گزارش خبر
NEWSREPORT
کد خبر: ۴۵۲۶۴۵
دوشنبه ۲۱ تیر ۱۴۰۰ ۸:۲۶

حواستان به خطرات اینترنت باشد!

حملات سایبری و بدافزارها یکی از بزرگترین تهدیدات اینترنتی هستند براین اساس آشنایی با انواع بدافزار و سازوکار و راه‌های مقابله با آن از الزامات این روزها محسوب می‌شود چه بسا بسیاری از این نرم افزارهای مخرب زندگی‌هایی را از هم پاشیده و تمام دارایی افراد را به جیب زده‌اند.

به گزارش خبرنگاران علم و فناوری گزارش خبر، بدافزار یا malware کوتاه شده عبارت «malicious software» به معنی نرم‌افزار مخرب است در واقع نرم افزارهای مخرب یا بدافزار برنامه‌های رایانه‌ای هستند که به دلیل آزار رساندن و ایجاد خسارت به کاربران به این نام مشهورند البته طیف گسترده ای از انواع نرم افزارهای مخرب وجود دارد که می‌توان به ویروس های رایانه ای، کرم‌ها، اسب‌های تروآ، باج افزار، جاسوس‌افزارها، آگهی‌افزارها، روت‌کیت‌ها، هرزنامه‌ها، نرم افزار سرکش و ترس‌افزار اشاره کرد، البته برنامه ها اگر مخفیانه بر خلاف منافع کاربر رایانه عمل کنند نیز بدافزار تلقی می شوند.
بدافزار توسط مهاجمان سایبری با نیت دسترسی یا آسیب‌رسانی به کامپیوتر یا شبکه اینترنتی طراحی می‌شود و در اغلب موارد، قربانی حمله از وجود آن در سیستم خود بی‌خبر است. زمانی‌که بدافزار وارد کامپیوتر شود، بدون اجازه، دسترسی هکرها را به اطلاعات، دستگاه‌ها و سیستم‌ها ممکن می‌سازد.
بدافزار ابتدا به عنوان نوعی خرابکاری سایبری طراحی شد و هدف آن خراب کردن کامپیوتر، تغییر عکس پس‌زمینه یا دسترسی به اطلاعات شخصی بود؛ اما با گذر زمان، در دست مجرمان سایبری به ابزاری برای کسب درآمد ازطریق سرقت اطلاعات باارزش برای باج‌گیری از کسب‌وکارها، هک کردن رمز عبور برای دسترسی به حساب‌های بانکی یا سرقت هویت تبدیل شده است. بدافزار در طول سال‌ها انواع مختلفی پیدا کرده است و با گسترش دسترسی گسترده به اینترنت، نرم افزارهای مخرب بیشتر برای سودآوری طراحی شده اند. برخی از بدافزارها برای ایجاد پول استفاده می شوند و در این نوع سرقت به نظر می رسد کاربر رایانه بر روی پیوند تبلیغاتی در یک سایت کلیک کرده و از تبلیغ کننده هزینه ای دریافت می کند. علاوه بر پول سازی، از بدافزارها می توان برای خرابکاری ها استفاده کرد آن هم اغلب برای انگیزه های سیاسی.
در این گزارش به انواع بدافزارهای مخرب اشاره می شود و خواندن این گزارش به همه افرادی که به نوعی با فضای مجازی و اینترنت سر و کار دارند توصیه می شود:
انواع رایج بدافزار:
باج‌افزار: اکثر بدافزارها ترجیح می‌دهند تا جای ممکن از دید کاربر مخفی بمانند تا بتوانند اطلاعات بیشتری را دور از چشم او سرقت کنند؛ اما باج‌افزار به خاطر ماهیت خاص خود معمولا برعکس عمل می‌کند. باج‌افزار اغلب ازطریق فایل پیوست یا لینکی در ایمیل‌های فیشینگ وارد سیستم می‌شود، آن را آلوده می‌کند و با رمزگذاری داده‌های کاربر یا بیرون انداختن او از سیستم، از او باج می‌خواهد و برای اینکه به کاربر دسترسی دوباره به سیستم یا اطلاعات قفل شده‌اش را بدهد، از او می‌خواهد ازطریق بیت‌کوین یا رمزارزهای دیگر، مبلغی به حساب هکر واریز کند.
شاید این روش به نظر ساده بیاید و با خودتان بگویید هیچ فردی فریب آن را نخواهد خورد؛ اما واقعیت این است که این روش مؤثر است و به دفعات، فعالیت شرکت‌ها، بیمارستان‌ها، ادارات پلیس و حتی کل شهر را با مشکل جدی روبه‌رو کرده. تنها در سال ۲۰۱۶، مجرمان سایبری بیش از یک میلیارد دلار ازطریق حملات باج‌افزار به جیب زدند. طبق گزارش یوروپل، حملات باج‌افزاری، بسیاری از تهدیدات سایبری جهان را در سال ۲۰۱۷ زیر سایه خود برده بودند.
اکثر باج‌افزارها مانند تروجان ازطریق نوعی مهندسی اجتماعی و دستکاری روانشناختی کاربر گسترش پیدا می‌کنند. بعد از اجرا شدن، اکثرا در چند دقیقه‌ی اول فایل‌های کاربر را پیدا و رمزگذاری می‌کنند؛ اگرچه تعدادی هم ممکن است از تکنیک انتظار استفاده کنند و با چند ساعت تماشای کاربر، برآورد کنند چقدر می‌توانند از او اخاذی کنند یا اگر بکاپی از فایل‌ها وجود دارد، آن‌ها را هم پاک یا رمزگذاری کنند.
مثل هر نوع بدافزار دیگری، می‌توان از حمله باج‌افزار جلوگیری کرد؛ اما به محض اجرا شدن، اگر بکاپ خوبی از فایل‌ها وجود نداشته باشد، به‌سختی می‌توان آسیب وارد‎شده به سیستم را برطرف کرد. طبق مطالعات، حدود یک‌چهارم قربانیان مبلغ باج را به هکر پرداخت می‌کنند و از این تعداد، ۳۰ درصد نمی‌توانند حتی بعد از پرداخت باج به فایل‌های رمزگذاری‌شده‌ی خود دسترسی داشته باشند. باز کردن قفل فایل‌های رمزگذاری‌شده، اگر ممکن باشد، به ابزارهای خاص و مقدار قابل توجهی خوش‌اقبالی نیاز دارد. برای در امان ماندن از حمله‌ی باج‌افزار، بهترین توصیه این است از تمام فایل‌های مهم و حیاتی خود به‌صورت آفلاین بکاپ تهیه کنید. البته اگر نابغه‌ای مثل الیوت آلدرسون سریال Mr. Robot بخواهد این حمله را سازمان‌دهی کند، تقریبا هیچ امیدی به در امان ماندن فایل‌های بکاپ‌تان نیست.
تروجان:یکی از رایج‌ترین انواع بدافزار، تروجان است که اغلب خود را به شکل ابزاری معتبر و کاربردی جا می‌زند تا کاربر را وادار به نصب خود کند. تروجان از ویروس قدیمی‌تر است؛ اما بیشتر از هر بدافزار دیگری به کامپیوترهای کنونی آسیب زده. اسم این بدافزار از داستان اسب تروآ گرفته شده است که در آن، یونانی‌های باستان داخل اسب چوبی غول‌پیکری که به‌عنوان هدیه به شهر تروآ داده شده بود، مخفی شدند و زمانی‌که اسب وارد شهر شد، یونانی‌ها از آن بیرون آمدند و شهر را تصاحب کردند. بدافزار تروجان کارکرد مشابهی دارد؛ به این صورت که مخفیانه و در قالب ابزاری کاربردی مانند به‌روزرسانی یا دانلود فلش وارد سیستم می‌شود و به محض ورود، حمله را آغاز می‌کند.
تروجان برای دسترسی پیدا کردن به اطلاعات سیستم باید توسط کاربر اجرا شود. این بدافزار اغلب ازطریق ایمیل یا بازدید از وب‌سایت‌های آلوده به سیستم منتقل می‌شود. رایج‌ترین نوع تروجان به‌طور طعنه‌آمیزی خود را به‌صورت برنامه‌ی آنتی‌ویروس نشان می‌دهد و به‌صورت پیام پاپ‌آپ ادعا می‌کند کامپیوتر شما به ویروس آلوده شده است و برای پاک کردن آن باید این «نرم‌افزار» را نصب کنید. کاربران هم فریب آن را می‌خوردند و با نصب بدافزار، تروجان را مانند خون‌آشامی که برای ورود به خانه‌ی قربانی نیاز به دعوت شدن دارد، به کامپیوتر خود دعوت می‌کنند.
تروجان بسته به قابلیت‌هایش می‌تواند به همه‌ی اطلاعات روی سیستم دسترسی داشته باشد؛ از جمله اطلاعات ورود به اکانت و رمز عبور، اسکرین‌شات‌ها، اطلاعات مربوط به سیستم، جزییات حساب‌های بانکی و بسیاری موارد دیگر؛ بعد از دسترسی، تروجان این اطلاعات را جمع‌آوری می‌کند و برای هکر می‌فرستد. گاهی تروجان به هکرها اجازه می‌دهد اطلاعات را تغییر بدهند یا برنامه‌ی ضد بدافزار سیستم را خاموش کنند.
به دو دلیل مقابله با تروجان دشوار است چرا که نوشتن تروجان آسان است و هر ماه میلیون‌ها نسخه از آن ساخته می‌شود و از سوی دیگر تروجان با فریب کاربر گسترش می‌یابد؛ به همین خاطر نمی‌توان با بسته‌های امنیتی یا فایروال یا روش‌های سنتی جلوی آن‌ها را گرفت.

کرم ها

سابقه حضور کرم‌ها در سیستم‌های کامپیوتری از ویروس‌ها بیشتر است و به دوران بزرگ‌رایانه‌ها برمی‌گردد. کرم‌های کامپیوتری با ظهور ایمیل در اواخر دهه‌ی ۱۹۹۰ پا گرفتند و به مدت تقریبا ۱۰ سال کارشناسان امنیت کامپیوتر در محاصره‌ی کرم‌های مخربی بودند که به‌صورت فایل‌های پیوست در ایمیل فرستاده می‌شد. کافی بود کاربر ایمیلی آلوده به کرم را باز کند تا در مدتی کوتاه کل شرکت آلوده شود.

کرم‌ها به این خاطر نسبت به ویروس‌ها مخرب‌تر و دردسرسازترند که می‌توانند بدون نیاز به اقدامی از طرف کاربر تکثیر شوند. ویروس‌ها برای فعال شدن به کاربری نیاز دارند تا آن‌ها را همراه برنامه‌ی آلوده اجرا کند؛ اما کرم، فایل‌ها و برنامه‌های دیگر را به کار می‌گیرد تا اعمال شرورانه‌اش را انجام دهند.

روت کیت‌ها

روت‌کیت بدافزاری است که با هدف کنترل از راه دور کامپیوتر، بدون اینکه کاربر یا نرم‌افزارهای امنیتی متوجه حضور آن شوند، طراحی شده است. مجرمان سایبری به کمک روت‌کیت می‌توانند فایل اجرا کنند، اطلاعات سرقت کنند، تنظیمات سیستم و نرم‌افزارها را دستکاری کنند یا حتی بدافزارهای دیگری نصب کنند. روت‌کیت می‌تواند ازطریق نصب و اجرای اپلیکیشن‌ها یا حملات فیشینگ و حفره‌های امنیتی به سیستم راه پیدا کند.

روت‌کیت یکی از خطرناک‌ترین تهدیدات سایبری به‌حساب می‌آید؛ چون می‌تواند حضور خود را پنهان کند و حتی برنامه‌های ضد بدافزار سیستم را از کار بیندازد و به اپلیکیشن‌های نصب‌شده آسیب جدی وارد کند. هکرها به کمک روت‌کیت می‌توانند جاسوسی کنند و داده‌های باارزش را سرقت کنند. برای جلوگیری و شناسایی حمله روت‌کیت، روی لینک‌های مشکوک که معمولا از طریق ایمیل به سیستم شما وارد می‌شوند، کلیک نکنید، از برنامه‌های تخصصی برای اسکن کامپیوتر استفاده کنید، سیستم خود را همیشه به‌روز نگه دارید و ترافیک اینترنت خود را کنترل کنید. پیدا کردن و از بین بردن روت‌کیت پس از نصب روی سیستم کار بسیار دشواری است؛ به همین دلیل متخصصان امنیت سایبری تأکید می‌کنند در این مورد مثل تمام موارد دیگر، پیشگیری بهتر از درمان است.

آگهی افزار

هدف غایی اغلب مجرمان سایبری کسب درآمد است و برای برخی از آن‌ها، استفاده از آگهی‌افزار روش خوب و کم‌دردسری برای این کار است. آگهی‌افزار دقیقا همان کاری که از اسمش برمی‌آید، انجام می‌دهد و طوری طراحی شده است تا تبلیغات را به کاربر تحمیل کند. در برخی موارد تنها راه خلاصی از شر این تبلیغات مزاحم، کلیک کردن روی آن‌ها است و هر کلیک هم برای مجرم سایبری، درآمدزایی می‌کند.

در بیشتر موارد، آگهی‌افزارها کاری به اطلاعات قربانی ندارند و آسیبی به دستگاه وارد نمی‌کنند؛ فقط بی‎نهایت آزاردهنده هستند و کاربر را مجبور می‌کنند مرتب روی پنجره‌های پاپ‌آپ کلیک کند تا آن‌ها را ببندد. بااین‌حال، اگر این اتفاق روی گوشی موبایل بیفتد، باعث کاهش سریع شارژ باتری می‌شود یا با اشغال کل صفحه‌ی نمایش، استفاده از گوشی را عملا غیر ممکن می‌کند.

جاسوس‌افزار

کار جاسوس‌افزار که از اسمش پیدا است؛ جاسوسی کردن و سرک کشیدن به کامپیوتر و دستگاه‌های دیگران. جاسوس‌افزار به سابقه‌ی مرورگر شما، اپلیکیشن‌هایی که استفاده می‌کنید یا پیام‌هایی که می‌فرستید، دسترسی دارد. جاسوس‌افزار می‌تواند به‌صورت تروجان یا روش‌های دیگر دانلود و وارد دستگاه شود.

برای مثال نوار ابزاری که برای مرورگر خود دانلود می‌کنید، ممکن است حاوی جاسوس‌افزاری باشد که فعالیت‌های شما را در اینترنت مشاهده می‌کند؛ یا تبلیغات مخرب ممکن است کد جاسوس‌افزار را ازطریق دانلود ناخواسته و به‌طور مخفیانه به کامپیوتر شما منتقل کنند. در برخی موارد، نوعی از جاسوس‌افزار به‌عنوان نرم‌افزاری با هدف کنترل استفاده از اینترنت کودک به والدین فروخته می‌شود و به گونه‌ای طراحی شده است تا نرم‌افزارهای امنیتی و آنتی‌ویروس آن را نادیده بگیرند. از طرفی، برخی شرکت‌ها از جاسوس‌افزار برای نظارت مخفیانه بر کارمندان خود استفاده می‌کنند.

جاسوس‌افزارها اغلب به‌آسانی قابل حذف‌اند؛ چون برخلاف بدافزارهای دیگر، قصد و غرض مخرب و شرورانه‌ای ندارند؛ کافی است فایل اجرایی جاسوس‌افزار را پیدا کنید و جلوی اجرا شدن آن را بگیرید. نیت جاسوس‌افزار به بدی دیگر بدافزارها، از جمله تروجان با دسترسی از راه دور نیست؛ اما هردو از روشی مشابه برای ورود به سیستم استفاده می‌کنند. در نتیجه، وجود جاسوس‌افزار در سیستم زنگ خطری است برای کاربر که سیستم او ضعفی دارد و باید قبل از مواجهه با تهدیدات جدی‌تر، برطرف شود.

راه‌های محافظت دربرابر بدافزارها

برخی از ابتدایی‌ترین روش‌های امنیت سایبری می‌تواند کمک زیادی به حفاظت سیستم‌ها و کاربران دربرابر حملات بدافزاری بکند. برای مثال، اطمینان از به‌روز بودن نرم‌افزارها و سیستم عامل به محض انتشار بسته‌های به‌روزرسانی و امنیتی، کاربران را دربرابر بسیاری از حملات سایبری محافظت می‌کند.

شاید به‌روزرسانی و نصب بسته‌های امنیتی مخصوصا در مورد شبکه بزرگی از سیستم‌های متصل، کار وقت‌گیری باشد؛ اما ثابت شده است با همین اقدام می‌توان از بسیاری از حملات بدافزارها و تبعات بعضا جبران‌ناپذیر آن‌ها جلوگیری کرد.

نصب نرم‌افزارهای امنیت سایبری می‌تواند در این زمینه کمک کند. بسیاری از این نرم‌افزارها به‌طور مرتب مکانیزم تشخیص و مقابله با بدافزارهای جدید را به‌روزرسانی می‌کنند تا برای هر تهدید احتمالی آمادگی لازم را داشته باشند.

کاربران نیز باید در خصوص امنیت سایبری، گشت‌وگذار امن در اینترنت و خطرات ایمیل‌های فیشینگ آموزش ببینند و نسبت به کلیک و دانلود لینک‌های مشکوک، محتاطانه‌تر رفتار کنند. اگر کاربران سطح آگاهی خود را در خصوص امنیت سایبری بالا ببرند، بسیاری از حملات بدافزاری در رسیدن به اهداف‌شان ناموفق خواهد بود.

هشدار پلیس

سرهنگ داوود معظمی گودرزی رئیس پلیس فتا پایتخت نیز چندی پیش نسبت به روند انتشار بدافزارها در فضای مجازی هشدار داد و گفت: مجرمان در فیشینگ تلفنی تلاش می‌کنند به اطلاعات بانکی کاربران دست یابد.

وی افزود: مجرمان فضای مجازی با تکنیک‌های مهندسی اجتماعی اقدام به سرقت اطلاعات کاربران و برداشت‌های غیرمجاز از حساب‌های بانکی طعمه هایشان می‌کنند.

رئیس پلیس فتا پایتخت ادامه داد : هکرها در این روش از طریق تلفن با طعمه های خود ارتباط برقرار می‌کنند و ضمن اینکه خود را نماینده بانک، شرکت معتبر و یا سازمانی که شما می‌شناسید معرفی می‌کنند از شما می خواهند جهت دریافت جایزه اطلاعات بانکی خود را در اختیارشان قرار دهید.

سرهنگ گودرزی گفت: برای واریز هر گونه وجه به حساب شما اعم از جایزه، پاداش و مزایا نیازی به اعلام رمز بانکی شما نخواهد بود. برای مقابله با هکرها و حملات فیشینگ این نکته را فراموش نکنید.

در پایان تاکید می شود که عمده‌ترین مشکلات سیستم‌های کامپیوتری، نبود یا منقضی شدن آنتی ویروس است که متاسفانه این موضوع اغلب توسط کاربران نادیده گرفته شده که می‌تواند عواقب خطرناکی به دنبال داشته و کاربر را با مشکلات متعدد مواجه کند. حفاظت از داده‌ها و اطلاعات، جلوگیری

از نفوذ ویروس‌ها، حذف بدافزارها و ویروس‌ها از جمله دلایلی است که استفاده از یک آنتی ویروس بروز و قوی را ضروری می‌کند براین اساس ضرورت دارد تا از نسخه‌های اصلی آنتی ویروس استفاده کرده و از نصب آنتی ویروس‌ها با لایسنس (در علم کامپیوتر به معنای مجوز استفاده از یک نرم افزار یا سخت افزار) غیر معتبر خودداری کرد.