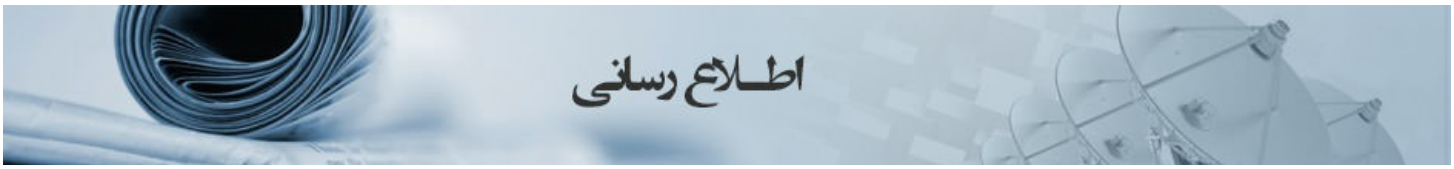

تازه ترین اخبار

- بازگشت حملات ماکرو با بدافزار Dridex
- اصلاح آسیب پذیری های جدی در مسیریاب های ...
- ابزار امنیتی متن‌باز گوگل
- آلوده شدن رایانه های ویندوز با تروجان ...
- ضد بدافزار رایگان مایکروسافت برای Azure

اطلاع رسانی

- اخبار
- راهنمای امنیتی
- امنیت در رایانه شما
- امنیت در گوشی های تلفن همراه
- پرسش و پاسخ
- سایتهای مرتبط

بازگشت حملات ماکرو با بدافزار Dridex

تاریخ انتشار: ۱۳۹۳/۰۸/۱۹ تعداد بازدید: ۶

این بدافزار با نام Dridex سعی می کند تا داده های کاربران را هنگام ورود به حساب بانکی آنلاین خود به سرقت ببرد.

شماره: IRCNE۲۰۱۴۱۱۲۳۷۲
تاریخ: ۱۸/۰۸/۹۳

بدافزاری که اخیرا با هدف سرقت اعتبارنامه های بانکی آنلاین منتشر شده است از روشی قدیمی برای نصب خود بر روی رایانه ها استفاده می کند.
این بدافزار با نام Dridex سـعی می کند تا داده های کاربران را هنگام ورود به حساب بانکی آنلاین خود به سـرقت ببرد. این بدافزار جانشـین قطعه بدافزاری به نام Cridex است که حساب های بانکی را هدف قرار می دهد.
تفاوت این دو بدافزار در نحوه آلوده ساختن رایانه ها می باشد. بدافزار Dridex خودش را در قالب یک ماکرو که در اسناد مایکروسافت ورد قرار دارد و از طریق یک پیام هرزنامه ای ارسال می کند.
مجرمان سایبری بیش از یک دهه است که از ماکروها سوء استفاده می کردند اما پس از آنکه مایکروسافت دفاع امنیتی ماکروها را ارتقاء داد دیگر از ماکروها سوء استفاده نشد. اما به نظر می رسد که تعدادی از هکرها دوباره سعی در سوء استفاده از ماکروها دارند.
Rhena Inocencio، یک مهندس امنیتی اظهار داشت: ماکرو ها در اغلب رایانه ها به طور پیش فرض غیرفعال می باشد. اما اگر یک فایل مخرب ورد باز شود، به کاربر توصیه می کند تا ماکروها را فعال نماید و اگر کاربری ماکرو را فعال کند، بدافزار Dridex بر روی رایانه دانلود می شود. این بـدافزار به گونه ای برنامه ریزی شـده است که زمانیکه بر روی رایانه نصب شد، عملیاتی را هنگام رجوع کاربر به سایت های بانکی انجام دهد.
پیام های هرزنامه ای اغلب از کشورهای ویتنام، تایوان، کره جنوبی و چین برای قربانیان فرستاده می شود در حالی بیش ترین آلودگی ها در سه کشور استرالیا، انگلستان و امریکا گزارش شده است.

چاپ