بانک سینا
معاونت فناوری اطلاعات و شبکه ارتباطات
مدیریت امنیت و توسعه سیستم‌ها
اداره امنیت فناوری اطلاعات – دایره ممیزی امنیت

هشدار در خصوص حمله Emmental

شهریور ماه ۱۳۹۳

Emmental نام نوعی پنیر سوئیسی است که از سال ۲۰۱۳ تاکنون، برای کاربران سیستم‌های بانکداری الکترونیک این کشور، مفهوم دیگری با عنوان «حمله برای ربودن حساب‌های کاربری اینترنتی» پیدا کرده است.

پیرو گزارشات اخیر، حملات موسوم به Operation Emmental، با هدف سیستم‌های بانکداری به ویژه برای کشورهای سوئیس، سوئد، اتریش و ژاپن، طراحی شده است و با ارسال یک بدافزار برای کاربران بانک‌ها اقدام به ربودن حساب کاربری آنها نموده و نهایتاً برای دور زدن مکانیزم‌های احراز هویت دو عاملی (به عنوان مثال برای کاربرانی که از توکن استفاده می-کنند) آنها را تشویق به نصب یک برنامه بر روی گوشی‌های تلفن همراه خود می‌نماید.

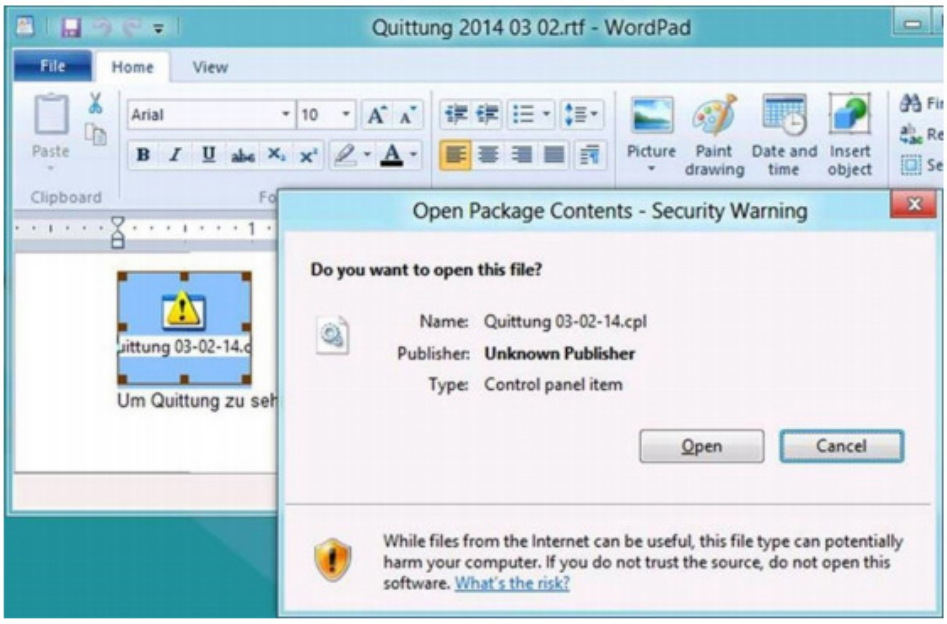
البته این حمله در حال حاضر با هدف بانک‌های خارجی انجام شده است اما ممکن است در آینده بانک‌های ایران نیز هدف قرار گیرد.

برای پیشگیری از رخداد این حمله، می‌بایست به طور مختصر با نحوه عملکرد آن آشنا گردید:

۱. در این حمله ابتدا یک ایمیل جعلی با عناوینی نظیر «صورتحساب از طرف یک شرکت معتبر» برای کاربران هدف ارسال می شود که حاوی **فایل ضمیمه‌ای با پسوند RTF.** می باشد.

در این فایل که به ظاهر مستند است، یک فایل اجرایی دیگر وجود دارد که در صورت اجرای آن یک گواهی SSL جعلی ساخته شده و کاربر را به سمت سایت جعلی بانک که از پیش طراحی شده است، هدایت می‌کند. از این طریق کاربر با وارد کردن نام کاربری و کلمه عبور خود برای ورود به اینترنت بانک، به راحتی اطلاعات احراز هویت خود را در اختیار مهاجمین قرار می‌دهد !

شکل زیر نمونه‌ای از فایل با پسوند RTF. و فایل مخرب درون آن را نشان می‌دهد:



۲. برای ورود به سامانه‌های بانکداری اینترنتی که دارای احراز هویت دو عاملی هستند، کار مهاجمان کمی پیچیده‌تر می‌شود و نیاز به همکاری بیشتر قربانی وجود دارد. در این مرحله با هدایت کاربر به صفحه جعلی بانک، وی را تشویق به نصب یک برنامه اندروید بر روی تلفن هوشمند خود می‌نماید. این برنامه که به ظاهر رمز عبور دوم را برای کاربر تولید می‌کند در واقع کنترل نشست‌های آنلاین بانکی کاربر را به دست می‌گیرد و از ارسال SMS های بانک برای

کاربر جلوگیری کرده و این SMSها را به سرور نفوذگران می‌فرستد. به این ترتیب مهاجمان به رمز دوم کاربر نیز دسترسی خواهند یافت.

راهکارهای پیشگیری از حمله Emmental

در صورت آلوده شدن سیستم و گوشی تلفن همراه کاربر، اطلاعات احراز هویت وی در اختیار مهاجم قرار گرفته و به سرعت امکان انجام کلاهبرداری و سرقت از حساب آنان فراهم می‌شود. لذا پیشگیری از این حمله بسیار مهم بوده و به علاوه با توجه به نقش کاربر در مسیر این حمله، راهکارهای پیشگیری از آلودگی به آن، با وجود سادگی، بسیار حیاتی می‌باشد. این راهکارها به شرح ذیل است:

۱. **نصب آنتی ویروس، اولین قدم پیشگیری از حمله است:** حتماً از یک آنتی ویروس معتبر بر روی سیستم خود استفاده نمایید. طبق برررسی‌های انجام شده، اکثر آنتی ویروس‌های معروف و معتبر، فایل مخرب این حمله را تشخیص می‌دهند. البته مهم است که آنتی ویروس شما مرتب بروز شود!

۲. **ایمیل از طرف فرستنده‌های ناآشنا را فراموش کنید:** جهت جلوگیری از آلودگی در مرحله اول حمله، هرگز ایمیل‌هایی که از طرف شرکت‌ها و نهادهای ناآشنا برای شما ارسال می‌شود را باز نکنید.

۳. **پیش از دانلود و بازکردن ضمایم ایمیل‌ها کمی درنگ کنید:** در صورتی که ایمیل از طرف شرکت‌ها، بانک‌ها و یا سایر نهادهایی باشد که سابقه دریافت ایمیل یا صورتحساب از آنها را دارید، از باز کردن سریع هرگونه ضمیمه و لینک موجود در آنها بپرهیزید. ابتدا علت ارسال ایمیل را بررسی نموده، در صورت نیاز به سایت شرکت یا بانک مراجعه نموده و یا با تماس تلفنی، علت ارسال آن را جویا شوید.

۴. **ضمایم ایمیل‌ها خطرناک هستند:** در صورت مشاهده فایل ضمیمه با پسوند EXE در ایمیل صورتحساب خود به هیچ عنوان آن را باز ننموده و چنانچه در داخل فایل RTF، هرگونه فایل دیگری یافتید نیز آن را باز ننمایید.

۵. **برای دانلود نرم‌افزارهای گوشی تلفن همراه، مراجع معتبر را برگزینید:** با گسترش به‌کارگیری تلفن هوشمند، این گوشی‌ها به یکی از ابزارهای خوب برای کمک به حملات مهاجمین تبدیل شده است. لذا در خصوص دانلود و نصب نرم‌افزارهای تلفن همراه خود نیز آنها را از سایت‌های معتبر تهیه نموده و نرم‌افزارهای بانکی را حتماً و فقط از سایت بانک مربوطه دریافت و نصب نمایید.