

به نام خدا

جلد نامہ تحقیق

کد تحقیق : ۶۴۴

محقق : اشکان حسنی

موضوع تحقیق : تروجان

اگر اهل گشت و گذار در اینترنت مخصوصا سایتهای امنیتی و یا هکری باشید حتماً با واجه تروجان آشنا هستید. شاید برداشت اکثریت ما از این واجه 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:

۱- کلاینت: که تنظیمات را انجام داده و آن را با توجه به نیازهایی که بیان کردیم تنظیم مینمایند

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 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 یا هو ختم میشد.

با گذشت زمان و علاقه برنامه نویسان به این نوع جاسوس ها 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:

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 **Mscoring** یا **Rigistry** 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 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:

۱- 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؟

۲- 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؟

۳- برایتان یک ایمیل میاید. ایمیلی که فرستنده آن نامشخص است آیا ایمیل سالم است؟
و...

تروجان ها بر خلاف ویروس ها 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 میبینید تروجان یک شکل مخصوص ندارد .

چگونه متوجه شویم که در کامپیوتر ما تروجان فعال است:

۱- در صورت از کار افتادن **Task Manager** و **Mscconfig**

۲- از کار افتادن ویروس کش

۳- تغییر در شکل تویی پسورد در مسنجر و یا سیون نشدن آن

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

۵- فعال بودن نرم افزارهای مشکوک مثل **Task Manager** و **Mscconfig**

۶- خوانده شدن ایمیل های که ما آنها را قبلا نخوانده ایم در ایمیلمان

پایان تحقیق

منابع : <http://www.persianhack.com/show.aspx?id=۲>

با تشکر از توجه شما کاربر گرامی خواهشمندم نظرات خود را به نشانی زیر بفرستید
Ashkan.hasani۲۰۰۹@gmail.com

وبلاگ : WWW.IECDL.blogfa.com

اشکان حسنی
