کشف بدافزار جدید کارتخوان های بانکی و تایید ورود آن به کشور - دیجیاتو

آرش پارساپور | یکشنبه، ۱۱ شهریور ۱۳۹۷

مرکز مدیریت راهبردی افتای ریاست جمهوری نسبت به کشف بدافزاری که سیستم های کارتخوان (POS) را هدف قرار می دهد هشدار داده و اعلام نموده که این ویروس، توسط شرکتی خارجی به نام Booz Allen Hamilton کشف شده و در بین هکرهای ایرانی نیز مشاهده شده است. این بدافزار بعد از قرار گرفتن روی دستگاه‌های کارتخوان (سیستم‌های POS) عمل اسکن اطلاعات را انجام می‌دهد و با اینکه چندان پیشرفته نیست ولی در هر حال می تواند برخی اطلاعات کارتهای عابربانک را سرقت کند.

بدافزار جدید نام RtPOS را یدک می‌کشد و به گفته کارشناسان تنها از مجموعه محدودی از توابع پشتیبانی می‌کند. برای مثال فایل اجرایی بدافزار فقط دو آرگومان (نصب و حذف) را قبول می‌کند. این سیستم می‌تواند با رصد کردن و خواندن حافظه دیجیتالی دستگاه‌های POS به اطلاعات شخصی حساسی چون شماره کارت‌های افراد دست پیدا کند. سایر بدافزارهای POS قابلیت‌های پیشرفته‌ای از قبیل امکانات ارسال و دریافت اطلاعات از سارق و تروجان‌های با دسترسی از راه دور دارند که ابزاری کامل برای جمع‌آوری داده توسط مهاجم به شمار می‌روند ولی این قابلیت‌ها در

بدافزار اخیر کشف شده وجود ندارد.

بدافزار RtPOS تنها یک کارکرد مخرب دارد و آن هم خوانش Ram سیستم و اسکن کردن آن است و شماره‌های کارت اعتباری را بعد از رصد در یک فایل DAT ذخیره می‌کند. گفتنیست به گفته مرکز مدیریت راهبری افتای ریاست جمهوری، این بدافزار اطلاعات دیگری از قبیل شماره‌های ملی، گذرواژه‌ها یا داده‌های مربوط به گواهینامه‌های رانندگی را ذخیره نمی‌کند. علاوه بر این، بدافزار RtPOS هیچ ویژگی مرتبط با شبکه نیز ندارد. از این رو ارتباطی با سرورهای از راه دور برقرار نمی‌کند تا دستورهای اضافی برای استخراج اطلاعات به سرقت رفته را اجرا کند.

با وجود سایت‌های شرط بندی که هم اکنون در حال فعالیت هستند، داشتن شماره کارت اعتباری و اطلاعات هویتی افراد مختلف هم می‌تواند تا حد زیادی برای برخی افراد مثمر ثمر واقع شود به خصوص وقتی که از موجودی حساب و انجام تراکنشات حساب مذکور با خبر باشند.

در حال حاضر پژوهشگران بین المللی دو سناریو را مطرح کردند؛ حدس اول بر این است که این بدافزار هنوز کامل نشده و همچنان در حال توسعه است و حدس دوم پژوهشگران این است که مهاجمان تنها به دلیل آلوده‌کردن کاربران و جمع‌آوری داده‌های پرداختی و دستیابی به یک Big Data آن را ساخته‌اند.

دیجیاتو