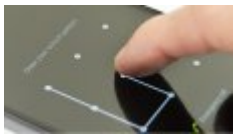
یک کی‌لاگر قدرتمند
بدافزاری که در ایمیل‌های بانکی جعلی پنهان می‌شود

کارشناسان امنیتی به تازگی گونه جدیدی از بدافزارها را شناسایی کرده‌اند که مشتریان بانک‌ها را هدف قرار داده است. تحلیل‌های اولیه نشان می‌دهند که بدافزار خود به منظور سرقت داده‌های کاربری همچون گذرواژه‌ها، بیت‌کوین‌ها و همچنین کیف پول ارز مجازی این گروه از کاربران طراحی شده است.

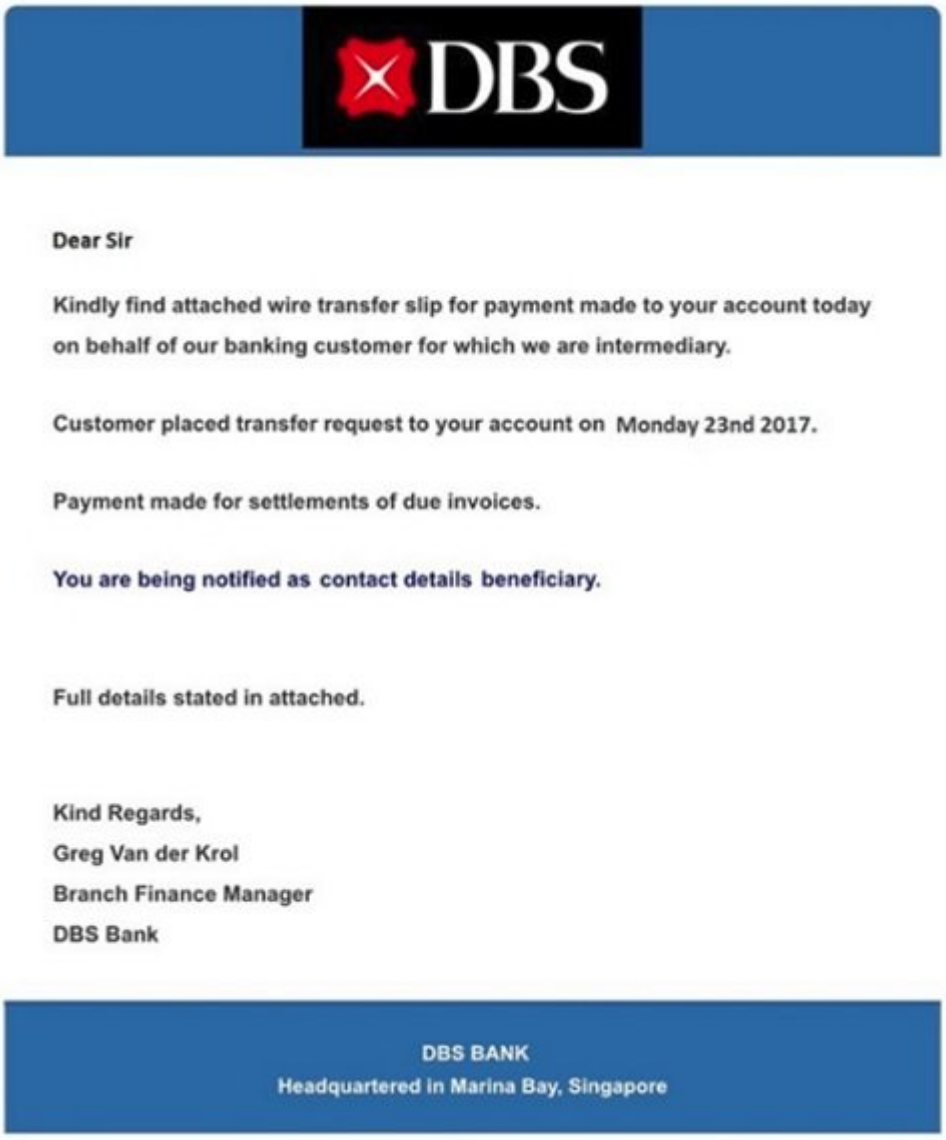
بدافزار فوق از سوی شرکت امنیتی Cyren شناسایی شده است. این شرکت اعلام کرده است که بدافزار فوق با سرعت بسیار بالایی در حال گسترش است. این بدافزار عملکردی همانند یک کی‌لاگر داشته و با استفاده از ضمیمه‌های ایمیلی برای کاربران ارسال می‌شود. ایمیل‌ها به گونه‌ای طراحی شده‌اند تا کاربر تصور کند ایمیل‌ها از طریق یک برنامه نقل و انتقالات بانکی برای او ارسال شده است.

مطلب پیشنهادی

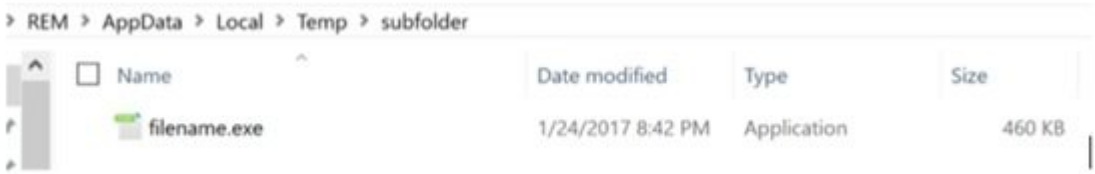


بینایی ماشینی در خدمت هکرها
قفل الگویی اندروید تنها پس از 5 مرتبه تلاش شکسته می‌شود

تحلیل‌های انجام گرفته از سوی Cyren نشان می‌دهد که ایمیل‌های فوق از سوی بات‌هایی در کشورهای امریکا و سنگاپور ارسال شده و این‌گونه وانمود می‌کنند که از سوی یکسری بانک‌ها همچون Emirates ارسال شده‌اند. به طور معمول، در بخش عنوان ایمیل‌ها کاربر عبارت "اطلاع‌رسانی در ارتباط با پرداخت‌های آنلاین" (wire transfer payment notification) را مشاهده می‌کند. جالب‌تر آن‌که ضمیمه‌های ارسال شده برای کاربر همراه با کدهای سوئیفت هستند. این کدهای سوئیفت (swift copy.zip، swift copy_pdf.ace و swift_copy.pdf.gz) به منظور مشخص کردن نوع بانک و موسسات مالی و همچنین برای نقل و انتقال جعلی مورد استفاده قرار می‌گیرند. این کدها سعی می‌کنند کاربر را متقاعد سازند که ایمیل ارسال شده واقعی است.



طراحی ضمیمه‌های آلوده بسیار هوشمندانه بوده است. در حالی که در ظاهر چنین به نظر می‌رسد که این فایل‌ها pdf هستند، با این وجود آن‌ها فایل‌های اجرایی هستند. Cyren می‌گوید: «به محض آن‌که این فایل اجرا می‌شود خود را پاک کرده و فایل جدیدی به نام filename.vbs را در پوشه startup ویندوز ایجاد کرده و اجرا می‌کند. هر زمان که یک سامانه کامپیوتری راه‌اندازی می‌شود این اسکریپت اجرا شده و بدافزار filename.exe که در مسیر AppData\Local\Temp\subfolder قرار دارد را اجرا می‌کند.»



این بدافزار سعی می‌کند گذرواژه‌ها و اطلاعات حساس کاربران را جمع‌آوری کند. تمرکز این بدافزار روی پروتکل ftp و مرورگرهای وب است. هر دو موردی که به آن‌ها اشاره گردید، طیف گسترده‌ای از اطلاعات ارزشمند همچون گواهی‌نامه‌های ایمیلی را در خود جای داده‌اند. این بدافزار قادر است از گذرواژه‌ها و نام‌های کاربری گرفته تا تاریخچه بازدیدها، کوکی‌ها و هر آن نوع داده‌ای که ارزشمند است را جمع‌آوری کند. اگر روی سیستم قربانی کیف پولی در ارتباط با ارزمجازی رمزنگاری شده وجود داشته باشد، بدافزار به سراغ این کیف پول نیز خواهد رفت. بدتر

آن‌که این بدافزار قادر است طیف بسیار گسترده و متنوعی از ارزهای مجازی را به سرقت ببرد. بیت‌کوین، لایت‌کوین، نیم‌کوین و.... از جمله این ارزهای مجازی هستند. بدافزار فوق در واقع یک رباینده کلیدها است. در نتیجه کاربر هر آن چیزی که روی صفحه کلید فشار می‌دهد یا با ماوس روی هر نقطه از صفحه‌نمایش کلیک می‌کند را ضبط کرده و تمامی این اطلاعات را ضبط می‌کند.

همانند گذشته یکبار دیگر به شما پیشنهاد می‌کنیم در زمان دریافت ایمیل‌ها و یا نقل و انتقال وجوه نقد بیش از پیش دقت کنید. زمانی که ایمیل‌هایی با عنوان مالی دریافت می‌کنید را به دقت مورد بررسی قرار داده و پیش از آن‌که روی آن‌ها کلیک کنید از آلوده نبودن آن‌ها اطمینان حاصل کنید.

تاریخ انتشار:

14 بهمن 1395

نشانی منبع: https://www.shabakeh-mag.com/security/6624