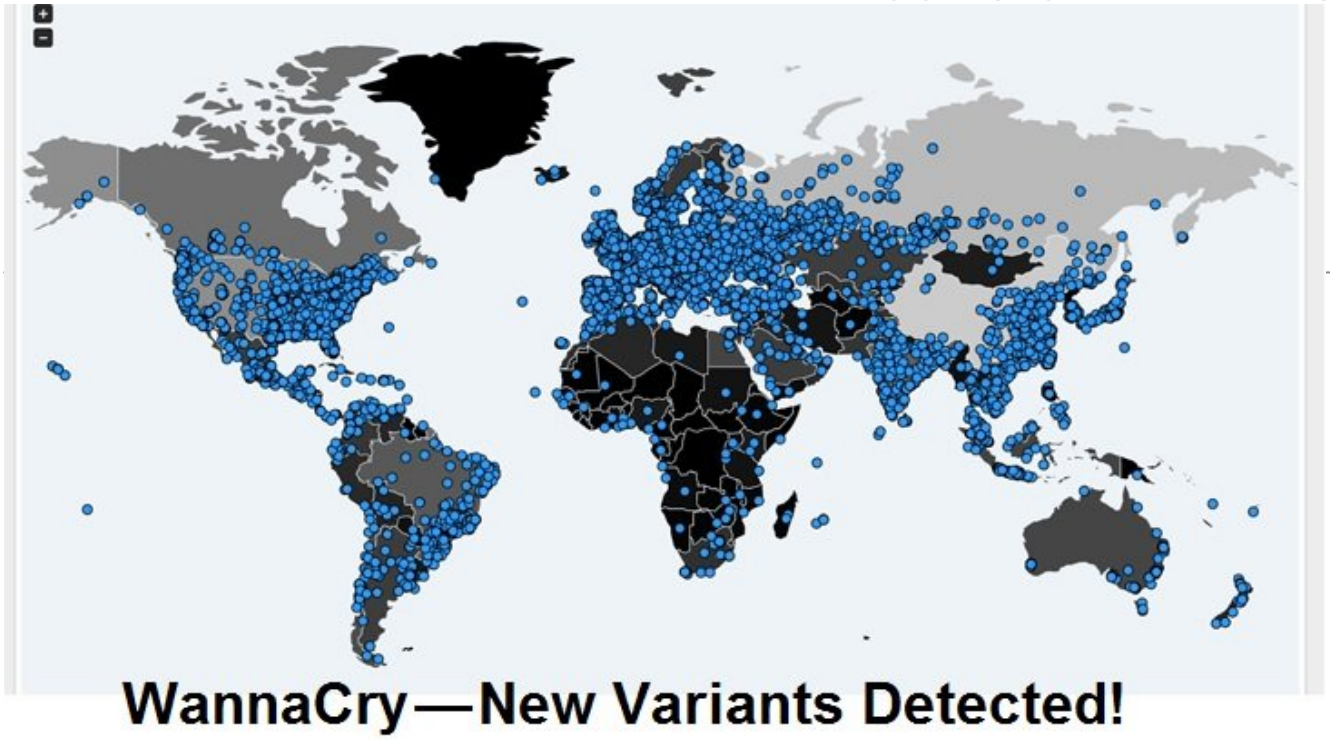
موج دوم حمله

گونه‌های جدیدی از باج‌افزار WannaCry شناسایی شدند



صبح امروز به شما گفتیم یک کارشناس امنیتی که خود را قهرمان تصادفی نامیده است با همکاری کارشناس امنیتی شرکت پروف‌پوینت موفق شدند به درون کدهای این باج‌افزار وارد شده و سوییچ مرگی که درون این باج‌افزار تعبیه شده بود را شناسایی کنند. در ادامه یک دامنه با نامی که در کدهای باج‌افزار قرار داشت را به ثبت رساند تا از کاربران در برابر این باج‌افزار محافظت کند. اما از صبح امروز دو نسخه از این باج‌افزار مشاهده شده است.

پیش‌بینی کارشناسان امنیتی در ارتباط با باج‌افزار WannaCry به حقیقت پیوست. اولین نسخه از این باج‌افزار روز جمعه شناسایی شد. باج‌افزاری که برای ارتباط با مجرمان سایبری به یک ارتباط اینترنتی نیاز داشت. «قهرمان تصادفی» موفق شد از طریق کشف سوییچ مرگ و ارتباط آن با دامنه‌ای به نام iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com کاربران را از شر باج‌افزار WannaCry نجات دهد. اما از صبح امروز دو نسخه جدید از این باج‌افزار شناسایی شده است. گونه اول در حالی کشف شده که یک مشکل اصلی داشته و قادر نیست فایل‌ها را رمزنگاری کرده و کاربران را در معرض تهدید جدی قرار دارد.

مطلب پیشنهادی

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

گونه دوم این باج‌افزار یک سوییچ مرگ داشته و با آدرس ifferfsodp9ifjaposdfjhgosurijfaewrwergwea.com ارتباط برقرار می‌کند. خوشبختانه شرکت‌های امنیتی و سیستم‌های ضدبدافزاری عرضه شده از سوی شرکت‌هایی همچون کسپرسکی و F-Secure در این زمینه به سرعت وارد عمل شده‌اند و قادر هستند گونه‌های جدید را شناسایی کنند. این سامانه‌ها قادر هستند تعدادی از نمونه‌هایی که در اینترنت مشاهده شده‌اند را به جای آن‌که از طریق آدرس اینترنتی آن‌ها شناسایی کنند، از امضایی که درون فایل بدافزاری وجود دارد، شناسایی کنند. آماری که به تازگی منتشر شده نشان می‌دهد که متاسفانه تعدادی از کاربران کشورمان نیز قربانی این باج‌افزار شده‌اند. هر چند تعداد کاربران آلوده به این باج‌افزار در مقایسه با کشورهایی همچون روسیه و انگلیس از شدت کمتری برخوردار است، اما یکبار دیگر به شما توصیه می‌کنیم سیستم‌عامل خود را به‌روز کرده و از فایل‌های مهم خود نسخه پشتیبان تهیه کنید. همچنین پروتکل SMB را سیستم‌عامل‌های ویندوزی غیر فعال کنید.

[[nid7874]]

در تصویر زیر گونه جدید را همراه سوییچ مرگ آن مشاهده می کنید.

تاریخ انتشار:

26 اردیبهشت 1396

نشانی منبع:
https://www.shabakeh-mag.com/security/7902/%DA%AF%D9%88%D9%86%D9%87%E2%80%8C%D9%87%D8%A7%DB%8C-%D8%AC%D8%AF%DB%8C%D8%AF%DB%8C-%D8%A7%D8%B2-%D8%A8%D8%A7%D8%AC%E2%80%8C%D8%A7%D9%81%D8%B2%D8%A7%D8%B1-wannacry-%D8%B4%D9%86%D8%A7%D8%B3%D8%A7%DB%8C%DB%8C-%D8%B4%D8%AF%D9%86%D8%AF