل نقاشی، یک فایل Setup و... پس مبینید تروجان یک شکل مخصوص ندارد.

چگونه متوجه شویم که در کامپیوتر ما تروجان فعال است:

- 1- در صورت از کار افتادن Task Manager و Msconfig
 - 2- از کار افتادن ویروس کش
 - 3- تغییر در شکل توپی پسورد در مسنجر و یا سیو نشدن آن
 - 4- در صورت دیدن علائم مشکوک در مسنجر (باز و بسته شدن یک پنجره پی ام)
 - 5- فعال بودن نرم افزارهای مشکوک مثل Task Manager و Msconfig
 - 6- خوانده شدن ایمیل های که ما آنها را قبلاً نخوانده ایم در ایمیلمان
- ولی ما برای مقابله با این نوع جاسوسها چه کارهایی باید انجام دهیم؟

1- داشتن یک ویروس کش قوی و به روز

2- داشتن یک فایروال خوب یا فعال کردن فایروال خود ویندوز (در مقالات بعدی این مبحث پرداخته میشود)

- 3- این را بدانید همیشه پسوند عکس (jpg,gif,..) میباشد و هیچ وقت یک عکس دارای پسوند exe نمیباشد و همیشه اگر فایل(عکس,نوشته و...) را گرفتید که داری پسوند مشکوک بود هرگز باز نکنید
 - 4- 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 فایلی باشید که مشکوک بود و آن را پاک کنید
 - 5- هرگز از کسی که شناخت کافی ندارید فایلی دریافت نکنید
 - 6- سعی کنید اگر میخواهید نرم افزار دانلود کنید از سایتهای معتبر دانلود کنید.
 - 7- در صورت مشکوک شدن به وجود تروجان سریع اطلاعات خود را عوض کنید(پسورد ای دی,پسورد ویندوز و...)
 - 8- سعی کنید ویندوز خود را عوض کنید و درایو ویندوز قبلی را فرمت کنید.
- در مقالات بعدی به شما خواهیم گفت چگونه برای خود پسورد انتخاب نمایید که امکان هک شدنتان را تا حد امکان کم کند

ERROR: syntaxerror
OFFENDING COMMAND: --nostringval--

STACK:

/Title
(Satanic)
/Author
(Nice PDF Creator - <http://www.nicepdf.com>)
/Producer
(Microsoft Word 11.0)
/Creator
-mark-