باسمه تعالی

تحلیل فنی باج‌افزار

Pylocky

مقدمه :

رصد فضای سایبری در حوزه باج‌افزار، از ظهور باج‌افزار Pylocky خبر می‌دهد. فعالیت این باج‌افزار از اواخر جولای ۲۰۱۸ میلادی شروع شده است. بر اساس گزارش سایت id-ransomware.blogspot.com تمرکز این باج‌افزار بر روی کاربران انگلیسی، فرانسوی، ایتالیایی و کره‌ای زبان می‌باشد. البته این مسئله در پیغام باج‌خواهی باج‌افزار مشهود است و متن آن در قالب یک فایل به چهار زبان ذکرشده، بیان شده است.

مشخصات فایل اجرایی :

نام فایل	PyLocky.exe
MD٥	٧feb٤٣da٤aefced٩f٦٤a٠٥٨a٣٨٥de٤١٦
SHA-١	٦٧a١fb٧٨f١٠٢١a٣٤b٧e٥f٨٧٤٣٣cb٧bac٢٩٨٧٨٤١٨
SHA-٢٥٦	١٩٤d١ccff٧ab٢٣٠٠٣b٣٤f٥٩٨٤f٣٩٦e٦d٤aaf٢٦١٥bfb٠٢d٥e٢٨cd٠b٨٥١٣c٥٧c٨٧
اندازه فایل	٧.٤ مگابایت

فایل این باج‌افزار دارای ٨ بخش است :

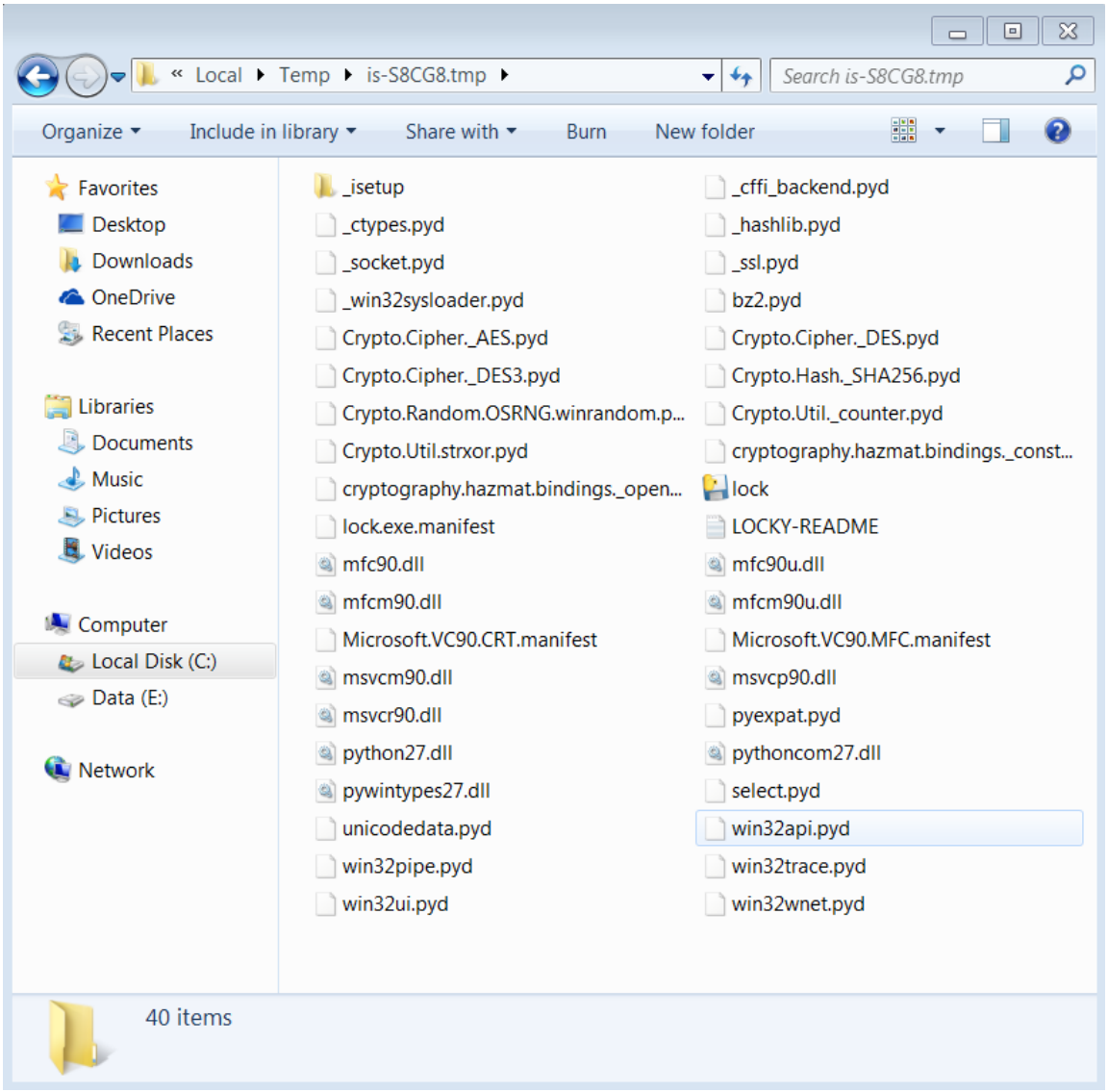
نام بخش	آنتروپی	آدرس مجازی	اندازه مجازی	اندازه خام
CODE	٦.٦٤	٤٠٩٦	٤١٤٢٤	٤١٤٧٢
DATA	٢.٧٤	٤٩١٥٢	٥٩٢	١٠٢٤
BSS	٠	٥٣٢٤٨	٣٧٣٢	٠
.idata	٤.٤٩	٥٧٣٤٤	٢٤٢٨	٢٥٦٠
.tls	٠	٦١٤٤٠	٨	٠
.rdata	٠.١٩	٦٥٥٣٦	٢٤	٥١٢
.reloc	٠	٦٩٦٣٢	٢٣٣٢	٠
.rsrc	٤.٩	٧٣٧٢٨	٧٢٧٦٤	٧٣٢١٦

تحلیل پویا :

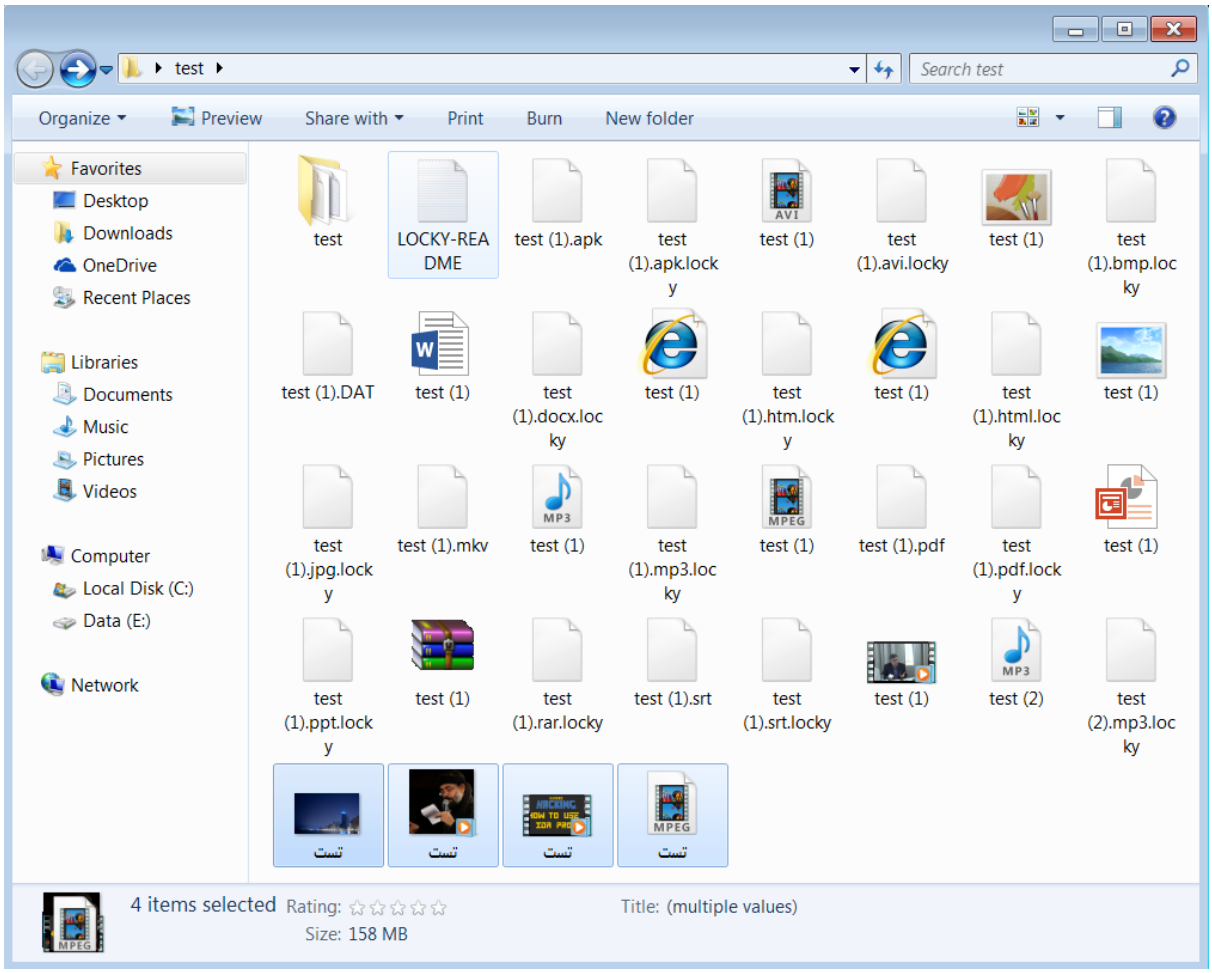
برای بررسی عمیق‌تر باج‌افزار Pylocky، فایل اجرایی آن را در محیط آزمایشگاهی اجرا کردیم تا عملکرد باج‌افزار را از نزدیک مورد بررسی قرار دهیم. این باج‌افزار به محض ورود به سیستم قربانی، پوشه‌ای به نام is-SΛCGΛ.tmp را در مسیر زیر ایجاد می‌کند:

C:\Users\Admin\AppData\Local\Temp

تصویر زیر، مربوط به محتوای این پوشه می‌باشد:



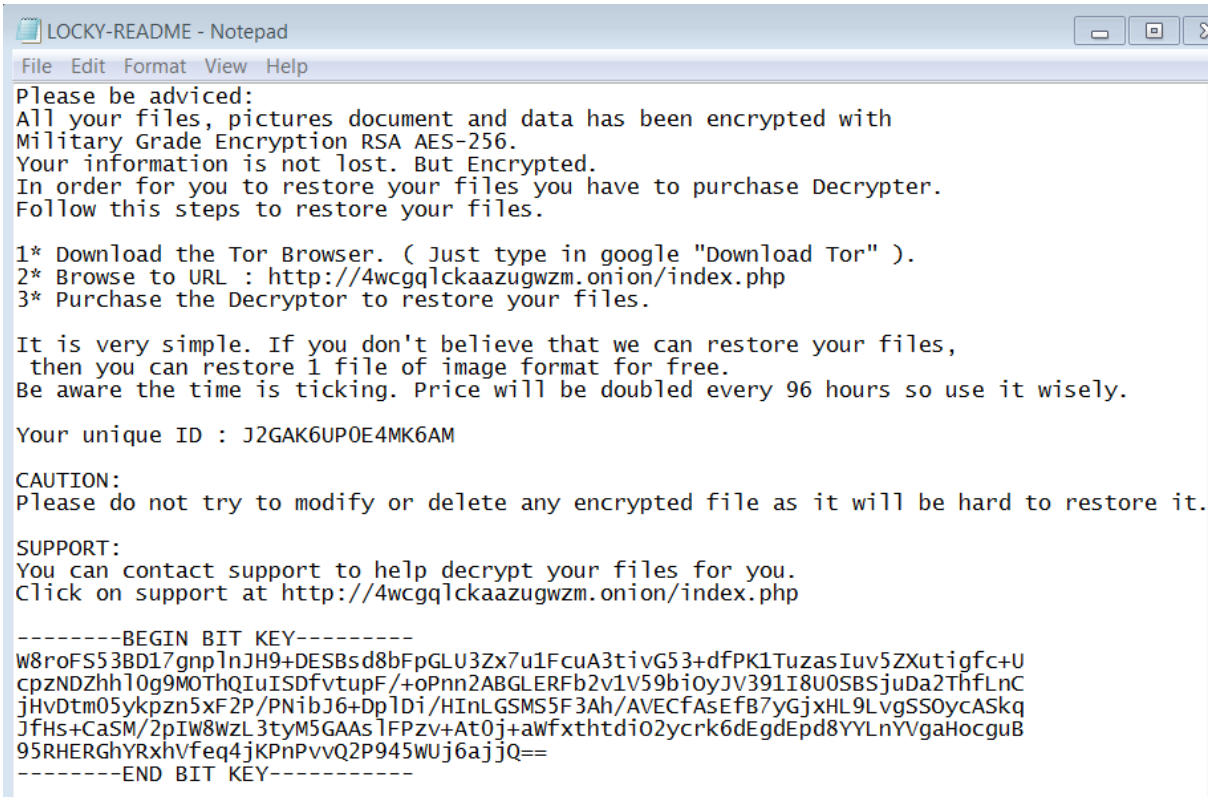
همانطور که در تصویر بالا مشاهده می‌کنید، تعدادی از فایل‌ها و کتابخانه‌های باج‌افزار در این پوشه قرار گرفته‌اند. فایل اجرایی lock.exe که در تصویر مشخص است، همان فایل اصلی باج‌افزار می‌باشد که به صورت خودکار اجرا شده و فایل‌ها را رمزگذاری می‌کند و فایل LOCKY-README نیز فایل پیغام باج‌خواهی باج‌افزار می‌باشد. پس از پایان فرآیند رمزگذاری، فایل‌های سیستم قربانی به شکل زیر تغییر پیدا می‌کنند:



طبق تصویر بالا، پسوند locky. به انتهای فایل‌های رمزگذاری شده اضافه شده است و یک فایل کپی از نام و آیکن آنها نیز ایجاد شده است. این فایل کپی، همان پیغام باج‌خواهی باج‌افزار است که به این شکل ایجاد شده است. البته فایل پیغام باج‌خواهی با عنوان اصلی آن که LOCKY-README می‌باشد نیز، در تصویر مشخص است. این فایل در هر پوشه حاوی فایل‌های رمزشده و همینطور بر روی صفحه نمایش سیستم قربانی نیز قرار می‌گیرد. طبق بررسی‌های صورت گرفته، این باج‌افزار فایل‌های با نام فارسی را رمزگذاری نمی‌کند که در تصویر بالا نیز مشخص می‌باشد. همچنین با بررسی‌های بیشتری که بر روی مسیرهای رمزگذاری فایل‌ها انجام دادیم متوجه شدیم که در درایو ویندوز سیستم عامل، تنها فایل‌های مسیر

C:\Users\Admin رمزگذاری شده‌اند. البته پوشه‌های My Music، My Picture و My Videos نیز، در این مسیر رمزگذاری نشده بودند. فایل‌های اجرایی با پسوند exe نیز، بدون هیچ مشکلی اجرا می‌شدند.

همانطور که در ابتدا ذکر شد، فایل پیغام باج‌خواهی این باج‌افزار به چهار زبان می‌باشد. تصاویر زیر مربوط به بخش‌های این فایل است که زبان‌های انگلیسی، فرانسوی، ایتالیایی و کره‌ای می‌باشد:


LOCKY-README - Notepad

File Edit Format View Help

```
Please be adviced:
All your files, pictures document and data has been encrypted with
Military Grade Encryption RSA AES-256.
Your information is not lost. But Encrypted.
In order for you to restore your files you have to purchase Decrypter.
Follow this steps to restore your files.

1* Download the Tor Browser. ( Just type in google "Download Tor" ).
2* Browse to URL : http://4wcgqlckaazugwzm.onion/index.php
3* Purchase the Decryptor to restore your files.

It is very simple. If you don't believe that we can restore your files,
 then you can restore 1 file of image format for free.
Be aware the time is ticking. Price will be doubled every 96 hours so use it wisely.

Your unique ID : J2GAK6UP0E4MK6AM

CAUTION:
Please do not try to modify or delete any encrypted file as it will be hard to restore it.

SUPPORT:
You can contact support to help decrypt your files for you.
Click on support at http://4wcgqlckaazugwzm.onion/index.php

--------BEGIN BIT KEY---------
W8roFS53BD17gnplnJH9+DESBsd8bFpGLU3Zx7u1FcuA3tivG53+dfPK1TuzasIuv5ZXutigfc+U
cpzNDZhhl0g9MOThQIuISDfvtupF/+oPnn2ABGLERFb2v1V59biOyJV391I8UOSBSjuDa2ThfLnC
jHvDtmO5ykpzn5xF2P/PNibJ6+DplDi/HInLGSMS5F3Ah/AVECfAsEfB7yGjxHL9LvgSSOycASkq
JfHs+CaSM/2pIW8WzL3tyM5GAAslFPzv+AtOj+aWfxthtdiO2ycrk6dEgdEpd8YYLnYVgaHocguB
95RHERGhYRxhVfeq4jKPnPvvQ2P945WUj6ajjQ==
--------END BIT KEY-----------
```

```
------------------------------
BEGIN FRENCH
------------------------------

S'il vous plaît soyez avisé:
Tous vos fichiers, images, documents et données ont été cryptés avec Military
Grade Encryption RSA AES-256.
Vos informations ne sont pas perdues. Mais chiffré.
Afin de vous permettre de restaurer vos fichiers, vous devez acheter Decrypter.
Suivez ces étapes pour restaurer vos fichiers.

1 * Téléchargez le navigateur Tor. (Il suffit de taper google "Télécharger Tor").
2 * Aller à l'URL: http://4wcgqlckaazugwzm.onion/index.php
3 * Achetez le Decryptor pour restaurer vos fichiers.

C'est très simple. Si vous ne croyez pas que nous pouvons restaurer vos fichiers,
alors vous pouvez restaurer 1 fichier de format d'image gratuitement.
Soyez conscient que le temps est compté. Le prix sera doublé toutes les 96 heures,
alors utilisez-le à bon escient.

Votre ID unique: J2GAK6UPOE4MK6AM

MISE EN GARDE:
N'essayez pas de modifier ou de supprimer un fichier crypté, car il sera difficile
de le restaurer.

SOUTIEN:
Vous pouvez contacter le support pour aider à déchiffrer vos fichiers pour vous.
Cliquez sur support à http://4wcgqlckaazugwzm.onion/index.php

------------------------------
END FRENCH
------------------------------
```

```
------------------------------
BEGIN ITALIAN
------------------------------

Si prega di essere avvisati:
Tutti i tuoi file, immagini, documenti e dati sono stati crittografati con Military
Grade Encryption RSA AES-256.
Le tue informazioni non sono perse. Ma crittografato.
Per poter ripristinare i tuoi file devi acquistare Decrypter.
Seguire questa procedura per ripristinare i file.

1 * Scarica il Tor Browser. (Basta digitare su google "Download Tor").
2 * Passa a URL: http://4wcgqlckaazugwzm.onion/index.php
3 * Acquista Decryptor per ripristinare i tuoi file.

È molto semplice Se non credi che possiamo ripristinare i tuoi file, puoi ripristinare
1 file di formato immagine gratuitamente.
Sii consapevole che il tempo stringe. Il prezzo sarà raddoppiato ogni 96 ore, quindi
usalo saggiamente.

Il tuo ID univoco: J2GAK6UPOE4MK6AM

ATTENZIONE:
Si prega di non provare a modificare o eliminare alcun file crittografato in quanto sarà
difficile ripristinarlo.

SUPPORTO:
È possibile contattare l'assistenza per decrittografare i file per conto dell'utente.
Clicca sul supporto in http://4wcgqlckaazugwzm.onion/index.php
------------------------------
END ITALIAN
------------------------------
```

```
------------------------------
BEGIN KOREAN
------------------------------
조언을 받으십시오 :
모든 파일, 사진 문서 및 데이터는 군용 등급 암호화 RSA AES-256으로 암호화되어 있습니다.
귀하의 정보는 손실되지 않습니다. 그러나 암호화.
파일을 복원하려면 Decrypter를 구입해야합니다.
이 단계에 따라 파일을 복원하십시오.

1 * Tor 브라우저를 다운로드하십시오. (구글에 "Tor 다운로드"만 입력하면됩니다.)
2 * URL 찾아보기 : http://4wcgqlckaazugwzm.onion/index.php
3 * 파일을 복원하려면 Decryptor를 구입하십시오.

그것은 매우 간단합니다. 파일을 복원 할 수 있다고 생각지 않으면 이미지 형식의 파일 1 개를 무료로 복원 할 수 있습니다.
시간이 똑딱 거리고 있다는 것을 알아 두십시오. 가격은 96 시간마다 두 배가되므로 현명하게 사용하십시오.

고유 ID : J2GAK6UPOE4MK6AM

주의:
암호화 된 파일을 수정하거나 삭제하지 마십시오. 복원하기가 어려울 수 있습니다.

지원하다:
지원 센터에 문의하여 파일의 암호를 해독하는 데 도움을받을 수 있습니다.
http://4wcgqlckaazugwzm.onion/index.php에서 지원을 클릭하십시오.
------------------------------
END KOREAN
------------------------------
```

همانطور که مشاهده می‌کنید، متن این فایل به چهار زبان مختلف می‌باشد. در این پیغام آمده است که تمام فایل‌ها، اسناد، تصاویر، اسناد، ویدیوها و داده‌های سیستم قربانی توسط الگوریتم AES ۲۵۶ بیتی رمزگذاری شده‌اند. در ادامه قربانی برای دریافت ابزار رمزگشایی باج‌افزار راهنمایی شده است. از قربانی خواسته شده که به آدرس وب‌سایت http://٤wcgqlckaazugwzm.onion/index.php در مرورگر Tor مراجعه کرده و ابزار را طبق دستورالعمل این وب‌سایت دریافت کند. لینک دانلود این مرورگر نیز در پیغام قرار داده شده است. در ادامه عنوان شده است که یک فایل، جهت ضمانت به قربانی به صورت رایگان رمزگشایی می‌شود. هچنین به قربانی هشدار داده شده است که در صورت عدم پرداخت باج در مدت ۹۶ ساعت، مبلغ آن به دو برابر افزایش پیدا می‌کند. آدرس شناسه قربانی نیز، در پیغام قرار داده شده است. همچنین عنوان شده است که تغییر یا حذف کردن فایل‌های رمزشده، بازیابی آن‌ها را سخت خواهد کرد.

فایل اجرایی این باج‌افزار پس از اتمام فرآیند رمزگذاری متوقف می‌شود اما از سیستم قربانی پاک نمی‌شود و درون پوشه حاوی فایل‌های باج‌افزار باقی می‌ماند.

تحلیل ایستا:

با بررسی کد فایل اجرایی باج‌افزار، نتایج زیر به دست آمد:

از قطعه کد زیر برای دریافت مسیر پوشه‌های Windows و System در سیستم عامل استفاده شده است:

```
CODE:00407118 sub_407118      proc near               ; CODE XREF: sub_407170+79↓p
CODE:00407118
CODE:00407118 Buffer          = byte ptr -108h
CODE:00407118
CODE:00407118                 push    ebx
CODE:00407119                 add     esp, 0FFFFFEFCh
CODE:0040711F                 mov     ebx, eax
CODE:00407121                 push    104h            ; uSize
CODE:00407126                 lea     eax, [esp+10Ch+Buffer]
CODE:0040712A                 push    eax             ; lpBuffer
CODE:0040712B                 call    GetWindowsDirectoryA
CODE:00407130                 mov     edx, ebx
CODE:00407132                 mov     eax, esp
CODE:00407134                 call    sub_405230
CODE:00407139                 add     esp, 104h
CODE:0040713F                 pop     ebx
CODE:00407140                 retn
CODE:00407140 sub_407118      endp
```

```
CODE:00407144 sub_407144      proc near               ; CODE XREF: sub_409520+6C↓p
CODE:00407144
CODE:00407144 Buffer          = byte ptr -108h
CODE:00407144
CODE:00407144                 push    ebx
CODE:00407145                 add     esp, 0FFFFFEFCh
CODE:0040714B                 mov     ebx, eax
CODE:0040714D                 push    104h            ; uSize
CODE:00407152                 lea     eax, [esp+10Ch+Buffer]
CODE:00407156                 push    eax             ; lpBuffer
CODE:00407157                 call    GetSystemDirectoryA
CODE:0040715C                 mov     edx, ebx
CODE:0040715E                 mov     eax, esp
CODE:00407160                 call    sub_405230
CODE:00407165                 add     esp, 104h
CODE:0040716B                 pop     ebx
CODE:0040716C                 retn
CODE:0040716C sub_407144      endp
```

از قطعه کد زیر برای دریافت مسیر پوشه Temp در سیستم عامل استفاده شده است. باج‌افزار پوشه حاوی فایل‌های خود را درون پوشه Temp می‌سازد:

```
CODE:004071A6 loc_4071A6:                             ; CODE XREF: sub_407170+29↑j
CODE:004071A6                 mov     edx, ebx
CODE:004071A8                 mov     eax, offset aTemp ; "TEMP"
CODE:004071AD                 call    sub_406EA8
CODE:004071B2                 cmp     dword ptr [ebx], 0
CODE:004071B5                 jz      short loc_4071C2
CODE:004071B7                 mov     eax, [ebx]
CODE:004071B9                 call    sub_406E84
CODE:004071BE                 test    al, al
CODE:004071C0                 jnz     short loc_4071EE
CODE:004071C2
CODE:004071C2 loc_4071C2:                             ; CODE XREF: sub_407170+45↑j
CODE:004071C2                 cmp     dword ptr ds:asc_40C078+4, 2
CODE:004071C9                 jnz     short loc_4071E7
CODE:004071CB                 mov     edx, ebx
CODE:004071CD                 mov     eax, offset aUserprofile ; "USERPROFILE"
CODE:004071D2                 call    sub_406EA8
CODE:004071D7                 cmp     dword ptr [ebx], 0
CODE:004071DA                 jz      short loc_4071E7
CODE:004071DC                 mov     eax, [ebx]
CODE:004071DE                 call    sub_406E84
CODE:004071E3                 test    al, al
CODE:004071E5                 jnz     short loc_4071EE
```

از قطعه کدهای زیر به ترتیب برای دریافت اندازه و نوع فایل‌ها، استفاده شده است:

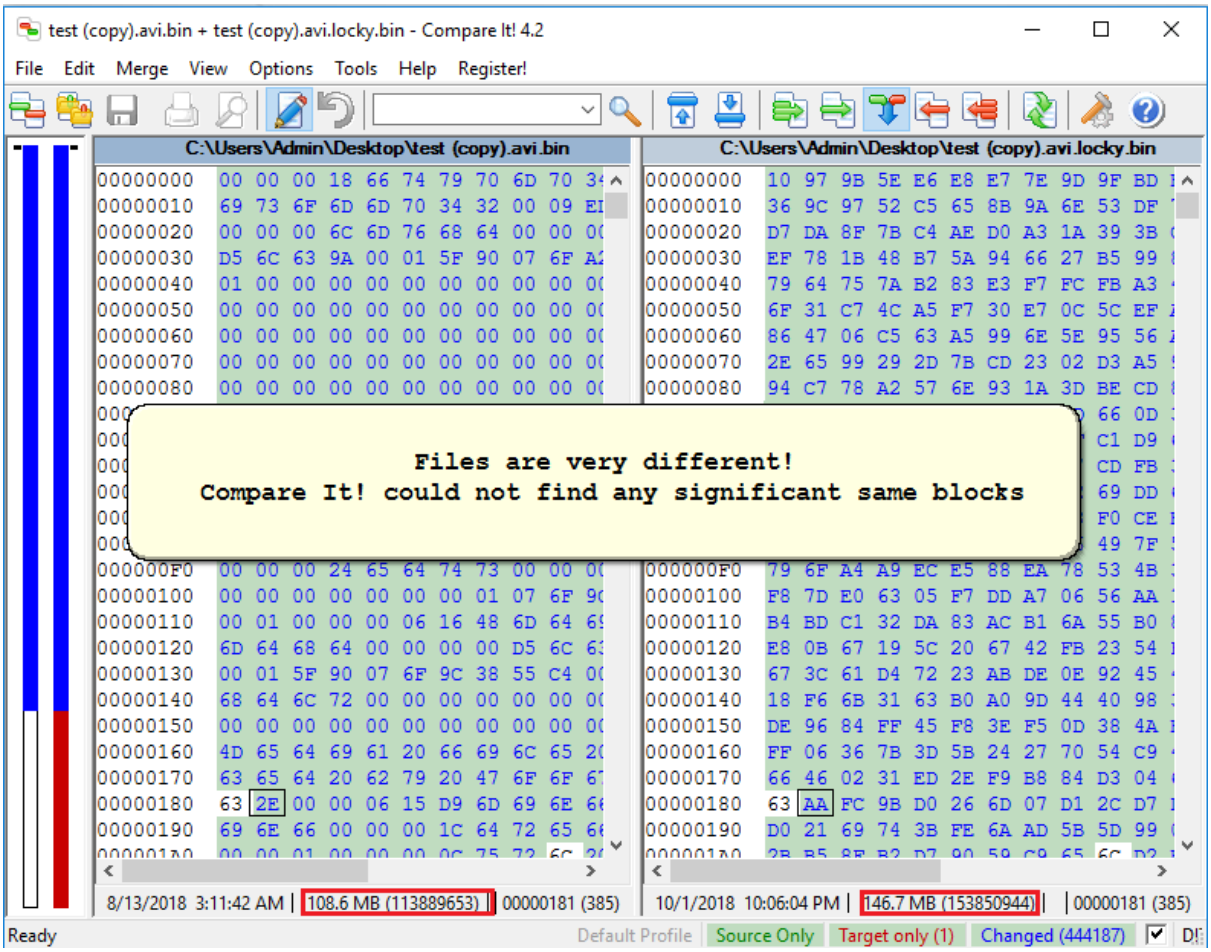
```
CODE:00403AF6 loc_403AF6:                             ; CODE XREF: CODE:00403ACD↑j
CODE:00403AF6                 mov     dword ptr [esi+24h], offset loc_403A7F
CODE:00403AFD                 mov     dword ptr [esi+20h], offset sub_403A4F
CODE:00403B04                 cmp     byte ptr [esi+48h], 0
CODE:00403B08                 jz      loc_403BBC
CODE:00403B0E                 push    0
CODE:00403B10                 push    80h
CODE:00403B15                 push    ecx
CODE:00403B16                 push    0
CODE:00403B18                 push    edx
CODE:00403B19                 push    eax
CODE:00403B1A                 lea     eax, [esi+48h]
CODE:00403B1D                 push    eax
CODE:00403B1E                 call    CreateFileA
CODE:00403B23                 cmp     eax, 0FFFFFFFFh
CODE:00403B26                 jz      loc_403C17
CODE:00403B2C                 mov     [esi], eax
CODE:00403B2E                 cmp     dword ptr [esi+4], 0D7B3h
CODE:00403B35                 jnz     loc_403BDE
CODE:00403B3B                 dec     dword ptr [esi+4]
CODE:00403B3E                 push    0
CODE:00403B40                 push    dword ptr [esi]
CODE:00403B42                 call    GetFileSize
CODE:00403B47                 inc     eax
CODE:00403B48                 jz      loc_403C17
CODE:00403B4E                 sub     eax, 81h
CODE:00403B53                 jnb     short loc_403B57
CODE:00403B55                 xor     eax, eax
```

```
CODE:00403BDE loc_403BDE:                             ; CODE XREF: CODE:00403B35↑j
CODE:00403BDE                                         ; CODE:00403B90↑j ...
CODE:00403BDE                 cmp     dword ptr [esi+4], 0D7B1h
CODE:00403BE5                 jz      short loc_403BFE
CODE:00403BE7                 push    dword ptr [esi]
CODE:00403BE9                 call    GetFileType
CODE:00403BEE                 test    eax, eax
CODE:00403BF0                 jz      short loc_403C02
CODE:00403BF2                 cmp     eax, 2
CODE:00403BF5                 jnz     short loc_403BFE
CODE:00403BF7                 mov     dword ptr [esi+20h], offset sub_403A52
```

از قطعه کد زیر برای اضافه نمودن پسوند موردنظر به فایل‌های رمزشده، استفاده شده است:

```
CODE:00403B9F loc_403B9F:                             ; CODE XREF: CODE:00403B9A↑j
CODE:00403B9F                 push    2
CODE:00403BA1                 push    0
CODE:00403BA3                 sub     eax, edx
CODE:00403BA5                 push    eax
CODE:00403BA6                 push    dword ptr [esi]
CODE:00403BA8                 call    SetFilePointer
CODE:00403BAD                 inc     eax
CODE:00403BAE                 jz      short loc_403C17
CODE:00403BB0                 push    dword ptr [esi]
CODE:00403BB2                 call    SetEndOfFile
CODE:00403BB7                 dec     eax
CODE:00403BB8                 jnz     short loc_403C17
CODE:00403BBA                 jmp     short loc_403BDE
```

بر اساس بررسی‌هایی که بر روی چند نمونه فایل رمزشده و با نمونه سالم آن‌ها انجام دادیم، متوجه شدیم این باج‌افزار تمام محتوای فایل‌های موردهدف خود را رمزگذاری می‌کند و مقدار متغیری با توجه به حجم فایل، به انتهای آن‌ها اضافه می‌کند. تصویر زیر مربوط به مقایسه یک نمونه از این فایل‌ها می‌باشد:



همانطور که در تصویر بالا مشاهده می‌کنید، این فایل به طور کامل رمزگذاری شده است. حجم آن قبل از رمزگذاری ۱۰۸.٦ مگابایت بوده است و پس از رمزگذاری به ۱٤٦.۷ مگابایت تغییر پیدا کرده است که با کادر قرمز رنگ در تصویر مشخص است.

فایل‌های با حجم چند صد مگابایت به طور کامل پاک می‌شوند و یک فایل کپی با نام و آیکن آن‌ها ایجاد می‌شود که محتوای آن، پیغام باج خواهی باج‌افزار می‌باشد.

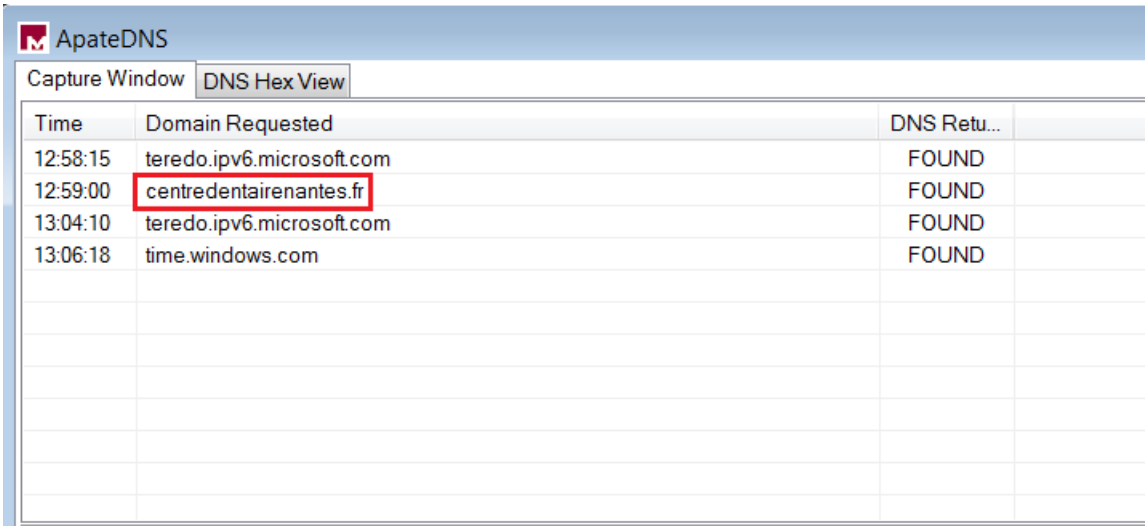
تحلیل ترافیک شبکه :

پس از بررسی وضعیت ترافیک شبکه ایجاد شده در سندباکس‌های آنلاین، پس از اجرای باج‌افزار، نتایج زیر حاصل گردید:

درخواست DNS:

دامنه	آدرس آی پی	کشور
centredentairenantes.fr	۲۱۷.۱۶۰.۰.۷۸	Germany

نتایج تحلیل ما در محیط آزمایشگاهی نیز، این اطلاعات را نشان می‌دهد. درخواست DNS مذکور با کادر قرمز رنگ در تصویر زیر مشخص شده است:



بر اساس گزارش سایت id-ransomware.blogspot.ru این آدرس مربوط به سرور فرمان و کنترل (C&C) باج‌افزار می‌باشد که از طریق پورت ۸۰ و پروتکل TCP با آن ارتباط برقرار می‌کند. بر اساس بررسی‌های ما در محیط آزمایشگاهی نیز، این باج‌افزار فقط در حالت اتصال به اینترنت فعال می‌شود و از آنجا که ارتباط آن فقط با آدرس ذکرشده در بالا صورت می‌گیرد، صحت این موضوع را تأیید می‌کند.

خروجی سامانه VirusTotal :

در حال حاضر تنها تعداد ۴۳ مورد از ۶۹ آنتی ویروس و آنتی بدافزار موجود در سامانه VirusTotal قادر به شناسایی این باج‌افزار بوده وآن را حذف یا غیرفعال می‌کنند.

Ad-Aware	Trojan.GenericKD.40350015	AhnLab-V3	Trojan/Win32.PyLocky.C2265541
ALYac	Trojan.Ransom.PyLocky	Avast	FileRepMalware
AVG	FileRepMalware	Avira	TR/Ransom.mnafx
AVware	Trojan.Win32.Generic!BT	BitDefender	Trojan.GenericKD.40350015
CAT-QuickHeal	Trojan.IGENERIC	ClamAV	Win.Trojan.Agent-6625864-0
Cylance	Unsafe	Cyren	W32/Trojan.HOXL-9323
DrWeb	Trojan.Encoder.25732	Emsisoft	Trojan.GenericKD.40350015 (B)
eScan	Trojan.GenericKD.40350015	ESET-NOD32	Python/Filecoder.BL
F-Secure	Trojan.GenericKD.40350015	Fortinet	Python/Filecoder.BL!tr
GData	Trojan.GenericKD.40350015	Ikarus	Trojan-Ransom.Locky
K7AntiVirus	Trojan (00539a1d1)	K7GW	Trojan (00539a1d1)
Kaspersky	Trojan-Ransom.Python.Agent.p	Malwarebytes	Ransom.Locky
MAX	malware (ai score=100)	McAfee	Ransomware-Locky
McAfee-GW-Edition	Ransomware-Locky	Microsoft	Trojan:Win32/Tiggre!rfn
NANO-Antivirus	Trojan.Win32.Filecoder.fgditz	Palo Alto Networks	generic.ml
Panda	Trj/CI.A	Qihoo-360	Win32/Trojan.Ransom.dab
Sophos AV	Troj/Ransom-EZJ	Sophos ML	heuristic
Symantec	Trojan Horse	TACHYON	Ransom/W32.PyLocky.2396720
TrendMicro	Ransom_PYLOCKY.B	TrendMicro-HouseCall	Ransom_PYLOCKY.B
VIPRE	Trojan.Win32.Generic!BT	ViRobot	Trojan.Win32.S.PyLocky.7759952
Webroot	W32.Trojan.Gen	Zillya	Trojan.GenericKD.Win32.122674
ZoneAlarm	Trojan-Ransom.Python.Agent.p		

خروجی سامانه ویروس‌کاو مرکز ماهر :

در حال حاضر ۸ مورد از ۱۱ آنتی ویروس و آنتی بدافزار موجود در سامانه ویروس‌کاو قادر به شناسایی این باج‌افزار بوده وآن را حذف یا غیرفعال می‌کنند.

نتیجه اسکن 194d1ccff7ab23003b34f5984f396e6d4aaf2615bfb02d5e28cd0b8513c57c87.bin

آنتی‌ویروس	نسخه آنتی‌ویروس	نتیجه اسکن
پادویش	2.3.190.2675	Clean
sophos	9.15.0	Clean
f_secure	11.00	Dangerous: Trojan.GenericKD.40350015
kaspersky	5.5	Dangerous: Trojan-Ransom.Python.Agent.P
eset	4.5.3.38828	Dangerous: Python/Filecoder.BL
drweb	11.0.1.1607061217	Dangerous: Trojan.Encoder.25732
clam_av	0.99.2	Dangerous: Win.Trojan.Agent-6625864-0
comodo	1.1.268025.1	Dangerous: Malware
bitdefender	11.0.1.18	Dangerous: Trojan.GenericKD.40350015
avast	2.1.2	Clean
symantec	7.9.0.30	Dangerous: Trojan Horse