باسمه تعالی

تحلیل فنی باج‌افزار

MedusaLocker

فهرست مطالب

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 ۲۵۶بیتی جهت رمزگذاری فایل‌های موردنظر خود در سیستم قربانی بهره می‌برد، پسوند .encrypted را به انتهای هر فایل رمزشده اضافه می‌نماید.

۲. مشخصات فایل اجرایی :

نام فایل	svchostt.exe
MD5	129d3661a7341d3b069868a43714b425
SHA-1	7ba4d0d2d606179c2aab2e2ebee975e05e3d74e1
SHA-256	3a5b015655f3aad4b4fd647aa34fda4ce784d75a20d12a73f8dc0e0d866e7e01
نوع فایل	Win32 EXE
اندازه فایل	٦٦٠.٥ کیلوبایت

فایل اجرایی این باج‌افزار دارای ۵ بخش است :

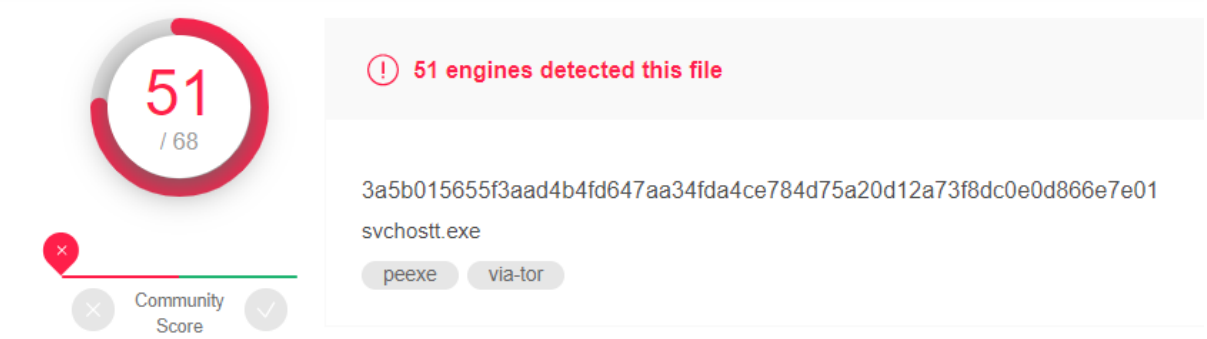
نام بخش	آنتروپی	آدرس مجازی	اندازه مجازی	اندازه خام
.text	6.55	4096	461814	461824
.rdata	4.57	466944	174786	175104
.data	4.76	643072	19304	14848
.rsrc	4.69	663552	480	512
.reloc	6.61	667648	23000	23040

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.

٤. میزان تهدید فایل باج‌افزار

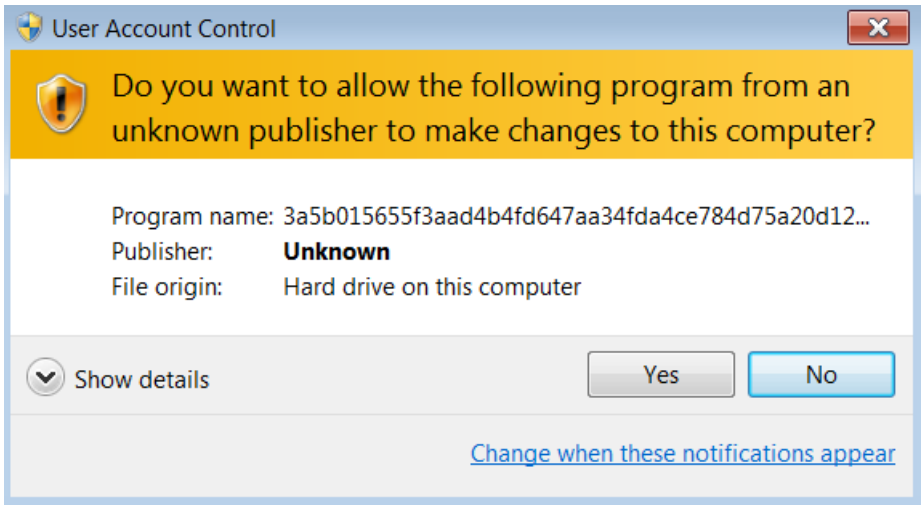
درحال حاضر تعداد ۵۱ مورد از ٦٨ ضدبدافزار سامانه VirusTotal، قادر به شناسایی، توقف و یا حذف این باج‌افزار می‌باشند.



٥. تحلیل پویا

٥-١ آناتومی حمله:

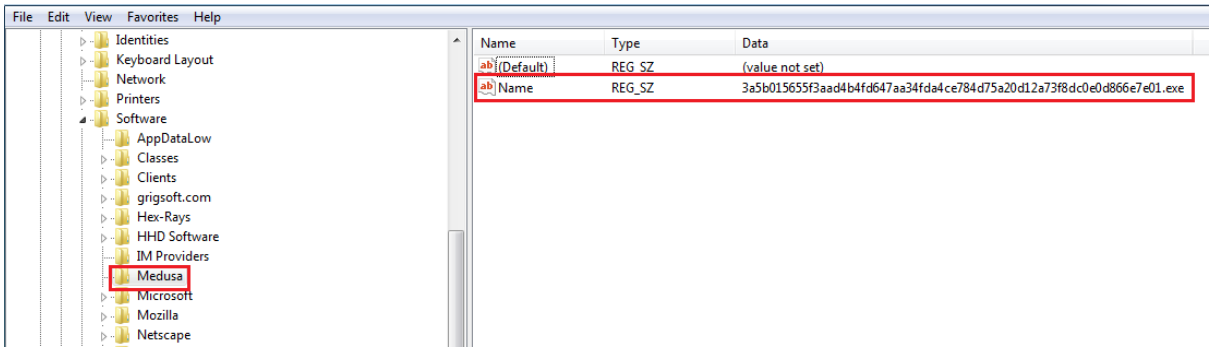
باج‌افزار MedusaLocker، مکانیزم UAC سیستم‌عامل را جهت اجرای فایل خود، دور نمی‌زند.



طبق آزمایش‌های صورت گرفته، این باج‌افزار در حالت آفلاین و بدون اتصال به اینترنت نیز اجرا می‌شود.

باج‌افزار MedusaLocker، به محض شروع فعالیت خود در سیستم قربانی، ابتدا مقدار رجیستری زیر را در سیستم قربانی، ایجاد می‌کند.

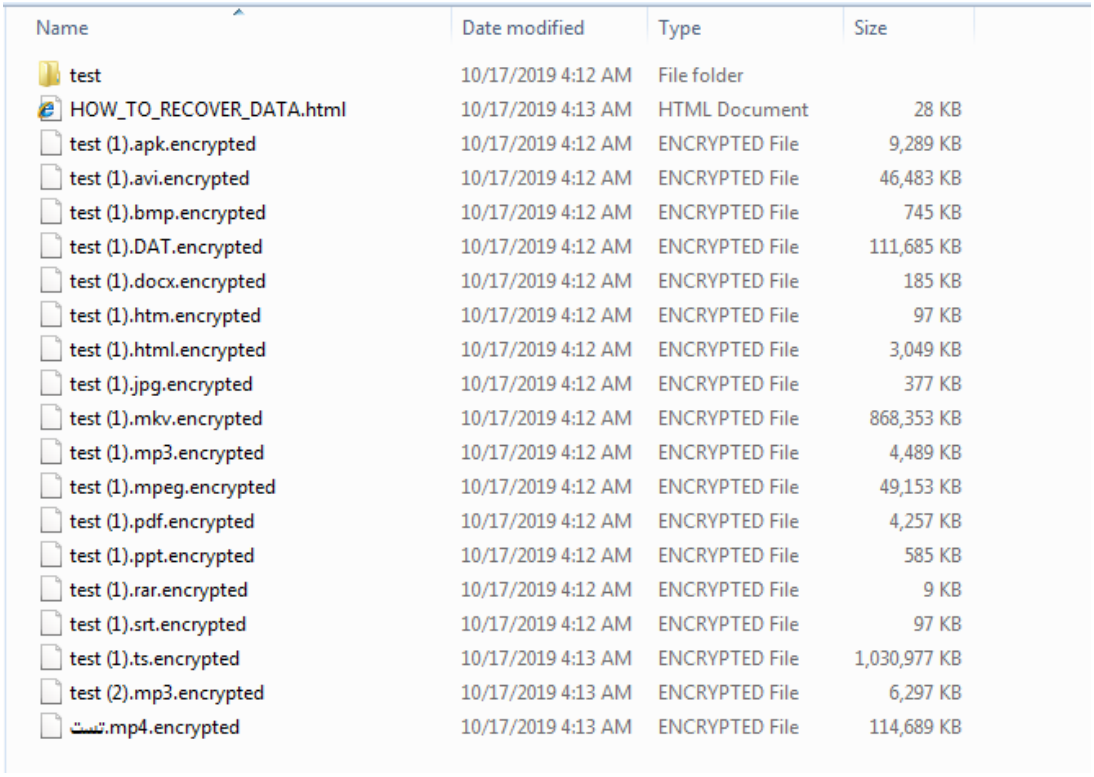
HKU\S-1-5-21-3764654997-3676272905-2098358544-1000\Software\Medusa\



در ادامه، دستورات زیر را اجرا می‌کند.

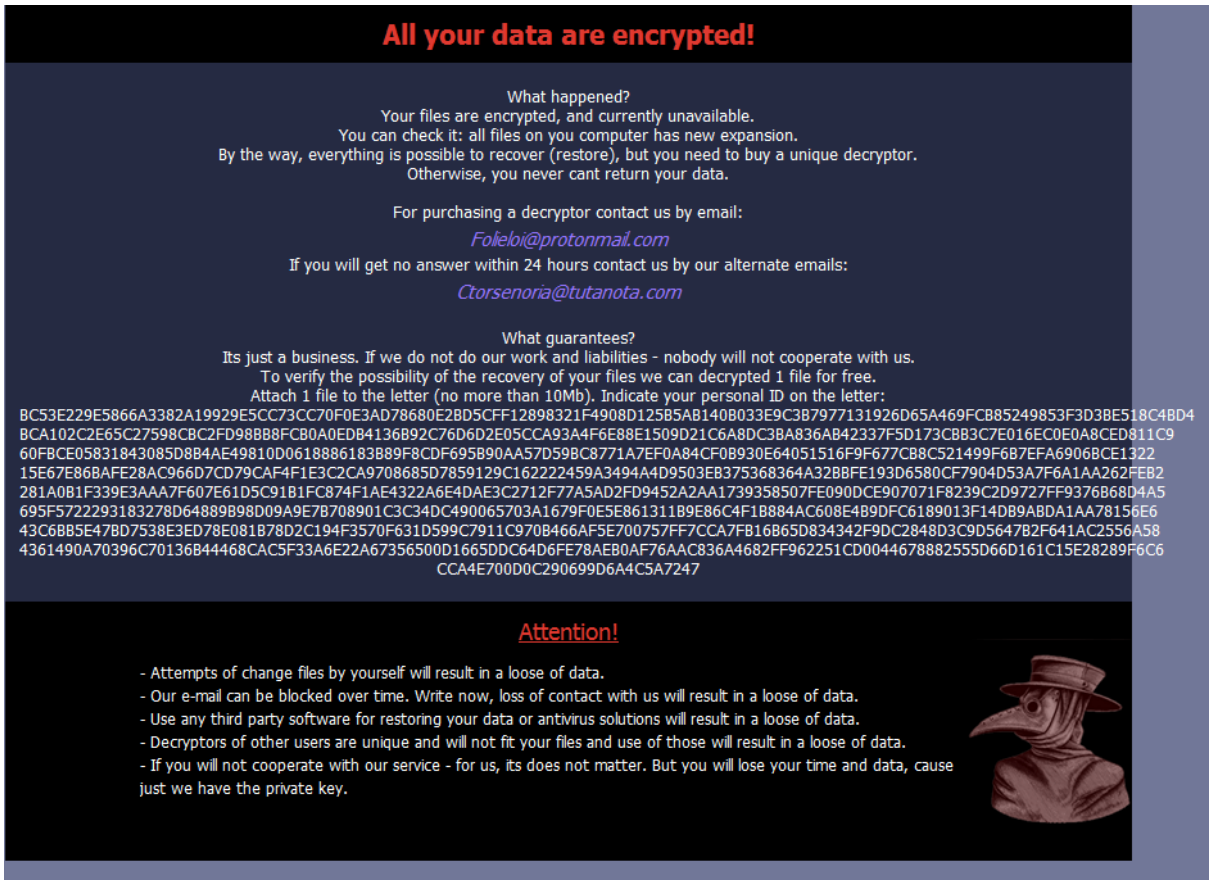
حذف فضای VSS	*vssadmin.exe Delete Shadows /All /Quiet*
غیرفعال کردن قابلیت بازیابی فایل‌ها	*bcdedit.exe /set {default} recoveryenabled No*
غیرفعال کردن پنجره Error Recovery هنگام بوت ویندوز	*bcdedit.exe /set {default} bootstatuspolicy ignoreallfail*
حذف بکآپ‌های گرفته شده توسط WBS	*wbadmin DELETE SYSTEMSTATEBACKUP*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

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
تست.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 رمزشده قرار می‌گیرد.



براساس 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 ۲۴ساعت، باید به آدرس Ctorsenoria@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 رمزشده، 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 رمزنشده درون سیستم قرار گیرد، اقدام به رمزگذاری آن می‌نماید.

۵-۲ روش انتشار:

با توجه به اینکه مدت زمان زیادی از مشاهده این باج‌افزار نمی‌گذرد، تاکنون، روش نفوذ و انتشار مشخصی برای این باج‌افزار گزارش نشده است.

۵-۳ روش جلوگیری:

از آنجا که تاکنون روش مشخصی برای نفوذ این باج‌افزار منتشر نشده است، در گام اول، به‌روزرسانی سیستم‌عامل و نرم‌افزارهای امنیتی نصب شده بر روی آن همچون آنتی‌ویروس، می‌تواند بسیار مفید باشد. در گام بعد، اگر به صورت فعال از پروتکل RDP استفاده می‌کنید حتماً باید اقدامات مربوط به امن‌سازی این پروتکل همچون تنظیم رمزعبور پیچیده، تنظیم احراز هویت دوعاملی و ... را انجام دهید و در گام آخر، توجه بیشتر در بازدید از وبسایت‌ها، عدم استفاده از کرک‌های جعلی جهت شکستن قفل نرم‌افزارها و بازنکردن پیوست ایمیل‌های دریافتی ناشناس و مشکوک، می‌تواند در جلوگیری از نفوذ این باج‌افزار، بسیار مؤثر باشد.

٦. تحلیل ایستا

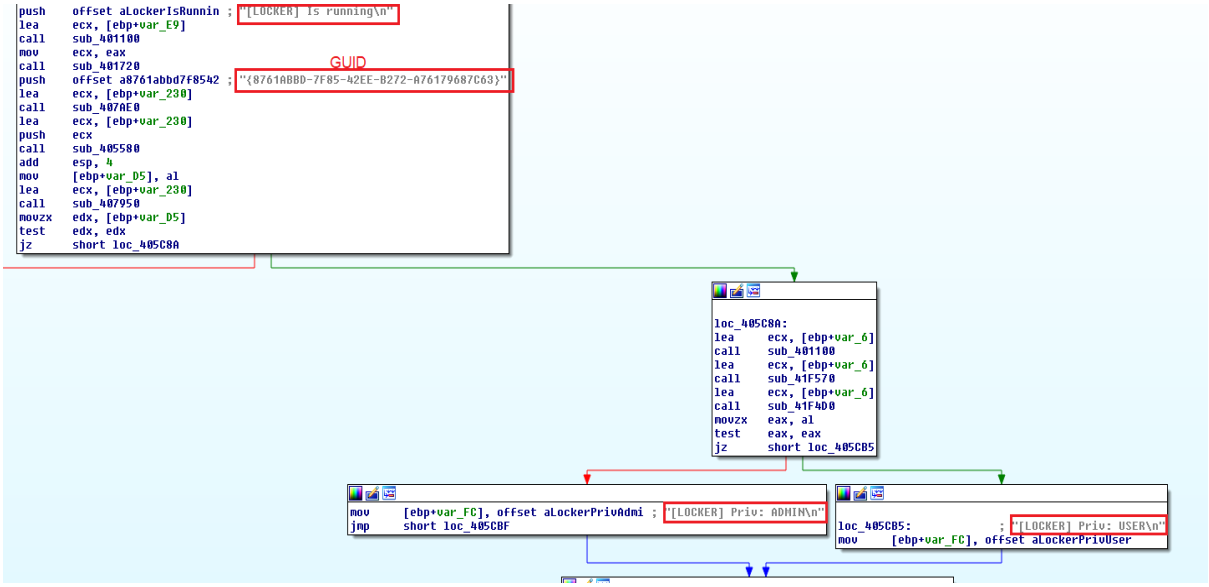
٦-١ تحلیل کد:

پس از تحلیل کد باج‌افزار، نتایج زیر حاصل گردید:

این باج‌افزار، بر روی تمام نسخه‌های ۳۲ و ٦٤ بیتی از سیستم‌عامل ویندوز ویستا به بعد قابل اجرا می‌باشد:

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	

باج‌افزار MedusaLocker، در همان ابتدا با دریافت سطح دسترسی مدیر سیستم (Administrator)، اقدام به اجرای دستورات و فعالیت خود در سیستم قربانی می‌کند.



در ادامه، اقدام به آماده سازی فرآیند رمزنگاری و تخصیص یک شناسه یکتا برای قربانی درون فایل پیغام باج‌خواهی، می‌کند.

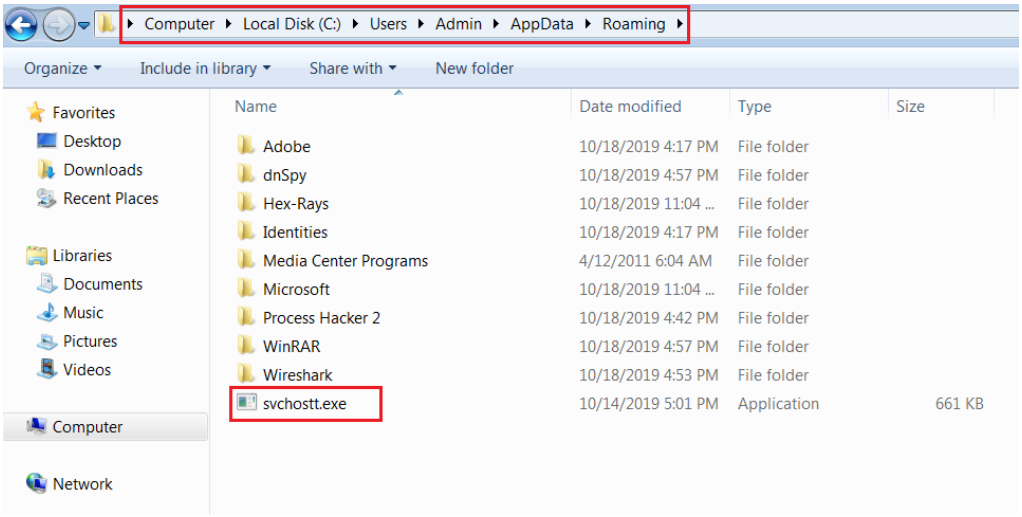
سپس، فایلی با عنوان svchostt.exe را به صورت خودکار اجرا می‌کند.

```
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 ; "svchostt"
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 باج‌افزار است که توسط تابع مشخص شده در قطعه کد زیر درون سیستم قربانی کپی می‌شود.

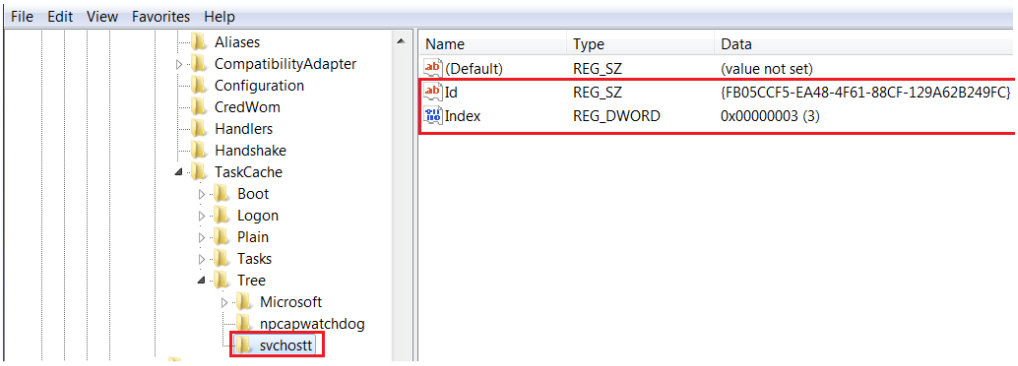
```
push    offset aAppdata_1 ; "AppData"
lea     ecx, [ebp+var_5C]
call    sub_407AE0
lea     eax, [ebp+var_5C]
push    eax
lea     ecx, [ebp+var_28]
push    ecx
mov     ecx, [ebp+var_44]
call    sub_41EF30
lea     ecx, [ebp+var_5C]
call    sub_407950
lea     ecx, [ebp+var_28]
call    sub_4077B0
movzx   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 ; "svchostt"
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 می‌دهد.

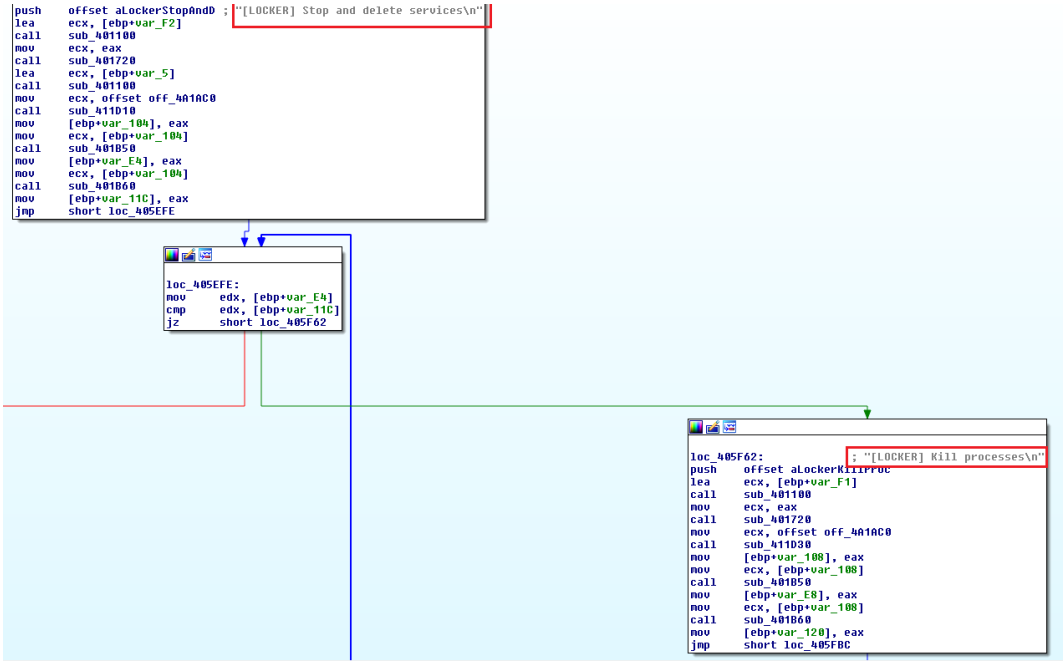


فایل اشاره شده، مقدار رجیستری زیر را در سیستم قربانی ایجاد می‌کند.

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

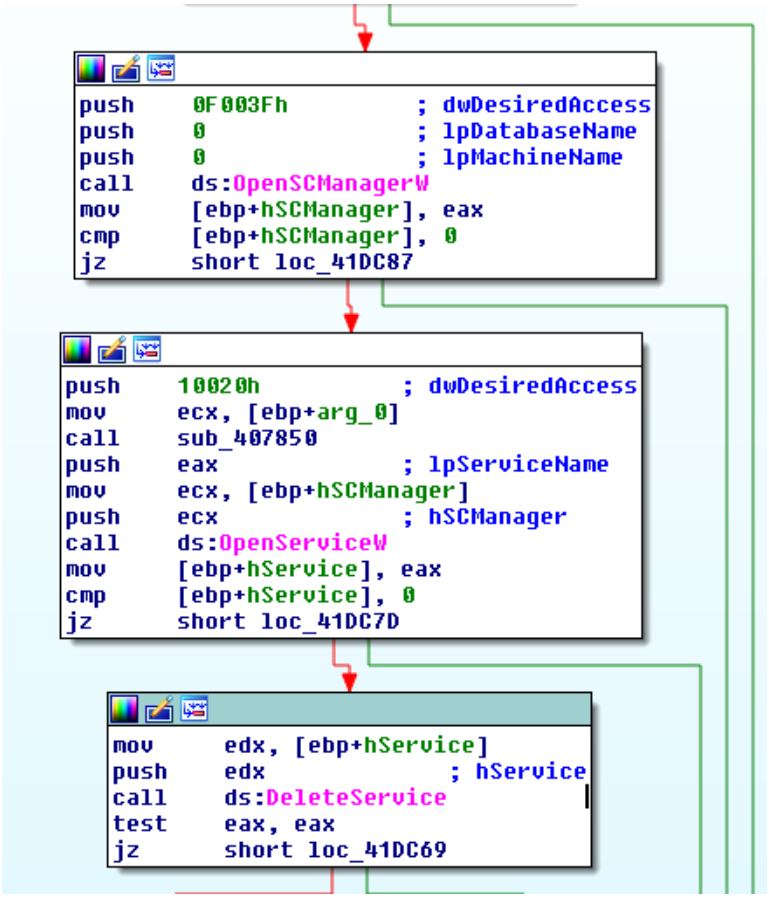


سپس، فرآیندها و سرویس‌های زیر را متوقف و از سیستم قربانی حذف می‌کند.

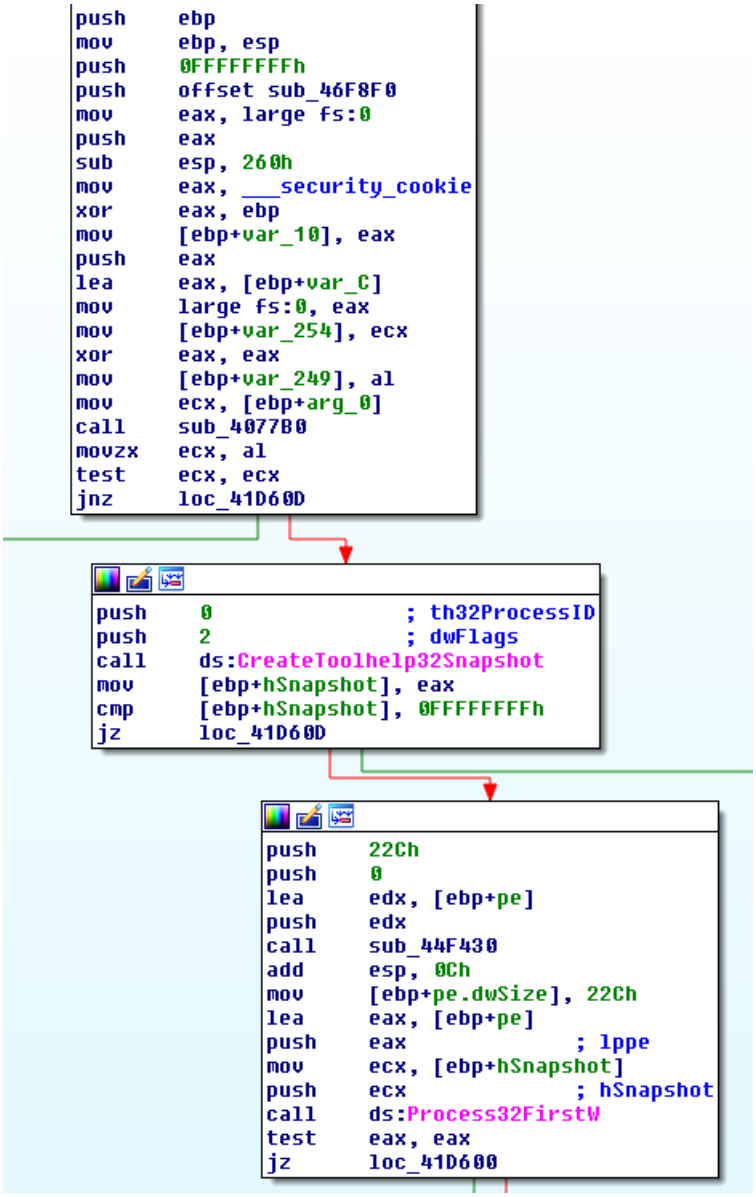


```
push    offset aWrapperDefwatc ;'wrapper,DefWatch,ccEvtMgr,ccSetMgr,SavRoam,sqlservr,sqlagent,sqla'
lea     ecx, [ebp+var_70]                       ; DATA XREF: sub_411370+B4↑o
call    sub_407E10                              'dhlp,Culserver,RTVscan,sqlbrowser,SQLADHLP,QBIDPService,Intuit.Qu'
push    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
mov     ecx, [ebp+var_10]                       سرویس ها
add     ecx, 48h
push    ecx                                     ;'wxServer.exe,wxServerView,sqlservr.exe,sqlmangr.exe,RAgui.exe,sup'
mov     ecx, [ebp+var_10]                       ; DATA XREF: sub_411370+DE↑o
call    sub_411760                              'ervise.exe,Culture.exe,RTVscan.exe,Defwatch.exe,sqlbrowser.exe,wi'
lea     ecx, [ebp+var_70]                       'nword.exe,QBW32.exe,QBDBMgr.exe,qbupdate.exe,QBCFMonitorService.e'
call    sub_407D60                              'xe,axlbridge.exe,QBIDPService.exe,httpd.exe,fdlauncher.exe,MsDtSr'
push    offset aWxserver_exeWx                  'vr.exe,tomcat6.exe,java.exe,360se.exe,360doctor.exe,wdswfsafe.exe'
lea     ecx, [ebp+var_88]                       ',fdlauncher.exe,fdhost.exe,GDscan.exe,ZhuDongFangYu.exe',0
                                                فرآیندها
```

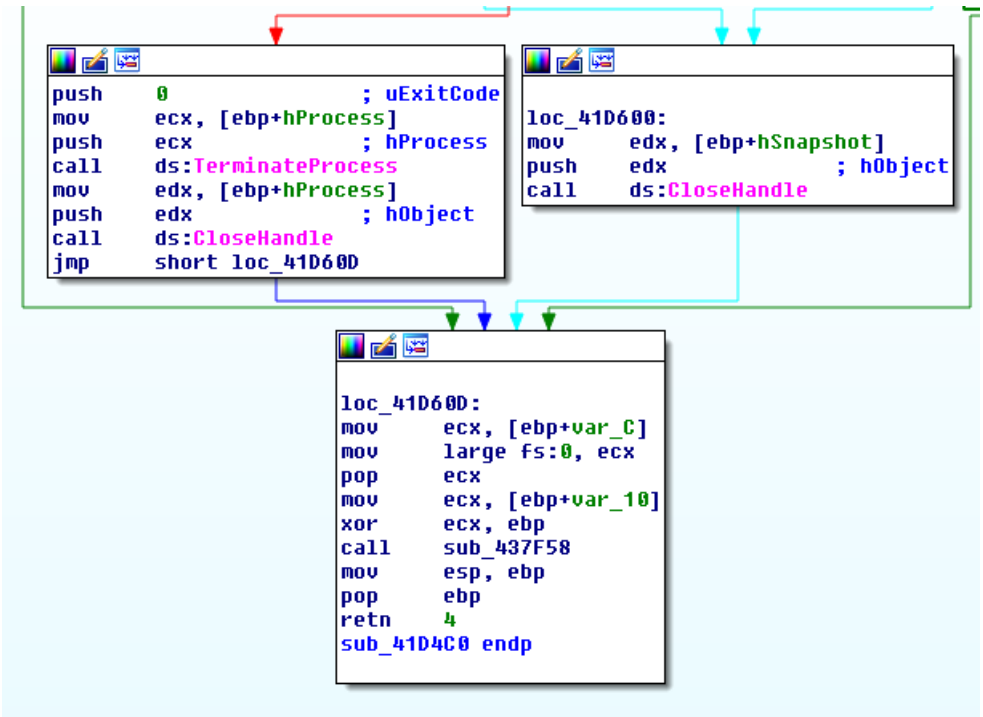
حذف سرویس‌ها، با دسترسی به پایگاه داده سرویس‌های سیستم‌عامل و طی فرآیند زیر صورت می‌گیرد.



فرآیندها نیز، طی روال زیر متوقف می‌شوند.




loc_41D565:
lea edx, [ebp+pe.szExeFile]
push edx
lea ecx, [ebp+var_26C]
call sub_407AE0
lea eax, [ebp+var_26C]
push eax
mov ecx, [ebp+arg_0]
push ecx
lea ecx, [ebp+var_11]
call sub_41D630
mov [ebp+var_241], al
lea ecx, [ebp+var_26C]
call sub_407950
movzx edx, [ebp+var_241]
test edx, edx
jz short loc_41D5E4
mov eax, [ebp+pe.th32ProcessID]
push eax ; dwProcessId
push 0 ; bInheritHandle
push 1 ; dwDesiredAccess
call ds:OpenProcess
mov [ebp+hProcess], eax
cmp [ebp+hProcess], 0
jz short loc_41D5E4
loc_41D5E4:
lea eax, [ebp+pe]
push eax ; lppe
mov ecx, [ebp+hSnapshot]
push ecx ; hSnapshot
call ds:Process32NextW
test eax, eax
jnz loc_41D565


push 0 ; uExitCode
mov ecx, [ebp+hProcess]
push ecx ; hProcess
call ds:TerminateProcess
mov edx, [ebp+hProcess]
push edx ; hObject
call ds:CloseHandle
jmp short loc_41D60D
loc_41D600:
mov edx, [ebp+hSnapshot]
push edx ; hObject
call ds:CloseHandle
loc_41D60D:
mov ecx, [ebp+var_C]
mov large fs:0, ecx
pop ecx
mov ecx, [ebp+var_10]
xor ecx, ebp
call sub_437F58
mov esp, ebp
pop ebp
retn 4
sub_41D4C0 endp

در ادامه فعالیت باج‌افزار در سیستم قربانی، دستورات زیر به منظور حذف فضای VSS و حذف بکآپ‌های گرفته شده توسط سیستم‌عامل 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_41D910
push    offset aVssadmin_exeDe ; "vssadmin.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_41D860
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_41D860
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_41D860
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_41D860
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_41D860
lea     ecx, [ebp+var_248]
call    sub_407950
push    offset aWmic_exeShadow ; "wmic.exe SHADOWCOPY /nointeractive"
```

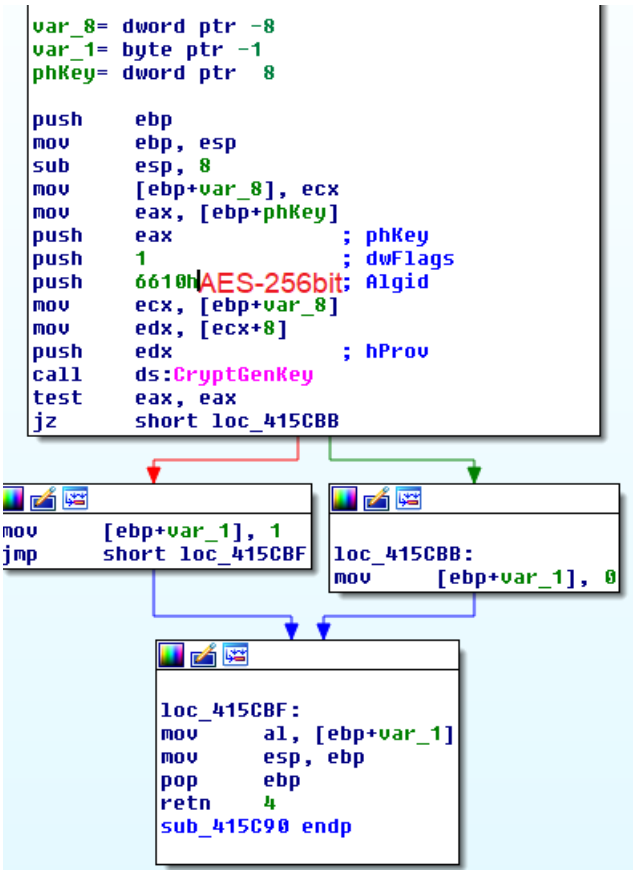
باج‌افزار MedusaLocker، در مدت زمان کوتاهی پس از آغاز فعالیت خود، فضای اختصاص یافته به قسمت Recycle Bin سیستم‌عامل را نیز پاک می‌کند تا قربانی دیگر امکان دسترسی به فایل‌های آن قسمت را نداشته باشد.

```
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
```

فایل‌های زیر، در لیست سفید باج‌افزار قرار داشته و از رمزگذاری توسط باج‌افزار در امان می‌مانند.

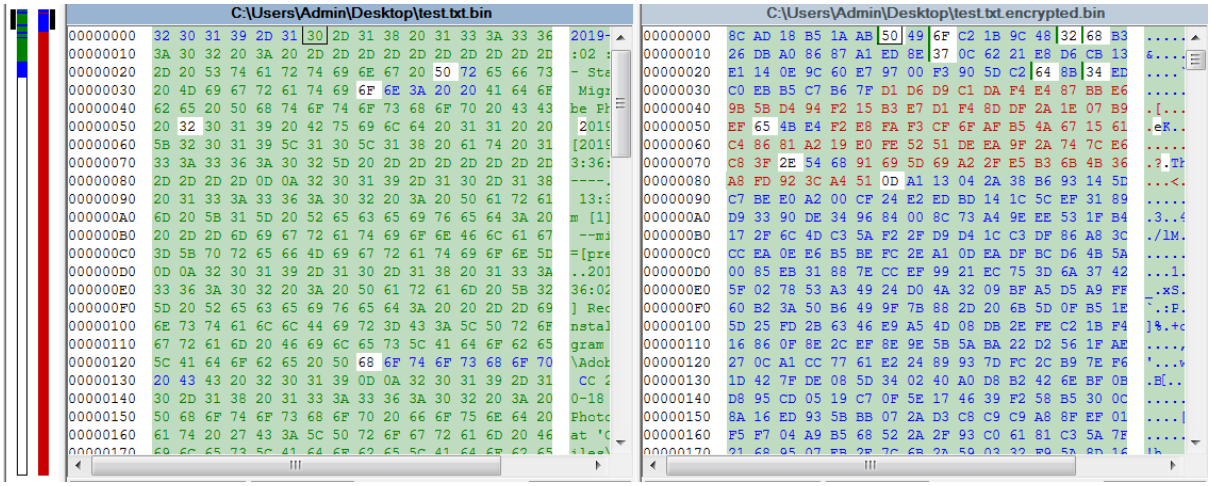
```
.exe,.dll,.sys,.ini,.lnk,.rdp,.encrypted
```

این باج‌افزار از الگوریتم‌های رمزنگاری AES و RSA به صورت همزمان در فرآیند رمزگذاری خود بهره می‌برد. فایل‌های قربانی توسط الگوریتم AES ۲۵۶بیتی رمزگذاری می‌شوند.

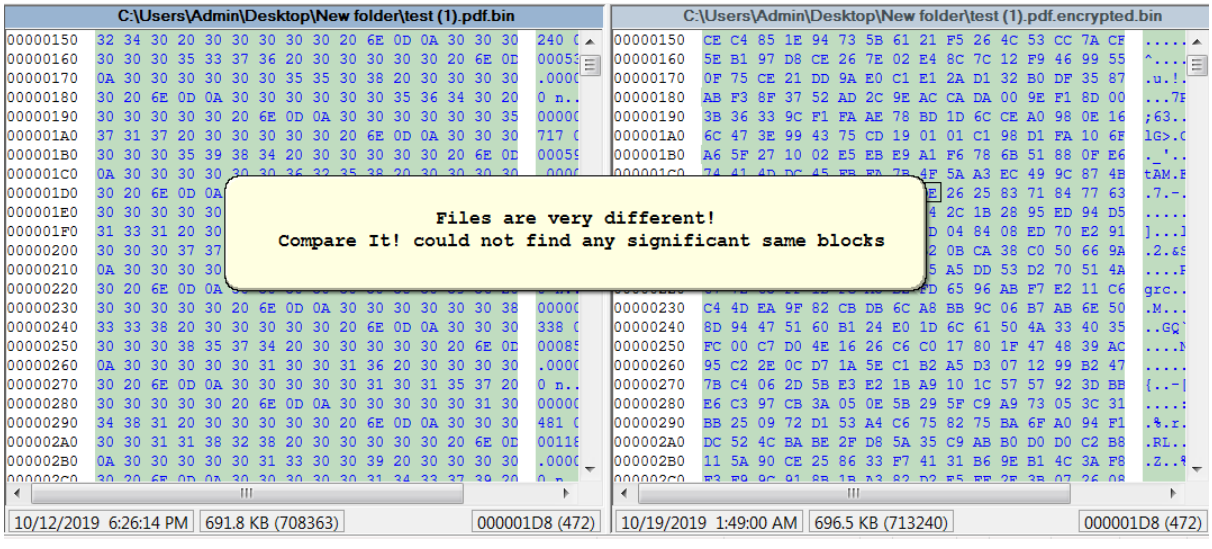


سپس این کلید، توسط جفت کلید عمومی/خصوصی الگوریتم نامتقارن RSA رمزگذاری می‌شود. کلید عمومی جهت رمزگذاریِ کلید AES استفاده شده در رمزگذاری فایل‌ها و کلید خصوصی جهت رمزگشاییِ کلید عمومی استفاده می‌شود که به سرور فرمان و کنترل باج‌افزار (C&C) ارسال شده و رمزگشایی فایل‌ها بدون در اختیار داشتن این کلید (خصوصی)،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

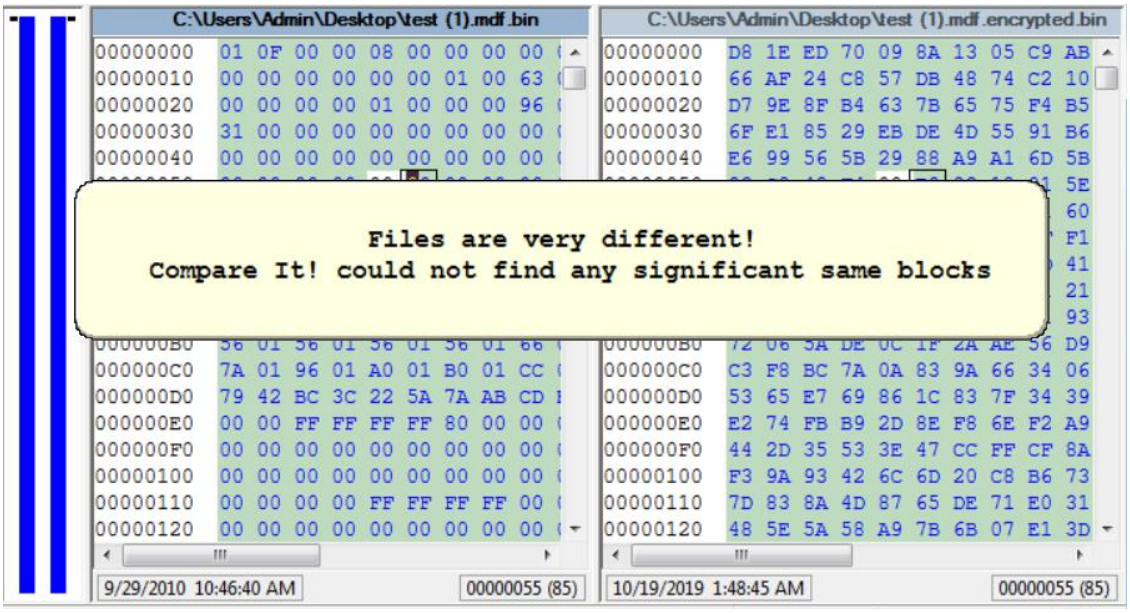
طبق آزمایش‌های صورت گرفته بر روی چند نمونه فایل سالم و رمزگذاری شده، رفتار باج‌افزار MedusaLocker در رمزگذاری فایل‌های با حجم مختلف، متفاوت است.



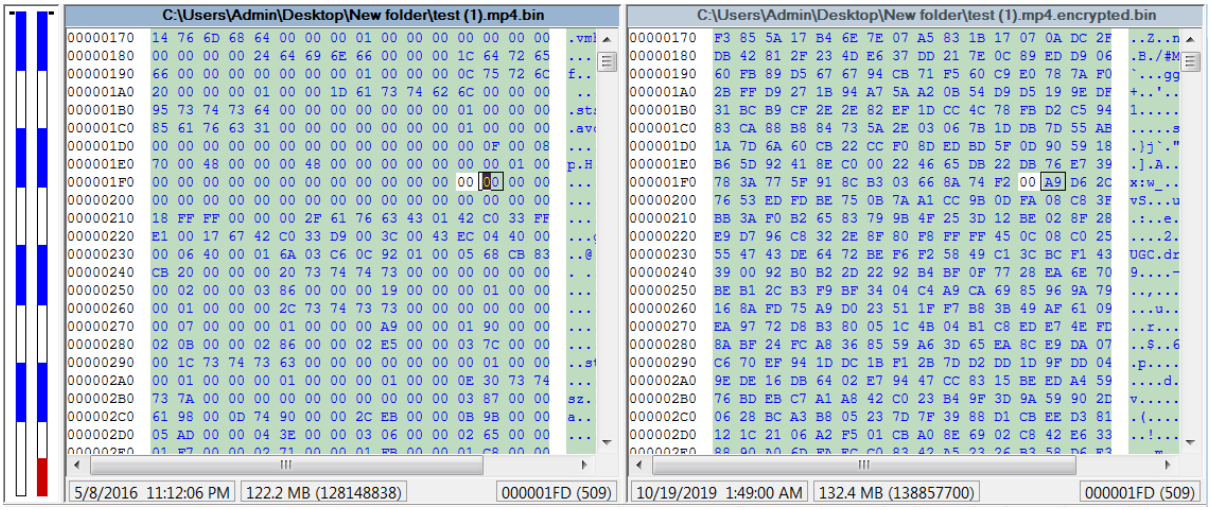
کمتر از ۱۰ کیلوبایت



کمتر از ۱ مگابایت



کمتر از ۱۰۰ مگابایت



کمتر از ۱ گیگابایت

۶-۲ تحلیل ترافیک شبکه:

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

۶-۳ رمزگشایی:

تاکنون، هیچ‌گونه ابزاری جهت رمزگشایی این باج‌افزار ارایه نشده است.