ماهنامه ای برای آگاهی کاربران رایانه از امنیت اطلاعات

OUCH!

دراین شماره..

- بدافزار چیست؟
- چه کسی بدافزار را درست می کند؟
- از خود محافظت کنید

بد افزار چیست

مقدمه

ممکن است هنگامی که مردم راجع به امنیت صحبت می کنند کلماتی مثل ویروس، تروجان، بدافزار باج گیرنده یا روتکیت شنیده باشید. همه این کلمات یك چیز مشابه را توصیف می کنند، انواع برنامه هایی که مجرمین برای آلوده کردن کامپیوترها و دستگاهها استفاده می کنند. کلمه رایج برای توصیف همه اینها بدافزار است. در این شماره توضیح خواهیم داد که بدافزار چیست، چه کسی آنرا درست می کند و چرا، و از همه مهمتر چه کاری جهت محافظت از خودتان در برابر بدافزارها می توانید انجام دهید.

سردبیر مهمان

Lenny Zeltser بـر حافظـت از عملیـات فنـاوری اطلاعـات در شرکت NCR تمرکـز دارد و دوره مقابلـه بـا بدافـزار را در SANS تدریـس مـی کنـد. Lenny در توییـتر بـا نشـانی **@lennyzeltser** فعـال اسـت و وبـلاگی در مـورد امنیـت اطلاعـات در آدرس **Zeltser.com** دارد.

بد افزار چیست؟

به زبان ساده، بد افزار نرم افزار -برنامه کامپیوتری- برای انجام عملیات خرابکاری است. در حقیقت، کلمه بدافزار ترکیب کلمات malicious و software است. مجرمان سایبری بدافزار را روی کامپیوتر یا دستگاه نصب می کنند تا کنترل آنها را بدست بگیرند یا به محتویات آنها دسترسی پیدا کنند. بعد از نصب، این حمله کنندگان از بد افزار ها برای جاسوسی از فعالیت های آنلاین تان ، دزدیدن رمز عبور یا پرونده هایتان، یا استفاده از سیستم تان جهت حمله به دیگران استفاده می کنند. بدافزار حتی می تواند مانع دسترسی شما به فایل هایتان شود و از شما باجگیری کند تا بتوانید دوباره کنترل آنها را بدست بگیرید.

بعضی مردم به اشتباه فکر می کنند که بدافزار فقط مشکلی برای کامپیوترهایی که از ویندوز استفاده می کنند است. ویندوز بطور گسترده ای استفاده می شود، پس هدف بیشتر بدافزار هاست. بدافزار هرگونه دستگاهی مثلا کامپیوترهای مك، تلفن های هوشمند، یا تبلت را آلوده می کند. هر چقدر مجرمان سایبری کامپیوتر و دستگاه بیشتری را آلوده کنند پول بیشتری بدست می آورند. در نتیجه، همه هدف حمله آنها هستند حتی شما.

چه کسی بدافزار درست می کند؟

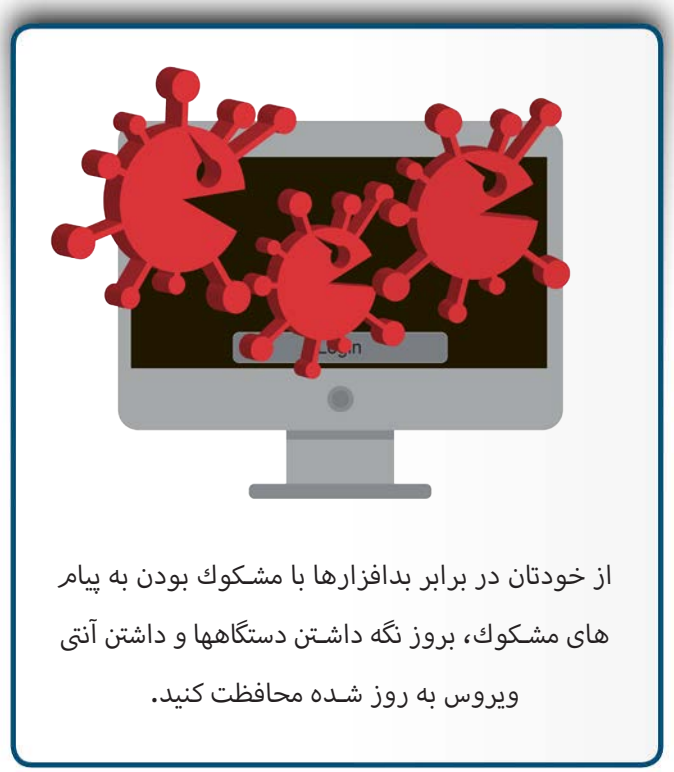
بدافزار دیگر تفنی یا توسط هکر های تازه کار درست نمی شود، بلکه توسط مجرمان سایبری بسیار پیچیده درست می شود. هدف آنها بدست آوردن پول از کامپیوتر یا دستگاه آلوده شما، شاید با فروش داده هایی که از شما بدست آورده اند، فرستادن اسپم، حمله DOS (مختل کردن سرویس) یا اخاذی می باشد. دامنه کسانی که دست به ساخت و توزیع بدافزار می زنند و از آن بهره می برند از اشخاصی که برای خودشان اینکار را انجام می دهند تا گروههای خلافکار بخوبی سازمان یافته یا حتی سازمان های دولتی می باشد. کسانی که امروزه بدافزارهای پیچیده را می سازند اغلب به اینکار متعهد هستند و گسترش بدافزار

بد افزار چیست

ها شغل تمام وقتشان است. بعلاوه، هنگامی که بد افزارشان را توسعه دادند اغلب آن را به اشخاص یا سازمان های دیگر می فروشند، حتی به «مشتریانشان» خدمات بروز رسانی و پشتیبانی عرضه می کنند.

از خود محافظت کنید

یك راه معمول برای حفاظت از خود، نصب کردن آنتی ویروس از یك فروشنده مورد اعتماد است. اینگونه ابزار، که گاهی نرم افزار ضد بد افزار نامیده می شود برای کشف و توقف بد افزار ها طراحی می شوند. اما، آنتی ویروس نمی تواند همه برنامه های خرابکارانه بلاك کند و بزداید. مجرمان سایبری بطور مداوم در حال نو آوری، توسعه بد افزار های جدید و پیچیده تر هستند که ممکن است کشف نشوند. در عوض، فروشندگان آنتی ویروس بطور مداوم در حال بروز رسانی محصولات شان با توانایی جدید برای کشف بد افزارهستند. سالهای متمادی این کار تبدیل به رقابت تسلیحاتی شده است، و طرفین سعی کرده اند از طرف مقابل زیرك تر باشند. متاسفانه تبهکاران معمولا یك قدم جلو ترند. به این دلیل که نمی توانید فقط به آنتی ویرووس متکی باشید در اینجا قدم های بیشتری که باید برای محافظت از خود بردارید را می آوریم:



از خودتان در برابر بدافزارها با مشکوك بودن به پیام های مشکوك، بروز نگه داشتن دستگاهها و داشتن آنتی ویروس به روز شده محافظت کنید.

- مجرمان سایبری اغلب با بهره برداری از آسیب پذیری های نرم افزار های موجود در کامپیوتر ها و دستگاهها آنها را آلوده می کنند. هر چه نرم افزارتان رایج تر باشد آسیب پذیری هایش کمتر است و آلوده کردنش برای مجرمان سایبری مشکل تر است. بنابراین حتما سیستم های عامل، اپلیکیشن ها و دستگاههایتان بطور خودکار بروز رسانی ها را نصب کنند.
- راه رایجی که مجرمان سایبری موبایل شما را آلوده می کنند، ساخت اپلیکیشن های جعلی، ارسال آن به اینترنت، و سپس فریب مردم به دانلود و نصب آن است. به این دلیل فقط از فروشگاههای آنلاین مورد اعتبار دانلود و نصب کنید. بعلاوه، فقط اپلیکیشن های موبایلی نصب کنید که مدت زیادی است به اینترنت فرستاده شده اند، تعداد زیادی از مردم آنرا دانلود کرده اند، و تعدادی نظر مثبت در مورد آن داده اند.
- در کامپیوتر ها، از حساب کاربری استانداری استفاده کنید که اختیارات کمتری نسبت به حسابهای مدیریتی و اصلی دارد. اینکاراز اینکه انواع متنوعی از بدافزار ها خودشان را نصب کنند بطور مضاعف جلوگیری می کند.
- مجرمان سایبری اغلب مردم را با نصب بدافزار برایشان فریب می دهند. برای مثال، ممکن است برایتان ایمیل ظاهرا قانونی بزنند که شامل ضمیمه یا لینکی می باشد. شاید اینطور بنظر بیاید که ایمیل از بانك تان یا دوستی است. اما، اگر ضمیمه را باز کنید یا روی لینك کلیك کنید، ممکن است کد مخربی را فعال کنید که بدافزاری را روی سیستم نصب کند. اگر پیامی حس قوی فوریت ایجاد می

بد افزار چیست

کند، گیج کننده است، یا خیلی خوب بنظر می رسد بطوریکه باور کردنی نباشد، می تواند یك حمله باشد. ظنین باشید، عقل سلیم معمولا بهترین دفاع شماست.

- بطور مرتب از سیستم و فایل هایتان بر خدمات مبتنی بر سیستم ابری پشتیبان گیری کنید یا فایلهای پشتیبان را بصورت آفلاین مثلا بر درایورهای خارجی که به اینترنت وصل نیستند ذخیره کنید. اینکار اجازه نمی دهد بدافزاری تلاش به پاك کردن یا انکریپت کردن پشتیبان هایتان را کند. پشتیبان ها حیاتی هستند، آنها اغلب تنها راه دریافت مجدد فایلها بعد از آلودگی به بدافزار هستند.

در نهایت، بهترین راه برای دفاع علیه بدافزار بروز نگهداشتن نرم افزار است ، نرم افزار آنتی ویروس مورد اعتمادی از فروشنده خوشنام نصب کنید و نسبت به هر کسی که تلاش در جهت فریب دادنتان جهت آلوده سازی سیستم تان دارد هوشیار باشید.

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

فیشینگ:	https://securingthehuman.sans.org/ouch/2015#december2015
مهندسی اجتماعی:	https://securingthehuman.sans.org/ouch/2014#november2014
استفاده امن از اپلیکیشن موبایل:	https://securingthehuman.sans.org/ouch/2015#january2015
امن کردن تبلت:	https://securingthehuman.sans.org/ouch/2016#january2016
پشتیبان گیری:	https://securingthehuman.sans.org/ouch/2015#august2015

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