شرکت های مالی فیلیپین
قربانی حملات هدفمند پیشرفته

بررسی اجمالی

آزمایشگاه های تحقیقاتی تهدیدات کوییک هیل در طی چند روز گذشته چندین حملات هدفمند علیه شرکت‌های خصوصی و مؤسسات مالی فیلیپین مشاهده کرده اند. این حملات از طریق ایمیل های اسپم که شامل فایل پیوستی که در درون آنها فایل های اجرایی مخرب وجود دارد گسترش یافته است.

نکته قابل توجه در مورد این حملات، این است که پس از آن که اجزاءِ سازنده توسط قربانیان اجرا شود، محموله‌های مخرب به طور هوشمندانه از شناسایی جلوگیری می‌کنند. آنها مطمئن می‌شوند که سیستم آنالیز خودکار محصولات امنیت شبکه فعال نیست. این شناسایی ها تایید می‌کند که علاقه بدافزار نویس ها استفاده از Anti-VM پیشرفته (ماشین مجازی) و ترفندهای Anti-Sandbox برای دور زدن آنالیز خودکار نرم افزار های امنیتی می‌باشد.

علاوه بر این، این محموله ها به طور خاص برای نظارت بر کاربران برای تصرف کلیدنگارها، عکس گرفتن از صفحه نمایش و برای سرقت اطلاعات ورودی اعتبارنامه ساخته شده است.

قابلیت های این حمله

مکانیزم این حمله هدفمند کاملاً مشابه روش مورد استفاده توسط APT های قبلاً دیده شده (تهدیدات مداوم پیشرفته) می باشد. هنگامی که تمام اجزا رمزگشایی و بر روی دستگاه قربانی دانلود شدند، مهاجم از راه دور به طور کامل به دستگاه دسترسی دارد و قادر به انجام فعالیت های مخرب زیر است:

- سرقت اطلاعات کاربری برنامه Outlook و حساب های Live Mail
- انجام فعالیت های کلیدنگار (keylogging)
- عکس گرفتن از صفحه نمایش

- نسخه برداری از اطلاعات کلیپ بورد
- دانلود و اجرای دیگر اجزای مخرب

آنالیز پیوست های مخرب

فایل پیوست مخرب که کشف شده است، حاوی فایل اجرایی به نام "**fraudulent trns.exe**" می‌باشد. این نام کاربران کنجکاو را ترغیب می‌کند تا بر روی فایل کلیک کنند و بار مفید بیشتری در سیستم گسترش یابد. فایل اطلاعات سرآیند در دسترس نشان می‌دهد که فایل در دوم اگوست، سال ۲۰۱۵ ایجاد شده است. پس از این که محموله وارد سیستم شد، با سرور خارجی C&C (Command & Control) ارتباط برقرار می‌کند و اطلاعات محرمانه را از دستگاه آلوده به اشتراک می‌گذارد.

اطلاعات سرور از راه دور C&C

پس از آنالیز جزئیات سرور C&C، مشاهدات زیر در مورد این حمله صورت گرفته است:

• پنل سرور C&C با نام "KeyBase Web Panel" فعال است

• این پنل روی "**elley080.com**" میزبان شده است

• آدرس IP، 85.159.237.152 است و ۶۰ سایت دیگر در آدرس IP میزبان هستند

• به نظر می‌رسد نام ثبت شده "Jocelyn Santosd" از مبدا فیلیپین باشد

• محل IP در Roosendaal، منطقه North-Brabant، هلند واقع شده است

نتیجه گیری

این حمله به طور خاص سازمان های مالی و دیگر مؤسسات فیلیپین را هدف قرار داده است. آنالیز این حمله ی هدفمند بیشتر نشان دهنده این است که چگونه این تهدید پیشرفته با Anti-VM، ضد شبیه سازی و مکانیزم های Anti-Sandbox برای جلوگیری از آنالیز خودکار مسلح شده است. تاریخ ایجاد فایل کمی بیش از ۱۰ روز قدمت دارد، که نشان می‌دهد که این یک حمله جدید است و هنوز هم در حال پیشرفت است.