بدافزار چیست؟

گروه شرکت های آرک

نرم افزارهایی مطمئن، هوشمند و کارآمد

بدافزار چیست؟

Malwareیا بدافزار در اصل قطعه کدهایی هستند که توسط برنامه نویسان نوشته می شوند تا بوسیله آن بدون اجازه مالک سیستم، آن را آلوده و اقدام به کارهای ناخواسته یا خرابکارانه کنند. این واژه به صورت عمومی به تمامی کدها و برنامه های مخرب اطلاق می شود و به طور کلی هر نوع کدی که روی سیستم شما قرار بگیرد و عملیاتی ناخواسته را انجام دهد به عنوان بدافزار شناخته می شود، می تواند گوشی تلفن، تبلت و کامپیوترها را آلوده کند.

Malware پس از ورود به سیستم شما می تواند کارهایی مانند ارسال ایمیل های اسپم، سرقت اطلاعات و رمز عبورهای اکانت هاستینگ انجام دهد.

بدافزارها می توانند از انواع روش ها و تکنیک های مختلف برای اجرای خود استفاده کنند. مثلا بعضی از آنها از سیستم شما به عنوان قربانی برای انجام عملیات تخریب روی دیگر سیستم ها استفاده می کنند، بعضی از آنها اقدام به جمع آوری اطلاعات شخصی کاربران مانند شماره حساب بانکی، رمز عبور و نام های کاربری و ... می کنند و حتی ممکن است باعث تخریب در سیستم کاربران شوند.

Malware همچنین می تواند از طریق حفره های امنیتی موجود بر روی برنامه سایت شما وارد سیستم شود.

انواع بدافزارها می تواند شامل موارد زیر باشد:

ویروس ها- Virus

بدافزار چیست؟

ویروس ها برنامه هایی هستند که خود را تکثیر می کنند. این برنامه ها علاوه بر تکثیر عملیات خرابکارانه نیز انجام می دهند. ویروس ها برای تخریب و آلوده کردن سیستم ها نیاز به اجرا شدن توسط یک برنامه یا کاربر را دارند.

کرم ها -Worm

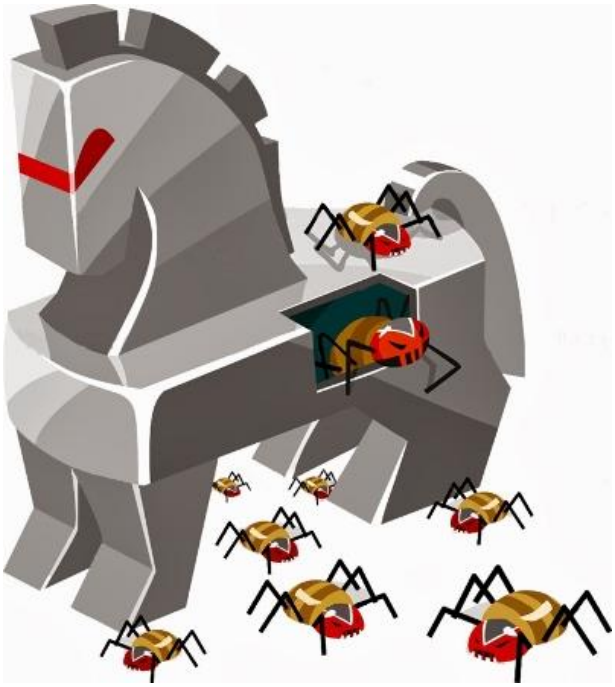
کرم ها بدافزارهایی هستند که از طریق حفره های شبکه ای کامپیوتر، به آن نفوذ می کنند. کرم ها پس از ورود به شبکه اقدام به انجام اعمال مخرب یا سودجویانه می کنند، مانند:

- در شبکه کامپیوترها را جستجو می کنند تا سیستم های آسیب پذیر را پیدا کنند.

- به کامپیوتر ناامن حمله کرده و برنامه ای روی آن اجرا می کنند.

- از این سیستم برای حمله به سیستم های دیگر استفاده می کنند.

بدافزار چیست؟



اسب تروجان - Trojan Horse

به برنامه هایی گفته می شود که مفید به نظر می رسند و کاربر را برای اجرا اغفال می کنند در صورتی که به جز انجام عمل موردنظر کاربر، اعمال خرابکارانه دیگری را نیز مخفیانه انجام می دهند.

مثلا کاربر یک نرم افزار از اینترنت دانلود و اجرا می کند، در حالی که همراه با اجرای نرم افزار، ویروس نیز وارد سیستمش می شود.

بدافزار چیست؟

بکدُر Backdoor/Trapdoor

زمانی که به یک سیستم حمله می شود هکر یک یا چند برنامه بکدُر را در سیستم قرار می دهد تا در زمان آینده بتواند از طریق راه های مخفی وارد سیستم شود.

نرم افزار جاسوسی - Spyware

این بدافزارها اطلاعات را از سیستم های کامپیوتری سرقت می کنند Spywareها می توانند توسط دیگر بدافزارها مانند اسب تروجان یا کرم ها، نصب شوند و یا اینکه نفوذگر مستقیما آنها را نصب کند.

بدافزار چیست؟

یکی دیگر از روش های انتشار نرم افزارهای جاسوسی استفاده از روش های تحریکات جمعی یا مهندسی اجتماعی مانند استفاده از ایمیل برای ترغیب کاربران به نصب یک برنامه ظاهرا مفید، است.

برخی از نرم افزارهای جاسوسی به نام Keylogger وجود دارند که پس از اجرا هر اطلاعاتی که کاربر تایپ می کند را در جایی ذخیره می کنند و حتی می توانند از کارهای کاربر فیلم تهیه کرده و در شبکه یا اینترنت برای دیگران ارسال نمایند.

رد گم کن Rootkit

وقتی هکر اقدام به نصب بدافزار می کند سعی می کند که این کار به صورت مخفیانه صورت گیرد و تمامی فایل های برنامه و حتی اجرای برنامه به صورت مخفیانه باشد. برنامه های روتکیت با دستکاری سیستم عامل این امکان را برای نفوذگران فراهم می کنند. به همین دلیل هدف از روتکیت ها مخفی سازی دیگر بدافزارها است.

بدافزار چیست؟

تبلیغات ناخواسته:Adware

Adwareها برنامه هایی هستند که بدون خواست کاربر نمایش داده می شوند. مانند صفحات پاپ آپ popup

میزان تخریب این بدافزارها متغیر است. مثلا اگر بر روی سیستم عامل نصب شده باشد می تواند اطلاعات کاربر را سرقت کند یا در دیگر نرم افزارها مشکلاتی را ایجاد کند. اما برنامه های تبلیغاتی که روی مرورگرها قرار می گیرند آسیب کمتری دارند. در واقع هدف این بدافزارها بازکردن صفحات خاص اینترنتی با هدف تجاری و تبلیغی است.

جلوگیری از ورود بدافزارها:

روش های انتشار اغلب بدافزارها نسبتا شناخته شده است و می توان با رعایت نکات زیر تا حدی از آلودگی کامپیوتر جلوگیری کرد:

صفحات مطمئن را باز کنید. اگر به لینکی اعتماد ندارید پس از بازکردن آن خودداری کنید. بیشتر بدافزارها در سایت هایی که دارای محتوای غیرقانونی هستند، وجود دارند.

اجرای دستورات Html را در ایمیل خود غیر فعال کنید. ایمیل یکی از موثرترین روش های انتشار بدافزارهاست. وقتی یک ایمیل که محتوای آن آلوده است، را باز می کنید بدافزارها می توانند به صورت خودکار و بدون اطلاع نصب و اجرا شوند.

فایل های پیوست ناشناس را دانلود نکنید

بدافزار چیست؟

فلش دیسک هایی که به کامپیوتر وصل می کنید را چک کنید و قبل از بازکردن محتوای آن از طریق آنتی ویروس آن را اسکن کنید.

برنامه های مطمئن و شناخته شده را روی سیستم نصب کنید

و در نهایت توصیه ما به شما این است که از یک آنتی ویروس خوب و قدرتمند استفاده کنید و دائم آن را به روز رسانی کنید. چنانچه با رعایت تمام موارد بدافزارها به سیستم شما راه یافتند می توانید با استفاده از آنتی ویروس، بسیاری از این بدافزارها را از بین ببرید.