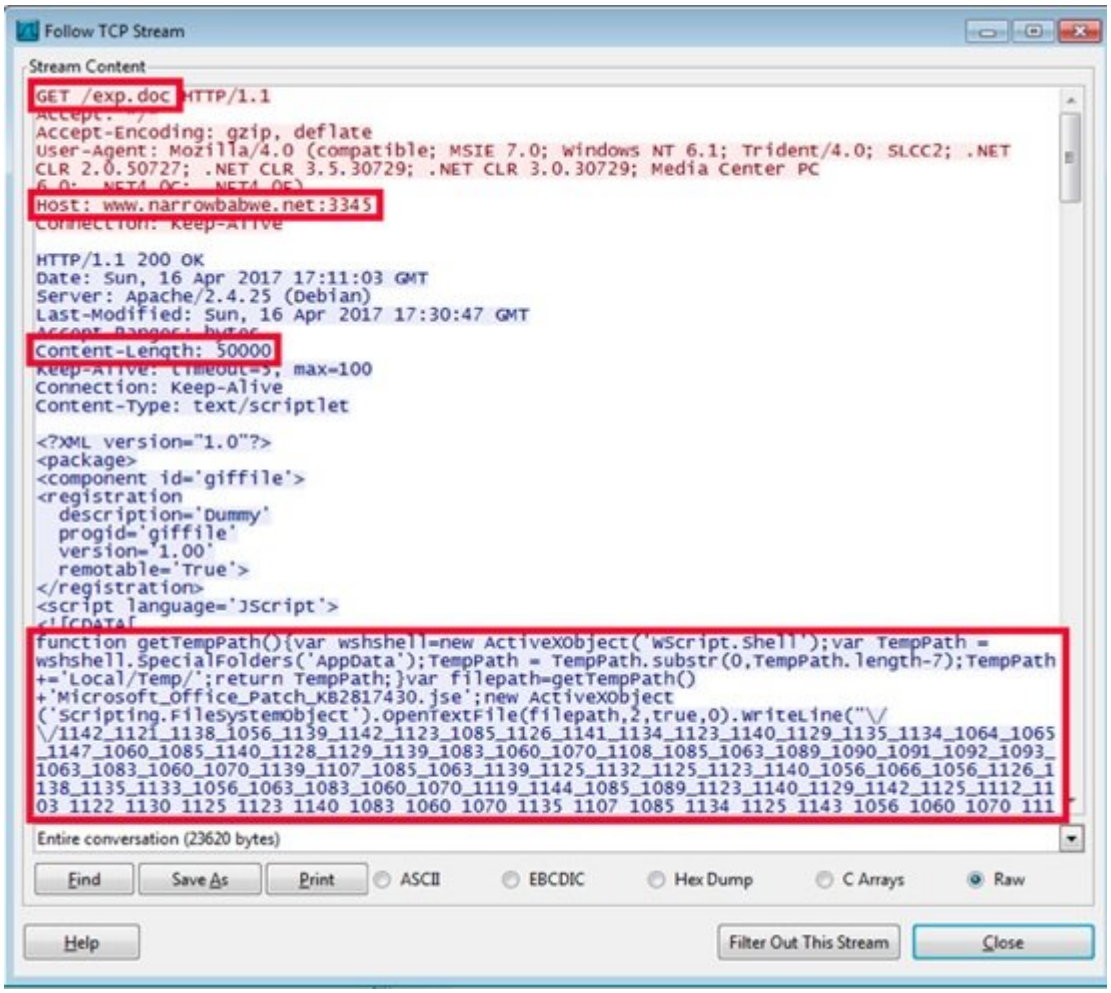
توزیع بدافزار از طریق پاورپوینت

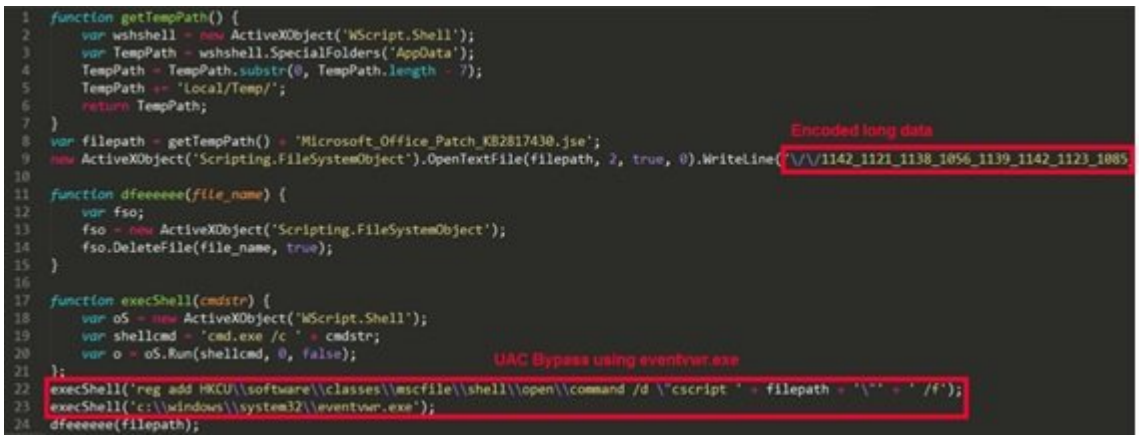
هکرها از فایل‌های پاورپوینت برای انجام فعالیت‌های مجرمانه استفاده می‌کنند

پژوهشگران امنیتی گزارش کرده‌اند به تازگی کمپین هکری جدیدی را شناسایی کرده‌اند که از طریق فایل‌های آلوده پاورپوینت و با اتکا بر آسیب‌پذیری وصله شده از سوی مایکروسافت برای حمله به مراکز مهمی همچون سازمان ملل، وزارت امور خارجه و سازمان‌های بزرگ بین‌المللی استفاده کرده‌اند.

در این سری از حملات فایل آلوده ADVANCED DIPLOMATIC PROTOCOL AND ETIQUETTE SUMMIT.ppsx همراه با آسیب‌پذیری شناسایی شده پاورپوینت به شماره CVE-2017-0199 استفاده شده است. مایکروسافت آسیب‌پذیری فوق را در ماه آوریل ترمیم کرد، اما این دومین باری است که هکرها از آسیب‌پذیری فوق بهره‌برداری کرده‌اند. تقریبا یک ماه پیش بود که هکرها موفق شدند بدافزارهای Latentbot، WingBrid، Dridex و Godzilla را بر اساس آسیب‌پذیری فوق توزیع کنند.



آسیب‌پذیری فوق به هکرها اجازه می‌داد به راحتی سامانه‌های کامپیوتری کاربران را آلوده کنند. در آن حمله زمانی که قربانی یک فایل پاورپوینت را در وضعیت نمایش اسلاید باز می‌کرد همزمان با این کار یک اسکریپت روی سامانه او اجرا می‌شد.

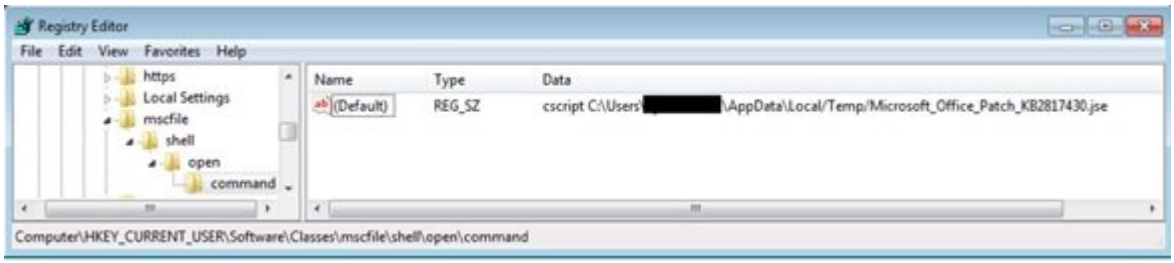


این اسکریپت به منظور دانلود از راه دور کدهای مخرب از درون یک فایل XML مورد استفاده قرار می‌گرفت. کدهایی که از سایت narrowbabwe.net دانلود می‌شدند. پس از انجام اینکار زمانی که کاربر وضعیت نمایش اسلاید را در پاورپوینت اجرا می‌کرد، کدهای مخرب نیز اجرا می‌شدند.

مطلب پیشنهادی

بهره‌برداری از یک آسیب‌پذیری وصله شده
یک فایل پاورپوینت به این شکل کامپیوتر شما را آلوده می‌کند

اکسپلویت فوق به هکرها اجازه می‌دهد به رجیستری ویندوز نفوذ کرده و به راحتی از سد ویژگی کنترل حساب کاربری عبور کرده و فایل eventvwr.exe را اجرا کنند. در حالی که آسیب‌پذیری گذر از مکانیزم امنیتی سال گذشته میلادی شناسایی شد اما هکرها هنوز هم می‌توانند از آن استفاده کنند. کدهای جاوااسکریپتی که درون فایل XML قرار دارند، این توانایی را دارند تا فایلی را به پوشه آفیس وارد کرده و به بسته آفیس نشان دهند فای لفوق وصله‌ای ارائه شده از سوی مایکروسافت هستند.

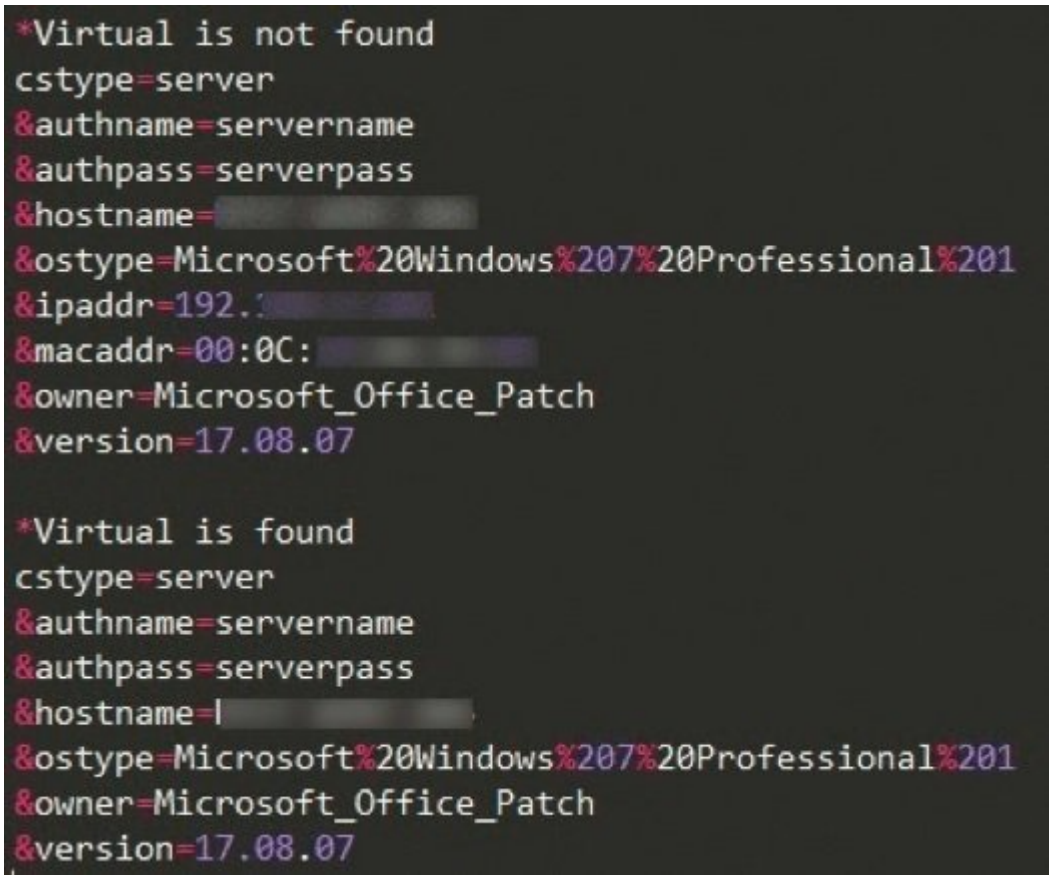


جالب‌تر آن‌که اسکریپت فوق به اندازه‌ای هوشمند است که می‌تواند تشخیص دهد درون یک ماشین مجازی یا روی یک ماشین واقعی اجرا شده است.

مطلب پیشنهادی

نفوذ از طریق پاورپوینت
بدون کلیک و فقط با بردن ماوس روی لینک به بدافزار آلوده می‌شوید!

اگر تشخیص دهد که درون یک ماشین مجازی اجرا نشده است، در ادامه داده‌هایی را برای سرور راه دور ارسال می‌کند. دستوراتی که از سوی سرور برای بدافزار ارسال می‌شوند برای انجام کارهای مختلفی مورد استفاده قرار می‌گیرند. دستوراتی که همگی آن‌ها از طریق تابع eval() اجرا می‌شوند. زمانی که دستورات با موفقیت اجرا شوند بدافزار پیغام موفقیت‌آمیز بودن را برای سرور ارسال می‌کند. اوایل ماه جاری میلادی نیز پژوهشگران امنیتی شرکت سیسکو اعلام داشتند هکرها از طریق بهره‌برداری‌های موجود در بسته آفیس به منظور گذر از مکانیزم‌های امنیتی و همچنین افزایش نرخ تحویل بدافزارها استفاده می‌کنند.



این گروه از کارشناسان موفق به شناسایی کدهایی درون بدافزارها شدند که نشان می‌داد بدافزارها از راهکارهای جدیدی برای گذر از مکانیزم‌های تشخیصی و همچنین ارتقا امتیازهای خود استفاده کرده‌اند. در حال حاضر هکرها از راهکارهای اسکریپت‌های چندگانه جایگذاری شده در کدها، اتصال چندگانه به آدرس‌های اینترنتی، جایگذاری آدرس‌های اینترنتی مربوط به سرورهای کنترل و فرمان‌دهی درون فایل‌های Jpeg استفاده می‌کنند.

==========

تاریخ انتشار:
23 شهریور 1396

نشانی منبع:
https://www.shabakeh-mag.com/news/world/9583/%D9%87%DA%A9%D8%B1%D9%87%D8%A7-%D8%A7%D8%B2-%D9%81%D8%A7%DB%8C%D9%84%E2%80%8C%D9%87%D8%A7%DB%8C-%D9%BE%D8%A7%D9%88%D8%B1%D9%BE%D9%88%DB%8C%D9%86%D8%AA-%D8%A8%D8%B1%D8%A7%DB%8C-%D8%A7%D9%86%D8%AC%D8%A7%D9%85-%D9%81%D8%B9%D8%A7%D9%84%DB%8C%D8%AA%E2%80%8C%D9%87%D8%A7%DB%8C-%D9%85%D8%AC%D8%B1%D9%85%D8%A7%D9%86%D9%87-%D8%A7%D8%B3%D8%AA%D9%81%D8%A7%D8%AF%D9%87-%D9%85%DB%8C%E2%80%8C%DA%A9%D9%86%D9%86%D8%AF