OUCH!

ماهنامه ای برای آگاهی کاربران رایانه از امنیت اطلاعات

توقف بدافزارها

مقدمه

شاید در صحبت با دیگران کلماتی نظیر ویروس، تروجان، باج گیر و یا روت کیت را شنیده باشید. این کلمات بیانگر برنامه های مخربی هستند که بدافزار نامیده میشوند و مجرمان سایبری با استفاده از این ابزار وسایل و کامپیوتر شما را آلوده میکنند. در صورت نصب شدن آن بر روی سخت افزار شما، مجرمان هر کاری بخواهند میتوانند انجام دهند. بدانیم و اگاه باشیم که بدافزار چیست، چقدر خطرناک است، و از همه مهمتر برای محافظت از خود چا اقداماتی باید انجام بدهیم.

بدافزار چیست؟

به بیان ساده، بدافزارها برنامه هایی هستند- یک برنامه کامپیوتری - که برای انجام اعمال مخرب بکار گرفته میشوند. این جمله ترکیبی از دو کلمه مخرب و برنامه است. مجرمان سایبری بدافزار را بر روی تجهیزات شما نصب میکنند تا کنترل آن را در دست بگیرند. با نصب بدافزار مجرمان میتوانند بر روی فعالیت های آنلاین شما جاسوسی کرده، فایل ها و یا رمزعبور شما را بدزدند و حتی میتوانند از سیستم شما برای حمله به دیگران استفاده کنند. بدافزارها حتی میتوانند با از بین بردن فایلهای شما برای برگرداندن آن از شما تقاضای پول کنند. بعضی ها فکر میکنند که بدافزارها فقط مختص کامپیوترهای ویندوز هستند. متاسفانه بدافزارها قادر هستند هر نوع وسیله ای اعم از کامپیوتر های مک تا گوشی های هوشمند و حتی سیستم های ذخیره سازی دوربین های مدار بسته را آلوده کنند. هرچه تجهیزات و کامپیوتر های بیشتری توسط مجرمان آلوده شوند، میتوانند از این طریق پول بیشتری به دست بیاورند. به همین دلیل همه افراد میتوانند بعنوان اهداف این نوع حملات باشند حتی شما.

محافظت از خود با متوقف کردن بدافزار

ممکن است فکر کنید همه کاری که برای جلوگیری از آلوده شدن باید بکنید نصب کردن برنامه های امنیتی نظیر ضدویروس است. متاسفانه، ضدویروس قادر نیست همه بدافزارها را متوقف کند. مجرمان سایبری بطور دائم در حال انتشار و توسعه بدافزارهای جدید و قدرتمند هستند که به سختی قابل شناسایی باشند. در مقابل فروشندگان ضدویروس نیز بطور دائم در حال بروزرسانی محصولاتشان هستند تا بدافزارها را شناسایی کند. در بسیاری از موارد رقابت بین ای دو مشابه یک مسابقه شانه به شانه است و مجرمان عموما یک قدم جلوتر هستند. درنتیجه به این دلیل که نمیتوان فقط به عملکرد ضدویروس ها تکیه کرد، در ذیل اقدامات بیشتری که نیاز است برای حفاظت از خود بردارید را اشاره میکنیم :

مجرمان سایبری اغلب تجهیزاق را آلوده میکنند که حاوی آسیب پذیری در نرم افزارهای نصب شده بر روی آن باشد. هرچه نرم افزارهای شما به روزتر باشد، نقاط آسیب پذیر کمتری خواهد داشت و درنتیجه برای مهاجمان آلوده کردن آن نیز سخت تر خواهد بود. مطمئن شوید که سیستم عامل ها، برنامه های کاربردی، مرورگرهای شما همیشه به روز هستند. راحت ترین راه برای اطمینان از این امر، فعال کردن بروزرسانی خودکار در تجهیزات است.

روش معمولی که مجرمان سایبری برای آلوده کردن کامپیوتر ها و یا تلفن های همراه بکار میبرند نوشتن برنامه های جعلی و یا اپ های تقلبی و انتشار آن در فضای اینترنت است و در قدم بعدی شما را مجاب میکنند تا آن را دانلود و نصب کنید. فقط و فقط برنامه ها و اپ ها را از فروشگاه های آنلاین مطمئن دانلود کنید. همچنین از نصب برنامه های موبایل که جدید بوده یا دارای نظرات مثبت کمتری از طرف استفاده کنندگان هستند یا به ندرت بروزرسانی میشوند و یا اافراد کمی آن را دانلود کرده اند پرهیز کنید.اگر از برنامه و یا اپ در کامپیوتر و یا موبایل خود برای مدت طولانی استفاده نمیکنید آن را پاک کنید.

مهاجمان سایبری اغلب افراد را با حقه مجاب میکنند تا بدافزار را نصب کنند. برای این کار، آنها میبایست برای شما ایمیلی ارسال کنند که به نظر قانونی و درست بوده و حاوی فایل ضمیمه و یا یک لینک میباشد. ممکن است به نظر برسد که آن ایمیل از طرف یک دوست و یا بانک شما ارسال شده است. به هر حال، اگر فایل ضمیمه آم ایمیل را باز کنید و یا روی لینک کلیک کنید، کد مخرب را بر روی سیستم خود فعال کرده و بدافزار بر روی آن نصب خواهد شد. اگر پیامی دریافت کردید که بیانگر اقدام فوری از طرف شما بود و یا بیش از حد خوب به نظر میرسید که درست باشد، میتواند یک حمله باشد. عقل سلیم اغلب بهترین وسیله برای دفاع است، گاهی اوقات مشکوک باشید.

بطور منظم از از سیستم و فایلهای خود بر روی سرویس های کلاد و یا بر روی هاردهای خارجی پشتیبان بگیرید. این کار در مواقعی که بدافزار سعی در رمزگزاری و یا پاک کردن فایلها شما بکند از شما محافظت خواهد کرد. گرفتن پشتیبان ضروریست، گاها تنها راه نجات شما زمانیکه آلوده شده اید استفاده از پشتیبان است.

در خاتمه، بهترین روش برای دفاع در مقابل بدافزارها این است که همیشه نرم افزارها و برنامه های خود را بروز نگهدارید، در صئرت امکان برنامه های ضدویروس مطمئن نصب کنید و در مقابل حقه های دیگران و تلاش آنها برای آلوده کردن سیستم های شما به هوش باشید. اگر موارد بالا کمکی به شما نکردند، پشتیبان گیری منظم میتواند تنها راه نجات شما باشد.

سردبیر مهمان

لنی زلتسر(Lenny Zeltser) از مدرسین انستیتو SANS بوده و با تولید محصولات امنیت نقطه انتهایی (Endpoint Securit) در شرکت Minerva Labs در حال نبرد با انواع بدافزار ها میباشد. لنی در توییتر با حساب @lennyzeltser فعال بوده و در وبلاگ امنیت به ادرس zeltser.com مطلب مینویسد.

منابع

باج افزار: https://www.sans.org/u/EdI

پشتیبان گیری: https://www.sans.org/u/EdN

توقف حملات فیشینگ: https://www.sans.org/u/EdS