ماهنامه ای برای آگاهی کاربران رایانه از امنیت اطلاعات

OUCH!

دراین شماره..

ضد ویروس چیست؟

مقدمه

ضد ویروس نرم افزاری برای حفظ امنیت رایانه ای است که بر روی رایانه و یا دستگاه تلفن همراه برای محافظت از آلوده شدن به بدافزارها نصب میشوند. اصطلاح «بدافزار» یک اصطلاح کلی برای هر نوع برنامه مخرب مانند ویروس ها، کرم ها، تروجان ها و نرم افزارهای جاسوسی است. در واقع، اصطلاح بدافزار(malware) از ترکیب کلمات بد (malicious) و نرم افزار(software) است. اگر رایانه شما به بدافزاری آلوده شده باشد، هکرها می توانند به رایانه شما نفوذ کنند مثلا تمام کلید هایی که روی صفحه کلید میزنید را ببینند، مدارک و اسناد روی رایانه اتان را سرقت کنند و با استفاده از رایانه شما به رایانه یا سِرور دیگران حمله کنند. برخلاف باور برخی از مردم، همه سیستم عامل ها، از جمله سیستم عامل Mac OS X و لینوکس نیز می توانند آلوده شوند.

سردبیر مهمان

جیک ویلیامز (Jake Williams) بنیانگذار(www.renditioninfosec.com) Rendition Infosec و مربی مورد تایید و مولف دروس موسسه SANS است. او در توییتر با نشانه @MalwareJake فعال است. همچنین در وبلاگ خود به آدرس malwarejake.blogspot.com مینویسد.

شما می توانید نرم افزار ضد ویروس را به عنوان یک نرم افزار تکی یا معمولا به عنوان بخشی از یک بسته نرم افزاری خریداری کنید. مشکل این است که ضد ویروس ها نمی توانند دیگر به پای هکرها برسند. هکرها دائما در حال توسعه و انتشار انواع جدیدی از بدافزارها هستند. هر روز نسخه های جدید بدافزارها تولید و منتشر میشوند که هیچ ضد ویروسی قادر به شناسایی و محافظت در برابر همه آنها نیست. برای همین مهم است بدانید که در حالی که ضد ویروس به حفاظت از رایانه شما کمک خواهد کرد، اما نمی تواند هر نوع بدافزار جدید را تشخیص و یا مقابله کند. برای درک بهتر دلیل، بیایید به چگونگی کارکرد بسیاری از این برنامه ها نگاهی بیندازیم.

ضد ویروس چگونه کار میکند؟

به طور کلی ضد ویروس ها به دو طریق بدافزارها را شناسایی میکنند. یکی به روش شناسایی از روی نشانه ها و یکی شناسایی از روی رفتار. شناسایی از روی نشانه ها مثل سیستم ایمنی بدن انسان کار میکند. ضدویروس رایانه شما را برای یافتن نشانه ها و ویژگی های بدافزارهای شناخته شده جستجو میکند. این کار را با جستجو در یک بانک اطلاعاتی و مقایسه با نشانه های بدافزارهای شناخته شده در این بانک انجام میدهد، اگر چیزی بر روی رایانه شما با الگویی که در این بانک اطلاعات است مطابقت کرد، برنامه ضدویروس، بدافزار را تشخیص و آن را خنثی میکند. مانند سیستم ایمنی بدن انسان، این طریقه شناسایی نیاز به بروز رسانی دائم دارد، مانند واکسن آنفولانزا، برای حفاظت در برابر گونه های جدید، ضدویروس هم باید برای شناسایی گونه های جدید خود را بروز کند. ضد ویروس تنها می تواند در برابر بدافزارهایی که تا کنون شناسایی شده اند محافظت کند. مشکل این است که هکرها چنان سریع بدافزارهای جدید میسازند که فروشندگان ضد ویروس نمی توانند به پای آنها برسند. در نتیجه، بدون توجه به اینکه چقدر ضد ویروس خود را بروز کنید، همیشه گونه جدیدی از بدافزار هست که بالقوه می تواند ضد ویروس شما را دور بزند.

ضد ویروس چیست؟

در روش شناسایی از روی رفتار، ضد ویروس در پی شناسایی بدافزارهای شناخته شده نیست، بلکه رفتار نرم افزارهای نصب شده بر روی رایانه شما را زیر نظر میگیرد. وقتی برنامه ای به طرز مشکوکی عمل می کند، مثلا تلاش برای دسترسی به یک فایل محافظت شده میکند یا در پی تغییر برنامه دیگری است، این نوع ضد ویروسها رفتارهای مشکوک را تشخیص و به شما آنرا هشدار میدهند. این روش در برابر انواع جدید بدافزارها که هنوز در هیچ بانک ویروس ها وجود ندارد مقابله میکنند. مشکل این روش ها این است که ممکن است هشدارهای غلط تولید کنند. شما، به عنوان کاربر رایانه، ممکن است مطمئن نباشید که به چه برنامه ای اجازه بدهید یا ندهید که کارش که مشکوک است را انجام دهد و ممکن است در طول زمان حساسیت خود را به تمام هشدارها از دست بدهید. ممکن است بعد از هر هشداری وسوسه شوید که بر روی «پذیرش-Accept» کلیک کنید، و اینگونه رایانه خود را مستعد هک و آلوده شدن کنید. علاوه بر این، وقتی رفتار مشکوک تشخیص داده شد، ممکن است که این بدافزار به احتمال زیاد بر روی دستگاه شما کارهایی را انجام داده و شما ممکن است ندانید چه اقداماتی این بدافزار قبل از اینکه نرم افزار ضد ویروس آنرا شناسایی کند انجام داده است.

در حالی که ضد ویروس، بخش مهمی از امنیت شماست، اما نمی تواند همه هک ها را شناسایی و یا جلوگیری کند. نهایتاً شما بهترین سپر هستید، نه فن آوری به تنهایی.

ضد ویروس، بخش مهمی از تامین امنیت رایانه و دستگاه های تلفن همراه شما محسوب میشود، در صورت امکان توصیه می کنیم که آنرا نصب و از آنها حتما استفاده کنید. با این حال، نکته کلیدی که باید به خاطر داشته باشید این است که بدون در نظر گرفتن اینکه چگونه ضد ویروس شما کار میکند، هرگز نمی تواند شما را از تمام انواع بدافزارها محافظت کند. در نهایت، شما و نه فن آوری ها به تنهایی، بهترین سپر در برابر حملات سایبری امروزه هستید.

نکاتی درباره ضد ویروس

۱. نرم افزارهای ضد ویروس را فقط از منابع و فروشندگان قابل اعتماد تهیه کنید. هکرهای سایبری شگردی متداول دارند که ضد ویروس های جعلی منتشر میکنند که در واقع بدافزار و ویروس می باشند.

۲. حتما آخرین نسخه نرم افزار ضد ویروس را نصب کنید و نیز اشتراک سالانه آن را پرداخت کرده و ضدویروس را فعال نگه دارید، و ضد ویروس را طوری تنظیم کنید که به طور خودکار بروز شود. اگر رایانه شما برای مدتی متصل به اینترنت نبوده یا مدتی خاموش بوده، نرم افزار ضد ویروس نیاز به بروز رسانی دارد. هنگامی که آن را روشن می نمایید و یا دوباره به اینترنت وصل می شوید، این به روز رسانی را به تعویق نیاندازید.

۳. حتما ضد ویروس طوری تنظیم شده باشد که به طور خودکار دیسکهای قابل حمل مانند USB را برای وجود ویروس بررسی کند و نیز اینکه ضدویروس تمام برنامه ها را قبل از اجرا برای آلوده نبودن کنترل کند. این قابلیت را real-time protection گویند.

۴. به هشدارها و اخطارهایی که توسط نرم افزار ضد ویروس روی صفحه نمایش ظاهر میشوند دقت و توجه کنید. اکثر هشدارها گزینه ای برای گرفتن اطلاعات بیشتر و یا پیشنهاد برای اقدام مناسب بعدی نمایش میدهند. اگر شما هشداری روی رایانه محل کار دریافت کردید، بلافاصله به مرکز کامپیوتر سازمان و یا سرپرست خود اطلاع دهید.

ضد ویروس چیست؟

۵. نرم افزار ضد ویروس خود را به خاطر اینکه احساس می کنید سرعت رایانه را کم کرده، یا اینکه دسترسی به وب سایتی را ممنوع کرده یا از نصب برنامه ای جلوگیری میکند، حذف نکنید. غیر فعال کردن ضد ویروس، شما را در معرض دردسرهای غیر ضروری قرار میدهد و ممکن است منجر به وقوع هک یا آلودگی رایانه اتان شود. اگر مشکلات بر روی رایانه شما همچنان باق است، با مرکز رایانه سازمان تماس بگیرید. اگر مشکلات بر روی رایانه شخصی شما باق ماند، سعی کنید با فروشنده ضد ویروس تماس بگیرید، یا از وب سایت آنها برای اطلاعات بیشتر بازدید کنید و یا ضد ویروس خود را با یک محصول جدید تعویض کنید.

۶. چند برنامه ضد ویروس را همزمان بر روی رایانه خود نصب نکنید. انجام این کار به احتمال زیاد باعث اختلاط این برنامه ها با یکدیگر میشود و در واقع ممکن است امنیت رایانه شما را کاهش دهد.

۷. سعی کنید با هشدارهای مختلفی که نرم افزار ضد ویروس شما تولید می کند آشنا شوید. هکرها وب سایت هایی راه اندازی میکنند که در آنها پیام هایی شبیه پیامهای ضدویروس ها نمایش میدهد که بسیار واقعی به نظر می آیند و به شما پیشنهاد کمک میکنند تا رایانه شما را از آلودگی رفع کنند. کلیک بر روی لینک و یا دکمه های این وب سایت ها در واقع می تواند به رایانه شما آسیب برساند و رایانه اتان را آلوده کند.

بیشتر بدانید

با مراجعه به آدرس زیر، مشترک ماهنامه OUCH! شوید و به آرشیو خبرنامه آگاهی از امنیت OUCH! دسترسی داشته باشید، و در مورد راه حل‌های افزایش آگاهی‌های امنیتی موسسهSANS بیشتر بدانید.

آدرس: http://www.securingthehuman.org

یادداشت مترجم

سایت www.sycurity.com مرجع امنیت اطلاعات برای کاربران فارسی زبان در سراسر دنیا.

منابع

مقایسه انواع نرم افزارهای ضد ویروس: http://www.av-test.org/en/

مهندسی اجتماعی: http://www.securingthehuman.org/ouch/2014#november2014

پست الکترونیک حملات فیشینگ: http://www.securingthehuman.org/ouch/2013#february2013

من هک شدم، حالا چه کنم؟: http://www.securingthehuman.org/ouch/2014#may2014

هیأت تحریریه : Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis

ترجمه شده توسط : سعید میرجلیلی