ماهنامه ای برای آگاهی کاربران رایانه از امنیت اطلاعات

OUCH!

دراین شماره..

- بدافزار چیست؟
- چه کسی و چرا؟
- محافظت از خود

بدافزار چیست؟

مقدمه

شاید اصطلاحاتی مانند ویروس، کرم، تروجان و یا rootkit که بر روی اینترنت مکرر گفته میشود را شنیده باشید. این واژه ها نام انواع برنامه های مخربی هستند که توسط خرابکاران اینترنتی برای آلوده کردن و تحت کنترل در آوردن رایانه ها و دستگاه های تلفن همراه استفاده میشوند. امروزه به همه این نرم افزارهای مخرب بدافزار می گویند. در این خبرنامه، توضیح داده خواهد شد که بدافزارها چه هستند؟ چه کسی و به چه دلیل آنها را میسازد، و شما برای محافظت از خود در برابر آنها چکار می توانید انجام دهید.

سردبیر مهمان

لنی زلتسر (Lenny Zeltser) در زمینه حفاظت از فعالیت های IT مشتریان در شرکت NCR Corp کارمیکند و نیز درس مقابله با بدافزارها را در موسسه SANS تدریس میکند. لنی در توییتر با نام **@lennyzeltser** فعال است و در وبلاگی **blog.zeltser.com** درباره امنیت می نویسد.

بدافزار چیست؟

به عبارت ساده، بدافزارها (Malware) نوعی نرم افزار هستند، یک برنامه کامپیوتری که برای انجام اقدامات مخرب ساخته میشوند. در واقع اصطلاح بد افزار (نرم افزارهای مخرب= (malware ترکیبی از دو واژه بد (مخرب =(malicious و نرم افزار (software) است. هدف نهایی خرابکارهای اینترنتی نصب نرم افزارهای مخرب بر روی کامپیوتر یا دستگاه های تلفن همراه شما است. پس از نصب، خرابکارها به طور بالقوه میتوانند کنترل کامل دستگاه شما را بدست بگیرند. بسیاری از مردم این تصور غلط را دارند که نرم افزارهای مخرب تنها مشکلی برای رایانه های ویندوز هستند. ولی چون ویندوز به طور گسترده ای استفاده می شود، طبیعتا بیشتر مورد حمله قرار میگیرد، ولی بدافزارها می توانند هر دستگاه رایانه ای از جمله گوشی های هوشمند و رایانه های لوحی را آلوده کنند. در واقع، شیوع نرم افزار مخرب که دستگاه های تلفن همراه را آلوده میکنند بطور فزاینده در حال رشد است. علاوه بر این، به خاطر داشته باشید که همه کاربران هدف حمله بدافزارها هستند، از جمله شما. هر چه کامپیوتر و دستگاه های تلفن همراه بیشتری را خرابکاران اینترنتی آلوده کنند، پول بیشتری به دست می آورند. این خرابکارها معمولا اهمیتی نمی دهند که دستگاه چه کسی را آلوده میکنند، و به تعداد دستگاههای آلوده بیشتر اهمیت میدهند.

چه کسانی و چرا؟

الان دیگر بدافزارها فقط توسط علاقمندان کنجکاو و یا هکرهای آماتور ساخته نمیشوند، بلکه توسط خرابکاران اینترنتی حرفه ای که در پی هدفی خاص هستند انجام میشود. این اهداف می تواند شامل سرقت اطلاعات محرمانه، بدست آوردن کلمه عبور و اطلاعات ورود به سیستم، ارسال ایمیل های ناخواسته (هرزنامه)، اجرای حملاتی که سیستم را از کار انداخته، اخاذی یا سرقت هویت باشد. به عنوان مثال، بدافزاری معروف به Cryptolocker است که توسط خرابکاران اینترنتی برای آلوده کردن و رمزکردن تمام فایل ها بر روی کامپیوتر شما مورد استفاده میشود. پس از آلوده و رمزگذاری کردن، خرابکارها خواستار باج در ازای رمز گشایی فایل های شما میشوند.

© The SANS Institute 2014

بدافزار چیست؟

بهترین راه برای محافظت از خود در برابر نرم افزارهای مخرب، به روز نگه داشتن دستگاه خود، نصب ضد ویروس و به روزرسانی مداوم، و در نهایت هوشیار بودن در مقابل حملات و فریب ها.

افرادی که از ایجاد و توزیع نرم افزارهای مخرب بهره می برند از گروههای مختلفی هستند. افرادی که به تنهای برای اهداف شخصی اینکار میکنند تا گروه های تبهکارانه سازمان یافته و یا سازمانهای دولتی. علاوه بر این، افرادی که نرم افزارهای مخرب پیچیده امروزی ایجاد میکنند، اغلب روی اینکار سرمایه گذاری کرده اند و ساخت نرم افزارهای مخرب کار تمام وقت آنها است. در واقع، وقتی آنها نرم افزارهای مخرب خود را ساختند، اغلب آنرا به دیگر افراد و یا سازمانها فروخته و خدمات به روز رسانی منظم و پشتیبانی از آنها را به « مشتریان» ارائه میکنند. هنگامی که خریداری شدن، دیگر خرابکارها با نصب نرم افزارهای مخرب بر روی میلیون ها سیستم قربانی های بی گناه، یک شبکه ای از سیستم های آلوده (botnet) تشکیل میدهند که مانند یک ارتشی که از راه دور کنترل میشوند عمل میکنند، که خرابکاران کامپیوتری می توانند برای اهداف مورد نظر خود استفاده، و یا این شبکه کامپیوترهای آلوده را به سایر مجرمان و خرابکاران اینترنتی بفروشند.

محافظت از خود

یک گام متداول برای حفاظت از کامپیوتر یا دستگاه های تلفن همراه خود در مقابل نرم افزارهای مخرب، نصب نرم افزار ضد ویروس از تولیدکنندگان مورد اعتماد است. آنتی ویروس، گاهی اوقات به نام نرم افزار امنیتی ضد بدافزار نیز نامیده میشود، برای شناسایی و متوقف کردن برنامه های مخرب است. با این حال، ضد ویروس نمی تواند تمام بدافزارها را مسدود و یا حذف کند. مهاجمان سایبری به طور مداوم در حال نوآوری و توسعه حملات جدید و پیچیده تر هستند که می توانند این برنامه های ضد ویروس را دور بزنند. به نوبه خود، تولیدکنندگان ضد ویروس نیز دائما در حال به روز رسانی محصولات خود با قابلیت های جدید برای شناسایی نرم افزارهای مخرب جدید هستند. به عبارت دیگر، یک مسابقه تسلیحاق هست که هر دو طرف برای زرنگ تر بودن از دیگری تلاش میکنند. متاسفانه، خرابکاران اینترنتی تقریبا همیشه دست بالا را دارند. به این ترتیب، به یاد داشته باشید که در حالی که نرم افزارهای ضد ویروس می توانند بسیاری از نرم افزارهای مخرب را شناسایی و جلوگیری کنند، همیشه نسخه های جدید بدافزارها ایجاد خواهد شد که از زیر دست ضدبدافزارها در میروند. در نتیجه شما نمی توانید فقط به ضد ویروس ها برای محافظت از دستگاههایتان اعتماد کنید و شما باید برای محافظت از خودتان گامهای دیگری نیز بردارید.

نخست، حتما سیستم عامل و برنامه های کاربردی را طوری تنظیم کنید که به صورت خودکار به روز رسانی های امنیتی را نصب کنند. هر چه نرم افزار شما به روز تر باشد، برای خرابکاران اینترنتی آلوده کردن رایانه های شما و یا دستگاه های تلفن همراه سخت تر است.

دوم، به یاد داشته باشید که خود شما یکی از بهترین موانع در برابر نرم افزارهای مخرب می باشید. معمولا در روند آلوده سازی بدافزارها مهندسی اجتماعی هم هست، که این چیزی بیش از نیست که مهاجمان شما را فریب میدهند تا نرم افزارهای مخرب را برای آنها نصب کنید. یکی از نمونه های رایج حملات فیشینگ است، که ظاهرا ایمیل های عادی هستند ولی در حقیقت تقلبی طراحی شده اند تا کامپیوتر شما را آلوده کنند. به عنوان مثال، خرابکار سایبری ممکن است به شما یک ایمیل که به ظاهر از بانک شما آمده بفرستد و از شما درخواست کلیک بر روی

© The SANS Institute 2014

بدافزار چیست؟

لینکی کند. اگر شما بر روی لینک کلیک کنید شما به یک وب سایت هدایت میشوید که به طور خودکار تلاش میکند که کامپیوتر شما را آلوده کرده یا هک کند. یا ممکن است ایمیل به شما بفرستند که در آن نوشته که بسته پستی شما را نمی توانند تحویل دهند و از شما بخواهند که فایل ضمیمه ایمیل را که سند ردیابی بسته است را باز کنید که با باز کردن فایل رایانه شما آلوده میشود.

حملات مهندسی اجتماعی همچنین روی فن آوری های دیگر رایانه ای نیز اتفاق می افتد مانند تلفن شما. به عنوان مثال، هکرها ممکن است با شما تماس بگیرند و تظاهر کنند که از پشتیبانی فنی مایکروسافت هستند و به شما اطلاع دهند که کامپیوتر شما آلوده است. داستان آنها دروغ است، کامپیوتر شما به احتمال زیاد مشکلی ندارد و هدف آنها این است که شما را گول بزنند تا باور کنید که رایانه تان آلوده است و سپس شما را فریب دهند تا به آنها دسترسی از راه دور به سیستمتان بدهید و یا نرم افزار امنیتی آنها را بخرید که چیزی بیش از یک نرم افزارمخرب نیست. هوشیار باشید و اگر یک تماس تلفنی و یا پیامی عجیب و غریب، مشکوک و یا بیش از حد خوب به نظر می رسد، به احتمال زیاد فریب است و بدافزار است.

در نهایت، بهترین راه برای دفاع در برابر نرم افزارهای مخرب به روز نگه داشتن نرم افزارهای خود، نصب نرم افزار ضد ویروس قابل اعتماد از فروشندگان معروف، و هوشیار بودن در برابر کسانی میباشد که تلاش برای فریب و یا گول زدن شما برای آلوده کردن کامپیوتر شما دارد.

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 syscurity.com مرجع امنیت اطلاعات برای کاربران فارسی زبان در سراسر دنیا.

منابع

مقاله ای از خبرنامه وای! در مورد فیشینگ:
www.securingthehuman.org/resources/newsletters/ouch/2013#february2013
شماره از خبرنامه وای! در مورد ایمن کردن رایانه تان:
www.securingthehuman.org/resources/newsletters/ouch/2012#december2012
آنها بدنبال شما هستند:
http://www.securingthehuman.org/resources/posters

OUCH! توسط برنامه «زندگی امن» موسسه SANS تحت مجوز Creative Commons BY-NC-ND ۳.۰ منتشر و توزیع شده است. اجازه توزیع این خبرنامه به شرط ذکر منبع، بدون تغییر محتوا و نداشتن مقاصد تجاری داده میشود. برای اطلاعات بیشتر، لطفا با ouch@securingthehuman.org تماس بگیرید.

هیأت تحریریه : Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
ترجمه شده توسط : سعید میرجلیلی