ماهنامه ای برای آگاهی کاربران رایانه از امنیت اطلاعات

OUCH!

دراین شماره..

من هک شدم، چه کار باید کرد؟

مقدمه

شما حتما به حفاظت از رایانه و اطلاعات خود اهمیت میدهید و قدم هایی را برای امن کردن آنها برداشته اید. با این حال، درست مانند رانندگی اتومبیل، هر چقدر هم با رعایت قوانین رانندگی کنید، دیر یا زود ممکن است تصادفی داشته باشید. در این خبرنامه ما به شما آموزش میدهیم چگونه بفهمید که آیا رایانه شما هک شده است، و اگر چنین شده چه اقداماتی میتوانید انجام دهید. در مجموع، هر چه سریعتر بفهمید رایانه شما هک شده است و سریعتر به آن پاسخ دهید، بهتر می توانید هر گونه آسیب به شما و یا سازمان تان را کاهش دهید.

سردبیر مهمان

جیک ویلیامز (**@MalwareJake** . **malwarejake.blogspot.com**)
پژوهشگر ارشد گروه مشاورین امنیت رایانهCSRgroup است.
او همچنین یکی از نویسندگان دوره های بازرسی قانونی حافظه (FOR526) و مهندسی معکوس تروجان (FOR610) در موسسه SANS است.

نشانه های هک شدن

نخست، باید بدانید که معمولا به چند نشانه برای تعیین اینکه آیا رایانه شما هک شده است نیاز است و نه فقط یک نشانه. اگر شما ترکیبی از این نشانه ها را شناسایی کردید، میتوان نتیجه گرفت که رایانه شما هک شده است. در اینجا چند نمونه ذکر میشود:

- برنامه ضد ویروس شما هشدار بدهد که رایانه شما آلوده است، به خصوص اگر بگوید که قادر به حذف یا قرنطینه کردن فایل آلوده هم نیست.
- صفحه ابتدای مرورگر شما به طور غیر منتظره ای تغییر کرده است و مرورگر رایانه شما را به وبگاه هایی میبرد که شما نمیخواهید.
- حساب های کاربری جدیدی در رایانه شما ایجاد شده که قبلا وجود نداشته است.
- برنامه های جدیدی در حال اجرا هستند که شما نصب نکرده اید.
- رایانه شما به طور مداوم قفل میکند و یا بسیار کند شده است.
- برنامه ای بر روی رایانه تان درخواست مجوز برای ایجاد تغییرات بر روی سیستم شما میکند، درحالی در حال نصب و یا به روز رسانی هیچ برنامه ای نیستید.
- برنامه فایر وال هشدار میدهد که برنامه ناشناسی درخواست مجوز برای دسترسی به اینترنت دارد.

من هک شدم، چه کار باید کرد؟

چه باید کرد؟

اگر فکر می کنید رایانه شما هک شده است، هر چه زودتر به رفع مشکل بپردازید، بهتر است. اگر رایانه ای که استفاده میکنید کارفرما به شما داده است یا برای کار استفاده می شود، سعی نکنید خودتان آنرا تعمیر کنید و رایانه را خاموش نکنید. نه تنها شما ممکن است آسیب بیشتری به جای بهبود به رایانه بزنید، بلکه ممکن است شواهد و رد پاهای ارزشمندی که میشد برای تحقیقات بعدی استفاده شود را از بین ببرید. در عوض، حادثه را فوری به کارفرما گزارش دهید، معمولا با تماس با مرکز رایانه ای سازمان، تیم امنیتی و یا سرپرست خود. اگر به هر دلیلی نمی توانید با سازمان خود تماس بگیرید، و یا نگران تاخیر در کار هستید، رایانه خود را از شبکه قطع کنید و سپس آن را در حالت خواب، حالت تعلیق یا تعلیق بلد مدت بگذارید (کامل خاموش نکنید). حتی اگر مطمئن نیستید که هک شده اید، خیلی بهتر است که محض احتیاط حادثه را گزارش دهید. سازمان به احتمال زیاد دارای فرآیندها و یک تیم در محل دارد که مسئول رسیدگی به شرایط این چنینی هستند، اجازه دهید آنها شرایط را اداره کنند.

دیر یا زود ممکن است رایانه شما هک شود، هر چه سریع تر آنرا شناسایی و واکنش نشان دهید، بهتر است.

اگر رایانه برای استفاده شخصی است، در اینجا برخی از اقداماتی که خودتان میتوانید انجام دهید عبارتند از:

- **پشتیبان گیری:** مهمترین گام پشتیبان گیری است که نوعی آمادگی قبلی مواجه با هک است. مخصوصا نسخه پشتیبان را به طور منظم و دوره ای بررسی کنید که قادر به بازیابی فایل ها از نسخه پشتیبان باشید. اغلب زمانی که رایانه ای هک شده است، تنها گزینه پاک کردن دیسک سخت سیستم و نصب مجدد سیستم عامل و یا خرید یک رایانه جدید است. در هر صورت نیاز به نسخه پشتیبان برای بازیابی داده های شخصی تان دارید.
- **تغییر رمز عبور:** همه رمزهای عبورتان را حتما تغییر دهید؛ نه تنها رمزهای عبور بر روی رایانه تان و دستگاه های تلفن همراه، بلکه همه رمزهای عبور آنلاین. تمام رمزهای عبور آنلاین را از طریق رایانه متفاوتی که مطمئن هستید آلوده نیست تغییر دهید.
- **ضد ویروس:** اگر نرم افزار ضد ویروس شما از وجود فایلی آلوده خبر میدهد، می توانید اقداماتی که نرم افزار توصیه میکند دنبال کنید. این معمولا می تواند شامل قرنطینه کردن فایل، رفع آلودگی فایل و یا حذف فایل باشد. اکثر نرم افزارهای ضد ویروس لینکی ارائه میکنند که می توانید برای اطلاعات بیشتر دنبال کنید و بیشتر در مورد ویروسهای خاص بدانید. اگر شک دارید، فایل را قرنطینه کنید. در صورتی که امکان پذیر نیست، آن را حذف کنید.
- **نصب مجدد:** اگر قادر به تمیز کردن رایانه با ضد ویروس نمی باشید، یکی از امن ترین راه ها برای بازسازی رایانه نصب برنامه ها از ابتدا است. اول رایانه را از شبکه قطع کنید. سپس دستورالعمل سازنده رایانه خود را دنبال کنید، در اکثر موارد اینکار یعنی استفاده

من هک شدم، چه کار باید کرد؟

از پارتیشن بازیابی برای نصب مجدد سیستم عامل. اگر پارتیشن بازیابی از دست رفته، خراب شده و یا آلوده است، با کارخانه سازنده تماس و درخواست یک DVD بازیابی کنید. سیستم عامل را از نسخه پشتیبان نصب مجدد نکنید. نسخه پشتیبان ممکن است همان آسیب پذیری داشته باشد که به هکر اجازه دسترسی داده بوده است. تنها موردی که شما باید از نسخه پشتیبان استفاده کنید اطلاعات شخصی شما است. همچنین، اگر رایانه شما قدیمی و یا منسوخ شده است، ممکن است به جای صرف ساعت ها وقت برای بازسازی آن خرید رایانه جدیدی ساده تر (و شاید حتی ارزان تر) باشد.

- **کمک گرفتن از یک متخصص:** اگر نگران هستند که هک شده اید، اما احساس می کنید مهارت یا دانش تعمیر آن را نداشته باشند، ممکن است بهتر باشد رایانه خود را به یک حرفه ای تحویل دهید. به عنوان مثال، پس از هک شما ممکن است متوجه شوید که پشتیبان گیری انجام شده ناقص و یا منسوخ شده است. ممکن است وسوسه شوید فایل های مهم مانند عکس، اسناد و یا فیلم ها را از دستگاه آلوده خود به یک دستگاه جدید انتقال دهید. با این حال با انجام این کار ممکن است سهوی نرم افزارهای مخرب و آلوده را به رایانه جدید خود انتقال دهید. یک جایگزین به مراتب امن تر تحویل رایانه آلوده به یک متخصص واجد شرایط است که با خیال راحت می تواند این فایل ها را به صورت امن بدون خطر ویروس انتقال دهد.

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

وای! پشتیبان گیری :	http://www.securingthehuman.org/ouch/2013 # september2013
وای! رمز عبور :	http://www.securingthehuman.org/ouch/2013 # may2013
وای! چه تروجان :	http://www.securingthehuman.org/ouch/2014 # february2014
پوستر کشف شرور:	https://digital-forensics.sans.org/media/poster_2014_find_evil.pdf

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