ماهنامه ای برای آگاهی کاربران رایانه از امنیت اطلاعات

OUCH!

دراین شماره..

- مقدمه
- نشانه های هك شدن
- چگونگی واکنش به آن

من هك شده ام، حالا چکار کنم؟

مقدمه

ما می دانیم که شما به حفاظت از کامپیوتر و موبایلتان اهمیت می دهید و قدم هایی برای امنیتشان بر می دارید. اما، فارغ از اینکه چقدر امن از تکنولوژی استفاده می کنید، دیر یا زود ممکن است هك شوید یا در معرض خطر قرار بگیرید. در این شماره یاد خواهید گرفت چگونه مشخص کنید که آیا موبایل یا کامپیوترتان هك شده است و اگر چنین است چکار می توانید انجام دهید. در نهایت، هر چه سریعتر بفهمید اشکالی وجود دارد و هر چه سریعتر واکنش نشان دهید، شانس بیشتری برای کاهش آسیبی که حمله کننده سایبری می زند خواهید داشت.

سردبیر مهمان

Samantha Davison (@sam_e_davison) مدیر برنامه آموزش و اطلاع رسانی امنیت در Uber است که کارکنانشان را در همه دنیا در بیش از ۳۵۰ شهر آموزش می دهد.

نشانه هایی که هك شده اید

اغلب بیش از یك راه برای فهم اینکه هك شده اید وجود دارد و به همین دلیل ممکن است کارسختی باشد. در عوض هکرها معمولا نشانه هایی از خود بجا می گذارند که اغلب شاخص نامیده می شود. هر چه همخوانی سیستم با هر کدام از این نشانه ها بیشتر باشد، احتمال اینکه هك شده باشید بیشتر می شود.

- سیستم آنتی ویروس اخطاری مبنی بر اینکه سیستم آلوده شده است را نشان دهد، مخصوصا اگر بگوید که قادر به حذف یا قرنطینه فایل های آلوده نمی باشد.
- صفحه نخست مرورگرتان بطور غیر منتظره ای عوض شده باشد یا مرورگرتان شما را به وب سایت هایی می برد که نمی خواستید بروید.
- حساب های کاربری جدیدی در کامپیوتر یا وسیله تان وجود دارد که شما ایجاد نکرده اید، یا برنامه هایی در حال اجرا می باشند که شما نصب نکرده اید.
- کامپیوتر یا اپلیکیشن ها مرتبا بهم می ریزند، آیکنی برای اپلیکیشن های ناشناخته یا پنجره های عجیبی که مرتبا باز می شوند وجود ندارد.
- برنامه ای خواستار اجازه شما برای انجام تغییرات بر روی سیستم تان می شود، در حالیکه بطور فعال هیچ اپلیکیشنی را نصب یا بروز رسانی نمی کنید.
- رمز عبور ورود به سیستم یا حساب آنلاینتان دیگر کار نمی کند، هر چند می دانید رمز عبورتان را صحیح وارد می کنید.

© SANS Institute 2016

من هك شده ام، حالا چكار كنم؟

- دوستانتان می پرسند چرا هرزنامه برایشان می فرستید در حالیکه شما اینکار را نکرده اید.
- موبایلتان هزینه غیر مجاز از طریق إرسال اس ام اس به شماره هایی که هزینه بردار هستند به شما تحمیل می کند.
- ناگهان و بطور غیر منتظره مصرف باتری یا داده در موبایلتان بالا می رود.

دیر یا زود کامپیوتر یا دستگاهتان ممکن است در معرض خطر قرار گیرد، هر چه زود تر واقعه را تشخیص دهید و زودتر نسبت به آن واکنش نشان دهید بهتر است.

چگونه واکنش نشان دهیم؟

اگر فکر می کنید کامپیوتر یا دستگاهتان هك شده است، هر چه زود تر واکنش نشان دهید بهتر است. اگر کارفرمایتان این کامپیوتر یا دستگاه را به شما داده یا از آن در کارتان استفاده می کنید سعی نکنید که خودتان آنرا تعمیر کنید. چون نه تنها ممکن است بیشتر کار را خراب کنید، بلکه ممکن است شواهد ارزنده جهت تحقیق و بررسی را از بین ببرید. بجای اینکار سریعا این موضوع را به کارفرمایتان اطلاع دهید. اینکار معمولا با اطلاع دادن به مرکز پشتیبانی انفورماتیك ، تیم امنیت یا سرپرستتان انجام می شود. اگر بنا به دلائلی نمی توانید با سازمانتان تماس بگیرید یا نگران تاخیر هستید، کامپیوتر یا دستگاهتان را از شبکه جدا کنید و سپس در حالت sleep یا مد هواپیما یا معوق قرار دهید. حتی اگر مطمئن نیستید که هك شده اید بهتر است گزارش کنید تا اگر احیانا مشکلی بود بررسی شود. اگر کامپیوتر یا دستگاه برای مصرف شخصی است این قدم ها را بردارید:

- **رمز عبورتان را عوض کنید:** اینکار شامل عوض کردن رمز عبور کامپیوتر و دستگاه و همچنین رمز عبور تمام حساب های آنلاینتان می شود. از کامپیوتری که هك شده است برای عوض کردن رمز عبور استفاده نکنید. از کامپیوتر یا دستگاه دیگری که می دانید امن است استفاده کنید.
- **آنتی ویروس.** اگر نرم افزار آنتی ویروس یك فایل آلوده را به شما خبر می دهد، اقداماتی که پیشنهاد می دهد را دنبال کنید. این کار معمولا شامل قرنطینه کردن فایل، حذف ویروس از فایل یا پاك کردن فایل می شود. بیشتر نرم افزار های آنتی ویروس لینك هایی دارند که با دنبال کردن آنها می توانید در مورد خاصی از آلودگی بیشتر یاد بگیرید. وقتی شك دارید فایل را قرنطینه کنید، اگر امکان قرنطینه نیست آنرا پاك کنید.
- **دوباره ساختن.** اگر قادر به رفع آلودگی نیستید یا می خواهید بطور قطع مطمئن شوید که سیستم ترمیم شده است، انتخاب امن دیگر دوباره ساختن است. برای کامپیوتر ها دستورالعمل های سازنده سیستم را دنبال کنید. در بیشتر موارد اینکار به معنی استفاده از امکانات گنجانده شده در ویندوز برای نصب مجدد سیستم عامل است. اگر این امکانات وجود ندارند، خراب شده اند یا آلوده شده اند، برای راهنمایی گرفتن با تولید کننده سیستم عامل تماس بگیرید یا به وب سایتشان مراجعه کنید.سیستم عامل را از پشتیبان ها دوباره نصب نکنید. آنها ممکن است همان ضعف و آسیب پذیری ای داشته باشند که در اصل به هکر اجازه دسترسی داد . پشتیبان

من هك شده ام، حالا چكار كنم؟

ها تنها باید جهت بازیابی داده ها استفاده شوند. برای دستگاههای موبایل دستورالعمل های تولید کننده دستگاه یا خدمات ارائه که در سایتشان موجود است را دنبال کنید. در بیشتر موارد اینکار به سادگی بازگرداندن موبایل به تنظیمات پیش فرض کارخانه است. اگر با فرایند دوباره ساختن راحت نیستید، از خدمات حرفه ای کمك بگیرید. یا، اگر کامپیوتر یا دستگاهتان قدیمی است، ممکن است ساده تر یا حتی ارزان تر باشد اگر دستگاه جدیدی بخرید. در نهایت، یك مرتبه که کامپیوتر یا دستگاهتان را دوباره ساختید، یا دستگاه جدید خریدید مطمئن شوید که کاملا بروز و جدید است و هرگاه ممکن است بروز رسانی خودکار را فعال کنید.

- **پشتیبان ها**. مهمترین قدمی که جهت محافظت از خود می توانید بردارید تهیه مرتب و منظم پشتیبان هاست. هر چه به کرات بیشتری پشتیبان بگیرید بهتر است. بعضی راه حل ها بطور خودکار از هر فایل جدید یا تغییر یافته بطور ساعتی پشتیبان می گیرند. صرفنظر از اینکه از کدام راه حل بطور دوره ای استفاده می کنید چك کنید که آیا قادر به بازگرداندن این فایل ها هستید. اغلب بازیابی فایل ها از پشتیبان ها تنها راه بازیابی و ترمیم فایل هاست.
- **اعمال قانون**. اگر از هر طریق احساس تهدید شدن می کنید، واقعه را به مجاری قانونی گزارش کنید.

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

پشتیبان ها:	https://securingthehuman.sans.org/ouch/2015#august2015
عبارت عبور:	https://securingthehuman.sans.org/ouch/2015#april2015
بد افزار چیست:	https://securingthehuman.sans.org/ouch/2016#march2016
امن سازی تبلت جدید:	https://securingthehuman.sans.org/ouch/2016#january2016

OUCH! توسط برنامه «زندگی امن» موسسه SANS تحت مجوز Creative Commons BY-NC-ND ۴.۰ 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

securingthehuman.org/blog /securethehuman @securethehuman securingthehuman.org/gplus