**Emmental کلاهبردار خطرناک حساب های بانکی اینترنتی**

تا کنون یکی از امن ترین سیستم های تأیید هویت، سیستم تأیید هویت دو مرحله ای بوده است، اما هم اکنون گزارش شده است که یکی از خطرناک ترین و پیچیده ترین ویروس ها و حملات سایبری شناسایی شده که قادر است این سیستم تایید هویت را دور بزند. این حمله سایبری خطرناک Emmental نام دارد.

این حملات با هدف سیستم های بانکداری به ویژه برای کشورهای سوئیس، سوئد، اتریش و ژاپن طراحی شده است. این حمله با ارسال یک بدافزار برای کاربران بانک ها اقدام به ربودن حساب کاربری آنها نموده و نهایتاً برای دور زدن سیستم های احراز هویت دو عاملی، آن ها را ترغیب به نصب یک برنامه بر روی گوشی های تلفن همراه می نماید.

در این حمله ابتدا یک ایمیل جعلی با عناوینی نظیر : "صورت حساب از طرف یک شرکت معتبر " برای کاربران ارسال می شود که حاوی یک فایل ضمیمه ای با پسوند RTF است. در این فایل، یک فایل اجرایی دیگر وجود دارد که در صورت اجرای آن یک گواهی ssl جعلی ساخته می شود و کاربر را به سمت یک سایت جعلی که از پیش طراحی شده است، هدایت می کند. پس از آن هنگامی که کاربر نام کاربری و کلمه عبور خود را برای ورود به اینترنت بانک وارد می کند، به راحتی اطلاعات احراز هویت خود را در اختیار مهاجمین قرار می دهد.

بر طبق گزارشات شرکت امنیتی trend micro حملات Emmental بد افزار اندرویدی از احراز هویت دو عاملی گذشته و کد مخربی را اجرا می کند که تنظیمات DNS کامپیوتر را تغییر می دهد سپس آن نقاط توسط مهاجم اداره خواهد شد. خرابکاران اقدام خود را با ارسال بد افزار از طریق حملات فیشینگ لینک های آلوده یا فایل ضمیمه شده از طرف فروشندگان محصولات مختلف شروع می کنند. این بد افزار تنظیمات روی سیستم را تغییر می دهد و سپس خودش را حذف می کند.

جالب اینکه این بد افزار حتی ssl certificate جعلی را روی سیستم ها نصب می کند که باعث می شود سرورهای HTTPS آلوده به صورت پیش فرض امن و مطمئن جلوه کنند و کاربران هیچ هشدار امنیتی را دریافت نکنند و متوجه حضور آن ها نشوند.

کار دیگر Emmental این است که تولید رمز session انجام دهد. در واقع پیامک هایی را از بانک رهگیری کرده و به سمت سرور کنترل و فرمان که همان c&c است، به شماره موبایل دیگری ارسال می کند و با این کار مهاجم نه تنها نام کاربری و رمز عبور بانکی را بدست می آورد، بلکه رمز های session بانکی آنلاین را نیز می دزدد. به این ترتیب کنترل کاملی روی حساب های کاربری قربانی بدست می آورند.

منبع:

http://www.cyberpolice.ir

[ایران هشدار](http://www.iranhoshdar.ir)