

تهدیدها و حملات شبکه های کامپیوتری

خرداد 18, 1394

به گزارش خبرنگار [نشریه الکترونیکی نگاه](#)، هنگام [وبگردی](#) و [*](#) مشاهده صفحات وب ممکن است اتفاقاتی پشت پرده بیفتد که حتی در ظاهر قابل مشاهده و درک نباشد، این اتفاقات و تغییرات ممکن است سیستم شما را در برابر حملات آسیب پذیر کند. خوشبختانه با مرور زمان و با پیشرفت تکنولوژی، کاربران اینترنت با انواع حملات و تهدیدات اینترنت آشنا شده و نحوه ایمن سازی سیستمها در برابر این حملات را فرا میگیرند.

می توان گفت صفحاتی که دارای دکمه های دانلود بیشتر و لینک های هستند که کاربران را وادار به دانلود می کنند، دیگر کمتر سیستمها را در معرض خطر قرار می دهند. زیرا اطلاعات کاربران در این زمینه بیشتر شده و مرورگرها نیز در برابر این حملات آسیب پذیر نیستند. البته کسانی هم هستند که در اثر اطلاعات کم و نداشتن آگاهی فریب آگهی ها و دکمه های دانلود نامربوط را می خورند حال در ابتدا باید انواع تهدیدها را بشناسیم؛ در این راستا گفتگویی با سرهنگ "کوره بلاغی" رئیس پلیس فتای فرماندهی انتظامی استان آذربایجان غربی صورت گرفته است.

توضیحاتی در خصوص حملات شبکه های کامپیوتری بفرمایید؟

Malware : نرم افزارهای مخرب

کلمه Malware مخفف عبارت «Malicious Software» به معنای [نرم افزار مخرب](#) است. این نرم افزار حاوی انواع ویروسها و نرم افزارهای جاسوسی است که بدون این که شما متوجه شوید روی کامپیوتر و تلفن هوشمند یا روی دستگاه های قابل حمل نصب می شود. این برنامه ها، عامل اصلی توقف اجرای برنامه ها یا هنگ کردن آنها در دستگاهها به شمار آمده و از این برنامه ها برای کنترل و نظارت بر فعالیت های کاربران در فضای مجازی استفاده می شود. هکرها از این برنامه ها برای دزدیدن اطلاعات شخصی و ارسال اسپم و انجام فعالیت های مجرمانه استفاده می کنند

مقابله با نصب نرم افزارهای مخرب

مکرراً نرم افزارهاي امنيتي و آنتيويروسهاي خود را بروز رساني کنيد. نصب يک نرم افزار ضد جاسوسي و فايروال مجزا توصيه ميشود. نرم افزارهاي امنيتي، مرورگر اينترنتي و سيستم عامل خود را به گونه اي تنظيم کنيد تا به صورت خودکار بروز رساني شوند. در صورت اطلاع از محتواي لينکها، بر روي آنها کليک کنيد، و همچنين بر روي فايل هاي ضميمه شده در ايميلهاي ناشناس کليک نکنيد؛ مگر آن که فرستنده ايميل را بشناسيد. کليک کردن بر روي لينک ها و فايل هاي ضميمه، حتي در ايميل هايي که به نظر مي رسد از طرف دوستان و يا خانواده فرستاده شده است ميتواند باعث نصب نرم افزارهاي مخرب در کامپيوتر شود. نرم افزارها را تنها از وبسايتهايي که مي شناسيد و به آنها اطمينان داريد، دانلود و نصب کنيد. دانلود کردن بازيهاي رايجان و برنامه هاي به اشتراک گذاري فايل و نوار ابزارهاي شخصي در ظاهر جذاب و فريبنده هستند؛ اما نرم افزارهاي مخرب اغلب با نرم افزارهاي رايجان دانلود مي شوند. دانلودهاي ناخواسته را به حداقل برسانيد. اطمينان حاصل کنيد که امنيت مرورگر شما به قدری بالاست که قادر به شناسايي دانلودهاي ناخواسته است. پنجرههاي پاپآپ را مسدود کنيد و بر روي لينک هايي که در پنجرههاي پاپآپ ظاهر مي شود، کليک نکنيد. از اطلاعات خود به طور مرتب، نسخه پشتيبان تهيه کنيد.

ويروسها

ويروس کامپيوتري، نرم افزاري است که دائماً از خود کپي ميگيرد و آنها را در فايلها و برنامههاي ديگر قرار ميدهد. اين فايلها پس از وارد شدن به کامپيوتر اقدامات غيرمنتظره اي انجام ميدهند. با وجود اين که همه ويروسها خطرناک نيستند، ولي بسياري از آنها با هدف تخريب انواع مشخصي از فايلها، برنامههاي کاربردي يا سيستم عامل نوشته شده اند. ويروسها هم مشابه همه برنامههاي ديگر از منابع سيستم مانند حافظه و فضاي ديסק سخت، توان پردازنده مرکزي و ساير منابع بهره ميگيرند و ميتوانند اعمال خطرناکي را انجام دهند بايد براي تشخيص ويروسهاي جديد آنتي ويروسها را مرتباً به روز رساني کرد.

Adware : ابزارهاي تبليغاتي

اين ابزارها به عنوان ابزارهاي تبليغاتي مزاحم شناخته ميشوند که توسط هکرهاي آنلاين براي به دست آوردن غير قانوني پول زياد توسعه مييابند. اين ابزارهاي تبليغاتي مزاحم معمولاً همراه با نرم

افزارهاي رایگان کاربران را وادار میکنند تا آنها را از وبسایتهای مشکوک دانلود کنند. زمانی که کاربر در حال گشت و گذار در اینترنت است، تعداد زیادی از پاپ‌آپها، لینکها و دیگر تبلیغات مزاحم نمایش داده میشود. این ابزارها برای کاربران بسیار آزاردهنده هستند، زیرا لینکهای موجود در این تبلیغات آلوده هستند. به واسطه کلیک روی این تبلیغات، کاربر به سایت دیگری هدایت شده و کامپیوتر در معرض خطر قرار میگیرد. این ابزارهای تبلیغاتی مزاحم و زننده، ترافیک وب کاربر را جمع آوری کرده و آنها را برای دیگر وبسایتهای مشکوک منتقل میکنند.

تروجان و دربهای پشتی

تروجان، برنامه مخربی است که به صورت یک نرم افزار جالب به نظر میرسد. برخلاف ویروسها، تروجانها تکثیر نمیشوند؛ ولی به اندازه ویروسها مخرب هستند. تروجان ابتدا به قسمتهای مختلف نفوذ میکند، سپس راهی برای آسیب به آنها پیدا خواهد کرد.

دربهای پشتی همان گونه که از نام آن معلوم است یک راه نفوذ پیش بینی نشده برای ورود غیر مجاز ایجاد میکنند. درپشتی نوعی بدافزار است که به ظاهر برنامه‌های ساده و سالم است ولی در شرایطی خاص زمینه ورود و دسترسی مهاجمان به داده‌های سیستمی را که روی آن نصب شده است مهیا میکند.

برای جلوگیری از این نوع آسیب پذیرچه مواردی باید رعایت بشه؟

1) هرگز پیوست ایمیل‌های دریافتی را از سوی کاربران ناشناس باز نکنید.

در بسیاری از وبسایتهای کلیدهای با عنوان دانلود در نزدیکی لینکهای واقعی دانلود وجود دارد. حتما قبل از کلیک کردن روی آنها از هدف آن لینکها، با نگه داشتن ماوس و مشاهده آدرسی که با کلیک کردن به آن هدایت خواهید شد، مطمئن شوید.