لطفاً مراقب اطلاعات خود باشید

خانواده ای از تروجان های Ransom (ویروس های باج گیر) که فایل ها را رمزگذاری و به آن پسوند xtblو ytbl و ... اضافه می کند.

این تروجان در اواخر سال ۲۰۱۴ و اوایل سال ۲۰۱۵ به وجود آمده و خود را به سرعت در کنار سه ویروس Trojan – ransom.win 32و cryaklو Trojan – ransom.bat scatter در کشور روسیه قرار داده است. بر اساس طبقه بندی شرکت کسپرسکی، این ویروس Trojan – ransom.win32.shadeنامگذاری شده است. نام اصلی این ویروس و سازنده آن هنوز مشخص نمی باشد ولی شرکت های امنیتی دیگر این ویروس را با نام Trojan.encoder.858و ransom:win32/troldeshشناسایی کرده اند.

لطفا موارد زیر را برای به حداقل رساندن خطر آلودگی سیستم ها، رعایت نمایید:

۱. تحت هیچ شرایطی، ضمیمه ی ایمیلی از سمت ارسال کننده ناشناس باز نشود. (فرستنده می تواند از طرف فیسبوک یا linkdin یا از طریق invoiceبانکی)

۲. تحت هیچ شرایطی، لینکی از طریق ایمیل ناشناس باز یا کلیک نشود. به سایت های متفرقه مراجعه نشود.

۳. با توجه به اینکه هیچ راه حلی برای برای بازیابی کردن اطلاعات وجود ندارد، از کلیه اطلاعات سیستم Backup تهیه نمایید.

لازم به ذکر است در صورت آلوده شدن سیستم به این ویروس، کلیه فایل های PDF ,Word, PowerPoint و برخی از فایل های دیگر از قبیل پایگاه داده های آن سیستم را تخریب نموده و دیگر قابل بازیابی نمی باشند.