دوشنبه 22 خرداد 1391 - 07:32

# تغییردهنده DNS پایان جهان نیست

طبق گزارش‌های موجود، 9 جولای با قیامت در اینترنت مواجه خواهیم بود! به همین علت است که چند وب‌سایت محبوب، ناگزیر درباره ویروس تغییردهنده DNS سخن گفته‌اند.

جام جم آنلاین: ویروس تغییردهنده DNSChanger (DNS) قیامتی در اینترنت برپا خواهد کرد.
طبق گزارش‌های موجود، 9 جولای با قیامت در اینترنت مواجه خواهیم بود! به همین علت است که چند وب‌سایت محبوب، ناگزیر درباره ویروس تغییردهنده DNS سخن گفته‌اند.

تغییردهنده DNS یك بدافزار واقعی به‌شمار می‌رود (این ویروس، گونه‌ای از خانواده TDSS/Alureon تروجان‌هاست) و با مشارکت FBI 8 نوامبر 2011 و طی عملیاتی با نام «کلیك ارواح» یك مشکل جدی را ایجاد کرده بود.

تا قبل از آن، تغییردهنده DNS تیتر بسیاری از اخبار دراین زمینه را به‌خود اختصاص داده بود که با هشدارهای ترسناك نیز همراه بود حتی برنامه‌های خبری کانال‌های تلویزیونی محلی با عباراتی نظیر این که «بدترین چیز این است که رایانه شما به این ویروس آلوده شود» به این مسأله می‌پرداختند.

انتشارتیترهای وحشت برانگیز مانند «تروجان جدید مك، صفحه ماوس شما را از کار می‌اندازد» (تردید نکنید چرا که ماوس مك تنها یك دکمه دارد) یا «وارد ویندوز شوید و تمام اطلاعات خود را از دست بدهید» اگرچه به نظر تهدیدی ساده و البته اغراق‌آمیز به نظر می‌رسد، اما ارائه توصیه و راهنمایی‌های مناسب اصلا کار ساده‌ای نیست. در این شماره قصد داریم به این موضوع بپردازیم.

تغییردهنده DNS دقیقا چه‌کاری انجام می‌دهد؟

با این تخمین که حدود چهار میلیون رایانه آلوده به این ویروس وجود دارد (که نیم‌میلیون آن تنها در آمریکاست)، تغییردهنده DNS یکی از بزرگ‌ترین بدافزار در نوع خودش است که تاکنون پیاده‌سازی شده است ولی برخلاف مقالاتی که ممکن است خوانده باشید این بات‌نت (botnet) برای دزدیدن شماره‌های کارت اعتباری یا رمزهای عبور حساب بانکی شما طراحی نشده است.

تغییردهنده DNS به مرورگر شما یك مسیر دوباره به وب‌سایت‌هایی می‌دهد که اغلب قرص‌های آبی کوچك، آنتی‌ویروس‌هایی که اصلا کار نمی‌کند و دیگر چیزهای بی‌مصرف می‌فروشند.

افرادی که پشت تغییردهنده DNS قرار دارند از این شرکت‌های داروسازی تقلبی، سایت‌های آنتی‌ویروس خرابکار و دیگر شخصیت‌های بد سایبری، کمیسیون دریافت می‌کنند البته این کمیسیون مبلغ اندکی نیست و طبق اعلام FBI تقریبا بیش از 14 میلیون دلار است.

معمولا تغییردهنده DNS، سیستم‌ها را به‌وسیله جا زدن خود به‌عنوان یك codec که برای تماشای ویدئوهایی در سایت‌ها قرار دارد، آلوده می‌کند.

هنگامی که شما برای مشاهده این ویدئوهای تله روی آنها کلیك می‌کردید، ویندوز مدیا پلیر اعلام می‌کرد که codec مناسب برای اجرای آن ویدئو را در اختیار ندارد سپس برخی کاربران، آن codec را از سایت دانلود کرده و به آن اجازه نصب نیز می‌داد و بقیه ماجرا را خودتان می‌توانید حدس بزنید. با وجود گوناگونی زیادی که TDSS/Alureon دارد، آلودگی توسط آن نیز خطرناك خواهد بود که شناسایی آن را مشکل و پاکسازی را سخت‌تر می‌کند.

در ویندوز، این ویروس سرور DNS رایانه شما را تغییر می‌دهد که معمولا توسط تغییر در رجیستری انجام می‌گیرد. با وجود یك سرور DNS تغییر کرده ممکن است بعد از تایپ www.google.com در مرورگر خود (نوع مرورگر تفاوتی ندارد) سایت www.buyonlinepharmaceuticalsifyoudare.com را مشاهده کنید. افراد سوءاستفاده‌کننده، سرورهای مختلفی را که همین کار را انجام می‌دهند، تنظیم می‌کنند.

به‌طور طبیعی اگر بخواهید به آدرس‌های معمول وب در زمینه آنتی‌ویروس نظیر اسکن توسط آنتی‌ویروس، به‌روزرسانی، توصیه یا

حتی اخبار درباره تغییردهنده DNS ارائه می‌کنند بروید، مسیردهی دوباره شده‌اید و مرورگر شما به تغییردهنده DNS تعلق پیدا می‌کند!

مقابله با DNS در دو قاره

بسیاری از سازمان‌ها توانسته‌اند با این ویروس مقابله کنند و آن را از بین ببرند. اگرچه سال‌ها طول می‌کشد، ولی سازمان‌های مسوول در یافتن افرادی که به‌طور مستقیم در کلاهبرداری دست داشته‌اند، موفق شده‌اند شش نفر را در استونی به دام بیندازند.

همچنین این سازمان‌ها آدرس‌های IP سرورهای تغییردهنده DNS را پیدا کرده‌اند که تمام آنها در آمریکا قرار دارند.

در يك اقدام هماهنگ پلیس استونی توانست بسیاری از این افراد را دستگیر کند. برای حداقل کردن اختلالات سرویس اینترنت رایانه چهار میلیون کاربر آلوده، FBI و کنسرسیوم سیستم‌های اینترنت (يك شرکت غیرانتفاعی که از نرم‌افزار فراگیر سرور DNS نگهداری می‌کند) تکنیك فوق‌العاده‌ای را به کار بستند؛ آنها بسرعت سرورهای مخرب را با سرورهای DNS سالم جایگزین کردند (به‌همین علت با این که بسیاری از کاربران هنوز نمی‌دانند آلوده شده‌اند، ولی درنهایت به وب‌سایت‌های مورد نظرشان دسترسی پیدا می‌کنند).

عملیات مربوط به مزرعه سرور DNS به يك سازمان جدید به‌نام «گروه کاری تغییردهنده DNS» واگذار شد که از نمایندگان صنعت رایانه و همچنین مجریان قانون تشکیل شده است.

مقابله با عواقب ویروس

درباره آن 4 میلیون کاربر، هوشمندانه‌ترین حرکت چیست؟ این که آنها از این مساله که آلوده هستند مطلع نشوند و درعوض سرورها به‌طور کامل نگهداری شود یا بتدریج سرورها خاموش و در هر زمان ارتباط تعداد کمی از کاربران قطع شود؟ سازمان‌های مسوول تلاش می‌کنند تعدادی از صفحات مفید وب را جدا کرده و يك‌سری هشدارها را در آنها قرار دهند، ولی این کار نیز ممکن است بسیاری از کاربران اینترنت را بترساند و بخواهند به يك سرور DNS دیگر تغییر مسیر دهند!

در اصل سازمان FBI و گروه کاری تغییردهنده DNS از طریق دادگاه مجوز داشتند که مزارع سرورها را تا هشتم مارس در حالت اجرا نگاه دارند اما با پایان یافتن این مهلت و احتمال این که خاموش کردن بقیه ماشین‌های آلوده خرابی زیادی به بار آورد، آنها تصمیم گرفتند این زمان را تا 9 جولای تمدید کنند. احتمال زیادی دارد که گروه کاری تغییردهنده DNS بعد از 9 جولای نیز به کار خود ادامه دهد البته باید به‌یاد داشته باشید که برخی مجبور هستند برای درحالت اجرا ماندن مزارع موقت سرور، هزینه پرداخت کنند.

بنابراین اگر منتظر يك آرماگدون در اینترنت هستید چنین اتفاقی نخواهد افتاد! بلکه باید کار دیگري انجام دهید؛ به سایت تشخیص گروه کاری تغییردهنده DNS بروید (www.dcwg.org/detect) و در پایین صفحه روی زبان یا کشور مورد نظر خود کلیك کنید. هنگامی که صفحه بررسی تغییردهنده DNS باز شد يك گرافیك طولانی خواهید دید. اگر سبز بود مشکلی وجود ندارد ولی اگر قرمز بود متاسفانه شما نیز آلوده شده‌اید.

محمدحسین کردونی
منبع: windowssecrets