قربانیان باج افزار Thanatos اکنون می‌توانند فایل‌های خود را رایگان پس بگیرند - دیجیاتو

امین قیاسی | یکشنبه، ۱۰ تیر ۱۳۹۷

باج افزار Thanatos در بهمن ماه سال گذشته سیستم‌های ویندوز را هدف قرار داد و نسخه‌هایی مختلفی از آن نیز طی ماه‌ها بعد عرضه شد تا نشان دهد که طراحان این بد افزار هنوز خطری جدی به شمار می‌روند. بد افزار یاد شده پس از آلوده ساختن اطلاعات کاربر از او در خواست می‌کرد که با پرداخت مبلغی به خصوص، فایل‌های خود را پس بگیرد.

قربانیان باج افزار تاناتوس حتی با پرداخت مبلغ خواسته شده نیز قادر نبودند که فایل‌های خود را قفل گشایی کرده و آنها را پس بگیرند اما به نظر می‌رسد که اکنون مشکل رفع شده است.

در حال حاضر این قربانیان قادر خواهند بود که با استفاده از ابزار رمزگشایی جدیدی که پژوهشگران امنیتی ساخته‌اند بدون پرداخت هیچ مبلغی، فایل‌هایشان را دریافت کنند.

این بد افزار با نمونه‌های دیگر قدری متفاوت بود و بیت کوین درخواست نمی‌کرد اما در عوض از کاربر می‌خواست تا از طریق رمزپول‌های دیگر نظیر اِتریم، زد کَش یا بیت کوین کَش به پرداخت مبلغ خواسته شده بپردازد.

با این حال، اگر کاربری به پرداخت بهای خواسته شده تن می‌داد نیز قادر نبود فایل‌های خود را دریافت کند چرا که در پروسه‌ی رمزگذاری تاناتوس مشکلی اساسی وجود داشت. برخی معتقد بودند که این مشکل عمدی به وجود آمده و هکرهای طراح این باج افزارها قصد دارند که با نبود راهی برای قفل گشایی اطلاعات، توانایی خود را به رخ کاربران و دیگر هکرها بکشانند.

اکنون محققان گروه امنیتی سیسکو تالوس به منظور بازگرداننده اطلاعات قربانیان، یک ابزار رایگان به نام ThanatosDecryptor برای رمزگشایی دیتای آنها تولید کرده و عرضه نموده است.

این باج افزار نیز مشابه با دیگر موارد اشاره شده از طریق فایل‌های ضمیمه برای کاربران ارسال شده اما جالب اینجاست که ضمیمه‌ی ایمیل نبوده و طراحانش سعی کرده اند که با ارسال یک فایل

صوتی و یک پیغام این بد افزار را در سیستم‌های کاربران فعال کنند.

به نظر می‌رسد که هکرهای طراح این باج افزار در ساخت ابزار رمزگشاییشان دچار مشکل شده بودند چرا که در فایلی از تاناتوس نوشته شده بود که هیچ ابزاری برای قفل گشایی این بد افزار وجود ندارد و نمی‌توان از آن بهره‌ای گرفت.

کارشناسان باور دارند که طراحان این باج افزار قادر نبودند که ابزار رمزگشایی کارآمدی برای بد افزار خود طراحی کنند اما بازهم تاناتوس را بین کاربران پخش نمودند تا حداقل پولی به جیب بزنند.

تماشا کنید: آشنایی با حفره های امنیتی اسپکتر و ملتداون در پردازنده ها