Rombertic **بدافزاری که در صورت ردیابی خود را نابود می کند**

ویژگی منحصر به فرد بدافزار این است که به محض نصب و اجرا روی کامپیوتر قربانی، بررسی می کند که آیا ردیابی شده است یا خیر . بلافاصله تمام تلاش خود را می کند تا در صورت ردیابی، خود را نابود کند و ردپای خود را از بین ببرد.

ایران هشدار – تا کنون مطالب زیادی در مو.رد انواع بد افزارهای خطرناک ارائه داده ایم. تمامی بد افزارها خطرناک، مخرب و آسیب رسان هستند. اما برخی از آنها از این جهت که قابل ردیابی هستند، کمتر خطرناک هستند و برخی دیگر به دلیل اینکه قابل ردیابی نیستند، به مراتب خطرناک تر هستند.

یکی از خطرناک ترین بد افزار ها، بد افزار رامبرتیک است که می تواند به راحتی رد پای خود را پاک کند به طوری که هیچ کس متوجه حضور آن نشود. ویژگی منحصر به فرد بدافزار این است که به محض نصب و اجرا روی کامپیوتر قربانی، بررسی می کند که آیا ردیابی شده است یا خیر . بلافاصله تمام تلاش خود را می کند تا در صورت ردیابی، خود را نابود کند و ردپای خود را از بین ببرد.

در واقع این بدافزار خود را درون یک فایل اجرایی محافظ صفحه نمایش screen saver مخفی می سازد و زمانی که قربانی آن را اجرا کند، کد های خطرناک به مرورگر او وارد شده و کار خود را شروع می کنند. این بد افزار به طور بسیار مرموزی به سرقت اطلاعات و داده های کاربران می پردازد و از طریق هرزنامه ها و پیام های فیشینگ و spam منتشر و هر متن ساده ای را که وارد پنجره مرورگر کامپیوتر قربانی شود، برای ثبت و سرقت اطلاعات مهم، ردیابی می کند. رامبرتیک پس از اینکه فایل های موجود در پوشه خانگی را کد گذاری کرد، به صورت خودکار بوت می شود و قبل از اینکه سیستم بارگذاری شود، مجددا وارد حلقه تکرار می شود و این روند تا زمانی که سیستم عامل مجددا تعویض نشود، ادامه پیدا می کند و در نهایت تصویری با مفهوم "carbon crack attempt failed" به نمایش در می آید. رامبرتیک عموما از راه کلیک روی پیوست و همراه با نامه های آلوده ای که به صورت spam به افراد ارسال می شود، به کامپیوتر قربانی وارد می شود. این بد افزار قبلا کشور کره جنوبی را در سال ۲۰۱۳ مورد هدف قرار داده بود. لازم به ذکر است به دلیل عدم قابلیت ردیابی، که از ویژگی های منحصر به فرد این بدافزار است، حذف این بدافزار و پاکسازی سیستم به آسانی صورت نمی گیرد. حتی کاربر متوجه حضور آن نمی شود بنابراین توصیه می شود، هرگز لینک های ضمیمه شده به ایمیل های ناشناس را باز نکنید و هرگز به اجرای برنامه هایی که به صورت ناخواسته به شما پیشنهاد می شود، نپردازید.

اداره حراست آموزشکده شهید یزدانپناه سنندج