اشتباهات رایج دردسرساز

12 علت شایع هک شدن سامانه‌های کامپیوتری در مقیاس کوچک و بزرگ

اگر نگاهی به اخبار دنیای امنیت داشته باشید، مشاهده می‌کنید هر روزه بر تعداد کاربرانی که قربانی فعالیت‌های هکری آنلاین می‌شوند، افزوده می‌شود. به‌طوری که نه تنها این آمارها هیچ‌گاه روند کاهشی پیدا نمی‌کنند، بلکه با فراگیر شدن ابزارهای مختلفی که قابلیت اتصال به اینترنت را دارند، این روند با شتاب باور نکردنی رو به افزایش است.

اگر از آسیب‌پذیری‌های پنهان در برنامه‌های کاربردی و سیستم‌عامل‌ها صرف‌نظر کنیم، به یکسری اشتباهات انسانی می‌رسیم که بسیاری از آن‌ها زمینه‌ساز نفوذ هکرها به سامانه‌های شخصی و سازمانی می‌شوند. اغلب حملات هکری در اثر سهل‌انگاری عامل انسانی به وجود می‌آید. از جمله اشتباهات رایجی که باعث قربانی شدن کاربران می‌شود به موارد زیر می‌توان اشاره کرد.

به‌کارگیری گذرواژه‌های یکسان برای چند حساب کاربری

یکی از رایج‌ترین اشتباهات کاربران، حتا کاربران حرفه‌ای به‌کارگیری گذرواژه‌های یکسان برای حساب‌های کاربری مختلف است. کاربران برای آن‌که به ساده‌ترین شکل گذرواژه‌های حساب‌های خود را به یاد آورند تصمیم می‌گیرند از یک گذرواژه برای چند حساب کاربری استفاده کنند، در نگاه اول رویکرد خوبی است، اما زمانی که هکری یکی از حساب‌های کاربری شما را هک کند به آسانی می‌تواند به گذرواژه‌های مورد استفاده روی حساب‌های کاربری دیگر نیز دست پیدا کند. برای آن‌که بتوانید به ساده‌ترین شکل بر گذرواژه‌های خود مدیریت داشته باشید، پیشنهاد می‌کنیم از نرم‌افزارهای مدیریت گذرواژه‌ها همچون LastPass استفاده کنید.

به کارگیری گذرواژه‌های ضعیف یا عدم به‌کارگیری گذرواژه برای شبکه‌های بی‌سیم

اگر از یک ارتباط بی‌سیم بدون هیچ‌گونه گذرواژه‌ای استفاده می‌کنید یا از ساده‌ترین گذرواژه ممکن استفاده کنید به هکرها و حتا افرادی که در نزدیکی شما قرار دارند اجازه داده‌اید از پهنای باند شما با کمترین زحمت ممکن استفاده کنند. آمارها نشان می‌دهند حتا در سال جاری میلادی نیز مردم از گذرواژه‌هایی همچون 123456789 یا qwerty استفاده می‌کنند. در نتیجه بهتر است از گذرواژه‌هایی که اشاره به نام‌های خاص دارند استفاده نکنید و از ترکیب نام‌ها و اعداد به بهترین شکل استفاده کنید. همچنین در رابطه با ارتباطات بی‌سیم بهتر است ضمن به کارگیری گذرواژه‌های پیچیده ویژگی WPS را روی روتر خود غیرفعال کرده و از الگوریتم‌های رمزنگاری قدرتمند روی روتر خود استفاده کنید. همچنین گزینه‌هایی شبیه به ویژگی به اشتراک‌گذاری گذرواژه در ویندوز 10 را غیرفعال کنید.
فعال‌سازی این ویژگی باعث می‌شود تا به هر شخصی که در شبکه دوستان شما قرار دارد اجازه ورود دهید از ارتباط بی‌سیم شما استفاده کند.

کلیک کردن روی پیام‌های تبلیغی و ایمیل‌های فریبنده

باز کردن ایمیل‌ها و پیام‌های تبلیغی اغلب ساده‌ترین راه آلودگی یک سیستم است. هکرها از طریق مکانیزم فوق به راحتی موفق می‌شوند یک سامانه کامپیوتری را به انواع مختلفی از بدافزارها و باج‌افزارها آلوده سازند. آگهی‌هایی که در پنجره‌های تبلیغاتی ظاهر می‌شوند، در ظاهر ممکن است عادی به نظر می‌رسند، اما در خفا این آگهی‌ها می‌توانند به منظور روبایش کلیک‌ها، اجرای اسکریپت‌های آلوده یا هدایت کاربران به سمت سایت‌های فیشینگ به کار گرفته شوند. بنابراین توصیه می‌کنیم از افزونه‌های مسدودکننده تبلیغات همچون NoScript یا Adblock استفاده کنید.

به کارگیری سیستم‌عامل‌ها و نرم‌افزارهای وصله نشده

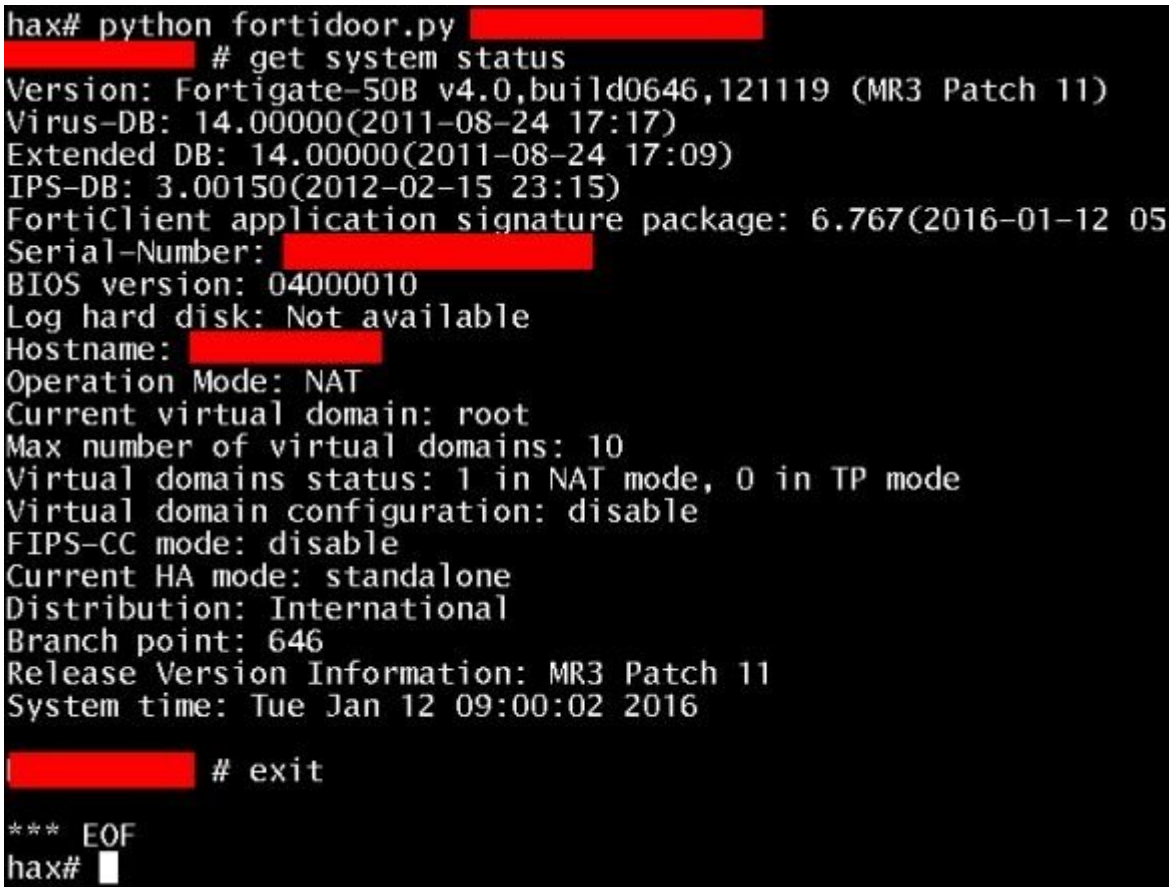
مجرمان سایبری به خوبی می‌دانند که بسیاری از کاربران و حتا سازمان‌های بزرگ در زمینه نصب وصله‌ها سهل‌انگار هستند. باج‌افزار واناکرای که سال گذشته در مقیاس جهانی سامانه‌های کامپیوتری را قربانی خود ساخت گواه این مطلب است. زمانی که آسیب‌پذیری شناسایی می‌شود جزییات مربوط به آن پس از 90 روز منتشر می‌شود. در شرایطی که شرکت سازنده در این بازه زمانی به‌روزرسانی مربوطه را عرضه می‌کند، اما بسیاری از کاربران یا حتا سازمان‌ها بدون توجه به این موضوع باز هم از یک سیستم‌عامل یا نرم‌افزار آسیب‌پذیر استفاده می‌کنند. همین موضوع باعث می‌شود تا هکرها به راحتی بتوانند تروجان‌ها و بدافزارهایی را بر اساس آسیب‌پذیری‌های شناسایی شده ایجاد کرده و به شکل گسترده منتشر کنند.

عدم به کارگیری یا فعال‌سازی دیوار آتش

دیوارهای آتش یکی از بهترین ابزارها برای مقابله با بدافزارها هستند. این نرم‌افزارها با کنترل بر داده‌های وارد و خارج شونده به یک سیستم مانع از آن می‌شوند تا بدافزارها به راحتی با سرورهای کنترل و فرمان‌دهی ارتباط برقرار کنند. این ابزارهای امنیتی به راحتی به کاربران اجازه می‌دهند بر ترافیک عبوری نظارت داشته و به شکل دقیق مطلع شوند چه برنامه‌هایی به اینترنت متصل می‌شوند و چه برنامه‌هایی به صورت بلادرنگ در حال دریافت یا ارسال داده‌ها هستند.

باز کردن ایمیل‌هایی که از منابع ناشناس ارسال شده است

ساده‌ترین راهکاری که بر مبنای تکنیک مهندسی اجتماعی کاربران را قربانی خود می‌سازد، ارسال ایمیل از سوی منابع به ظاهر معتبر و قانونی است. تکنیکی که به نام حمله فیشینگ از آن نام برده می‌شود. در این تکنیک هکرها وانمود می‌کنند ایمیلی را از یک سازمان بزرگ یا یک نهاد قانونی برای کاربر ارسال کرده‌اند و حتا در عنوان ایمیل و محتوای ایمیل به موضوعات مهمی اشاره می‌کنند. این موضوع باعث می‌شود تا کاربر به سادگی فریب بخورد و فایل ضمیمه ایمیل را باز کند. زمانی که این فایل ضمیمه باز شود که عمدتا یک سند ورد یا یک فایل پی‌دی‌اف است، اسکریپت‌ها و ماکروهای مخرب روی سیستم کاربر اجرا می‌شوند. اسکریپت‌هایی که در ادامه یک فایل مخرب را بارگیری می‌کنند.



به کارگیری نرم‌افزارهای دارای باگ یا نرم‌افزارهایی که در وضعیت بتا قرار دارند

تعدادی از آسیب‌پذیری‌های امنیتی به واسطه یک مشکل مرسوم برنامه‌نویسی موسوم به خطای سرریز بافر به وجود می‌آیند. مشکل سرریز بافر که به Stack overflow نیز مشهور است یکی از مشکلات رایج در برنامه‌نویسی است که به دلایل مختلفی بروز می‌کند. در خطای سرریز بافر امکان رونویسی بخش‌هایی از داده‌ها در حافظه وجود دارد. هکرها با استفاده از این تکنیک به آسانی می‌توانند به سامانه‌ها نفوذ کنند. هکرها به روش‌های مختلفی از خطای سرریز بافر اطلاع پیدا کرده و از آن استفاده می‌کنند. یکی از این روش‌ها کنترل قسمت‌هایی از یک برنامه کاربردی است که به عنوان گیت دریافت کننده ورودی عمل می‌کند. هکرها به آسانی می‌توانند این مکان‌ها را با داده‌های تصادفی مورد بررسی قرار دهند.

عدم به کارگیری بسته‌های ضدویروس

امروزه همه سیستم‌عامل‌های مدرن همچون ویندوز به حداقل قابلیت‌های امنیتی همچون دیوارآتش یا مکانیزم‌های شناسایی فعالیت‌های مخرب تجهیز شده‌اند. اما عدم وجود یک نرم‌افزار ضدویروس باعث می‌شود تا بدافزارها به راحتی و حتا با یک بازدید ساده از یک سایت مخرب به درون سامانه کامپیوتری شما وارد شوند، پردازه‌های در حال اجرا را آلوده ساخته یا یک درب پشتی روی سامانه شما نصب کنند. توجه داشته باشید ضدویروس‌ها زمانی عملکرد خوبی خواهند داشت که به‌روز باشند. در نتیجه به‌روزرسانی مستمر ضدویروس‌ها باید در اولویت قرار داشته باشد.

عدم به کارگیری ابزارهای ضدبدافزاری و ضدجاسوس‌افزاری

در حالی که به‌کارگیری نرم‌افزارهای ضدویروسی و دیوارهای آتش به میزان قابل توجهی از شدت حملات کم می‌کنند، اما به‌کارگیری ابزارهای ضدبدافزاری و ضدجاسوس‌افزاری نیز در این زمینه کمک فراوانی می‌کنند. درست است که این ابزارها بدافزارهای نصب شده روی سامانه‌ها را حذف نمی‌کنند، اما در مقابل کوچک‌ترین تحرکات بدافزاری را تشخیص داده و گزارش آن‌را در اختیار شما قرار می‌دهند. ضدبدافزار شرکت MalwareBytes یکی از موفق‌ترین گزینه‌ها در این زمینه به شمار می‌رود. پیشنهاد ما این است که یک ضدبدافزار روی سامانه خود نصب کنید. ابزارهای ضدجاسوس‌افزاری نیز مانع نصب شدن کی‌لاگرها (روباندگان کلیدها) و برنامه‌های استراق سمع می‌شوند.
نرم‌افزارهایی که بدون هیچ‌گونه فعالیت مخرب مشخصی تنها اطلاعات سامانه شما را جمع‌آوری کرده و برای هکرها

ارسال می‌کنند.

عدم توجه به ترافیک شبکه

زمانی که بدافزاری روی یک سامانه نصب می‌شود، سعی می‌کند در اولین و بهترین فرصت ممکن داده‌های جمع‌آوری شده را برای سرورهای تحت کنترل هکرها ارسال کند. اگر مشاهده کردید، روتر شما پیوسته در حال کار است، اما هیچ به‌روزرسانی دریافت نمی‌شود یا برنامه خاصی به اینترنت متصل نیست یا دستگاه‌های بی‌سیم به روتر شما متصل نیستند، آن‌گاه باید این مسئله را بررسی کنید. ساده‌ترین ابزاری که در این زمینه در اختیار شما قرار دارد Task Manager ویندوز است. این ابزار گزارش کاملی از فعالیت‌هایی که در حال انجام است ارائه می‌کند. اطلاعات موجود در ارتباط با ترافیک شبکه در زبانه Network ابزار Task Manager قرار دارد.

بی توجهی به سرویس‌های در حال اجرا روی یک سیستم

بدافزارها برای پنهان ساختن نشانه‌های خود سعی می‌کنند با اسامی شناخته شده به سامانه‌های کامپیوتری وارد شوند. به طور مثال بدافزاری ممکن است با نام chrome.exe فعالیت کند. در چنین شرایطی بسیاری از کاربران متوجه موضوع مشکوکی نمی‌شوند. اما برای آن‌که اطمینان حاصل کنید پردازه‌های در حال اجرا معتبر و قانونی هستند بهتر است مسیر اجرای آن‌ها را بررسی کنید. به‌طور مثال، پردازه‌ها و سرویس‌های ویندوز همیشه از پوشه‌های اصلی این سیستم‌عامل اجرا می‌شوند. برای مشاهده آدرس اجرای پردازه‌ها کافی است ابزار Task Manager را باز کرده، روی نام پردازه کلیک راست کرده و گزینه Open File Location را انتخاب کنید. این گزینه مسیر اجرای یک فایل را به شما نشان می‌دهد.

وجود آسیب‌پذیری در پروتکل‌های ارتباطی

ضروری است تا مدیران سایت‌ها و سازمان‌ها از پروتکل‌های ایمنی همچون HTTPS استفاده کنند. پیاده‌سازی حملات مرد میانی موسوم به man-in-the-middle که شبکه‌های بی‌سیم غیر ایمن را مورد تهدید قرار می‌دهند به واسطه به‌کارگیری پروتکل‌ها و مکانیزم‌های ضعیف ارتباطی است. شرکت SourceDNA، که در زمینه ساخت برنامه‌های جانبی برای گوشی‌های هوشمند به فعالیت اشتغال دارد اعلام کرده است که بسیاری از توسعه‌دهندگان از کتابخانه‌ها

و چهارچوب‌های قدیمی همچون AFNetworking برای ساخت برنامه‌های کاربردی استفاده می‌کنند. برنامه‌هایی که کاربران گوشی‌های آی‌فون و اندروید را در معرض خطر قرار می‌دهد.

تاریخ انتشار:
19 شهریور 1397

نشانی منبع:
https://www.shabakeh-mag.com/security/13743/12-%D8%B9%D9%84%D8%AA-%D8%B4%D8%A7%DB%8C%D8%B9-%D9%87%DA%A9-%D8%B4%D8%AF%D9%86-%D8%B3%D8%A7%D9%85%D8%A7%D9%86%D9%87%E2%80%8C%D9%87%D8%A7%DB%8C-%DA%A9%D8%A7%D9%85%D9%BE%DB%8C%D9%88%D8%AA%D8%B1%DB%8C-%D8%AF%D8%B1-%D9%85%D9%82%DB%8C%D8%A7%D8%B3-%DA%A9%D9%88%DA%86%DA%A9-%D9%88-%D8%A8%D8%B2%D8%B1%DA%AF