بهره‌برداری از یک آسیب‌پذیری وصله شده

یک فایل پاورپوینت به این شکل کامپیوتر شما را آلوده می‌کند

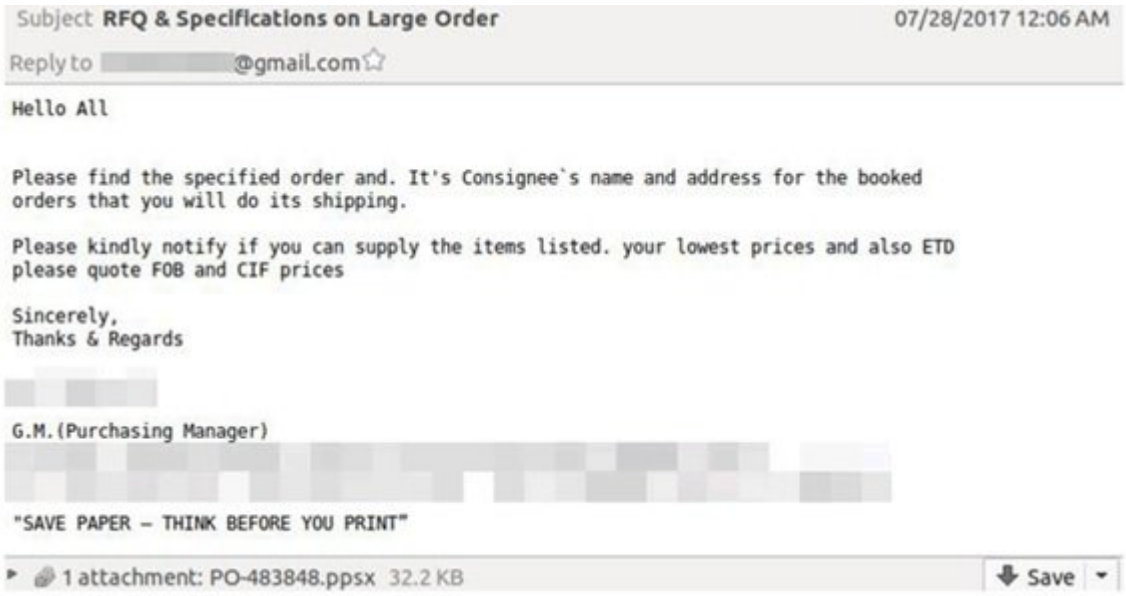
اگر به یاد داشته باشید چند ماه قبل به شما گفتیم، چگونه باز کردن یک فایل ورد به واسطه یک آسیب‌پذیری در بسته آفیس قادر است کامپیوتر شما را آلوده کند. آسیب‌پذیری فوق که در رابط‌های OLE قرار داشت به هکرها اجازه می‌داد از راه دور کدهای مخرب را روی سامانه قربانیان اجرا کنند. مایکروسافت در اردیبهشت ماه این آسیب‌پذیری را وصله کرد. اما هکرها با کنکاش در بسته آفیس موفق به شناسایی بخش‌های دیگری شدند که به آن‌ها اجازه می‌دهد از این آسیب‌پذیری استفاده کنند.

به تازگی کمپین بدافزاری جدیدی از سوی کارشناسان امنیتی شناسایی شده که از آسیب‌پذیری فوق استفاده می‌کند. اما برای اولین بار بدافزار فوق در پس زمینه فایل‌های پاورپوینت پنهان شده و از طریق ضمیمه‌های آلوده ایمیلی و در قالب فیشینگ کاربران را هدف قرار داده است.

مطلب پیشنهادی

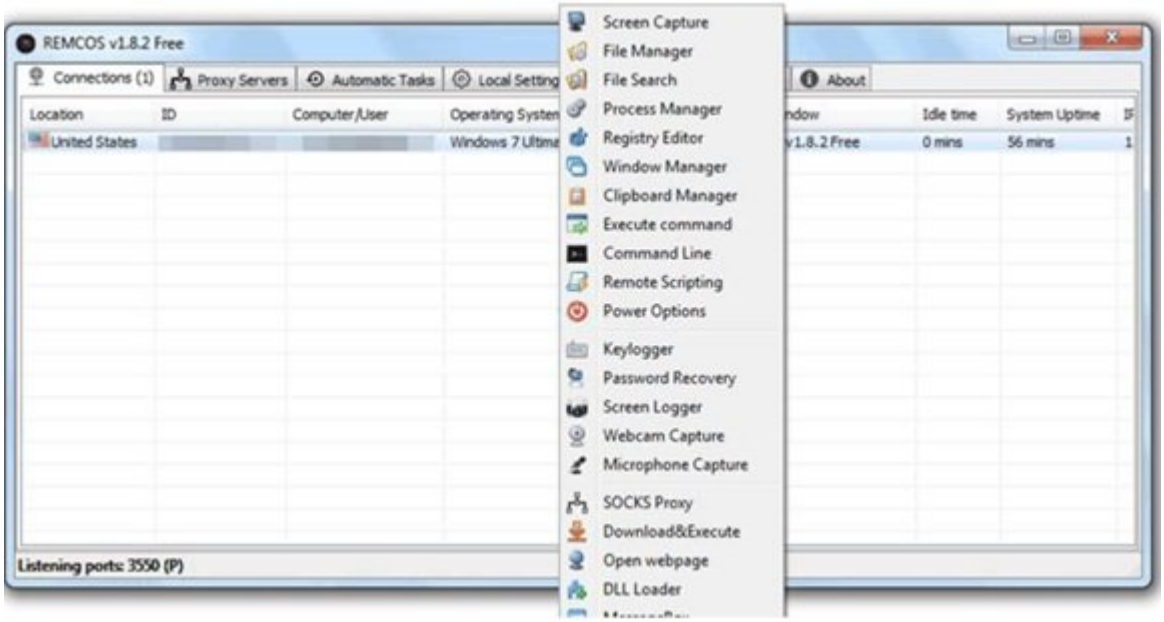
تنها نیم ساعت زمان برای شکستن قفل‌ها
قفل‌های الکترونیکی تا چه اندازه در برابر نفوذ ایمن هستند

بر اساس گزارش منتشر شده از سوی کارشناسان شرکت ترندمیکرو، کمپین بدافزاری شناسایی شده از طریق یک ارائه‌دهنده سرویس‌های کابلی توزیع شده و سعی می‌کند با یک پیغام ایمیلی قانع کننده مخاطب خود را مجاب کند که ایمیل را باز کند. ترندمیکرو گفته است که این کمپین عمدتا صنایع فعال در حوزه الکترونیک را هدف قرار داده است.



حمله فوق چگونه به مرحله اجرا در می‌آید؟

این حمله در چند مرحله انجام می‌شود. در مرحله اول یک ایمیل فیشینگ همراه با ضمیمه آلوده پاورپوینت ارسال می‌شود. در متن ایمیل ارسالی نوشته شده است اطلاعات مهمی در ارتباط با سفارش‌های مشتری باید در اختیار قربانی قرار گیرد. در مرحله دوم هنگامی که فایل باز شد، پاورپوینت یک فایل XML را فراخوانی می‌کند. فایل فوق به گونه‌ای ساخته شده که از راه دور فایلی به نام logo.doc را دانلود کرده و در ادامه از طریق ویژگی پویانمایی "نمایش پاورپوینت" این فایل را اجرا می‌کند.



در مرحله سوم فایل مخرب Logo.doc از آسیب‌پذیری CVE-2017-0199 استفاده می‌کند. این آسیب‌پذیری به هکرها اجازه می‌دهد فایل مخرب RATMAN.exe را روی سیستم قربانی نصب کند. در مرحله چهارم RATMAN.exe که نسخه آلوده شده‌ای از ابزار Remcos Remote Control است روی سیستم قربانیان نصب می‌شود. ابزار فوق به هکرها اجازه می‌دهد از راه دور سیستم‌های آلوده قربانیان را از طریق سرور کنترل و فرمان‌دهی تحت کنترل و نظارت قرار دهند. ابزار Remcos یک ابزار قانونی است که برای دسترسی از راه دور به سامانه‌های کامپیوتری و کنترل سامانه‌ها مورد استفاده قرار می‌گیرد. اما هکرها می‌توانند از ابزار فوق به منظور دانلود و اجرای دستورات، نصب روباینده کلیدها، تهیه اسکرین‌شات و ضبط ویدیو از میکروفون و وب‌کم استفاده کنند. بهره‌برداری از فایل‌های پاورپوینت به هکرها اجازه می‌دهد از سد مکانیزم امنیتی تشخیص بدافزار عبور کنند. برای پیشگیری از آلوده شدن به

این بدافزار باید جدیدترین وصله‌های مایکروسافت را روی سامانه خود نصب کنید.

تاریخ انتشار:
27 مرداد 1396

نشانی منبع:
https://www.shabakeh-mag.com/security/9202/%DB%8C%DA%A9-%D9%81%D8%A7%DB%8C%D9%84-%D9%BE%D8%A7%D9%88%D8%B1%D9%BE%D9%88%DB%8C%D9%86%D8%AA-%D8%A8%D9%87-%D8%A7%DB%8C%D9%86-%D8%B4%DA%A9%D9%84-%DA%A9%D8%A7%D9%85%D9%BE%DB%8C%D9%88%D8%AA%D8%B1-%D8%B4%D9%85%D8%A7-%D8%B1%D8%A7-%D8%A2%D9%84%D9%88%D8%AF%D9%87-%D9%85%DB%8C%E2%80%8C%DA%A9%D9%86%D8%AF