تهدیـــدها و حملات شبکـــه هـــای کامپیوتری

خرداد 18, 1394

به گزارش خبرنگار نشریه الکترونیکی نگاه، هنگام وب‌گردي و مشاهده صفحات وب ممکن است اتفاقاتي پشت پرده بيفتد که حتي در ظاهر قابل مشاهده و درک نباشد، اين اتفاقات و تغييرات ممکن است سيستم شما را در برابر حملات آسيب‌پذير کند. خوشبختانه با مرور زمان و با پيشرفت تکنولوژي، کاربران اينترنت با انواع حملات و تهديدات اينترنت آشنا شده و نحوه ايمن سازي سيستم‌ها در برابر اين حملات را فرا مي‌گيرند.

مي‌توان گفت صفحاتي که داراي دکمه‌هاي دانلود بيشتر و لينک‌هايي هستند که کاربران را وادار به دانلود مي‌کنند، ديگر کمتر سيستم‌ها را در معرض خطر قرار مي‌دهند. زيرا اطلاعات کاربران در اين زمينه بيشتر شده و مرورگرها نيز در برابر اين حملات آسيب‌پذير نيستند. البته کساني هم هستند که در اثر اطلاعات کم و نداشتن آگاهي فريب آگهي‌ها و دکمه‌هاي دانلود نامربوط را مي‌خورند حال در ابتدا بايد انواع تهديدها را بشناسيم؛ در اين راستا گفتگويی با سرهنگ "کوره بلاغي" رئيس پليس فتاي فرماندهي انتظامي استان آذربايجان غربي صورت گرفته است.

توضیحاتی در خصوص حملات شبکه های کامپیوتری بفرمایید؟

Malware : نرم افزارهاي مخرب

کلمه Malware مخفف عبارت «Malicious Software» به معناي نرم افزار مخرب است. اين نرم افزار حاوي انواع ويروس‌ها و نرم افزارهاي جاسوسي است که بدون اين که شما متوجه شويد روي کامپيوتر و تلفن هوشمند يا روي دستگاه‌هاي قابل حمل نصب مي شود. اين برنامه‌ها، عامل اصلي توقف اجراي برنامه ها يا هنگ کردن آن‌ها در دستگاه‌ها به شمار آمده و از اين برنامه‌ها براي کنترل و نظارت بر فعاليت هاي کاربران در فضاي مجازي استفاده مي‌شود. هکرها از اين برنامه ها براي دزديدن اطلاعات شخصي و ارسال اسپم و انجام فعاليت‌هاي مجرمانه استفاده مي‌کنند

مقابله با نصب نرم افزارهاي مخرب

مكررا نرم افزارهاي امنيتي و آنتي‌ويروس‌هاي خود را بروز رساني كنيد. نصب يک نرم افزار ضد جاسوسي وفايروال مجزا توصيه مي‌شود. نرم افزارهاي امنيتي، مرورگر اينترنتي و سيستم عامل خود را به گونه اي تنظيم كنيد تا به صورت خودكار بروز رساني شوند. در صورت اطلاع از محتواي لينک‌ها، بر روي آن‌ها كليک كنيد، و همچنين بر روي فايل هاي ضميمه شده در ايميل‌هاي ناشناس كليک نكنيد؛ مگر آن كه فرستنده ايميل را بشناسيد. كليک كردن بر روي لينک ها و فايل هاي ضميمه، حتي در ايميل هايي كه به نظر مي رسد از طرف دوستان و يا خانواده فرستاده شده است مي‌تواند باعث نصب نرم افزارهاي مخرب در كامپيوتر شود. نرم افزارها را تنها از وب‌سايت‌هايي كه مي شناسيد و به آنها اطمينان داريد، دانلود و نصب كنيد. دانلود كردن بازيهاي رايگان 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 رايگان دانلود مي شوند. دانلودهاي ناخواسته را به حداقل برسانيد. اطمينان حاصل كنيد كه امنيت مرورگر شما به قدري بالاست كه قادر به شناسايي دانلودهاي ناخواسته است. پنجره‌هاي پاپ‌آپ را مسدود كنيد و بر روي لينک هايي كه در پنجره‌هاي پاپ‌آپ ظاهر مي شود، كليک نكنيد. از اطلاعات خود به طور مرتب، نسخه پشتيبان تهيه كنيد.

ويروس‌ها

ويروس كامپيوتري، نرم افزاري است كه دائما از خود كپي مي‌گيرد و آن‌ها را در فايل‌ها و برنامه‌هاي ديگر قرار مي‌دهد. اين فايل‌ها پس از وارد شدن به كامپيوتر اقدامات غيرمنتظره‌اي انجام مي‌دهند. با وجود اين كه همه ويروس‌ها خطرناک نيستند، ولي بسياري از آن‌ها با هدف تخريب انواع مشخصي از فايل‌ها، برنامه‌هاي كاربردي يا سيستم عامل نوشته شده‌اند. ويروس‌ها هم مشابه همه برنامه‌هاي ديگر از منابع سيستم مانند حافظه و فضاي ديسک سخت، توان پردازنده مركزي و ساير منابع بهره مي‌گيرند و مي‌توانند اعمال خطرناكي را انجام دهندبايد براي تشخيص ويروس‌هاي جديد آنتي ويروس‌ها را مرتبا به روز رساني كرد.

Adware : ابزارهاي تبليغاتي

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

افزارهاي رايگان كاربران را وادار مي‌كنند تا آن‌ها را از وب‌سايت‌هاي مشكوک دانلود كنند. زماني كه كاربر در حال گشت و گذار در اينترنت است، تعدا زيادي از پاپ‌آپ‌ها، لينک‌ها و ديگر تبليغات مزاحم نمايش داده مي‌شود. اين ابزارها براي كاربران بسيار آزاردهنده هستند، زيرا لينک‌هاي موجود در اين تبليغات آلوده هستند. به واسطه‌ي كليک روي اين تبليغات، كاربر به سايت ديگري هدايت شده و كامپيوتر در معرض خطر قرار مي‌گيرد. اين ابزارهاي تبليغاتي مزاحم و زننده، ترافيک وب كاربر را جمع آوري كرده و آن‌ها را براي ديگر وب‌سايت‌هاي مشكوک منتقل مي‌كنند.

تروجان و درب‌هاي پشتي

تروجان، برنامه مخربي است كه به صورت يک نرم افزار جالب به نظر مي‌رسد. برخلاف ويروس‌ها، تروجان‌ها تكثير نمي‌شوند؛ ولي به اندازه ويروس‌ها مخرب هستند. تروجان ابتدا به قسمت‌هاي مختلف نفوذ مي‌كند، سپس راهي براي آسيب به آن‌ها پيدا خواهد كرد.

درب‌هاي پشتي همان گونه كه از نام آن معلوم است يک راه نفوذ پيش بيني نشده براي ورود غير مجاز ايجاد مي‌كنند. درپشتي نوعي بدافزار است كه به ظاهر برنامه‌اي ساده و سالم است ولي در شرايطي خاص زمينه ورود و دسترسي مهاجمان به داده‌هاي سيستمي را كه روي آن نصب شده است مهيا مي‌كند.

براي جلوگيري از اين نوع آسيب پذيريچه مواردی باید رعایت بشه؟

1)هرگز پيوست ايميل‌هاي دريافتي را از سوي كاربران ناشناس باز نكنيد.

در بسياري از وب‌سايت‌ها كليدهايي با عنوان دانلود در نزديكي لينک‌هاي واقعي دانلود وجود دارد. حتما قبل از كليک كردن روي آن‌ها از هدف آن لينک‌ها، با نگه داشتن ماوس و مشاهده آدرسي كه با كليک كردن به آن هدايت خواهيد شد، مطمئن شويد.