باسمه تعالی

تحلیل فنی باج افزار KeyPass

مقدمه :

مشاهده و رصد فضای سایبری در زمینه باج‌افزار، از شروع فعالیت نمونه جدیدی به نام KeyPass خبر می‌دهد. بررسی‌ها نشان می‌دهد که فعالیت این باج‌افزار در اوایل ماه آگوست سال ۲۰۱۸ میلادی شروع شده است و به نظر می‌رسد از خانواده باج‌افزار STOP باشد. این باج‌افزار از الگوریتم رمزنگاری AES-۲۵۶ برای رمزگذاری فایل‌ها استفاده می‌کند و پس از رمزگذاری، پسوند فایل‌ها را به ".KEYPASS " تغییر می‌دهد و از قربانیان تقاضای پرداخت مبلغ ۳۰۰ دلار به عنوان باج می‌کند. در حال حاضر روش ورود یا انتشار این باج‌افزار دقیقاً مشخص نیست اما طبق گزارشات بدست آمده از کاربران در نقاط مختلف جهان، احتمالاً از طریق وب‌سایت هایی که نرم افزارهای کرک شده و یا قفل شکسته ارائه می‌دهند منتشر می‌شود. ضمناً باج‌افزار مورد در حال حاضر اشاره فاقد رمزگشا بوده و تنها راه مقابله با آن، بازگردانی اطلاعات از طریق فایل‌های پشتیبان می‌باشد.

مشخصات فایل اجرایی :

نام فایل	ee۷٤c٦۳faa۲eb۹۷۰۹b۱d۷۳۸۷٦۲e۲۸۰۷۲aece۲e۷b۹eeffc٥۹۱۳eb٦a٥fd۱٥٦٤۷٥۲.exe STOP.exe Keypass.exe vatup.exe ٥.exe
MD٥	۹۰۱d۸۹۳f٦٦٥c٦f۹۷٤۱aa۹٤۰e٥f۲۷٥۹٥۲
SHA-۱	۳b٥۳٦۹c۰aeffe٥c۰d۰b۱٦٤a۳d۹۰ec۲٤٥b۰۹۳٦۷٤d
SHA-۲٥٦	ee۷٤c٦۳faa۲eb۹۷۰۹b۱d۷۳۸۷٦۲e۲۸۰۷۲aece۲e۷b۹eeffc٥۹۱۳eb٦a٥fd۱٥٦٤۷٥۲
اندازه فایل	۲.۸۲ MB
کامپایلر	VC۸ -> Microsoft Corporation
آیکن فایل اجرایی	

فایل اجرایی این باج افزار دارای پنج بخش است :

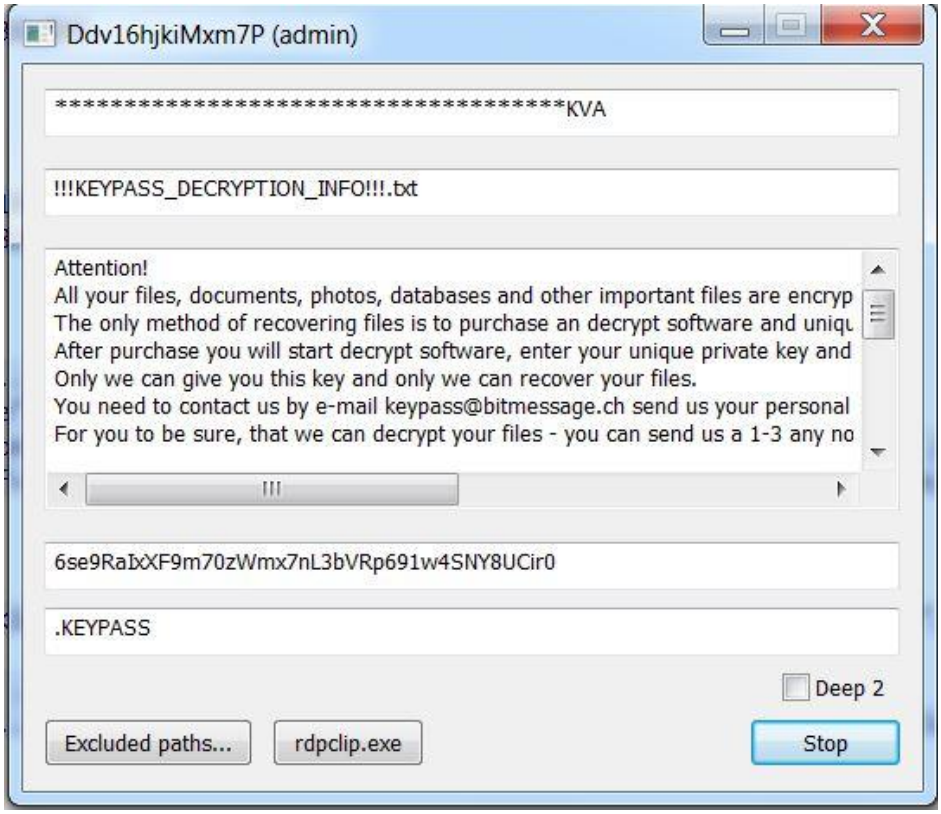
نام بخش	آنتروپی	آدرس مجازی	اندازه مجازی	اندازه خام
.text	٦.٦٣	٤٠٩٦	٢٠٨١٢٤٩	٢٠٨١٢٨٠
.rdata	٥.١١	٢٠٨٨٩٦٠	٤٨٨٨٩٤	٤٨٨٩٦٠
.data	٤.٩٨	٢٥٨٠٤٨٠	٨٧٥٩٦	٥٠٦٨٨
.rsrc	٤.٥١	٢٦٧٠٥٩٢	١٧٦٩٩٢	١٧٧١٥٢
.reloc	٦.٥	٢٨٥٠٨١٦	١٥٩٢٥٢	١٥٩٧٤٤

تحلیل پویا :

برای بررسی عمیق‌تر باج‌افزار KeyPass، فایل اجرایی آن را در محیط آزمایشگاهی اجرا کردیم تا عملکرد باج‌افزار را از نزدیک مورد بررسی قرار دهیم. نتایج بدست آمده حاکی از آن است که فرآیند اجرای این باج‌افزار نسبت به سایر باج‌افزارها اندکی متفاوت و پیچیده می‌باشد. باج‌افزار KeyPass پس از ورود به سیستم، ارتباط با سرور فرمان و کنترل بررسی محیط سیستم، اقدام به رمزگذاری فایل ها با استفاده از الگوریتم رمزنگاری خود می کند. از آنجایی که تمام فایل‌های موجود، رمزگذاری نمی‌گردند، به نظر می‌رسد استثنائاتی در فرآیند رمزگذاری این باج‌افزار وجود دارد. این باج‌افزار حتی فایل اجرایی نرم افزارها و میانبرهای آن ها را هم رمزگذاری و غیرقابل دسترس می نماید.

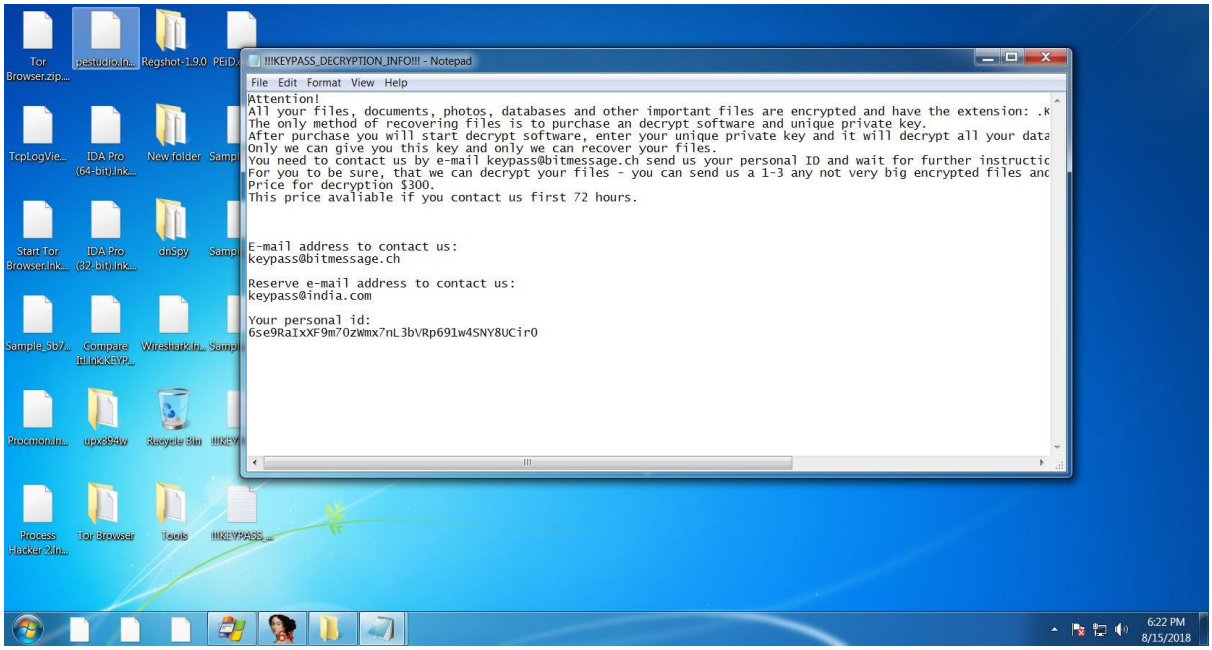
باج‌افزار KeyPass ابتدا فایل اجرایی خود را از مسیر جاری حذف نموده و یک نسخه از آن را در مسیر C:\Users\user\AppData\Local قرار می‌دهد که فرآیند اجرای باج‌افزار از آن مسیر ادامه می‌یابد. سپس فایل حاوی پیغام باج‌خواهی خود که به صورت یک فایل متنی و با عنوان !!!KEYPASS_DECRYPTION_INFO!!!.txt می‌باشد را در دایرکتوری‌های مختلفی از جمله Program Files و همچنین دسکتاپ قرار می‌دهد و پس از آن رابط گرافیکی خود را به کاربر نمایش می‌دهد. ضمناً باج‌افزار در دایرکتوری Startup ویندوز نیز قرار می‌گیرد تا با هر بار راه اندازی ویندوز، مجدداً اجرا گردد. این تغییرات در رجیستری نیز اعمال می‌گردند.

001FFCF8	UNICODE	Software\Microsoft\Windows\CurrentVersion\Policies\Comdlg32
001FFC08	UNICODE	Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
001FFC80	UNICODE	Software\Microsoft\Windows\CurrentVersion\Policies\Network
0023F736	UNICODE	]Software\Microsoft\Windows\CurrentVersion\Run

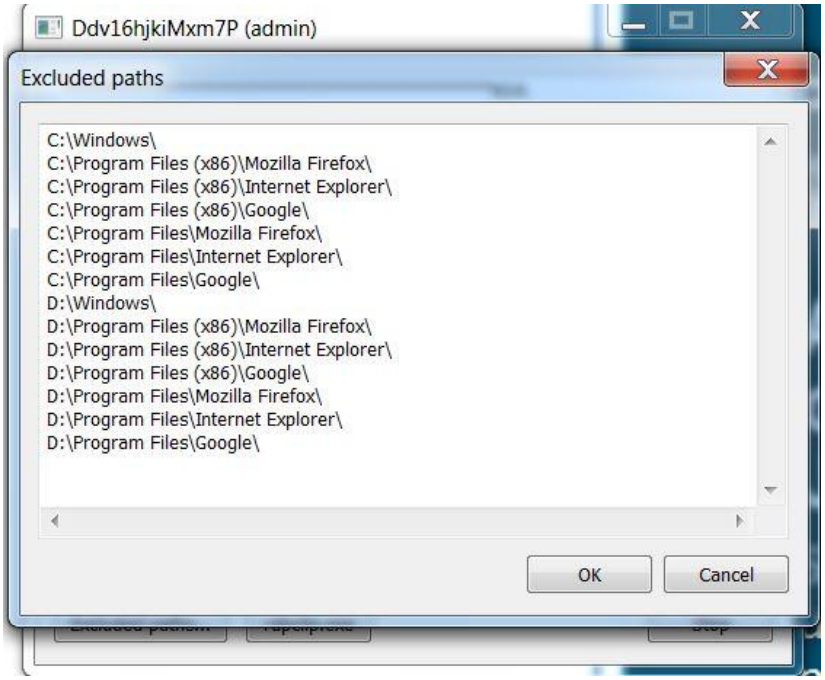


لازم به ذکر است که این باج‌افزار پس از اتمام فرآیند رمزگذاری، پسوند KEYPASS. را به انتهای نام فایل‌های رمز شده اضافه می‌کند.

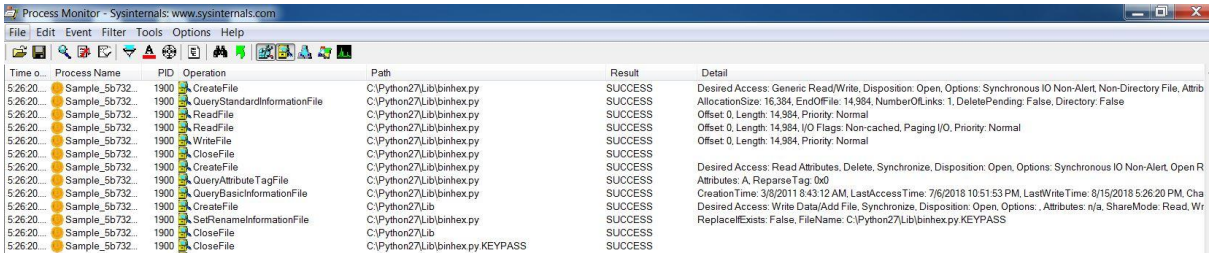
همانطور که قابل ملاحظه است در پیام باج‌خواهی این باج‌افزار به این مطلب اشاره شده که همه فایل‌های مهم سیستم رمز شده‌اند و قربانی به منظور بازگرداندن فایل‌های خود، می‌بایست رمزگشا را از مهاجم خریداری نماید. در ادامه نیز با اشاره به اینکه قربانی می‌تواند ۱ الی ۳ فایل که حجم زیادی نداشته باشند را همراه با شناسه ای که باج‌افزار به قربانی اختصاص داده است، به یکی از ایمیل‌های keypass@bitmessage.ch یا keypass@india.com ارسال نموده و به صورت رایگان فایل اصلی و غیر رمز شده خود را دریافت کند. همچنین مهاجم، مبلغ درخواستی باج را ۳۰۰ دلار اعلام نموده است. بدیهی است که ایمیل دوم به عنوان ایمیل رزرو در نظر گرفته شده است و اگر قربانی در برقراری ارتباط با ایمیل اول موفق نبود، می‌تواند ایمیل دوم را امتحان کند. تصویر زیر پیغام‌خواهی باج‌افزار KeyPass را نشان می‌دهد :



همانطور که پیشتر اشاره شد، این باج‌افزار استثنائاتی را در فرآیند رمزگذاری خود رعایت می‌کند و این استثنائات دایرکتوری‌های مربوط به مرورگرهای نصب شده بر روی سیستم و نیز دایرکتوری Windows می‌باشند. نکته ای که می‌توان یادآور شد آن است که این باج‌افزار دایرکتوری‌های مذکور را در درایوهای C و D در نظر گرفته است. بنابراین شرایطی در آن قربانی ویندوز خود را در درایو D نصب کرده باشد نیز در نظر گرفته شده است.

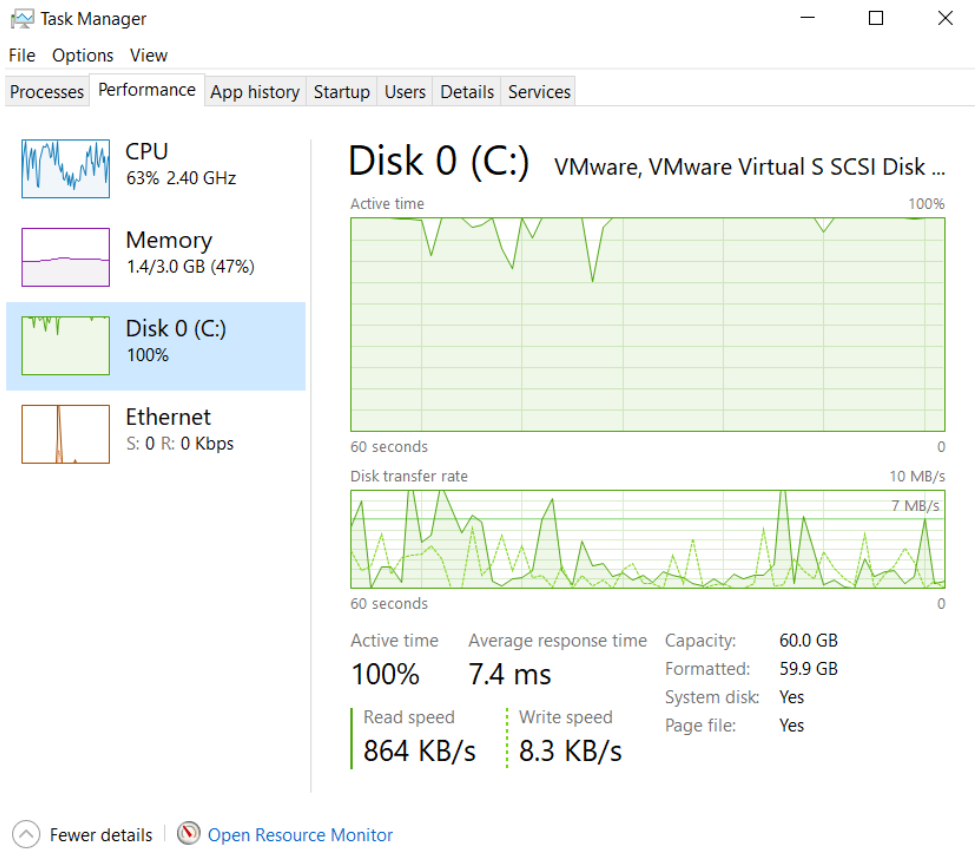


بررسی فعالیت‌های این باج‌افزار در سیستم، نحوه انجام فرآیند رمزگذاری برای هر فایل را آشکار می‌سازد.



همانطور که در تصویر بالا قابل ملاحظه است، باج‌افزار فایل هدف را با دسترسی خواندن و نوشتن گشوده و اندازه فایل که در حافظه اشغال شده است را پرسیده و سپس انتهای فایل را معین نموده است. در ادامه، باج‌افزار از ابتدای همان فایل تا انتهای فایل را می‌خواند و به همان اندازه نیز در فایل می‌نویسد که این بدین معنی است که فرآیند رمزگذاری محتوای فایل انجام شده است. سپس فایل را بسته و آخرین اطلاعات مربوط به آن که به روز شده است را می‌پرسد و پسوند KEYPASS. را به انتهای همان فایل اضافه می‌کند و سپس سراغ فایل بعدی می‌رود و این عمل را بر روی تمام فایل‌های هدف تکرار می‌کند.

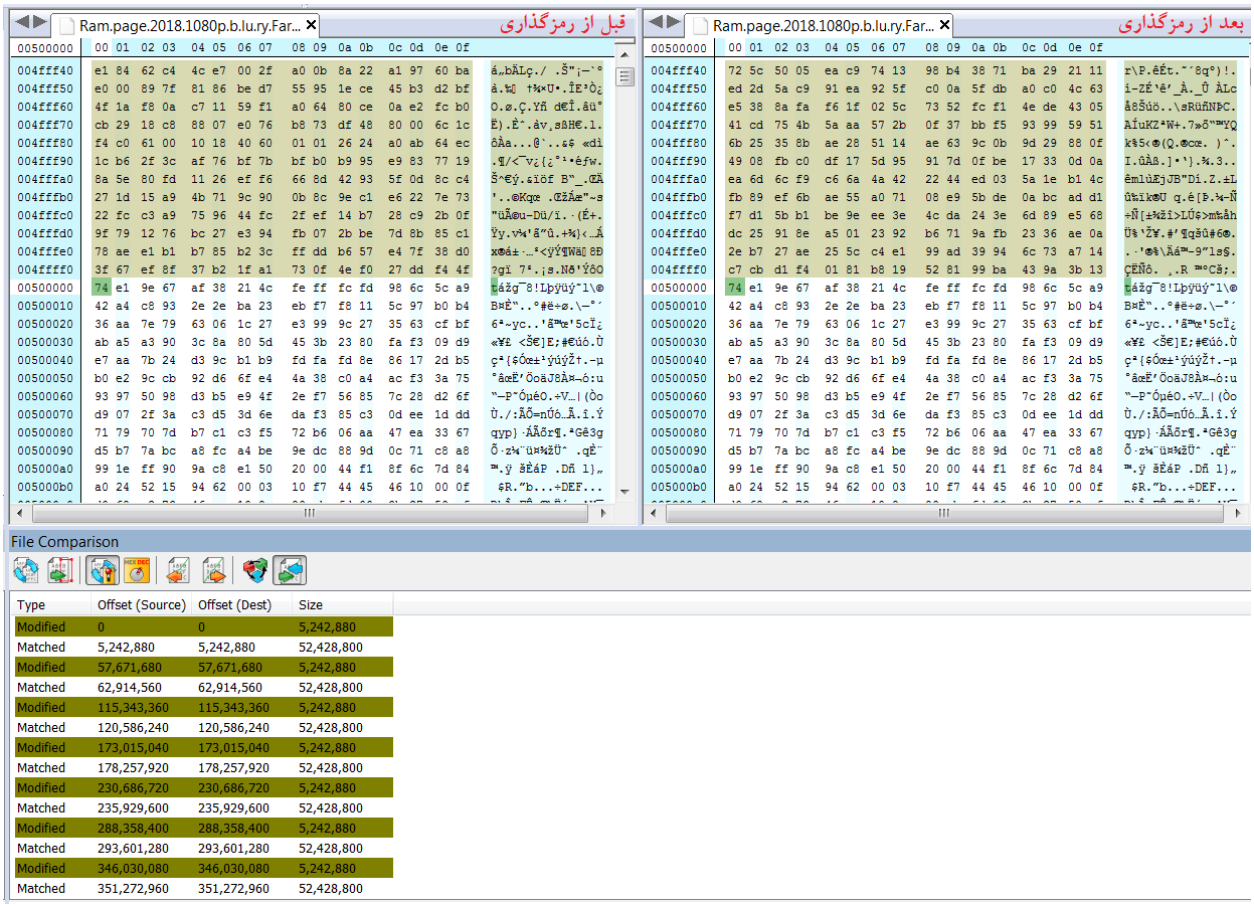
طبق بررسی‌های صورت گرفته، سرعت رمزگذاری فایل‌ها ارتباط مستقیمی با منابع سیستم قربانی دارد. در آزمایش‌های صورت گرفته، طبق تصویر زیر، باج‌افزار KeyPass بیش از همه، دیسک را درگیر می‌کند. لذا هرچه سرعت خواندن/نوشتن دیسک بالاتر باشد، فرآیند رمزگذاری سریعتر اتفاق می‌افتد. اما بطور میانگین این مدت زمان برای دیسکی با ظرفیت ۱۰۰ گیگابایت بین ۲ تا ٤ دقیقه است.



تحلیل ایستا:

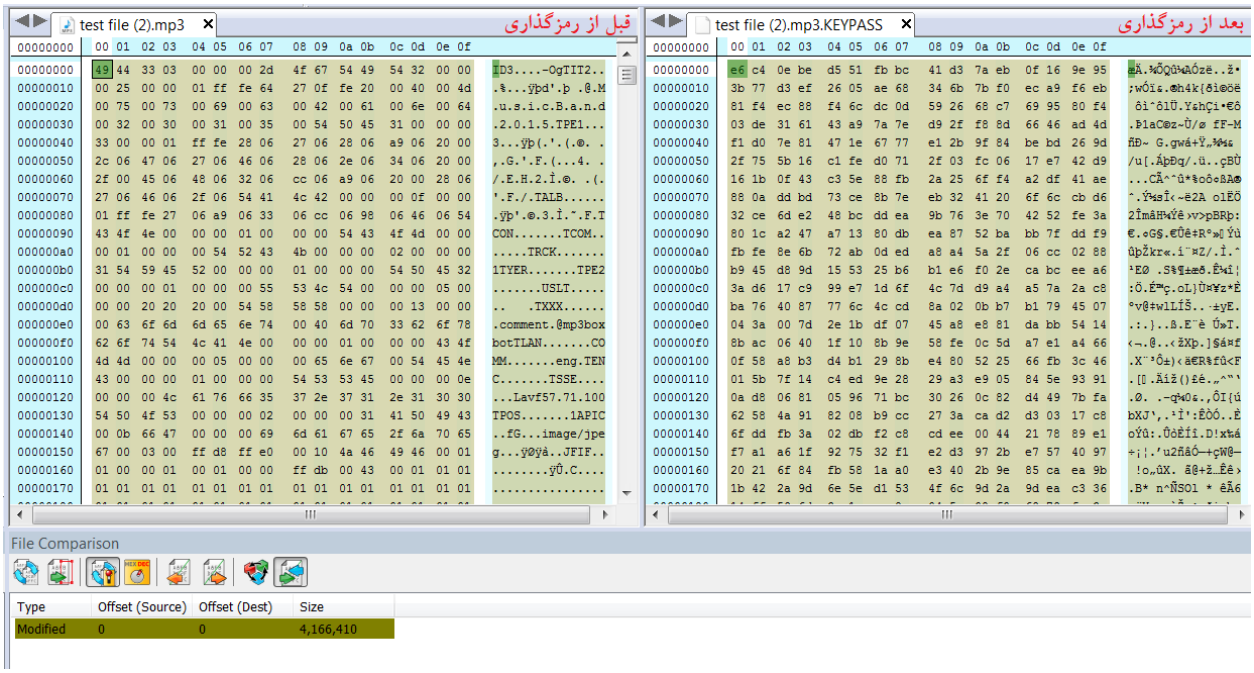
با بررسی بیشتر کد های باج افزار به نتایج زیر دست یافتیم.

طبق بررسی‌هایی که بر روی فایل‌های مختلف قبل و بعد از رمزگذاری انجام دادیم شاهد این بودیم که باج‌افزار KEYPASS تنها ساختار فایل‌هایی را که حجم آن‌ها کمتر از ۵.۲۴۲.۸۸۰ بایت است را به طور کامل تغییر می‌دهد و فایل‌هایی که حجم آن‌ها از این مقدار بیشتر است، را بدین صورت رمزگذاری می‌کند که ۵.۲۴۲.۸۸۰ بایت ابتدای فایل را تغییر می‌دهد و سپس در صورت حجیم بودن فایل، ۵.۲۴۲.۸۸۰ بایت ادامه‌ی ساختار آن را تغییری نمی‌دهد و دوباره ۵.۲۴۲.۸۸۰ بایت دیگر را تغییر می‌دهد، این روش رمزگذاری ساختار فایل تا انتهای آن ادامه می‌یابد. تصاویر زیر نمونه‌ای از تغییرات ساختار فایل‌ها را نشان می‌دهد :



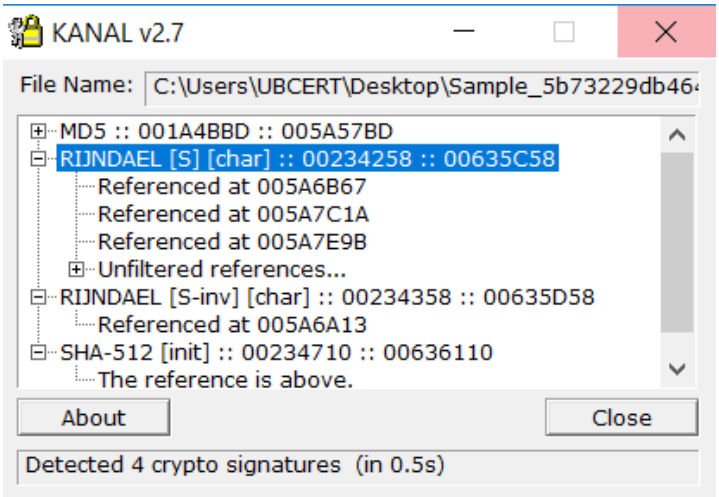
Type	Offset (Source)	Offset (Dest)	Size
Modified	0	0	5,242,880
Matched	5,242,880	5,242,880	52,428,800
Modified	57,671,680	57,671,680	5,242,880
Matched	62,914,560	62,914,560	52,428,800
Modified	115,343,360	115,343,360	5,242,880
Matched	120,586,240	120,586,240	52,428,800
Modified	173,015,040	173,015,040	5,242,880
Matched	178,257,920	178,257,920	52,428,800
Modified	230,686,720	230,686,720	5,242,880
Matched	235,929,600	235,929,600	52,428,800
Modified	288,358,400	288,358,400	5,242,880
Matched	293,601,280	293,601,280	52,428,800
Modified	346,030,080	346,030,080	5,242,880
Matched	351,272,960	351,272,960	52,428,800

تصویر ۱: فایل با حجم بیشتر از ۵.۲۴۲.۸۸۰ بایت که طبق روشی که اشاره نمودیم ساختار فایل‌ها را تغییر کرده است.

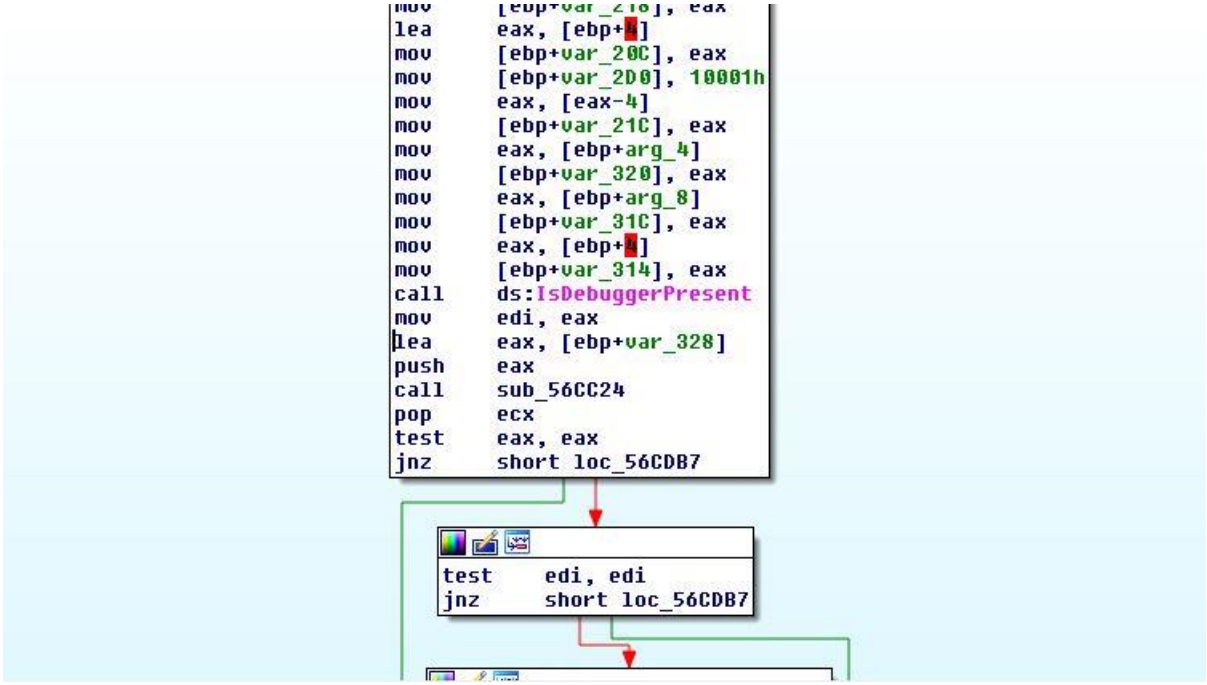


تصویر ۲: فایل با حجم کمتر از ۵.۲۴۲.۸۸۰ بایت که تمام ساختار آن تغییر کرده است.

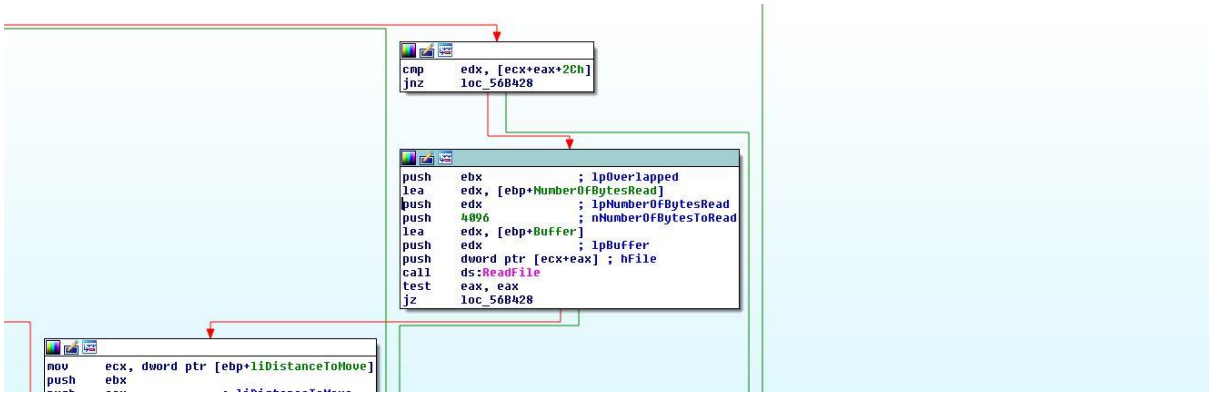
همانطور که در مقدمه اشاره شد باج افزار KeyPass از الگـوریتم رمزنگـاری AEC (Rijndael) – ۲۵۶ بـرای رمزگذاری فایل‌ها استفاده می‌کند.



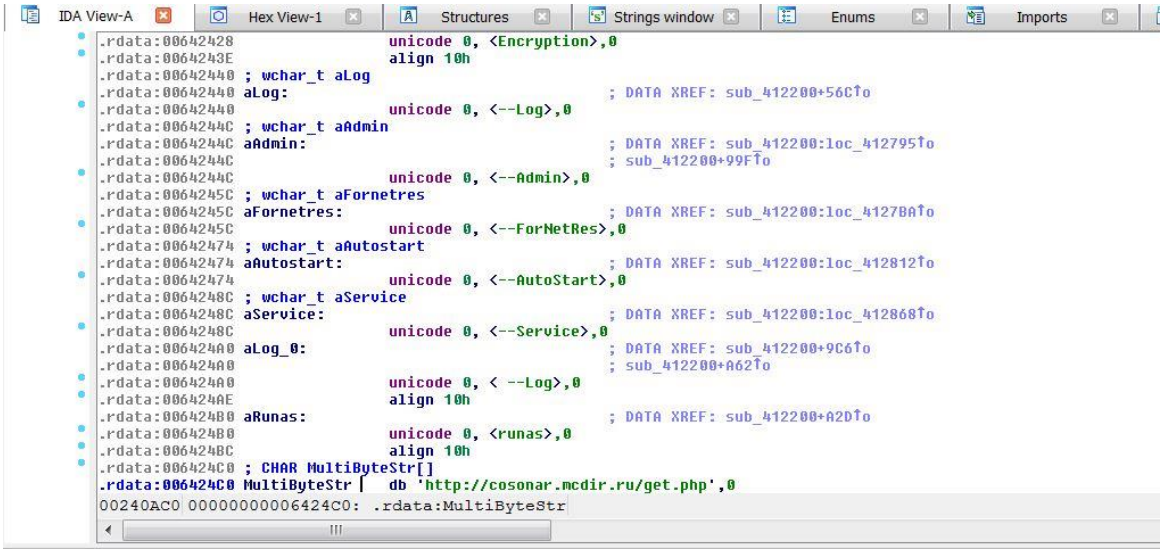
همچنین نتایج بدست آمده نشان می‌دهد که این باج‌افزار از تکنیک آنتی دیبـاگ (ضـد مهندسـی معکـوس) استفاده می‌کند و در صورتی که دیباگر در سیستم در حالت اجرا باشد این باج‌افزار، اجرا نخواهد شد.



همانطور که گفته شد باج افزار در هنگام رمزگذاری فایل‌ها، میزان فضای اشغال شده توسط فایل را در حافظه مشخص می‌کند. بررسی کدمنبع باج‌افزار گویای این مطلب است که در حالت عادی ۴۰۹۶ کیلوبایت فضای اشغال شده توسط فایل هدف در نظر گرفته می‌شود و در شرایط خاصی نیز این عدد تغییر می‌کند که احتمالا بسته به پارامترهای دیگر مربوط به فایل هدف از جمله حجم بالای آن است.



در ادامه به رشته‌های جالب توجهی برخوردیم که در تصویر زیر نمایان هستند:



همانطور که در تصویر بالا قابل ملاحظه است، رشته‌هایی نظیر --Log ، --Admin، --ForNetRes و ... و در انتها نیز آدرس http://cosonar.mcdir.ru/get.php جلب توجه می‌کنند.

با توجه به بررسی فرآیندهای اجرا شده در سیستم توسط این باج‌افزار، مشخص می‌گردد که این رشته‌های متنی برای باج‌افزار همانند یک سوئیچ خط فرمان کاربرد دارند و هر کدام از موارد بالا کارایی خاص خود را دارند.

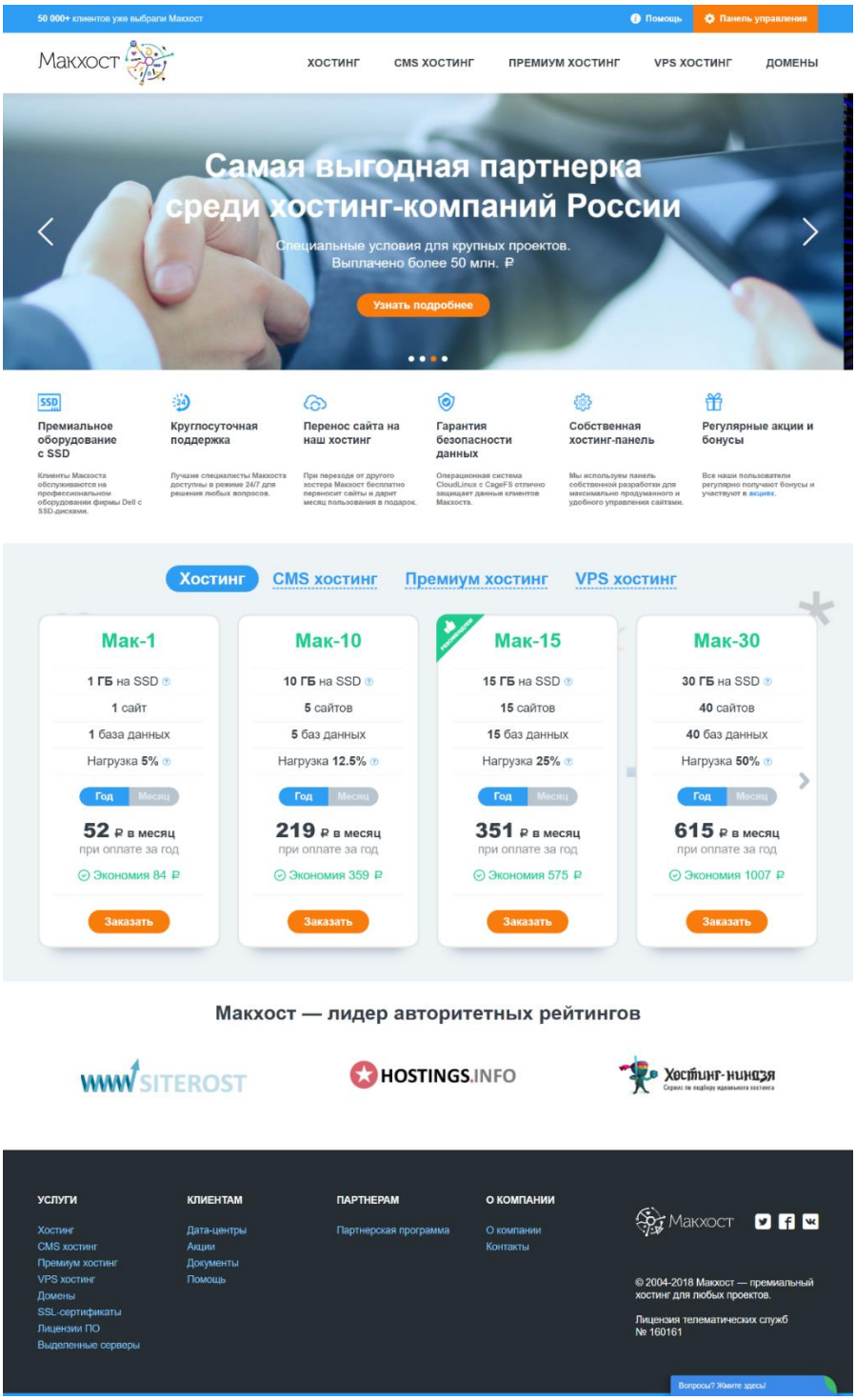
- Sample_٥b٧٣٢٢٩db٤٦٤a٩٦eb٦f٦٥٠٥c.exe ١٤٧٢
  - Sample_٥b٧٣٢٢٩db٤٦٤a٩٦eb٦f٦٥٠٥c.exe ٨٦٤
    - Sample_٥b٧٣٢٢٩db٤٦٤a٩٦eb٦f٦٥٠٥c.exe ٢٢٤٨ *--Admin*
      - Sample_٥b٧٣٢٢٩db٤٦٤a٩٦eb٦f٦٥٠٥c.exe ٢٤٨٨ *--ForNetRes*
        x٥١٧٤v ٤h٠٠٣xJ٠iyhUfHQ٨W٦o٠RDSicmSfg٧٢KVA
        ٦se٩RaIxXF٩m١٧٠zWmx١٧nL٣٣bVRp٦٩١w٤SNY٨UCir٠
        - Sample_٥b٧٣٢٢٩db٤٦٤a٩٦eb٦f٦٥٠٥c.exe ٢٦٣٢ *--Service*
          ٢٤٨٨x٥١٧٤v ٤h٠٠٣xJ٠iyhUfHQ٨W٦o٠RDSicmSfg٧٢KVA
          ٦se٩RaIxXF٩m١٧٠zWmx١٧nL٣٣bVRp٦٩١w٤SNY٨UCir٠
      - Sample_٥b٧٣٢٢٩db٤٦٤a٩٦eb٦f٦٥٠٥c.exe ٢٥٢٠ *--Service* ٢٢٤٨
        x٥١٧٤v ٤h٠٠٣xJ٠iyhUfHQ٨W٦o٠RDSicmSfg٧٢KVA
        ٦se٩RaIxXF٩m١٧٠zWmx١٧nL٣٣bVRp٦٩١w٤SNY٨UCir٠
    - cmd.exe ١٥١٢ *cmd /c ""C:\Users\user\AppData\Local\Temp\delself.bat""*

بنابراین، می‌توان نتیجه گرفت که آدرس موجود مربوط به سرور فرمان و کنترل باج‌افزار می‌باشد و هرکدام از رشته‌های موجود به مثابه یک دستور به باج‌افزار می‌باشند.

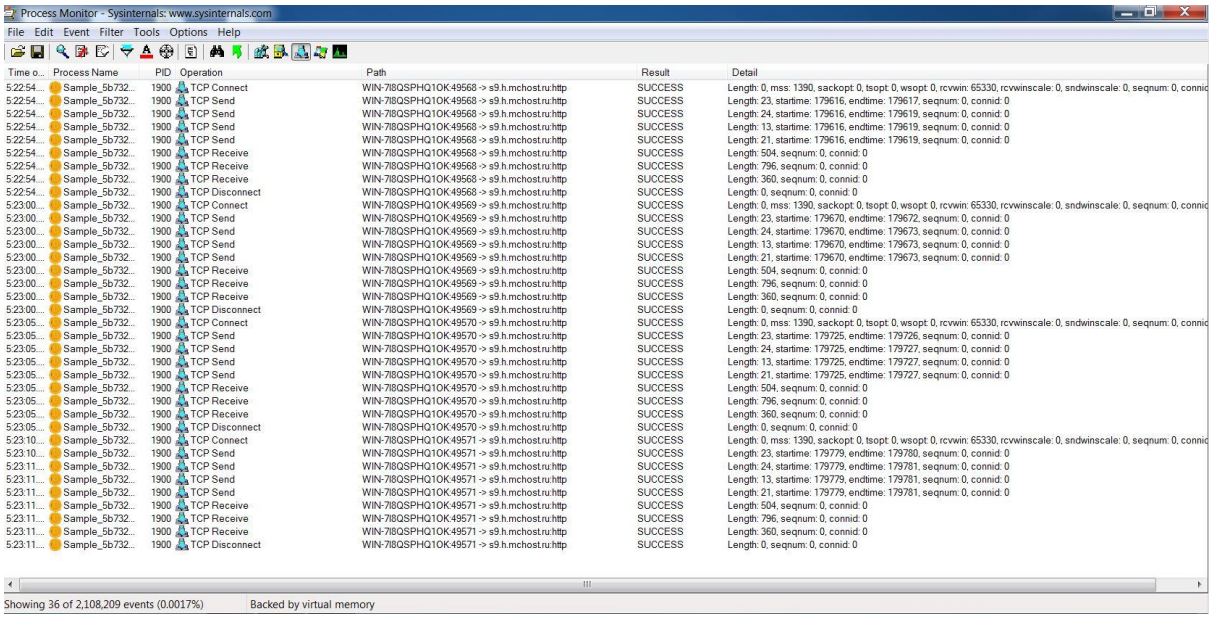
همچنین شایان ذکر است که باج‌افزار با انداختن فایل delself.bat در دایرکتوری Temp فایل اجرایی خود را از سیستم قربانی حذف می‌کند.

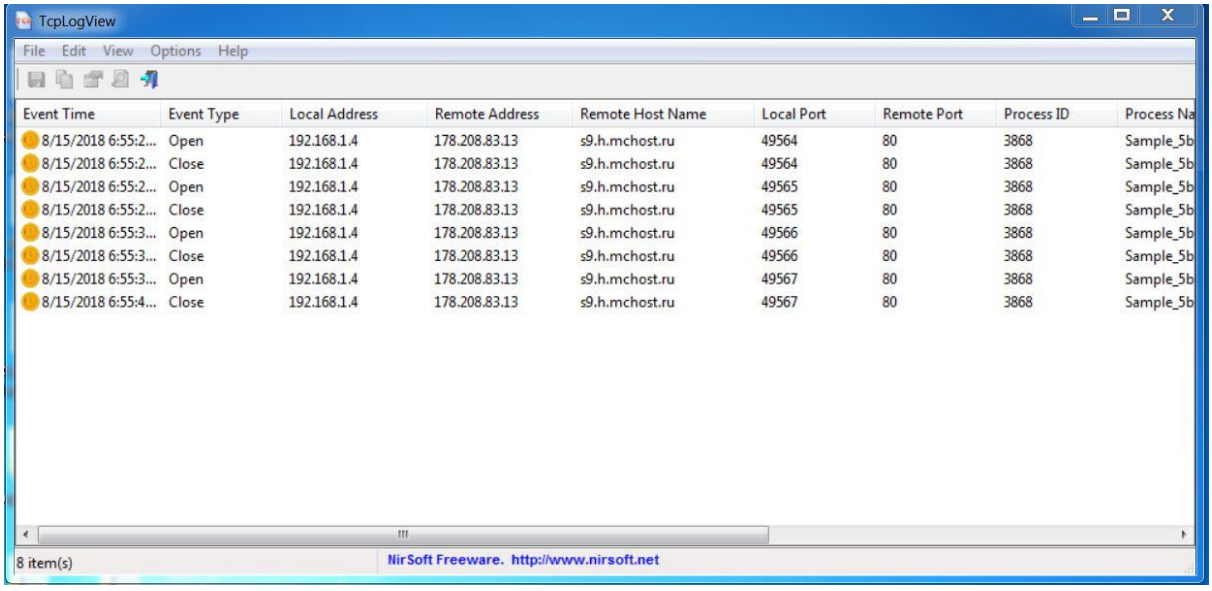
تحلیل ترافیک شبکه :

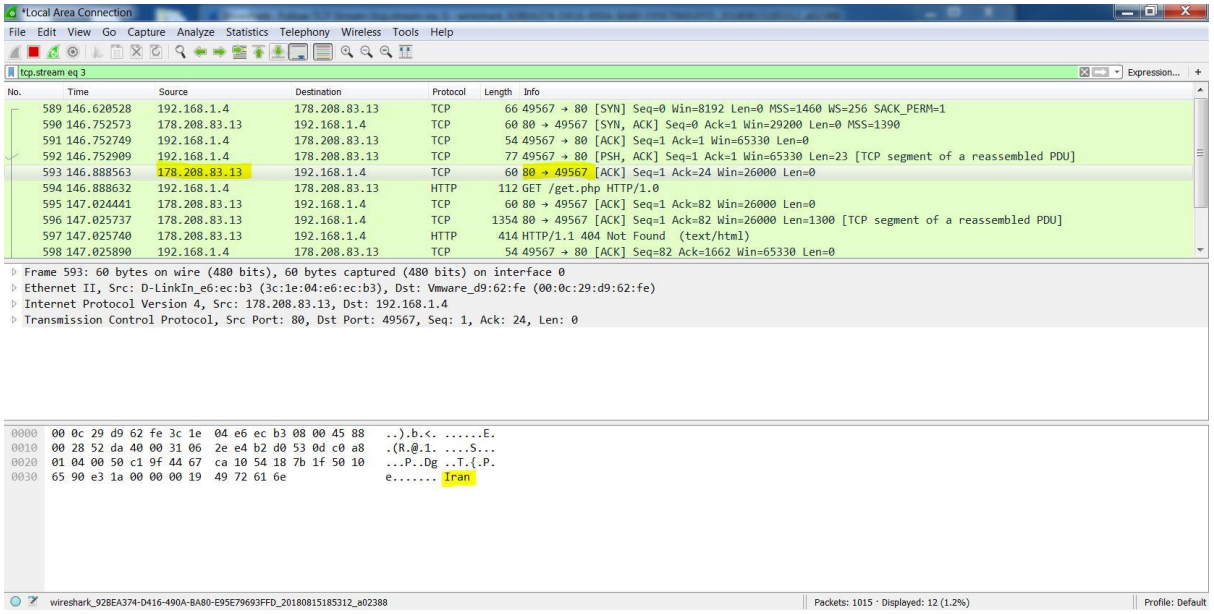
ترافیک شبکه ایجاد شده توسط باج‌افزار KeyPass نکات جالب توجهی دارد که از جمله می‌توان به اتصال این باج‌افزار به سایت خدمات هاستینگ در روسیه به نشانی https://mchost.ru از طریق پورت ۸۰ اشاره نمود. البته گفتنی است که باج‌افزار به میزبانی که این شرکت ارائه می‌دهد، متصل می‌گردد. تصویر زیر صفحه اول وب‌سایت مورد اشاره را نشان می‌دهد.



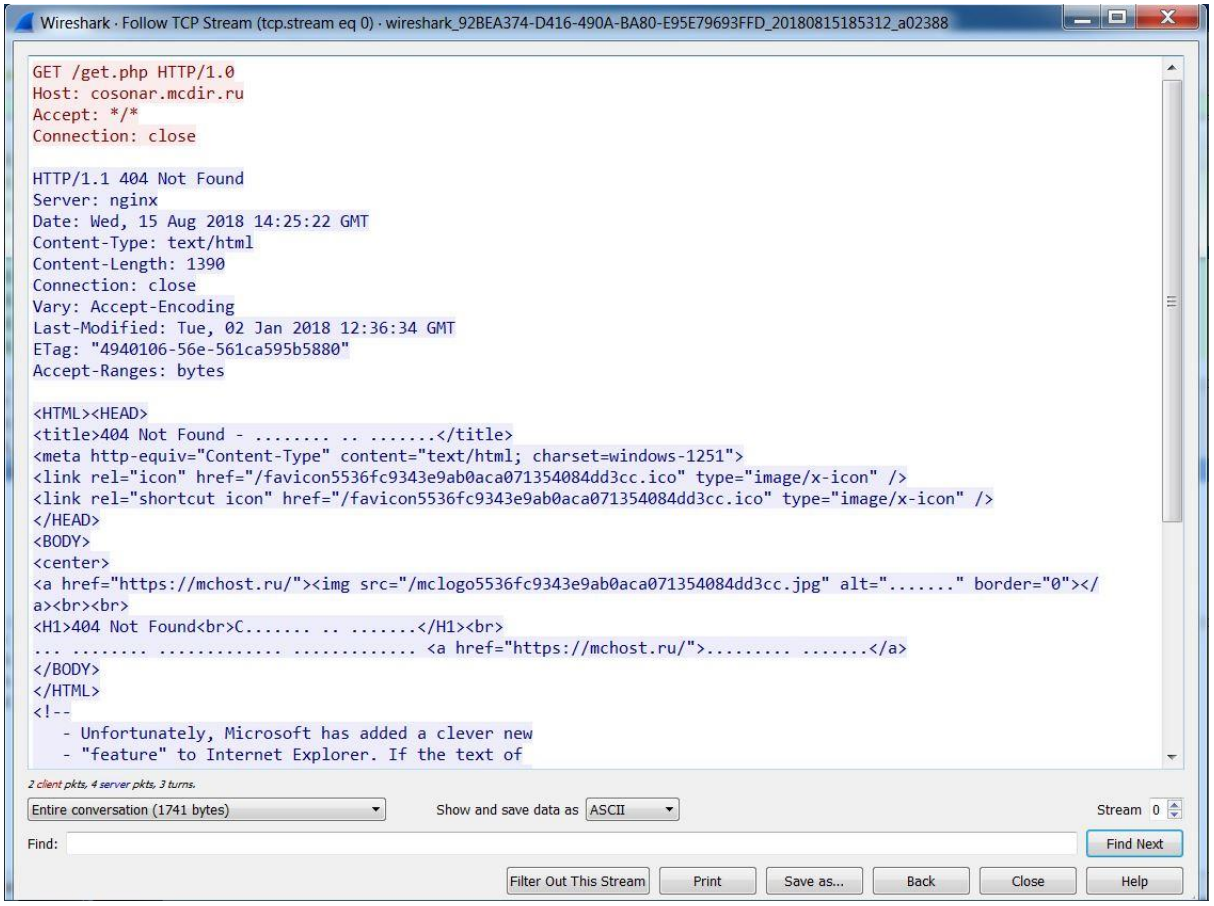
بررسی فعالیت باج‌افزار در سیستم و خروجی Wireshark و TCPLogView این موضوع را تایید می‌کنند. همانطور که در تصاویر زیر نمایان است، این باج افزار با سروری از همین شرکت خدمات دهنده به آدرس s9.h.mchost.ru و آی پی ۱۷۸.۲۰۸.۸۳.۱۳ در ارتباط است.





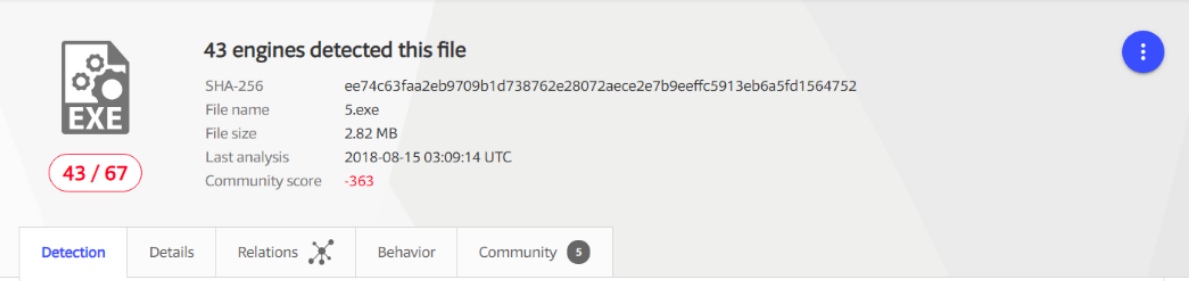


نکته قابل توجهی در بسته‌های دریافتی باج‌افزار KeyPass از سرور مذکور دیده می‌شود که آن، نام ایـران در چند بسته دریافتی می‌باشد. در تصویر زیر نیز، نظاره گر یک Conversation بین باج‌افـزار و سـرور مزبـور هستید.



خروجی سامانه VirusTotal :

در حال حاضر تعداد ۴۳ مورد از ۶۷ آنتی ویروس و آنتی بدافزار موجود در سامانه VirusTotal قادر به شناسایی این باج افزار بوده وآن را حذف یا غیرفعال می‌کنند.



Ad-Aware	Trojan.GenericKD.31166491	AhnLab-V3	Trojan/Win32.Ransom.R233970
ALYac	Trojan.Ransom.Filecoder	Arcabit	Trojan.Generic.D1DB901B
Avast	Win32:Trojan-gen	AVG	Win32:Trojan-gen
Avira	TR/FileCoder.pfzxh	BitDefender	Trojan.GenericKD.31166491
CAT-QuickHeal	Trojan.IGENERIC	ClamAV	Win.Trojan.Agent-6644902-0
Comodo	UnclassifiedMalware	CrowdStrike Falcon	malicious_confidence_100% (W)
Cylance	Unsafe	Cyren	W32/Trojan.YATI-8672
Emsisoft	Trojan.GenericKD.31166491 (B)	Endgame	malicious (moderate confidence)
eScan	Trojan.GenericKD.31166491	ESET-NOD32	Win32/Filecoder.NRR
F-Secure	Trojan.GenericKD.31166491	Fortinet	W32/Filecoder.NRR!tr
GData	Trojan.GenericKD.31166491	Jiangmin	Trojan.Encoder.a
K7AntiVirus	Trojan (0053a0921)	K7GW	Trojan (0053a0921)
Kaspersky	Trojan-Ransom.Win32.Encoder.n	Malwarebytes	Ransom.FileCryptor
MAX	malware (ai score=100)	McAfee	Artemis!901D893F665C
McAfee-GW-Edition	BehavesLike.Win32.BadFile.vh	Microsoft	Trojan:Win32/Occamy.C
Palo Alto Networks	generic.ml	Panda	Trj/GdSda.A
Qihoo-360	Win32/Trojan.Ransom.873	Rising	Ransom.FileCryptor!8.1A7 (CLOUD)
Sophos AV	Mal/Ransom-FS	Symantec	Trojan.Gen.2
TACHYON	Ransom/W32.Encoder.2958848	Tencent	Win32.Trojan.Encoder.Hoxx
TrendMicro	Ransom_ENCODER.THHADAH	TrendMicro-HouseCall	Ransom_ENCODER.THHADAH
Webroot	W32.Ransom.Gen	Zillya	Trojan.GenericKD.Win32.145894
ZoneAlarm	Trojan-Ransom.Win32.Encoder.n	AegisLab	Clean

خروجی سامانه ویروس‌کاو مرکز ماهر :

در حال حاضر یعنی در زمان نگارش این گزارش تعداد ۴۳ مورد از ٦٧ آنتی ویروس و آنتی بدافزار موجود در سامانه ویروس کاو مرکز ماهر قادر به شناسایی این باج افزار بوده وآن را حذف یا غیرفعال می‌کنند.