پایانی بر WannaCry با سوییچ مرگ

«قهرمان تصادفی» با سوییچ مرگ کاربران را از شر باج افزار WannaCry نجات داد

همان‌گونه که در اخبار خوانده‌اید، در کمتر از یک هفته باج‌افزاری موسوم به WannaCry دردسرهایی را برای کاربران سراسر جهان و سازمان‌ها به وجود آورد. باج‌افزار فوق به اندازه‌ای خطرناک بود که حتا مایکروسافت را که پیش از این گفته بود دیگر هیچ‌گونه پشتیبانی از ویندوز اکس‌پی به عمل نمی‌آورد را مجبور کرد برای سیستم‌عامل‌های قدیمی به‌روزرسانی امنیتی عرضه کند. اما کارشناسی با نام مستعار «قهرمان تصادفی» به یاری کاربران آمد.

یک کارشناس امنیتی که خود را «قهرمان تصادفی» نام نهاده موفق شد از طریق سوییچ مرگ (killer switch) باج‌افزار WannaCry را غیرفعال کند. اغلب تجهیزات الکترونیکی و حتا سرویس‌های کامپیوتری به سازوکاری موسوم به سوییچ مرگ مجهز هستند. این سوییچ‌ها اغلب زمانی مورد استفاده قرار می‌گیرند که یک شرایط بحرانی به وجود آمده و این امکان وجود ندارد تا یک دستگاه را در شرایطی عادی خاموش کرد.

مطلب پیشنهادی

باج‌افزاری با گستره تخریب جهانی
چگونه از خودمان در برابر باج‌افزار خطرناک WanaCry محافظت کنیم

این کارشناس امنیتی با همکاری دارین هاس، کارشناس امنیتی شرکت پروف پوینت موفق شدند به درون کدهای باج‌افزار فوق وارد شده و سوییچ مرگ تعبیه شده درون آن را شناسایی کنند. نویسنده این باج‌افزار به منظور غیرفعال کردن این باج‌افزار در شرایط اضطراری و ممانعت از گسترش غیرمتعارف WannaCry این سوییچ را به شکل هاردکد شده طراحی کرده بود. این سوییچ قادر است یک درخواست را برای دامنه‌ای با نام عجیب ارسال کند. اگر درخواست فوق با موفقیت به سمت دامنه کشف شده ارسال شود سوییچ مرگ فعال شده و مانع از گسترش باج‌افزار می‌شود. تنها کاری که این دو کارشناس انجام داده‌اند این بود که دامنه‌ای با همان نام شناسایی شده را ثبت کردند. دامنه‌ای که هکر آن‌را ثبت نکرده بود!

با این وجود، تعدادی از کارشناسان امنیتی می‌گویند: «به‌کارگیری سوییچ مرگ برای غیرفعال کردن این باج‌افزار به معنای توقف انتشار آن نخواهد بود. در مقطع فعلی این امکان وجود دارد تا هکرها در هر نقطه و هر لحظه‌ای کدهای باج‌افزار را تغییر داده و سوییچ مرگ را از درون آن حذف کنند. هکرها حتا می‌توانند نام دامنه‌ای که درخواست برای آن ارسال می‌شود را تغییر دهند.»

در جدیدترین گزارش منتشر شده از سوی شرکت امنیتی بیت‌دینفدر عنوان شده است که نزدیک به 180 هزار سامانه کامپیوتری قربانی باج‌افزار فوق شده‌اند. همچنین بالغ بر 102 نفر از قربانیان حاضر شده‌اند مبلغ 300 دلار باج مربوطه را از طریق بیت‌کوین پرداخت کنند. در نتیجه تا به این لحظه هکرها چیزی نزدیک به 27 هزار دلار از این باج‌افزار پول به جیب زده‌اند. تا قبل از به‌کارگیری سوییچ مرگ نزدیک به 104 کشور قربانی این باج‌افزار شدند. گزارش‌ها نشان می‌دهد کاربران و سازمان‌های مستقر در کشورهای انگلستان، روسیه، اوکراین، چین، هند، ایتالیا، مصر به ترتیب از قربانیان اصلی این باج‌افزار بوده‌اند.

داستان باج‌افزار فوق از آن‌جا شکل گرفت که یک گروه هکری موسوم به Shadow Brokers تصمیم گرفتند ابزارهایی که از سوی آژانس دولتی امریکا مورد استفاده قرار می‌گیرد را در فضای مجازی منتشر کنند. یکی از این ابزارها، ابزار EternalBlue بود که از طریق یک آسیب‌پذیری روز صفر در ویندوز به سامانه‌ها نفوذ می‌کرد. در حالی که مایکروسافت به‌روزرسانی مربوطه را برای این آسیب‌پذیری عرضه کرده بود، اما متاسفانه تعداد قابل توجهی از کاربران بی‌اعتنا به این موضوع از سیستم‌عامل‌های نفوذپذیر استفاده کردند. همین موضوع باعث شد تا امروز شاهد قربانی شدن تعداد زیادی از کاربران باشیم. در حال حاضر کاربران سیستم‌عامل‌های قدیمی ویندوز اکس‌پی، ویندوز سرور 2003 و ویندوز 8 قادر هستند به‌روزرسانی امنیتی عرضه شده از سوی مایکروسافت را دریافت کنند.

تاریخ انتشار:

25 اردیبهشت 1396

نشانی منبع:
https://www.shabakeh-mag.com/security/7892/%C2%AB%D9%82%D9%87%D8%B1%D9%85%D8%A7%D9%86-%D8%AA%D8%B5%D8%A7%D8%AF%D9%81%DB%8C%C2%BB-%D8%A8%D8%A7-%D8%B3%D9%88%DB%8C%DB%8C%DA%86-%D9%85%D8%B1%DA%AF-%DA%A9%D8%A7%D8%B1%D8%A8%D8%B1%D8%A7%D9%86-%D8%B1%D8%A7-%D8%A7%D8%B2-%D8%B4%D8%B1-%D8%A8%D8%A7%D8%AC-%D8%A7%D9%81%D8%B2%D8%A7%D8%B1-wannacry-%D9%86%D8%AC%D8%A7%D8%AA-%D8%AF%D8%A7%D8%AF