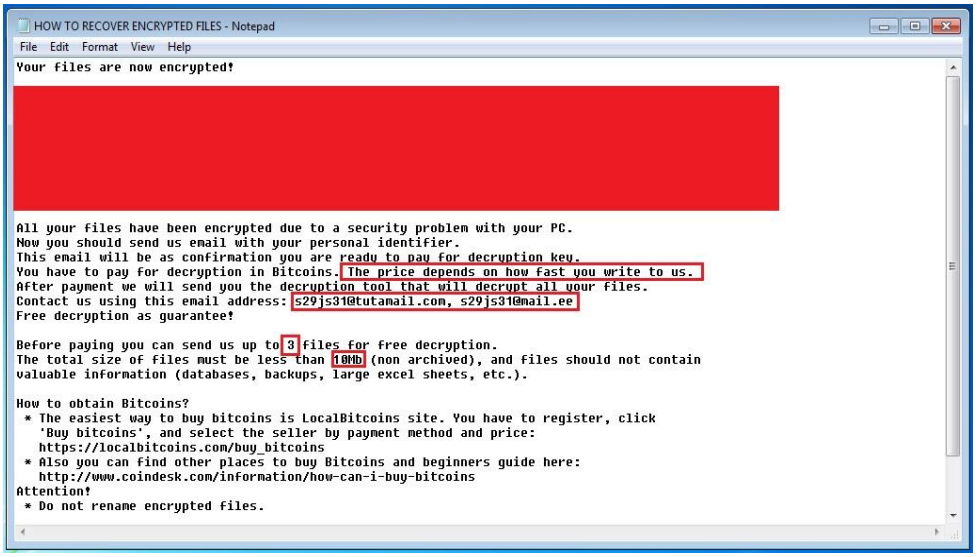
نمونه جدیدی از باج‌افزار Scarab با پسوند Hitler

در بررسی و مشاهده فضای سایبری در زمینه بدافزار، نسخه جدیدی از باج‌افزار Scarab مشاهده می‌شود که از طریق اسپم ایمیل انتشار می‌یابد. نام فایلی که برای باج‌افزار استفاده شده بصورت Abondon.exe و لوگوی آن شبیه به برنامه word می‌باشد.

باج‌افزار از طریق اسپم‌ایمیل انتشار یافته و بعد از انتقال به سیستم از کاربر درخواست دسترسی بالاتری را دارد. بعد از دریافت دسترسی لازم، دستوراتی را در محیط فرمان اجرا کرده و با استفاده از آن فایلی با نام sevnz را در مسیر C:\Users\Username\AppData\Roaming ایجاد کرده و اقدام به اجرای فایل ایجاد شده می‌کند. سپس با استفاده از فایل sevnz.exe پروسس mhsta.exe را اجرا کرده و با استفاده از cmd.exe اقدام به اجرای دستوراتی در این برنامه کرده و فایل‌های پشتیبان و ShodowCopy را حذف می‌کند. سپس ورودی‌های کیبورد را برای دکمه‌های ترکیبی مانند Ctrl+Alt+Delete غیرفعال کرده و شروع به رمزگذاری فایل‌های سیستم کرده و نام فایل و پسوند آن را به صورت [Random_Number_and_Digit].hitler تغییر می‌دهد که باعث می‌گردد نام فایل نیز غیرقابل دسترس گردد. در هنگام اجرا از بازکردن برنامه‌هایی مانند Process Explorer و Task Manager برای جلوگیری از توقف‌سازی باج‌افزار جلوگیری می‌کند. بعد از اتمام فرایند فایل متنی با نام HOW TO RECOVER ENCRYPTED FILES.TXT را در داخل هر پوشه ایجاد کرده و در پایان کار رمزگذاری، فایل متنی ایجاد شده را برای کاربر نشان می‌دهد. شکل زیر نمونه‌ای از فایل‌های رمزشده و همچنین فایل متنی ایجاد شده را نشان می‌دهد که تمامی فایل‌ها با نام‌های فارسی و انگلیسی را رمزکرده و نام و پسوند آن را تغییر داده است.

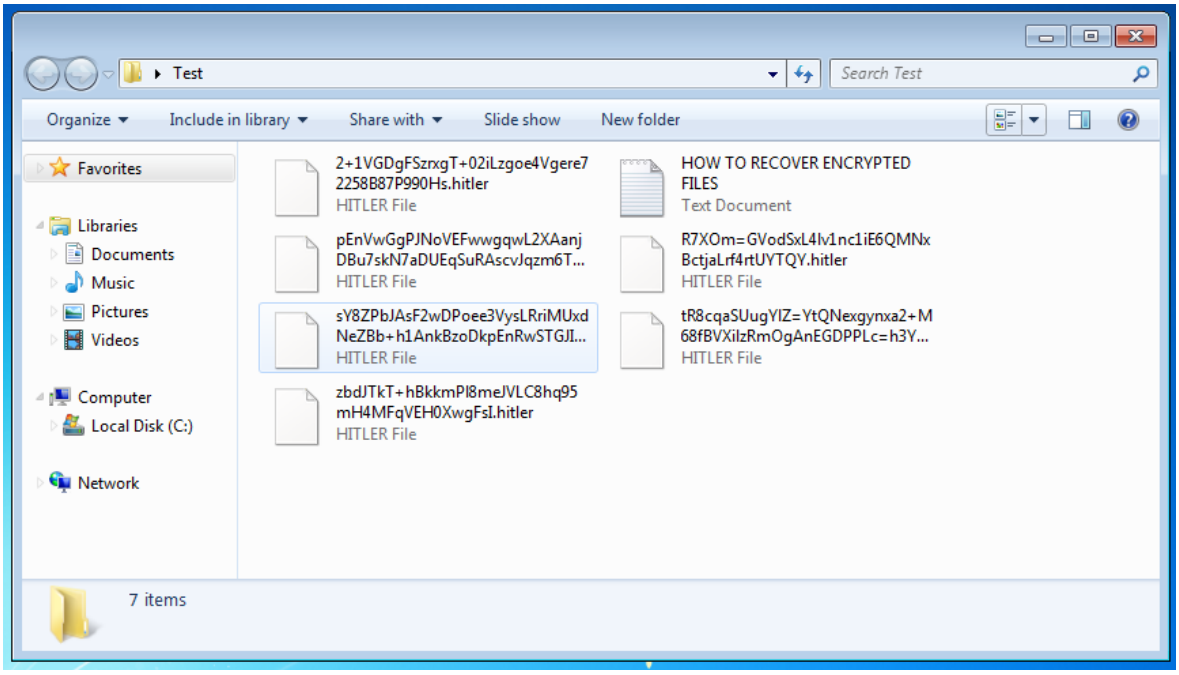


شکل ۱ – پیام متنی نشان داده‌شده برای کاربر

در این فایل متنی شناسه شخصی کاربر قرار داده شده است که رشته بزرگی از متشکل از رقم و حروف می‌باشد. مهاجمان از کاربر قربانی شده درخواست دارند تا برای بازگردانی فایل‌های رمزشده شناسه شخصی را به یکی از آدرس‌های s29js31@tutamail.com یا s29js31@mail.com ارسال کنند. مقدار باج در نظر گرفته شده بستگی به زمان ارسال این شناسه دارد که در صورت ارسال سریع این مقدار کمتر خواهد بود. همچنین برای اطمینان دادن از اینکه فایل‌های قابل رمزگشایی می‌باشد از کاربر درخواست دارد تا سه فایل که حجمشان کمتر از ۱۰ مگابایت می‌باشد ارسال کنند. و در آخر این فایل نحوه خرید بیت‌کوین را آورده و آدرس‌هایی که می‌توان از آن‌ها بیت‌کوین را خریداری کرد.

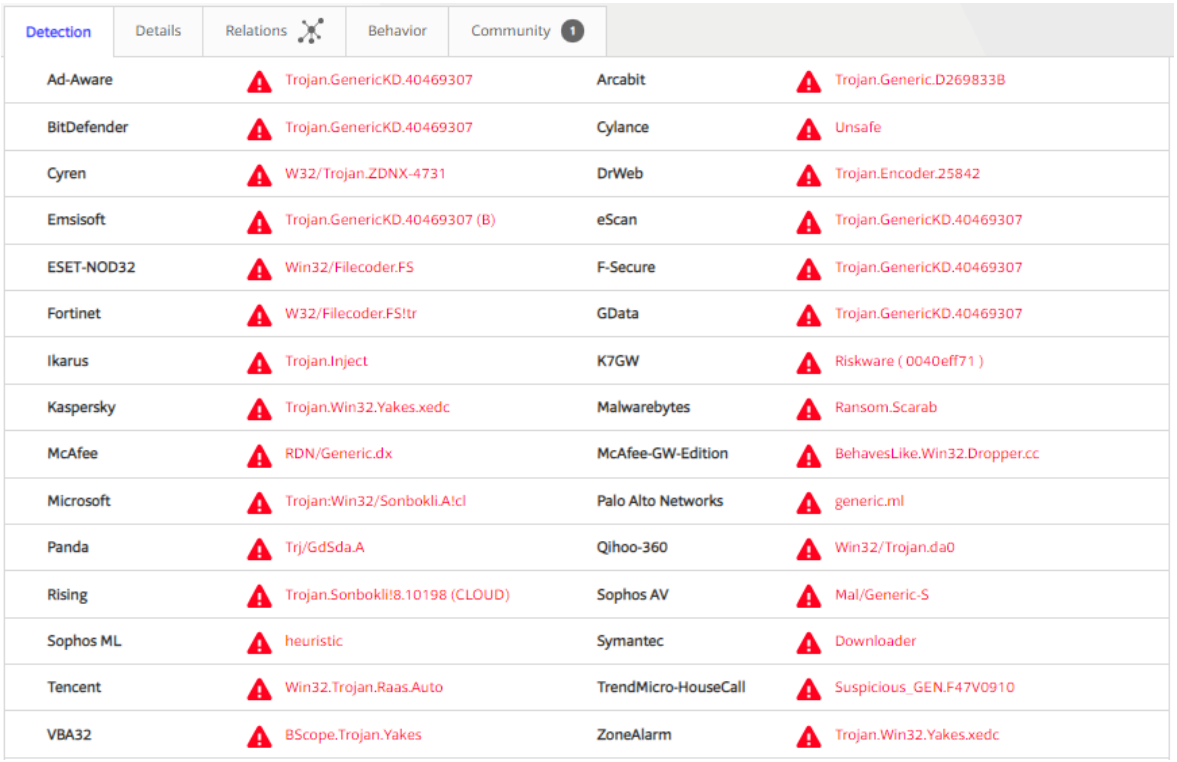
نحوه فعالیت بدافزار

نحوه شیوع و یا انتقال باج‌افزار به سیستم روش‌های زیادی از جمله ایمیل‌اسپم. بعد از ورود به سیستم با استفاده از الگوریتم رمزنگاری AES-256 اقدام به رمزگذاری فایل‌های سیستم کرده و نام و پسوند فایل بصورت [Random_Letters_and_Digits].hitler در می‌آورد.



شکل ۲- نمونه‌ای از فایل‌های رمزشده

همچنین در شکل زیر مشاهده می‌گردد که بیشتر آنتی‌ویروس‌های فعال قادر به شناسایی فایل به‌عنوان بدافزار شده‌اند و برای جلوگیری از فعالیت آن می‌توان آنتی‌ویروس خود را بروزرسانی کرده و استفاده کرد.



شکل ۳ - تشخیص فایل در آنتی‌ویروس‌ها

پاکسازی بدافزار از سیستم

برای پاکسازی بدافزار در سیستم در عمل کاری نمی‌توان انجام داد. ولی می‌توان با استفاده از فایل‌های پشتیبان که قبلا از سیستم گرفته‌است، اقدام به بازیابی اطلاعات کرد.

بعد از بازیابی فایل‌ها، سیستم را با استفاده از آنتی‌ویروس بروزشده، اسکن کرده و راهکارهای امنیتی را برای سیستم خود لحاظ می‌کنیم.

راه‌های مراقبت و پیشگیری

برای اینکه سیستم خود را ایمن نگه داریم و از افشای اطلاعات و سواستفاده از آن مراقبت کنیم باید راهکارهای زیر را در نظر بگیریم:

۱- از آنتی‌ویروس‌های قوی و معتبر استفاده کنیم.

بیشتر برنامه‌های آنتی‌ویروس قدرت لازم را برای تشخیص یک فایل بدافزار را ندارند و فقط اسم یک آنتی‌ویروس را بر روی خود دارند. هنگام استفاده از آن‌ها، بعد از تحقیق مختصری در مورد آن‌ها می‌توان یک آنتی‌ویروس قوی و خوبی را انتخاب کرد.

۲- از دانلود و نصب برنامه‌های مشکوک خودداری کنیم.

بیشتر برنامه‌هایی که از طریق تبلیغات یا از طریق کانال‌های دیگر ارائه می‌گردند مخرب بوده و احتمال آسیب رسیدن به سیستم می‌باشد. لذا از دانلود و نصب برنامه‌هایی که مشکوک به‌نظر می‌رسند باید خودداری کرد.

۳- پشتیبان‌گیری مداوم از فایل‌ها و اطلاعات

بیشتر بدافزارها از نوع باج‌افزار می‌باشند و می‌توانند فایل‌ها و اطلاعات موجود بر روی سیستم را رمز کرده و دسترسی به آن‌ها را ناممکن کنند و یا در برخی از بدافزارها امکان حذف یا خرابکاری بر روی اطلاعات وجود دارد. لذا برای درمان بعد از آلوده شدن به بدافزار، به فایل‌های پشتیبان نیاز پیدا می‌کنیم. برای این‌کار بصورت مداوم (هفتگی یا ماهانه) از فایل‌ها و اطلاعات حساس و مورد نیاز فایل پشتیبان ایجاد کرده و آن‌ها را در یک دستگاه دیگر نگهداری کنیم.

۴- عدم بازکردن ایمیل‌های مشکوک

بیشتر حملات باج‌افزاری از طریق اسپم ایمیل‌ها با عناوین گول‌زننده انتشار می‌یابند. لذا باید از باز کردن این نوع از ایمیل‌ها خودداری کرده و در همان لحظه آن‌ها را حذف کنیم. در این نوع از ایمیل‌ها، در داخل فایل‌های مانند word یا pdf بدافزار قرار داده شده و هنگام اجرای آن‌ها بدافزار اجرا شده و اقدام به نصب و راه‌اندازی خود در سیستم می‌کنند.

آزمایشگاه و مرکز تخصصی آپا دانشگاه محقق اردبیلی

شماره تماس: ۰۴۵ – ۳۱۵۰۵۷۱۸

آدرس اینترنتی: cert.uma.ac.ir

آدرس: اردبیل – خیابان دانشگاه- دانشگاه محقق اردبیلی – دانشکده فنی – مرکز آپا محقق اردبیلی