Namatek
True Education

Trojan

www.namatek.com

تروجان چیست؟

فهرست مطالب

اگر شما هم در حوزه امنیت شبکه و بدافزارهای کامپیوتری بررسی هایی داشته باشید حتما با نام Trojan آشنا شده اید و احتمالا این سوال برای شما پیش آمده که تروجان چیست؟

غالب افراد گمان می کنند که ویروس ها تنها نرم افزار های مخرب موجود در جهان هستند، اما این طور نیست؛ زیرا تروجان ها نیز از بدافزار های رایجی به حساب می آیند که هکرها از آن ها برای دستیابی به منافع خود استفاده می کنند. در ادامه این مطلب با ما همراه باشید تا به طور کامل به بررسی تروجان بپردازیم.

#۱ تعریف تروجان چیست؟

اگر فیلم تروی را دیده باشید متوجه خواهید شد که اصطلاح تروجان (Trojan) از داستان این فیلم گرفته شده است. تروجان در واقع اسبی بود که با فریب مردم یونان باستان، منجر به سقوط شهر تروی شد. بد افزار های تروجان نیز به همین شکل عمل می کنند. آن ها در برنامه های به ظاهر بی خطر پنهان می شوند.

بدین ترتیب افراد فریب می خورند و چنین برنامه هایی را دانلود می کنند. Trojan همانند ویروس ها و کرم ها تکثیر نمی یابد؛ بلکه این کاربران هستند که آن ها را به اشتباه نصب می کنند. تروجان ها مجرمان

سایبری را قادر می سازند تا جاسوسی کنند، اطلاعات مهم شما را به سرقت ببرند و پنهانی به سیستم شما دسترسی پیدا کنند.

#۲ انواع تروجان

تروجان ها بر اساس اعمالی که در رایانه های شما به انجام می رسانند طبقه بندی می شوند. در جهان امروزی این بد افزار ها گسترش بسیاری پیدا کرده اند و انواع زیادی دارند. در ادامه این بخش با رایج ترین انواع تروجان ها آشنا خواهید شد و به طور خلاصه به شما می گوییم که ویژگی انواع تروجان چیست.

- Backdoor تروجان ها: این نوع از تروجان ها به هکرها اجازه دسترسی به سیستم قربانیان را می دهند. ورود آن ها به هر

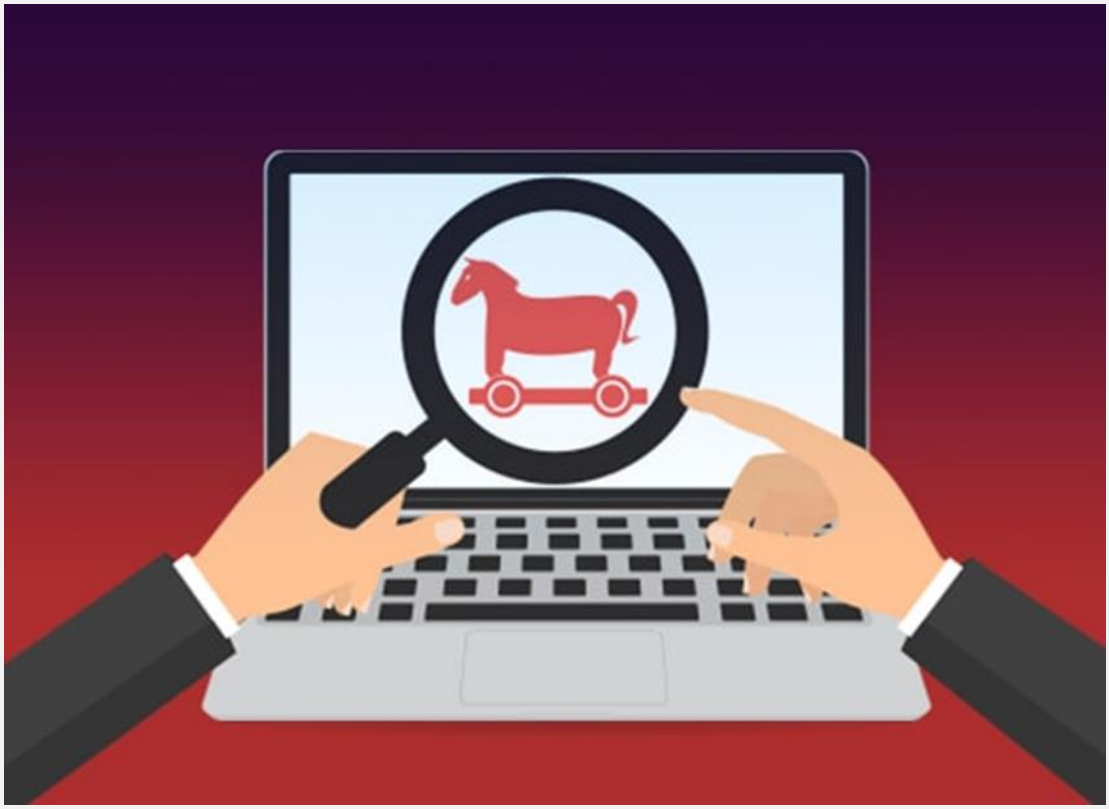
سیستمی اغلب با بارگیری و اجرای برنامه هایی توسط کاربران به انجام می رسد.

- Exploit تروجان ها: چنین تروجان هایی برنامه هایی با کدها و داده هایی خاص هستند که از ضعف یک سیستم برای آسیب به آن استفاده می کنند.
- Rootkit تروجان ها: این تروجان ها از کشف بد افزار هایی که از قبل بر روی سیستم وجود دارند، جلوگیری می کنند تا آسیب به حداکثر میزان خود برسد.
- Banker تروجان ها: چنین تروجان هایی به طور خاص اطلاعات شخصی مربوط به خدمات بانکی و خریدهای آنلاین را مورد هدف قرار می دهند.
- DDoS تروجان ها: این تروجان ها با حملات DDoS، سرور ها را از دسترس کاربران خارج می کنند.
- Downloader تروجان ها: چنین تروجان هایی می توانند برنامه های مخرب دیگر را بر روی سیستم شما بارگذاری نمایند.

#۳ شناسایی تروجان ها

در ادامه پاسخ به پرسش تروجان چیست، لازم می دانیم به نحوه شناسایی این بد افزار ها بپردازیم. بروز نشانه های زیر می تواند ناشی از وجود تروجان ها در سیستم شما باشد.

- عملکرد ضعیف دستگاه: سرعت پایین رایانه ها و وجود نواقصی در عملکرد آن ها می تواند نشانه وجود تروجان ها باشد.
- عملکرد عجیب دستگاه: اگر فرآیندهای غیر قابل توضیحی مانند اجرای برنامه هایی که بر روی دستگاه نصب نشده است ایجاد شود، احتمال آلودگی به تروجان وجود خواهد داشت.
- تبلیغات pop up و هرزنامه ها: مواجهه با تعداد زیادی تبلیغ در هنگام کار با مرورگر و یا دریافت ایمیل هایی که تمایلی به مشاهده آن ها ندارید یا به اصطلاح هرزنامه، می تواند به وجود تروجان ها اشاره داشته باشد.



اگر دستگاه شما این مشکلات را دارد، باید به وجود تروجان ها شک کنید. به دنبال هر برنامه ای بگردید که خودتان آن ها را بر روی سیستم نصب نکرده بودید. سپس با استفاده از نرم افزار های آنتی ویروس به بررسی دستگاه خود بپردازید.

#۴ روش پیشگیری از ورود تروجان چیست؟

در پاسخ به سوال تروجان چیست، قصد داریم روش های مبارزه با آن را نیز بیان کنیم. به طور کلی ترکیبی از نرم افرار های امنیتی و آنتی ویروس می تواند در محافظت از سیستم شما در برابر تروجان ها موثر باشد.

با این حال روش های پیشگیری از آلودگی به Trojan دیگری نیز وجود دارد که در ادامه با آن ها آشنا خواهید شد.

- احتیاط در دانلود ها: از دانلود برنامه ها از منابع ناشناس بپرهیزید.
- آگاهی در برابر تهاجم های فیشینگ (phishing): هرگز فایل های اتچ شده، برنامه ها و لینک هایی که از ایمیلی ناشناس دریافت می کنید را باز ننمایید.
- به روز رسانی: علاوه بر آپدیت سیستم عامل، همواره دیگر نرم افزارها و برنامه های موجود در سیستم خود را به روزرسانی کنید. آپدیت ها عموما امنیت برنامه ها را بالا می برند.
- بازدید از سایت های معتبر: یکی از مسائل مهمی که در پاسخ به پرسش روش پیشگیری از آلودگی به تروجان چیست مطرح می شود، مربوط به امنیت سایت هایی است که از آن ها بازدید می

کنید. آدرس وب سایتی که بازدید از آن، مشکلی را ایجاد نخواهد کرد با https:// شروع می شود. S در این آدرس ها به معنایsafe یا ایمن بودن است.

- نادیده گرفتن پاپ آپ ها: هرگز بر روی تبلیغاتی که ناآشنا هستند، هشداری در رابطه با آلودگی سیستم می دهند و یا پیشنهاد ویژه ای برای بهبود وضیت آن دارند، کلیک نکنید.
- بک آپ: بک آپ گرفتن از داده ها، سیستم ها را از آلودگی به تروجان محافظت نمی کند؛ اما باعث می شود در زمان ورود تروجان به دستگاه، اطلاعات کمتری را از دست بدهید.

علاوه بر تمام پیشنهادات فوق ما به شما نصب آنتی ویروس های قوی را پیشنهاد می دهیم؛ زیرا این روش بهترین راه مبارزه با تروجان ها به حساب می آید.

حرف آخر

همان طور که با مطالعه این مطلب در رابطه با تروجان چیست متوجه شده اید، تروجان ها می توانند با ورود به سیستم ها به حریم خصوصی افراد تجاوز کرده و جاسوسی هایی را به عمل آورند. در نتیجه همواره نسبت به این بدافزار ها آگاه باشید و با استفاده از روش های پیشگیری از آلودگی گفته شده، راه ورود تروجان ها را به دستگاه های خود مسدود نمایید.

امیدواریم توانسته باشیم با ارائه این مطلب به اکثر سوالات شما عزیزان در ارتباط با تروجان ها پاسخ مناسبی دهیم.