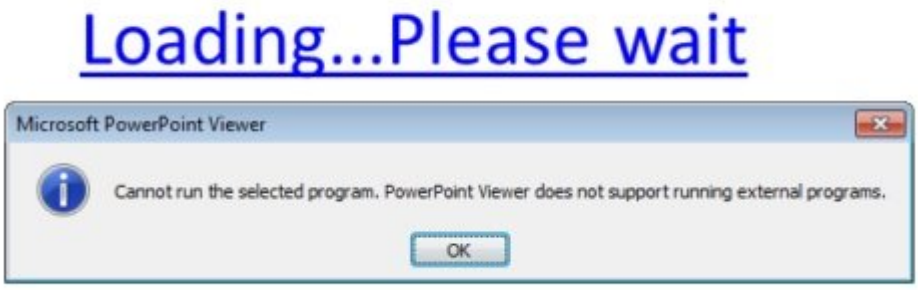
نفوذ از طریق پاورپوینت

بدون کلیک و فقط با بردن ماوس روی لینک به بدافزار آلوده می‌شوید!

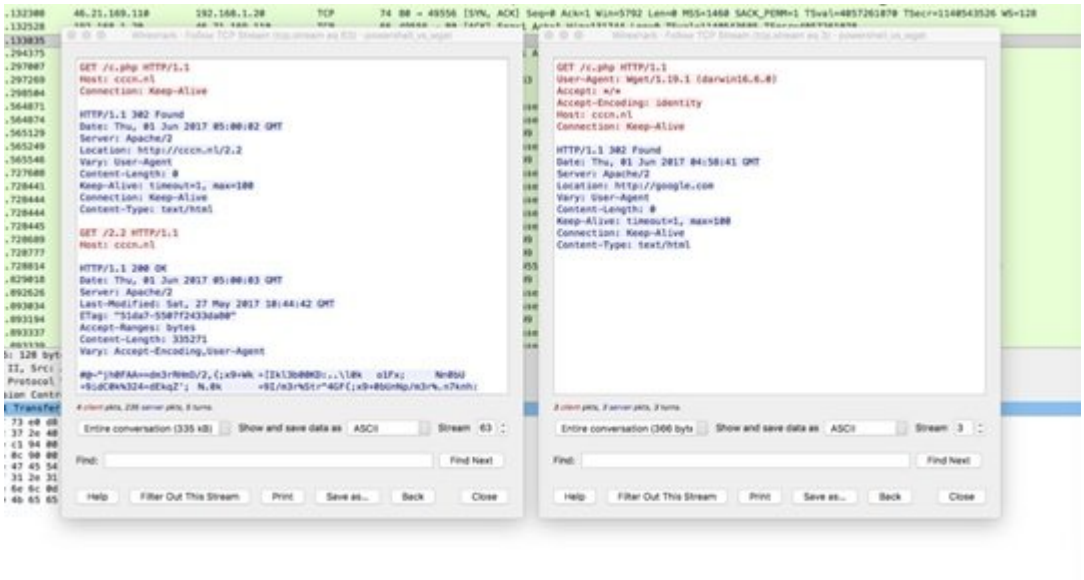
آزمایشگاه امنیتی SentinelOne Labs به تازگی موفق به شناسایی تکنیکی شده است که هکرها برای ارسال بدافزارها از آن استفاده می‌کنند. در این تکنیک هکرها از طریق فایل‌های پاورپوینت و به دام انداختن کلیک‌های ماوس روی یک شی برای اجرای کدهای مخرب دلخواه خود روی سامانه‌های قربانیان استفاده کرده و در ادامه ماشین قربانی را مجبور می‌سازند تا بدافزارهای موردنظر آن‌ها را دانلود کند.

به‌کارگیری اسناد و فایل‌های آفیس به منظور توزیع بدافزارها سابقه‌ای بس طولانی دارد. در گذشته هکرها به وفور از از فایل‌های ورد و ماکروهای مخرب به منظور گسترش بدافزارها استفاده می‌کردند. تکنیکی که عمدتا بر پایه روش‌های مهندسی اجتماعی کار می‌کند و قربانی را اغوا می‌کرد تا روی ماکروهای مخربی که درون یک سند قرار گرفته است کلیک کند. اما پژوهشگران آزمایشگاه فوق به تازگی کمپین‌هایی را مورد ارزیابی قرار داده‌اند که در آن‌ها از فایل‌های پاورپوینت و رخدادهای مرتبط با کلیک ماوس روی اشیا به منظور اجرای کدهای پاوشل استفاده می‌کند.



این فایل‌ها با اسامی همچون order.ppsx و invoice.ppsx نام‌گذاری شده و به شکل هرزنامه‌هایی با عنوان‌های رسید خرید یا تاییدیه برای قربانیان ارسال می‌شود. پژوهشگران امنیتی با بررسی فایل‌های پاورپوینت اطلاع پیدا کرده‌اند هنگامی که فایلی باز می‌شود پیغامی مبنی بر در «حال بارگذاری ... است، لطفا صبر کنید» در قالب یک لینک به کاربر نشان داده می‌شود. اگر کاربر نشانه‌گر ماوس خود را روی لینک ببرد و حتا روی لینک کلیک هم نکند کدهای پاورشل اجرا خواهد شد. مایکروسافت ویژگی امنیتی ویژه‌ای به نام مشاهده محافظت شده را برای همه

اسناد ،فیس فعال کرده است. ویژگی فوق که در حالت پیش فرض فعال است به کاربر هشدارهای امنیتی مختلفی را نشان می‌دهد. این هشدارها به ویژه زمانی که فایلی از بستر اینترنت دریافت شود نشان داده می‌شود.



اگر کاربر روی دکمه فعال کردن و ویرایش یک سند کلیک کند، کدهای مخرب به‌طور خودکار اجرا می‌شوند و به دامنه‌ای با آدرس cccn.nl متصل می‌شوند. در ادامه یک فایل از این دامنه دانلود شده و روی سامانه قربانی اجرا می‌شود. این فایل بدافزاری خواهد بود که سیستم کاربر را آلوده خواهد ساخت. پژوهشگران با بررسی دقیق این حملات اطلاع پیدا کرده‌اند که در این کمپین هکری سیستم‌های قربانیان به نسخه‌های پیشرفته‌تر و جدیدتری از بدافزارهای بانکی Tinba، Zusy و Tiny Banker آلوده می‌شوند. کارشناسان امنیتی اعلام کرده‌اند که اگر کاربر یک سند پاورپوینت را در حالت مرورگر پاورپوینت مشاهده کند، این حمله با شکست روبرو خواهد شد.

مطلب پیشنهادی

رخنه‌ای که گوگل آن‌را امنیتی نمی‌داند
آسیب‌پذیری جدید کروم اجازه ضبط مخفیانه ویدیوها و صداها را فراهم می‌کند

به واسطه آن‌که اکثر نسخه‌های آفیس این توانایی را دارند تا پیش از وقوع حمله به کاربر هشدار دهند. با این وجود این بردار حمله در بعضی مواقع قادر است به شکل کاملی اجرا شود. این گروه از پژوهشگران در پست خود نوشته‌اند: «کاربران به واسطه کنجکاوی، عجله یا کم صبر بودن ممکن است برنامه‌های خارجی را فعال کرده و تنها به مسدود کردن ماکروها در اسناد آفیس بسنده کرده باشند. همچنین در بعضی موارد مشاهده شده است که ماشین قربانی به گونه‌ای پیکربندی شده که هم اجازه اجرای برنامه‌های خارجی را می‌دهد و هم به ماکروها اجازه می‌دهد تا اجرا شوند. این دقیقا همان چیزی است که هکرها به دنبال آن هستند.»

تاریخ انتشار:

21 خرداد 1396

نشانی منبع:
https://www.shabakeh-mag.com/security/8151/%D8%A8%D8%AF%D9%88%D9%86-%DA%A9%D9%84%DB%8C%DA%A9-%D9%88-%D9%81%D9%82%D8%B7-%D8%A8%D8%A7-%D8%A8%D8%B1%D8%AF%D9%86-%D9%85%D8%A7%D9%88%D8%B3-%D8%B1%D9%88%DB%8C-%D9%84%DB%8C%D9%86%DA%A9-%D8%A8%D9%87-%D8%A8%D8%AF%D8%A7%D9%81%D8%B2%D8%A7%D8%B1-%D8%A2%D9%84%D9%88%D8%AF%D9%87-%D9%85%DB%8C%E2%80%8C%D8%B4%D9%88%DB%8C%D8%AF