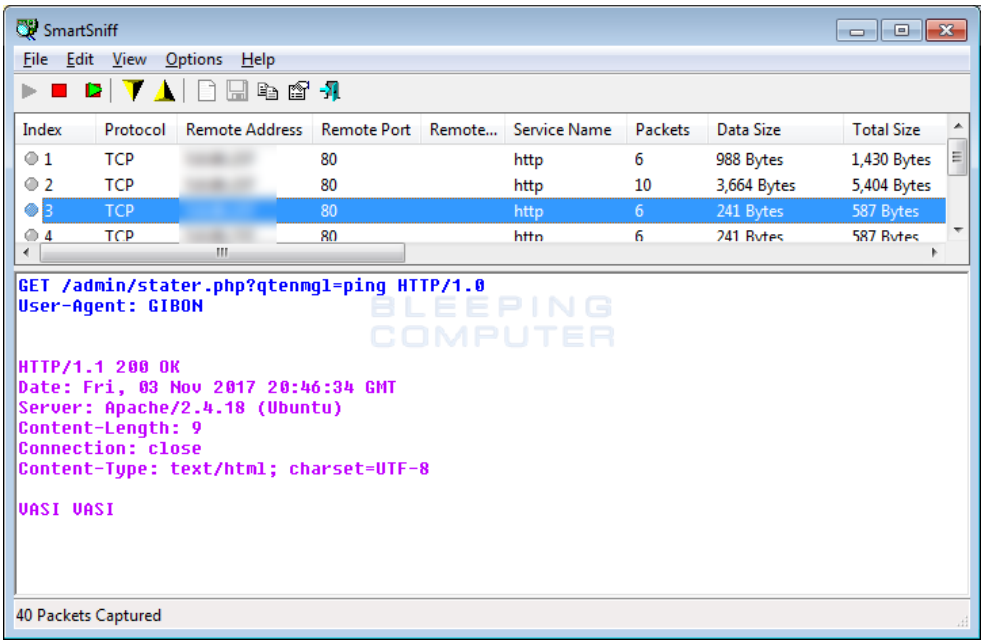
بسمه تعالی

باج افزار GIBON و رمزگشا برای آن

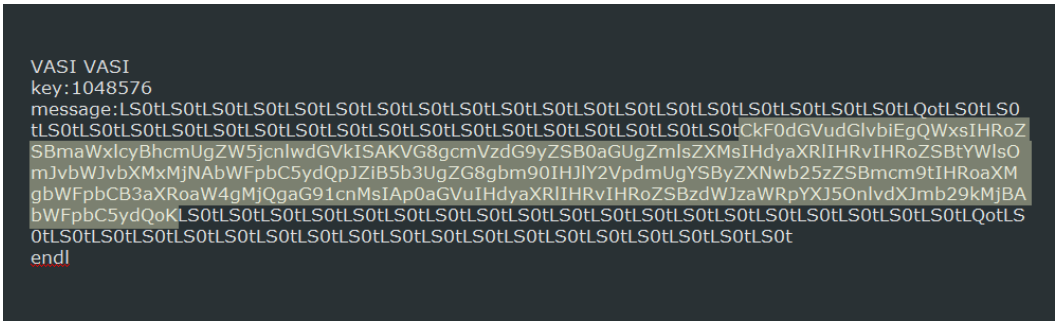
به تازگی باج افزار جدیدی با نام GIBON توسط مرکز تحقیقات امنیت سایبری ProofPoint شناسایی شده است که توسط ساختار malspam خود را منتشر می کندکه فایلهای Document آلوده به Script های مخرب macro جهت دانلود و اجرای فایل اصلی باج افزار بر روی سیستم قربانی را شامل می شود.

محققان همواره برای نامگذاری بدافزارها و باج افزارها با مشکل مواجه هستند!. گاهی اوقات از طریق پیدا کردن یک strings خاص در فایل اجرایی بدافزار، نامی را برای آن انتخاب می کنند. در مورد این باج افزار، نام GIBON در user agent درخواست های اینترنتی جهت اتصال به سرور C&C خود دیده می شود.

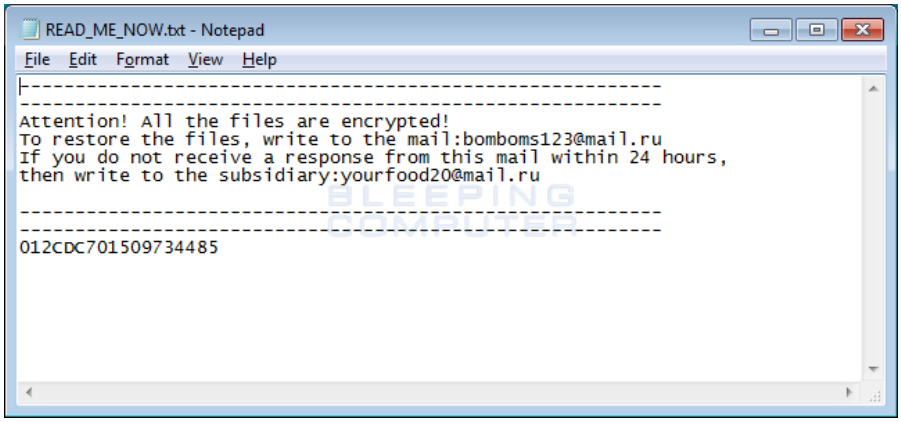


این باج افزار در اولین اقدام خود پس از اجرا شدن بر روی سیستم عامل ویندوز قربانی، خود را به سرور C&C متصل می کند و با استفاده از یک کد Base64 که شامل ترکیبی از timestamp، شماره نسخه سیستم عامل ویندوز و یک مقدار string مشخص با نام register می باشد. حال سرور C&C یک پیغام با فرمت Base64 را برای باج افزاری که بر روی سیتسم قربانی است می فرستد.

برای اولین بار که قربانی بر روی سرور C&C رجیستر می شود، یک کلید رمزنگاری را بر روی سیستم Local قربانی می سازد و آن را توسط یک ارسال رمزنگاری شده با استفاده از الگوریتم Base64 برای سرور C&C می فرستد. این کلید برای رمزنگاری فایلهای مشخصی بر روی سیستم قربانی به کار می رود. حال باج افزار شروع به جستجوی فایلها بر اساس extension های خاصی می کند و پس از یافتن فایلها، آنها را رمزنگاری کرده و پسوند encrypt. را به انتهای extension فایلهای رمز شده اضافه می کند.

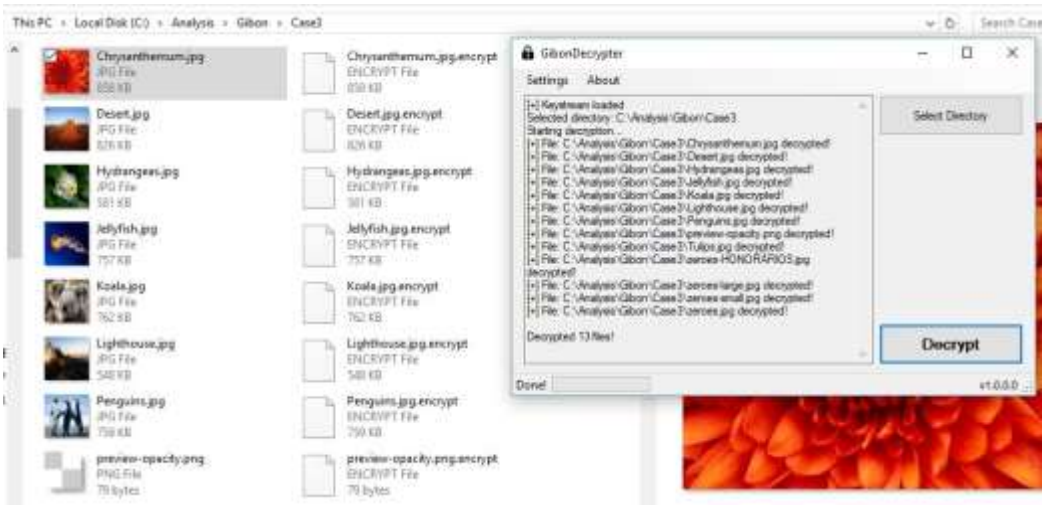


پس از رمزنگاری فایلهای مورد نظر در هر شاخه، فایلی متنی با نام READ_ME_NOW.txt را در هر پوشه می سازد که توضیحاتی در مورد اینکه چه اتفاقی برای فایلها افتاده است می دهد و دو آدرس ایمیل جهت ارتباط با هکر و پرداخت پول جهت بازیابی فایلهای رمزشده را شامل می شود. یک شماره ID منحصر به فرد هم در انتهای پیام دیده می شود.



در حال حاضر محققان تیم BleepingComputer یک Decryptor برای این باج افزار آماده کرده اند که توسط آن می توانید فایلهای رمزشده خود توسط این باج افزار را رمزگشایی نمایید. جهت دریافت GibonDecrypter می توانید به آدرس زیر مراجعه کنید. همچنین تصویری از محیط برنامه GibonDecrypter را در ادامه مشاهده می فرمایید:

https://www.bleepingcomputer.com/download/gibon-ransomware-decryptor/


This PC › Local Disk (C:) › Analysis › Gibon › Case3
Chrysanthemum.jpg
Chrysanthemum.jpg.encrypt
Desert.jpg
Desert.jpg.encrypt
Hydrangeas.jpg
Hydrangeas.jpg.encrypt
Jellyfish.jpg
Jellyfish.jpg.encrypt
Koala.jpg
Koala.jpg.encrypt
Lighthouse.jpg
Lighthouse.jpg.encrypt
Penguins.jpg
Penguins.jpg.encrypt
preview-opacity.png
preview-opacity.png.encrypt
GibonDecrypter
Settings
About
[+] Keystream loaded
Selected directory: C:\Analysis\Gibon\Case3
Starting decryption...
[+] File: C:\Analysis\Gibon\Case3\Chrysanthemum.jpg decrypted!
[+] File: C:\Analysis\Gibon\Case3\Desert.jpg decrypted!
[+] File: C:\Analysis\Gibon\Case3\Hydrangeas.jpg decrypted!
[+] File: C:\Analysis\Gibon\Case3\Jellyfish.jpg decrypted!
[+] File: C:\Analysis\Gibon\Case3\Koala.jpg decrypted!
[+] File: C:\Analysis\Gibon\Case3\Lighthouse.jpg decrypted!
[+] File: C:\Analysis\Gibon\Case3\Penguins.jpg decrypted!
[+] File: C:\Analysis\Gibon\Case3\preview-opacity.png decrypted!
[+] File: C:\Analysis\Gibon\Case3\Tulips.jpg decrypted!
[+] File: C:\Analysis\Gibon\Case3\zeroes-HONORABIOS.jpg decrypted!
[+] File: C:\Analysis\Gibon\Case3\zeroes-large.jpg decrypted!
[+] File: C:\Analysis\Gibon\Case3\zeroes-small.jpg decrypted!
[+] File: C:\Analysis\Gibon\Case3\zeroes.jpg decrypted!
Decrypted 13 files!
Select Directory
Decrypt
Done!
v1.0.0.0