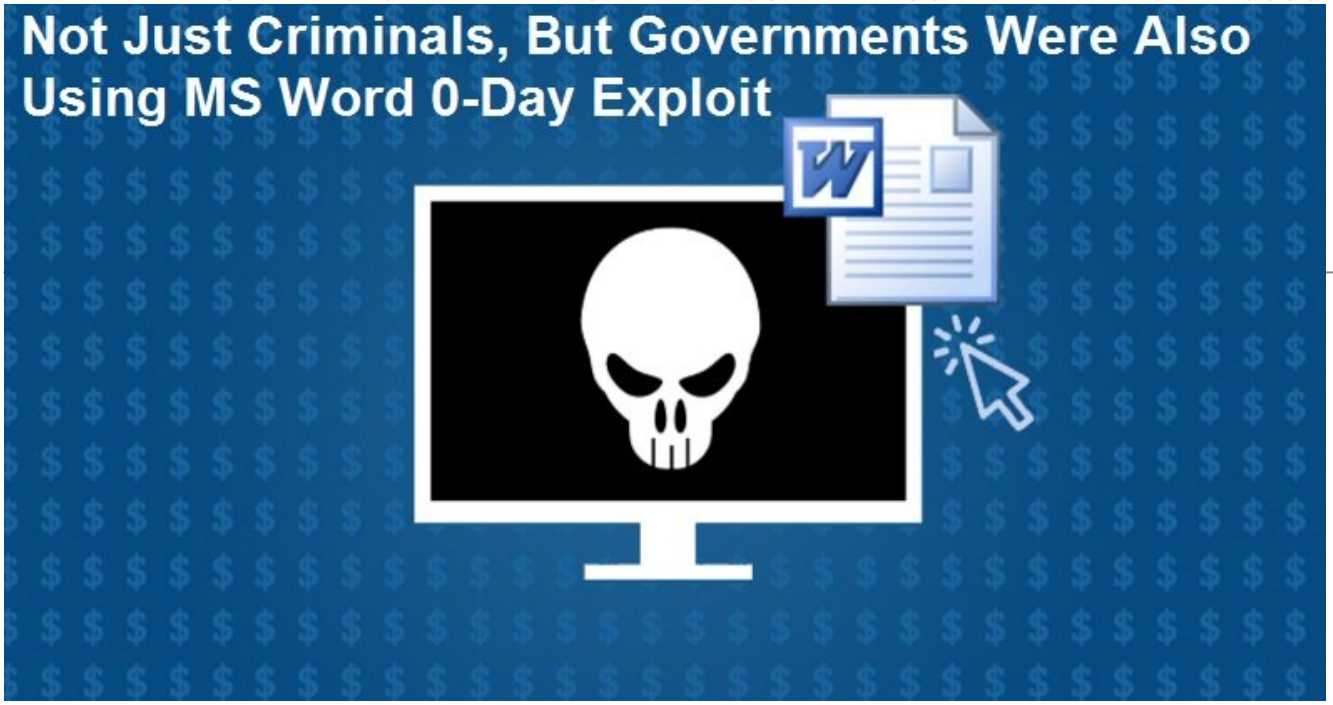
آسیب‌پذیری روز صفر دردسرساز

به‌روزرسانی حیاتی مایکروسافت ورد را دانلود کنید تا قربانی نشوید



نزدیک به یک هفته پیش خبری منتشر شد با این مضموم که هکرها موفق شده‌اند از آسیب‌پذیری روز صفر موجود در واژه‌پرداز مایکروسافت به منظور اجرای از راه دور کدها استفاده کنند. بدافزارهایی همچون Dridex و Latentboot نیز بر مبنای همین آسیب‌پذیری طراحی شده بودند.

شرکت امنیتی FireEye گزارش کرده است هکرها از ماه ژانویه تا به امروز در اختفای کامل از آسیب‌پذیری روز صفر موجود در واژه‌پرداز ورد به منظور نفوذ به سامانه‌های کاربران استفاده کرده‌اند. خبر جالب‌تری که در ارتباط با آسیب‌پذیری فوق وجود دارد، در ارتباط با خود هکرها است. هکرهایی که بدافزارهای مبتنی بر این آسیب‌پذیری را طراحی کرده‌اند، همگی تحت حمایت آژانس‌های دولتی قرار داشته‌اند. این آسیب‌پذیری به شماره CVE-2017-0199 به ثبت رسیده است. خبر مربوط به بهره‌برداری از این آسیب‌پذیری از سوی هکرهای دولتی پس از آن عمومی شد که شرکت امنیتی FireEye جزییات مربوط به آن‌را منتشر کرد. شرکتی که به طور مستقل آسیب‌پذیری موجود در نرم‌افزارها را شناسایی می‌کند، متوجه جاسوس‌افزاری به نام FinSpy شد. جاسوس‌افزاری که از ماه ژانویه تا به امروز برای انجام یکسری فعالیت‌های جاسوسی از آسیب‌پذیری موجود در واژه‌پرداز ورد آفیس سوءاستفاده می‌کرد. مایکروسافت در بولتن امنیتی که سه‌شنبه هفته گذشته منتشر کرد آسیب‌پذیری فوق را ترمیم کرد.

آسیب‌پذیری فوق به هکرها اجازه می‌داد یک برنامه مخرب HTML را دانلود کنند و این فایل HTML را در قالب یک سند مبتنی بر فرمت RTF مایکروسافت پنهان سازند. جاسوس‌افزار FinSpy که به نام FinFisher نیز معروف است با هدف نصب بدافزار Latentbot مورد استفاده قرار می‌گرفت. از این بدافزار به منظور پیاده‌سازی حملات سایبری در ارتباط با اهداف اقتصادی، به سرقت بردن داده‌ها و دستیابی به سیستم‌های کاربران استفاده می‌شد. Latentbot دارای چند ویژگی تخریبی است. این بدافزار قادر است، اعتبارنامه‌ها را سرقت کرده، آنتی‌ویروس‌ها را غیر فعال کرده، توابع راه دور را مورد استفاده قرار داده و داده‌های هارددیسک را پاک کند.

هکرها درست یک روز قبل از عرضه بولتن امنیتی مایکروسات، تغییراتی در شیوه عملکرد خود به وجود آوردند و بدافزار دیگری موسوم به Terdot را روی سیستم قربانیان نصب کردند. بدافزار فوق به محض آن‌که روی دستگاه قربانی نصب می‌شود با سرور کنترل و فرمان‌دهی ارتباط برقرار کرده و همچنین به منظور مصنون نگه داشتن خود از سامانه‌های تشخیص بدافزاری از تکنیک‌های پنهان‌سازی استفاده می‌کند. به طوری که سرور تحت کنترل هکرها غیر قابل شناسایی باشد. آن‌گونه که شرکت FireEye گزارش کرده است، جاسوس‌افزار FinSpy به شکل کاملا مهندسی شده‌ای از آسیب‌پذیری روز صفر واژه‌پرداز ورد برای آلوده ساختن هدف‌های خاص استفاده می‌کند.

تحلیل‌های انجام شده از سوی این شرکت نشان می‌دهد یک کارشناس امنیتی برای اولین بار موفق شده بود این آسیب‌پذیری را شناسایی کرده و آن‌را در ازای مبلغ قابل توجهی به آژانس‌های دولتی بفروشد. جالب آن‌که عصر روز دوشنبه، کارشناسان امنیتی شرکت ProofPoint موفق شدند یک کمپین ارسال هرزنامه‌ای را شناسایی کنند. کمپینی که به طور مستقیم میلیون‌ها کاربر شاغل در موسسات مالی کشور استرالیا را هدف قرار داده بود. هکرها از طریق

آسیب‌پذیری روزصفر واژه‌پرداز ورد موفق شده بودند تروجان بانکی Dridex را برای این کاربران ارسال کنند.

کارشناسان شرکت FireEye اعلام کرده‌اند به درستی مشخص نیست بدافزار Dridex چگونه طراحی شده است اما به نظر می‌رسد گزارشی که یک هفته قبل شرکت مک‌آفی منتشر کرد و جزییاتی را در رابطه با این آسیب‌پذیری ارائه کرد به هکرها کمک کرده است تا بدافزار فوق را طراحی کنند. همچنین این احتمال وجود دارد تا فردی که آسیب‌پذیری را کشف کرده آن‌را در اختیار هکرها قرار داده باشد.

مایکروسافت هفته گذشته وصله مربوط به ترمیم این آسیب‌پذیری را عرضه کرد. با توجه به آن‌که آسیب‌پذیری فوق با درجه بحرانی گزارش شده است به کاربران توصیه می‌کنیم در اولین فرصت ممکن وصله‌های جدید مایکروسافت را دانلود کنند تا از گزند حملات هکری به دور باشند.

تاریخ انتشار:

28 فروردین 1396

نشانی منبع: https://www.shabakeh-mag.com/security/7525