باسمه تعالی

گزارش تحلیل باج افزار LockCrypt(.BI_D)

مقدمه :

مشاهده و رصد فضای سایبری در زمینه باج افزار، از شروع فعالیت نمونه جدیدی از خانواده‌ی باج افزار LockCrypt خبر می‌دهد که پس از رمزگذاری فایل‌ها پسوند .BI_D را به انتهای فایل‌های رمزگذاری شده اضافه می‌کند. بررسی‌ها نشان می‌دهد که فعالیت این باج‌افزار در اواخر ماه می سال ۲۰۱۸ میلادی شروع شده و به نظر می‌رسد تمرکز آن بیشتر بر روی کاربران انگلیسی زبان می‌باشد. اولین نسخه باج‌افزار LockCrypt که فعالیت آن مربوط به ماه ژوئن سال ۲۰۱۷ می‌باشد، کشورهای ایالات متحده آمریکا، بریتانیا، آفریقای جنوبی، هند و فیلیپین را مورد حمله قرار داده بود. اما آماری از کشورهای مورد هدف در نسخه‌ای که به تازگی انتشار یافته است، در دسترس نیست. به نظر می رسد والد باج‌افزار LockCrypt، باج‌افزار Satan RaaS می‌باشد. این باج‌افزار همانند اکثر باج‌افزارها، پس از رمزگذاری فایل‌ها از قربانیان تقاضای بیت‌کوین می‌کند. باج‌افزار LockCrypt(.BI_D) تفاوت‌هایی با نسخه‌های قبلی خود دارد که می‌توان به عدم وجود سرور کنترل و فرمان در این نسخه اشاره نمود.

مشخصات فایل اجرایی :

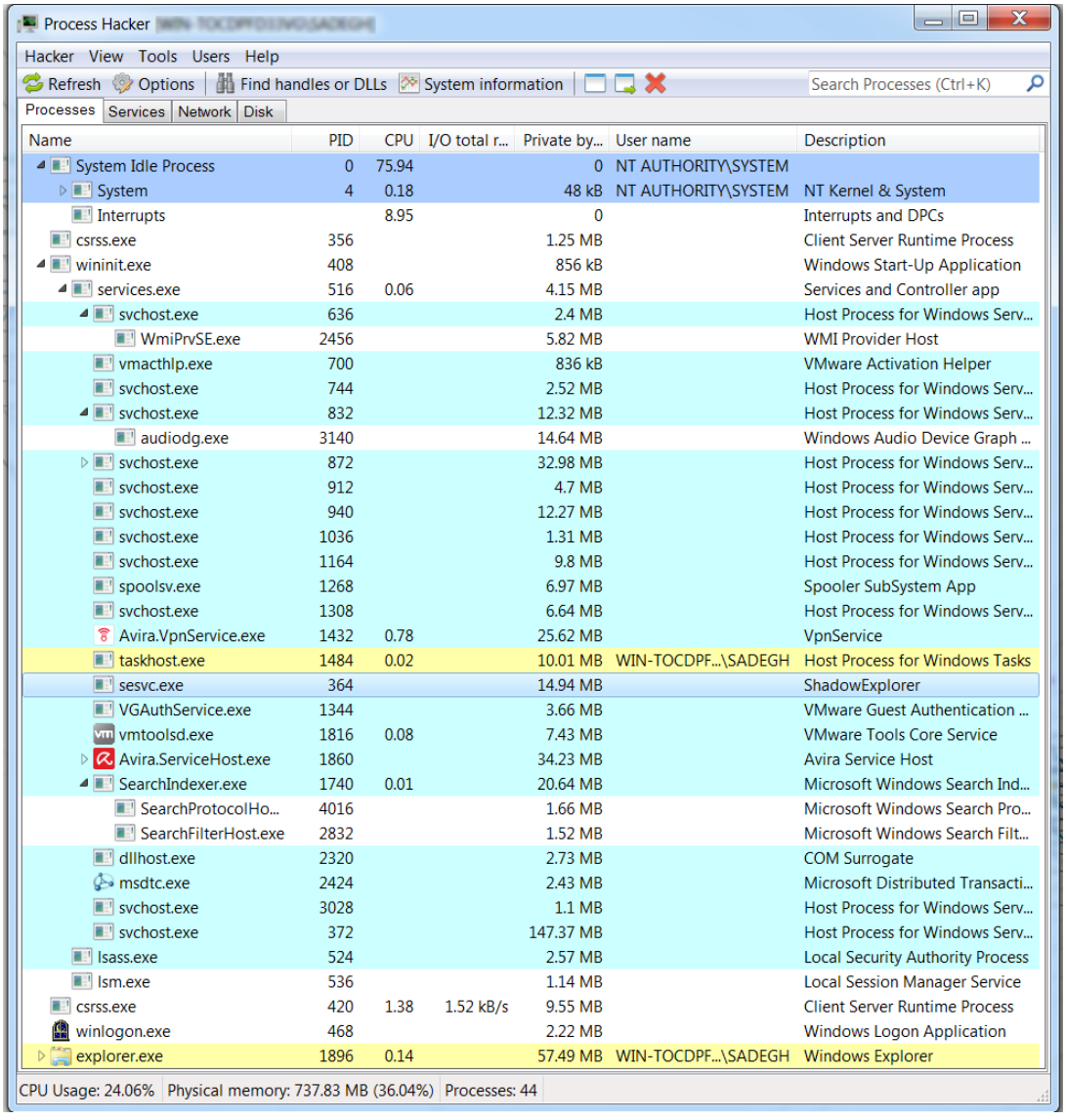
نام فایل	notepad+++.exe
MD۵	۳cf۸۷e٤۷٥a٦۷۹۷۷ab۹٦dff۹٥۲۳٠f۸۱٤٦
SHA-۱	۱fb۳dbd٦e٤ee۲۷bddfcd۱۹۳٥٠٦٥۳۳۹e٠٤dae٤۳٥c
SHA-۲٥٦	۳٠۷bca۹a٥۱٤b۱e٥٠۳۸۹۲٦a٠bafc۷bc٠۸d۱۳۱dd٦fe۳۹۹۸f۳۱cb۱e٦۱٤e۱٦effe۳۲
اندازه فایل	۱۱.٥ KB
کامپایلر / پکر	PE Diminisher v۰.۱

فایل اجرایی این باج افزار دارای چهار بخش است :

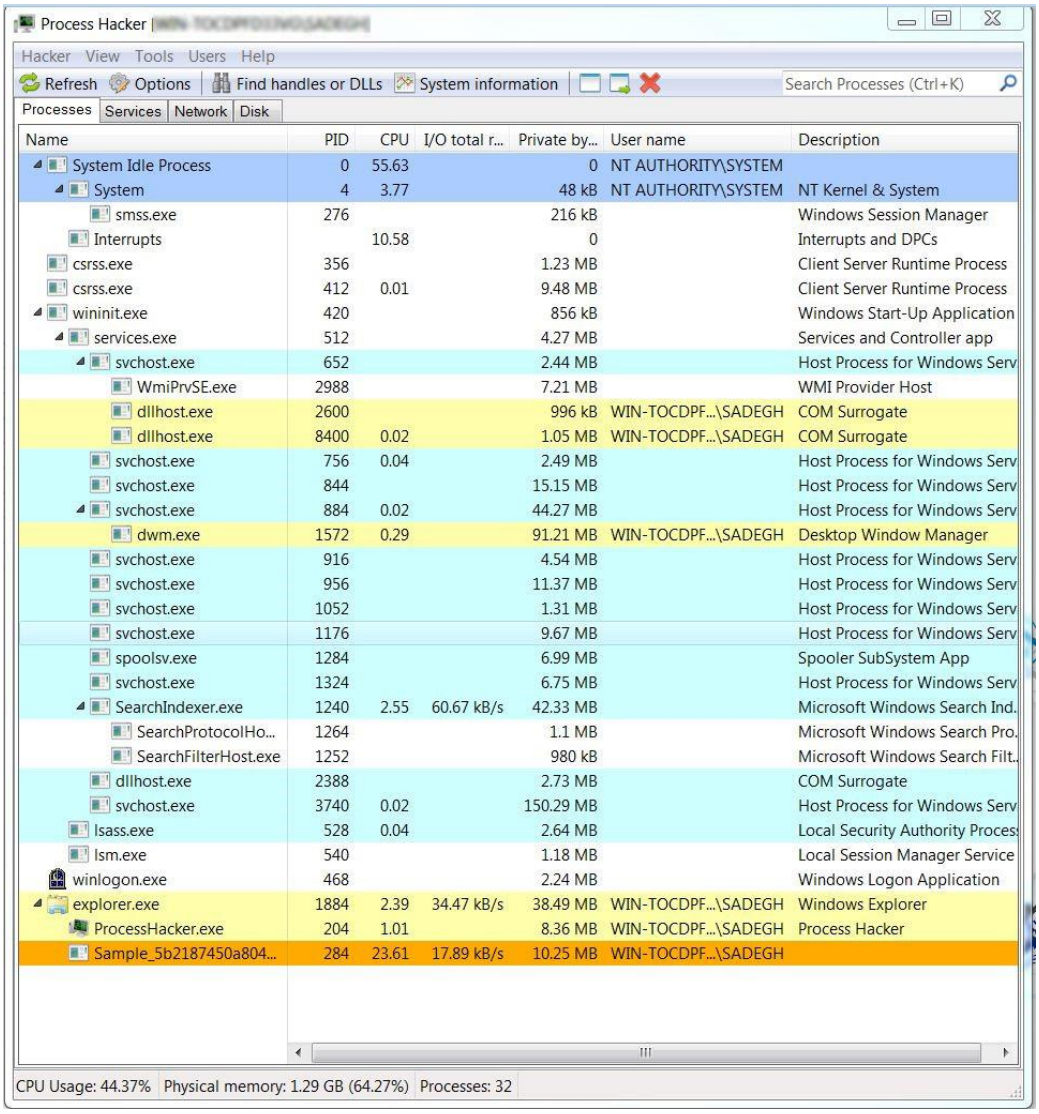
نام بخش	آنتروپی	آدرس مجازی	اندازه مجازی	اندازه خام
.text	٥.۷۲	٤۰۹٦	٤٥۷٤	٤٦۰۸
.rdata	٤.٤۳	۱۲۲۸۸	۲۰۹۸	۲٥٦۰
.data	٤.۸۸	۱٦۳۸٤	۲۸۹٦	۳۰۷۲
.rsrc	۱.۱٦	۲۰٤۸۰	۲۲٤	٥۱۲

تحلیل پویا :

برای بررسی عمیق‌تر باج‌افزار LockCrypt(.BI_D)، فایل اجرایی آن را در محیط آزمایشگاهی اجرا کردیم تا عملکرد باج‌افزار را از نزدیک مورد بررسی قرار دهیم. نتایج حاصل از این بررسی نشان داد که باج‌افزار باید در حالت Administrator اجرا شود تا حمله خود را کامل کند در غیر اینصورت قادر به توقف ادامه‌ی فعالیت فرایندها نمی‌باشد و نسخه‌ی مدنظر خود را در مسیر C:\WINDOWS ایجاد نمی‌کند. هنگامی که باج‌افزار در حالت Administrator اجرا می‌شود، یک نمونه از باج‌افزار در مسیر C:\WINDOWS با نام NOTEPAD+++.EXE ایجاد می‌شود. همچنین پس از اجرا، برخی از فرایندها و برنامه‌های در حال اجرا را متوقف کرده و از آغاز مجدد فعالیت آن‌ها جلوگیری می‌کند.

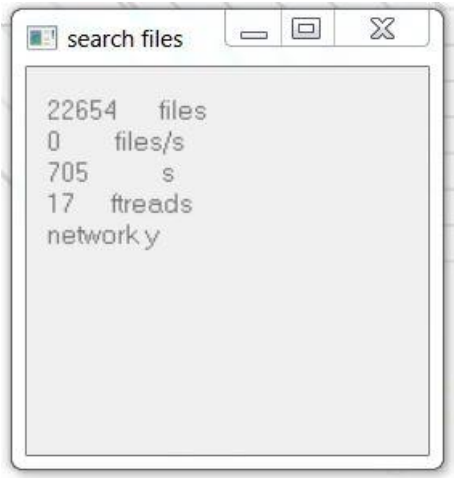


تصویر ۱: فرایندهای در حال اجرای سیستم عامل قبل از اجرای باج‌افزار



تصویر ۲: باج‌افزار در حال اجرا می‌باشد و از شروع فعالیت فرایندها و نرم‌افزارها جلوگیری می‌کند.

همچنین پس از اجرای باج‌افزار یک پنجره به شکل زیر به نمایش در می‌آید که به مواردی از جمله تعداد فایل‌های مورد هدف، مدت زمان اجرای باج‌افزار و ... اشاره می‌کند.



بررسی‌ها نشان می دهد که باج‌افزار LockCrypt(.BI_D) تمامی فایل‌ها، به جز فایل‌های موجود در دایرکتوری‌های زیر را رمزگذاری می‌کند.

Windows, Windows Sidebar, Windows Portable Devices, Windows Photo Viewer, windows nt, Windows Media Player, Windows Mail, Windows Journal, Windows Defender, Reference Assemblies, internet explorer, DVD Maker, Common Files\Services, Common Files\SpeechEngines

پس از اجرای باج‌افزار، یک فایل تحت عنوان How To Restore Files.txt در دایرکتوری‌های مختلف ایجاد می شود. تصویر زیر پیغام باج‌خواهی باج افزار LockCrypt را نشان می دهد.

بر اساس پیغام باج‌خواهی، یک کد شناسایی منحصربفرد برای هر قربانی وجود دارد که مهاجمین اعلام نموده‌اند که قربانیان برای رمزگشایی فایل‌ها باید یک ایمیل همراه با کد شناسایی به آدرس big_decryptor@aol.com ارسال نمایند. نحوه پرداخت باج از طریق کیف پول بیت‌کوین می باشد. اما مقدار آن مشخص نشده است. قربانیان جهت اطلاع از مبلغ باج‌خواهی می بایست با مهاجمین ارتباط برقرار نمایند و در ایمیل ارسالی برای مهاجمین یک فایل با نام DECODE.KEY که در مسیر C:\Windows پس از اجرای باج‌افزار ایجاد می‌شود را ارسال نمایند. ضمناً مهلتی برای پرداخت باج نیز تعیین نشده است. مهاجمین اعلام نموده‌اند هر گونه اقدام دیگر به جز پرداخت باج، جهت رمزگشایی فایل‌ها باعث از دست دادن فایل‌ها برای همیشه خواهد شد. پس از برقراری ارتباط با مهاجمین مبلغ باج‌خواهی ۱.۵ بیت کوین

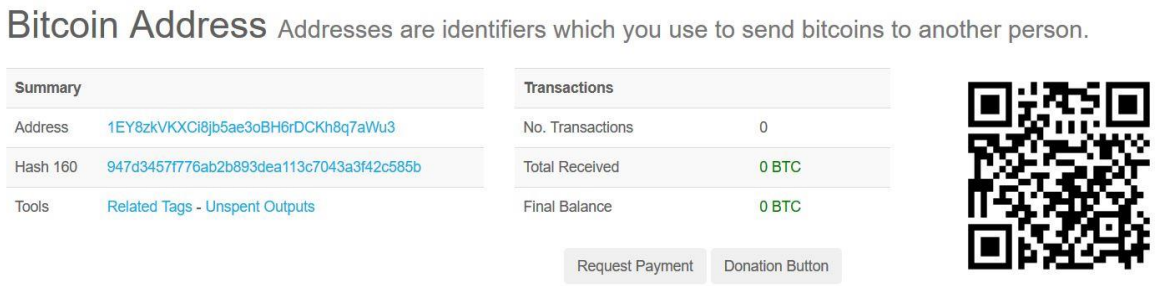
تعیین شد و همچنین آدرس کیف پول بیت کوین به آدرس ۱EY۸zkVKXCi۸jb۵ae۳oBH٦rDCKh۸q۷aWu۳ جهت پرداخت مبلغ باج‌خواهی ارسال شد. جزئیات بیشتر در تصویر زیر قابل مشاهده است :


big decryptor <big_decryptor@aol.com>
To: [redacted]

Hi! to restore the files you need to pay a ransom of 1.5 bitcoins
Our bitcoin address 1EY8zkVKXCi8jb5ae3oBH6rDCKh8q7aWu3
Encrypt a screenshot of the transaction confirmation
After receiving the foreclosure, we will send you a utility decoder
Here are our recommendations:
If you have no Bitcoin address register https://blockchain.info/wallet
fill up your wallet some of the ways
Btcdirect.eu - Good service for Europe
Bittylicious.com - Bitcoins through Visa / MC or through SEPA (EC) transfer
Localbitcoins.com - Here you can find people who want to sell Bitcoins directly (WU, in cash, SEPA, Paypal u.s.).
Cex.io - buy bitcoins with Visa / Mastercard or Wire Transfer.
Coincafe.com - Designed for quick and easy service. Payment methods: Western Union, Bank of America, cash by FedEx, Moneygram, as money transfer
Bitstamp.net - well known and established Bitcoins seller
Coinmama.com - Visa / Mastercard
Btc-e.com - Bitcoins vendor (Visa / Mastercard, etc.)
If you have not found any bitcoins in your region, try to find them here:
Buybitcoinworldwide.com - International Bicoins Exchange Directory
Bitcoin-net.com - Another directory of Bitcoins sellers
Howtobuybitcoins.info - International Bicoins Exchange Directory
Bittybot.co/eu - Directory for countries of the European Union
write to Google how to buy Bitcoin in your country?

> Show original message

طبق بررسی‌های انجام شده، در حال حاضر کیف پول مربوط به این باج‌افزار تراکنشی نداشته است.

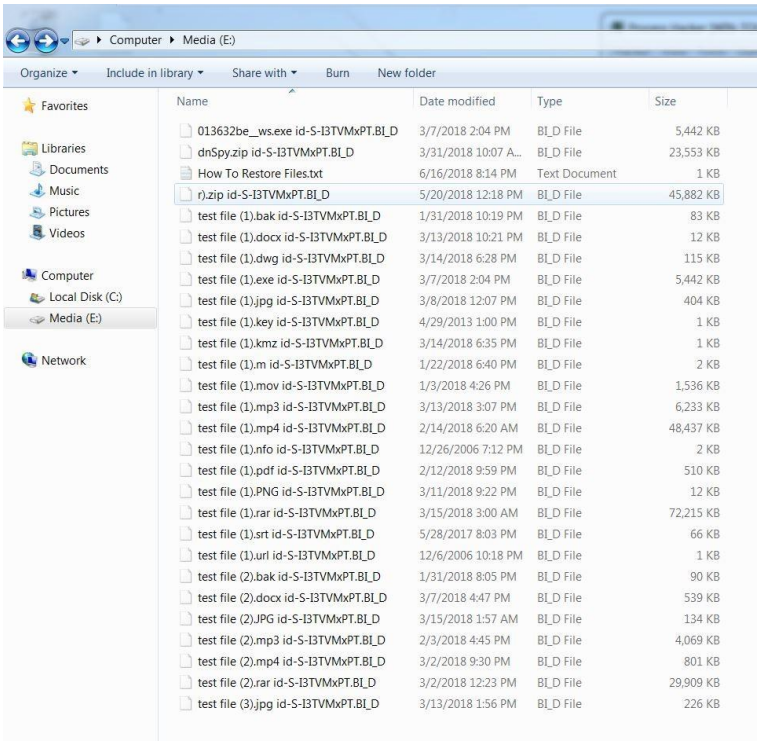

Bitcoin Address Addresses are identifiers which you use to send bitcoins to another person.

Summary	
Address	1EY8zkVKXCi8jb5ae3oBH6rDCKh8q7aWu3
Hash 160	947d3457f776ab2b893dea113c7043a3f42c585b
Tools	Related Tags - Unspent Outputs

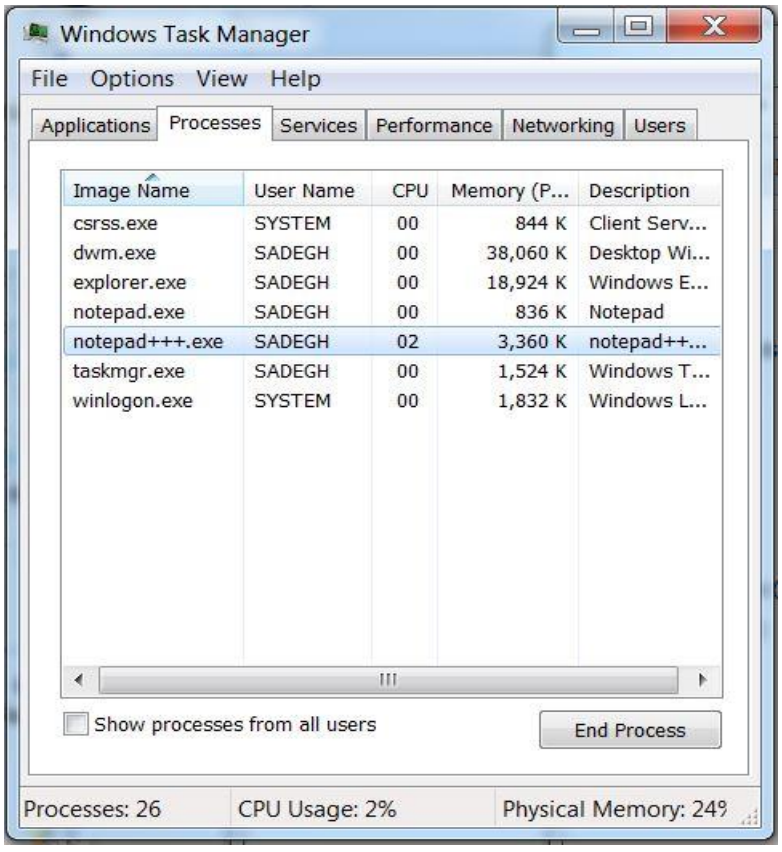
Transactions	
No. Transactions	0
Total Received	0 BTC
Final Balance	0 BTC

Request Payment | Donation Button

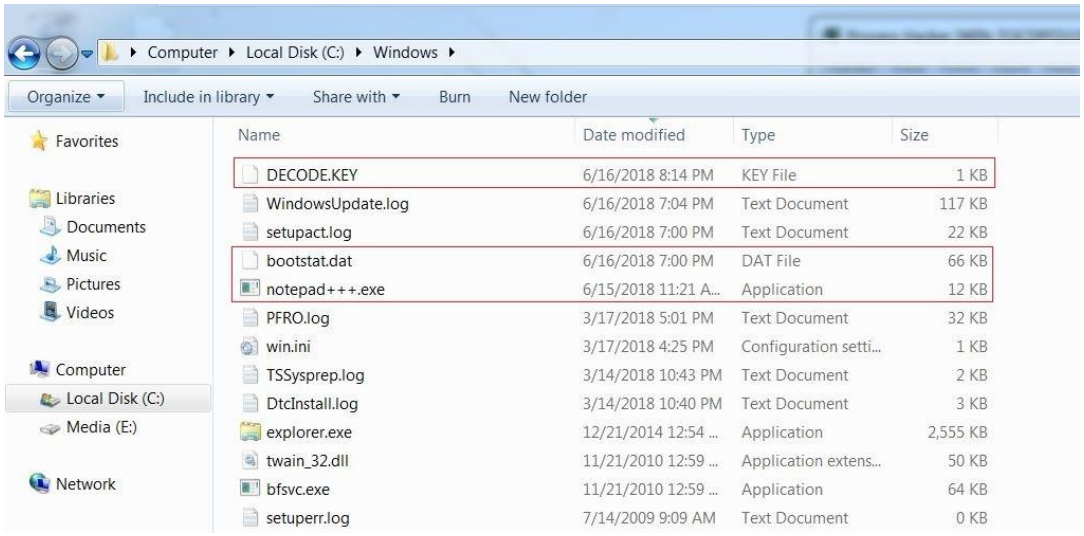
همانطور که پیشتر اشاره کردیم، این باج‌افزار تمامی فایل‌ها، به جز فایل‌های مرتبط به سیستم عامل در دایرکتوری‌هایی خاص را رمزگذاری می‌کند و پسوند فایل‌ها پس از رمزگذاری توسط باج‌افزار، به .BI_D تغییر می‌کند. همچنین شناسه مربوط به قربانی نیز بخشی از نام فایل‌ها می‌باشد. تصویر زیر نشان‌دهنده فایل‌های رمزگذاری شده توسط این باج افزار می‌باشد.



پس از راه اندازی مجدد رایانه، پیغام باج‌خواهی به نمایش در می‌آید و فایل NOTEPAD+++.EXE در پس زمینه اجرا می‌شود و از اجرای برخی فرایند و نرم‌افزارهای مختلف جلوگیری به عمل می‌آورد. که در تصویر زیر قابل مشاهده می‌باشد :



طبق بررسی ها انجام شده، باج‌افزار فایل‌های موجود در Recycle Bin را نیز حذف می‌کند و به دلیل رمزگذاری دایرکتوری مربوط به نرم‌افزارهای نصب شده بر روی سیستم قربانی هیچ یک از آن‌ها دیگر قابل استفاده نخواهند بود. تصویر زیر مربوط برخی از فایل‌های ایجاد شده توسط باج‌افزار می‌باشد :

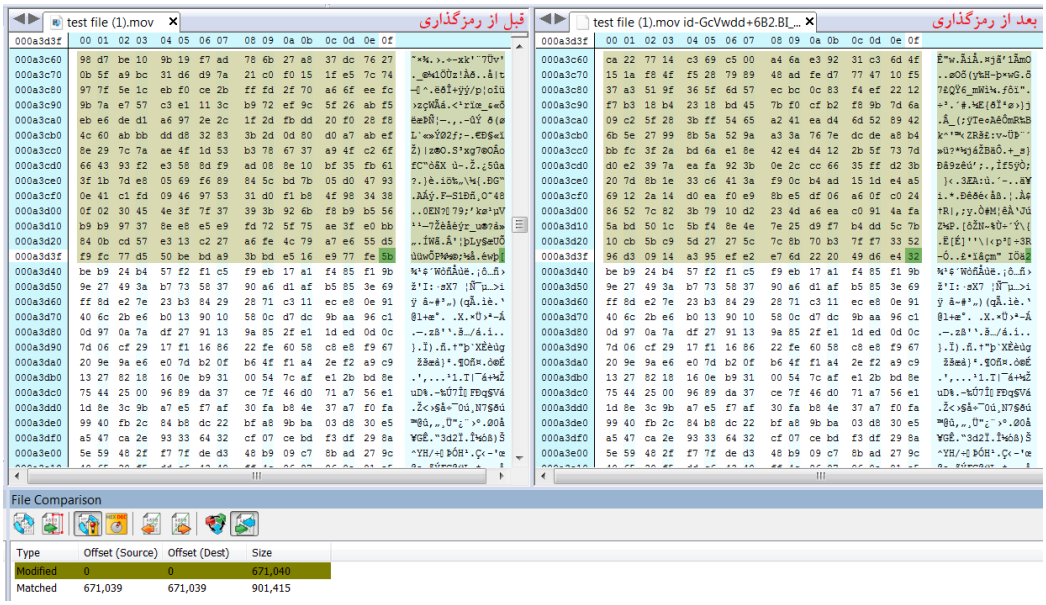


بررسی ها نشان می دهد انواع مختلف باج‌افزارهای خانواده LockCrypt از آسیب پذیری پروتکل RDP برای انتشار استفاده می‌کنند. هر چند طبق بررسی‌های انجام شده اکثر آنتی‌ویروس‌های معتبر، این باج‌افزار را به عنوان یک تروجان شناسایی نموده‌اند. لذا احتمال نفوذ باج‌افزار به سیستم از راه های متداول نیز مانند هرزنامه‌ها وجود دارد.

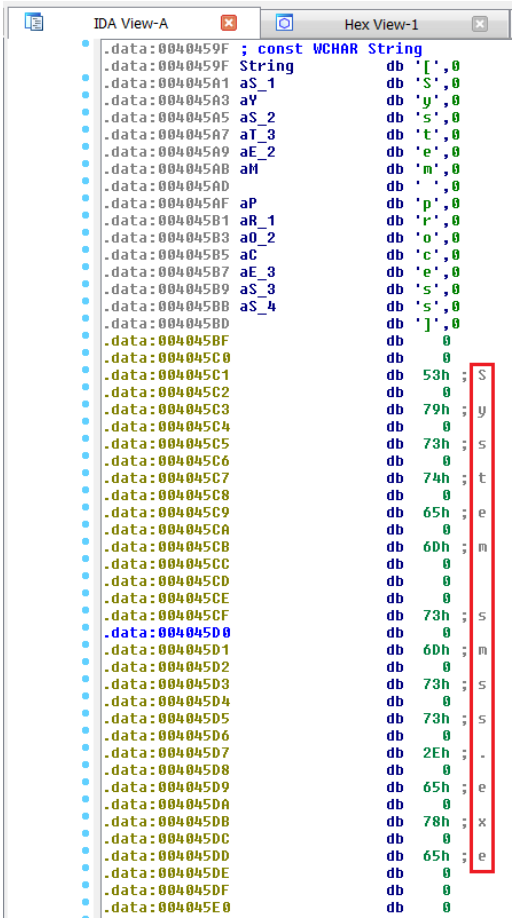
تحلیل ایستا:

پس از تحلیل کد باج‌افزار LockCrypt(.BI_D) به نتایج زیر دست پیدا کردیم.

طبق بررسی‌هایی که بر روی فایل‌های مختلف قبل و بعد از رمزگذاری توسط باج‌افزار، انجام دادیم شاهد این بودیم که باج‌افزار LockCrypt(.BI_D) ساختار فایل‌ها را پس از رمزگذاری به کلی تغییر نمی‌دهد و با توجه به حجم فایل‌ها درصد مختلفی از ساختار فایل‌ها را تغییر می‌دهد. بدین معنی که هرچه فایل‌ها دارای حجم بیشتری باشند درصد کمتری از ساختار آن‌ها تغییر پیدا می‌کند. نتایج این بررسی‌ها در تصویر زیر قابل مشاهده است.



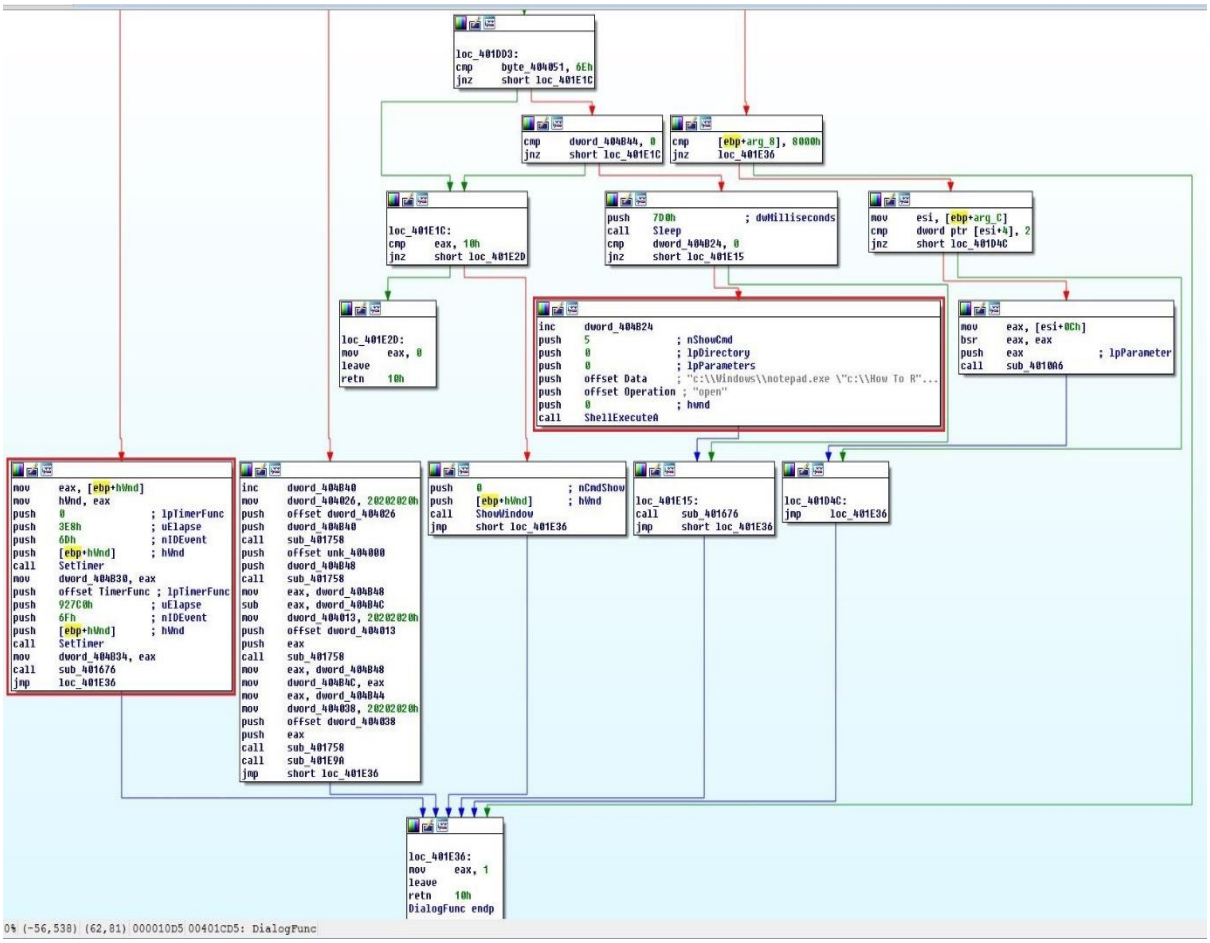
همانطور که اشاره نمودیم باج‌افزار پس از حمله، از اجرای بعضی از فرایندها جلوگیری می‌نماید. قطعه کد زیر مربوط به بخشی از لیست فرایندهایی می‌باشد که توسط باج‌افزار متوقف نمی‌شوند. در ادامه نیز لیست کامل که توسط باج‌افزار متوقف نمی‌شوند، آمده است :



لیست فرایندهای مورد اشاره که پس از اجرای باج‌افزار متوقف نمی‌شوند:

System, smss.exe, dllhost.exe, svchost.exe, csrss.exe, microsoft.activedirectory, webservices.exe, cmd.exe, mstsc.exe, find.exe, conhost.exe, pscan۲٤.exe, explorer.exe, ctfmon.exe, lsass.exe, services.exe, tasklist.exe, winlogon.exe, WmiPrvSE.exe, msdtc.exe, bfsvc.exe, AdapterTroubleshooter.exe, alg.exe, dwm.exe, issch.exe, rundll۳۲.exe, spoolsv.exe, wininit.exe, wmiprvse.exe, wudfhost.exe, taskmgr.exe, rdpclip.exe, logonui.exe, notepad.exe, lsm.exe, searchui.exe, searchindexer.exe,ProcessHacker.exe, getpassvord_x٦٤.exe, ٦٤.exe, ۳۲.exe, fontdrvhost.exe, sihost.exe, dfssvc.exe

قطعه کد زیر مربوط به تابع Start باج‌افزار می‌باشد که مواردی همانند تنظیم زمان‌سنج و ایجاد فایل پیغام باج‌خواهی در آن مشخص شده است :



قطعه کد زیر مربوط به ایجاد فایل جدید در مسیر C:\WINDOWS با نام NOTEPAD+++.EXE و کلید رجیستری که توسط باج‌افزار باز می‌شود، می‌باشد :

IDA View-A | Hex View-1 | Structures | Enums

```
.text:004018A0                push    ebp
.text:004018A1                mov     ebp, esp
.text:004018A3                add     esp, 0FFFFFF84h
.text:004018A6                mov     [ebp+nCmdShow], 0
.text:004018AD                mov     dword_404B24, 0
.text:004018B7                push    8000h           ; dwBytes
.text:004018BC                push    40h             ; uFlags
.text:004018BE                call    GlobalAlloc
.text:004018C3                mov     [ebp+lpString2], eax
.text:004018C6                push    8000h           ; nSize
.text:004018CB                push    eax             ; lpFilename
.text:004018CC                push    0               ; hModule
.text:004018CE                call    GetModuleFileNameA
.text:004018D3                push    [ebp+lpString2] ; lpString2
.text:004018D6                push    offset NewFileName ; "c:\\Windows\\notepad+++.exe"
.text:004018DB                call    lstrcmpiA
.text:004018E0                or      eax, eax
.text:004018E2                jz      short loc_40195E
.text:004018E4                lea     eax, [ebp+phkResult]
.text:004018E7                push    eax             ; phkResult
.text:004018E8                push    0F013Fh         ; samDesired
.text:004018ED                push    0               ; ulOptions
.text:004018EF                push    offset SubKey   ; "SOFTWARE\\Microsoft\\Windows\\CurrentVe".
.text:004018F4                push    80000002h       ; hKey
.text:004018F9                call    RegOpenKeyExA
.text:004018FE                push    offset Data     ; "c:\\Windows\\notepad.exe \"c:\\How To R".
.text:00401903                call    lstrlenA
.text:00401908                push    eax             ; cbData
.text:00401909                push    offset Data     ; "c:\\Windows\\notepad.exe \"c:\\How To R".
.text:0040190E                push    1               ; dwType
.text:00401910                push    0               ; Reserved
.text:00401912                push    offset ValueName ; "decrypt"
.text:00401917                push    [ebp+phkResult] ; hKey
.text:0040191A                call    RegSetValueExA
.text:0040191F                push    offset NewFileName ; "c:\\Windows\\notepad+++.exe"
.text:00401924                call    lstrlenA
.text:00401929                push    eax             ; cbData
.text:0040192A                push    offset NewFileName ; "c:\\Windows\\notepad+++.exe"
.text:0040192F                push    1               ; dwType
.text:00401931                push    0               ; Reserved
.text:00401933                push    offset aNotepad ; "notepad++"
.text:00401938                push    [ebp+phkResult] ; hKey
.text:0040193B                call    RegSetValueExA
.text:00401940                push    [ebp+phkResult] ; hKey
.text:00401943                call    RegCloseKey
.text:00401948                push    0               ; bFailIfExists
.text:0040194A                push    offset NewFileName ; "c:\\Windows\\notepad+++.exe"
.text:0040194F                push    [ebp+lpString2] ; lpExistingFileName
.text:00401952                call    CopyFileA
.text:00401957                mov     [ebp+nCmdShow], 5
```

قطعه کد زیر اشاره به ایجاد سایر فایل‌ها توسط باج‌افزار و حذف Shadowcopy دارد :

IDA View-A | Hex View-1 | Structures | Enums

```
.data:004042EA ; CHAR FileName[]
.data:004042EA FileName        db 'c:\Windows\DECODE.KEY',0 ; DATA XREF: sub_4018A0+1B2↑o
.data:00404300 ; CHAR aCWindowsClerin[]
.data:00404300 aCWindowsClerin db 'c:\Windows\clering.bat',0 ; DATA XREF: TimerFunc+15↑o
.data:00404300                                              ; TimerFunc+48↑o
.data:00404317 ; CHAR Name[]
.data:00404317 Name            db 'ComSpec',0           ; DATA XREF: .text:004017E3↑o
.data:00404317                                          ; sub_4018A0+32B↑o
.data:0040431F ; CHAR Operation[]
.data:0040431F Operation       db 'open',0              ; DATA XREF: DialogFunc+134↑o
.data:0040431F                                          ; TimerFunc+4D↑o
.data:00404324 a@echoOffForTo db '@echo off',0Dh,0Ah    ; DATA XREF: TimerFunc+2D↑o
.data:00404324                db 'for /F "tokens=*" %%G in (',27h,'wevtutil.exe el',27h,') DO (call:clear'
.data:00404324                db ' "%%G")',0Dh,0Ah
.data:00404324                db 'goto End',0Dh,0Ah
.data:00404324                db ':clear',0Dh,0Ah
.data:00404324                db 'wevtutil.exe cl %1',0Dh,0Ah
.data:00404324                db 'goto :eof',0Dh,0Ah
.data:00404324                db ':End',0Dh,0Ah
.data:00404324                db 'rd /s /q %systemdrive%\$RECYCLE.BIN',0Dh,0Ah
.data:00404324                db 'del %0',0
.data:004043D6 ; CHAR Parameters[]
.data:004043D6 Parameters      db '/c vssadmin delete shadows /all',0
```

قطعه کد زیر مربوط به پیغام باج‌خواهی در کدمنبع باج‌افزار می‌باشد :

IDA View-A | Hex View-1 | Structures | Enums

```
.data:00404054 ; const WCHAR String1
.data:00404054 String1:                                ; DATA XREF: sub_4013E3+55↑o
.data:00404054                                         ; sub_4013E3+3C↑o
.data:00404054                 unicode 0, <..>,0
.data:0040405A ; CHAR Buffer[]
.data:0040405A Buffer          db 'Important !!!',0Dh,0Ah ; DATA XREF: sub_401000+6A↑o
.data:0040405A                                         ; sub_401000+7B↑o
.data:0040405A                 db 'Your personal id -                ',0Dh,0Ah
.data:0040405A                 db 'Warning: all your files are infected with an unknown virus.',0Dh,0Ah
.data:0040405A                 db 'To decrypt your files, you need to contact at big_decryptor@aol.c'
.data:0040405A                 db 'om.',0Dh,0Ah
.data:0040405A                 db 'The decoder card is received by bitcoin.',0Dh,0Ah
.data:0040405A                 db 'You can buy bitcoins from the following links://blockchain.info/w'
.data:0040405A                 db 'allet',0Dh,0Ah
.data:0040405A                 db 'Do not try to restore files your self, this will lead to the loss'
.data:0040405A                 db ' of files forever',0Dh,0Ah
.data:0040405A                 db 'GUARANTEES!!!',0Dh,0Ah
.data:0040405A                 db 'You can send us 2-3 encoded files.',0Dh,0Ah
.data:0040405A                 db 'And attach to the letter a file from the folder c:\Windows\DECODE'
.data:0040405A                 db '.KEY for testing, we will return them to you for FREE',0
.data:0040427D ; const WCHAR String2
```

قطعه کد زیر مربوط به پسوند .BI_D می‌باشد که به انتهای فایل‌ها اضافه می‌شود :

IDA View-A | Hex View-1 | Structures | Enums

```
.data:004042C1 ; const WCHAR word_4042C1
.data:004042C1 word_4042C1     dw 20h                  ; DATA XREF: sub_4013E3+20D↑o
.data:004042C3                 db  69h ; i
.data:004042C4                 db    0
.data:004042C5                 db  64h ; d
.data:004042C6                 db    0
.data:004042C7                 db  2Dh ; -
.data:004042C8                 db    0
.data:004042C9 ; WCHAR WideCharStr
.data:004042C9 WideCharStr     dw 0                    ; DATA XREF: sub_4018A0+219↑o
.data:004042CB                 db    0
.data:004042CC                 db    0
.data:004042CD                 db    0
.data:004042CE                 db    0
.data:004042CF                 db    0
.data:004042D0                 db    0
.data:004042D1                 db    0
.data:004042D2                 db    0
.data:004042D3                 db    0
.data:004042D4                 db    0
.data:004042D5                 db    0
.data:004042D6                 db    0
.data:004042D7                 db    0
.data:004042D8                 db    0
.data:004042D9                 db    0
.data:004042DA                 db    0
.data:004042DB                 db    0
.data:004042DC                 db    0
.data:004042DD ; const WCHAR word_4042DD
.data:004042DD word_4042DD     dw 2Eh                  ; DATA XREF: sub_4013E3+1AA↑o
.data:004042DF                 db  42h ; B
.data:004042E0                 db    0
.data:004042E1                 db  49h ; I
.data:004042E2                 db    0
.data:004042E3                 db  5Fh ; _
.data:004042E4                 db    0
.data:004042E5                 db  44h ; D
.data:004042E6                 db    0
.data:004042E7                 db    0
.data:004042E8                 db    0
.data:004042E9                 db    0
```

نسخه‌های قبلی این باج‌افزار از الگوریتم رمزنگاری AES جهت رمزگذاری فایل‌ها استفاده می‌نمودند، با توجه به قطعه کد زیر علاوه بر الگوریتم مورد اشاره، این نسخه از الگوریتم رمزنگاری RSA نیز استفاده می‌نماید :

IDA View-A | Hex View-1 | Structures | Enums

```
.data:004049FD ; BYTE pbData
.data:004049FD pbData          db 6                    ; DATA XREF: sub_4018A0+115↑o
.data:004049FE                 db    2
.data:004049FF                 db    0
.data:00404A00                 db    0
.data:00404A01                 db    0
.data:00404A02                 db 0A4h ; ñ
.data:00404A03                 db    0
.data:00404A04                 db    0
.data:00404A05                 db  52h ; R
.data:00404A06                 db  53h ; S
.data:00404A07                 db  41h ; A
.data:00404A08                 db  31h ; 1
.data:00404A09                 db    0
.data:00404A0A                 db    8
.data:00404A0B                 db    0
.data:00404A0C                 db    0
.data:00404A0D                 db    1
.data:00404A0E                 db    0
```

این باج‌افزار از کتابخانه‌های ویندوزی به همراه توابعی از هرکدام از کتابخانه‌ها استفاده می‌کند که در تصویر زیر قابل مشاهده است. همچنین لیست کامل این کتابخانه‌ها به همراه توابع مورد استفاده نیز در ادامه‌ی متن آمده است:

IDA View-A | Hex View-1 | Structures | Enums | Imports | Exports

```
.idata:004030F8 ;
.idata:004030F8 ; Imports from mpr.dll
.idata:004030F8 ;
.idata:004030F8 ; DWORD __stdcall WNetEnumResourceA(HANDLE hEnum, LPDWORD lpcCount, LPVOID lpBuffer, LPDWORD lpBufferSize)
.idata:004030F8                 extrn __imp_WNetEnumResourceA:dword
.idata:004030F8                                         ; DATA XREF: WNetEnumResourceA↑r
.idata:004030F8                                         ; .rdata:00403184↓o
.idata:004030FC ; DWORD __stdcall WNetOpenEnumA(DWORD dwScope, DWORD dwType, DWORD dwUsage, LPNETRESOURCEA lpNetResource, LPHANDLE lphEnum)
.idata:004030FC                 extrn __imp_WNetOpenEnumA:dword ; DATA XREF: WNetOpenEnumA↑r
.idata:00403100 ; DWORD __stdcall WNetCloseEnum(HANDLE hEnum)
.idata:00403100                 extrn __imp_WNetCloseEnum:dword ; DATA XREF: WNetCloseEnum↑r
.idata:00403104
.idata:00403108 ;
.idata:00403108 ; Imports from shell32.dll
.idata:00403108 ;
.idata:00403108 ; HINSTANCE __stdcall ShellExecuteA(HWND hwnd, LPCSTR lpOperation, LPCSTR lpFile, LPCSTR lpParameters, LPCSTR lpDirectory, INT nShowCmd)
.idata:00403108                 extrn __imp_ShellExecuteA:dword ; DATA XREF: ShellExecuteA↑r
.idata:00403108                                         ; .rdata:00403178↓o
.idata:0040310C
.idata:00403110 ;
.idata:00403110 ; Imports from user32.dll
.idata:00403110 ;
.idata:00403110 ; BOOL __stdcall UpdateWindow(HWND hWnd)
.idata:00403110                 extrn __imp_UpdateWindow:dword ; DATA XREF: UpdateWindow↑r
.idata:00403110                                         ; .rdata:004031F0↓o
.idata:00403114 ; BOOL __stdcall TranslateMessage(const MSG *lpMsg)
.idata:00403114                 extrn __imp_TranslateMessage:dword
.idata:00403114                                         ; DATA XREF: TranslateMessage↑r
.idata:00403118 ; BOOL __stdcall ShowWindow(HWND hWnd, int nCmdShow)
.idata:00403118                 extrn __imp_ShowWindow:dword ; DATA XREF: ShowWindow↑r
.idata:0040311C ; UINT_PTR __stdcall SetTimer(HWND hWnd, UINT_PTR nIDEvent, UINT uElapse, TIMERPROC lpTimerFunc)
.idata:0040311C                 extrn __imp_SetTimer:dword ; DATA XREF: SetTimer↑r
.idata:00403120 ; LRESULT __stdcall SendMessageA(HWND hWnd, UINT Msg, WPARAM wParam, LPARAM lParam)
.idata:00403120                 extrn __imp_SendMessageA:dword ; DATA XREF: SendMessageA↑r
.idata:00403124 ; ATOM __stdcall RegisterClassExA(const WNDCLASSEXA *)
.idata:00403124                 extrn __imp_RegisterClassExA:dword
.idata:00403124                                         ; DATA XREF: RegisterClassExA↑r
.idata:00403128 ; BOOL __stdcall GetMessageA(LPMSG lpMsg, HWND hWnd, UINT wMsgFilterMin, UINT wMsgFilterMax)
.idata:00403128                 extrn __imp_GetMessageA:dword ; DATA XREF: GetMessageA↑r
.idata:0040312C ; HWND __stdcall GetDlgItem(HWND hDlg, int nIDDlgItem)
.idata:0040312C                 extrn __imp_GetDlgItem:dword ; DATA XREF: GetDlgItem↑r
.idata:00403130 ; LRESULT __stdcall DispatchMessageA(const MSG *lpMsg)
.idata:00403130                 extrn __imp_DispatchMessageA:dword
.idata:00403130                                         ; DATA XREF: DispatchMessageA↑r
.idata:00403134 ; HWND __stdcall CreateDialogParamA(HINSTANCE hInstance, LPCSTR lpTemplateName, HWND hWndParent, DLGPROC lpDialogFunc, LPARAM dwInitParam)
.idata:00403134                 extrn __imp_CreateDialogParamA:dword
.idata:00403134                                         ; DATA XREF: CreateDialogParamA↑r
.idata:00403138
.idata:00403138
```

comctl۳۲.dll	shell۳۲.dll
InitCommonControls	ShellExecuteA

KERNEL۳۲.dll	KERNEL۳۲.dll	user۳۲.dll	ADVAPI۳۲.dll	mpr.dll
CloseHandle	GlobalMemoryStatus	CreateDialogParamA	AdjustTokenPrivileges	WNetCloseEnum
CopyFileA	lstrcatW	DispatchMessageA	CryptAcquireContextA	WNetEnumResourceA
CreateFileA	lstrcmpiA	GetDlgItem	CryptDestroyKey	WNetOpenEnumA
CreateFileMappingA	lstrcmpiW	GetMessageA	CryptDuplicateKey	
CreateFileW	lstrcmpW	RegisterClassExA	CryptEncrypt	
CreateThread	lstrcpyW	SendMessageA	CryptExportKey	
CreateToolhelp32Snapshot	lstrlenA	SetTimer	CryptGenKey	
DeleteFileA	lstrlenW	ShowWindow	CryptImportKey	
ExitProcess	MapViewOfFile	TranslateMessage	LookupPrivilegeValueA	
FindClose	MoveFileW	UpdateWindow	OpenProcessToken	
FindFirstFileW	MultiByteToWideChar		RegCloseKey	
FindNextFileW	OpenProcess		RegOpenKeyExA	
GetCurrentProcessId	Process32FirstW		RegQueryValueExA	
GetEnvironmentVariableA	Process32NextW		RegSetValueExA	
GetFileAttributesW	RtlMoveMemory			
GetLogicalDrives	RtlZeroMemory			
GetModuleFileNameA	SetErrorMode			
GetModuleHandleA	SetFileAttributesW			
GlobalAlloc	SetFilePointer			
GlobalFree	SetThreadPriority			
UnmapViewOfFile	Sleep			
WriteFile	TerminateProcess			

بر اساس بررسی‌های صورت گرفته، باج‌افزار LockCrypt(.BI_D) پس از اجرا، فرایندهای زیر را ایجاد می‌کند :

LockCrypt.exe

- cmd.exe /c vssadmin delete shadows /all

برخی از فایل‌های نوشته شده توسط باج‌افزار :

%WINDIR%\notepad+++.exe
%APPDATA%\microsoft\crypto\rsa\s152112292728218429252461060284298100 3\f58155b4b1d5a524ca0261c3ee99fb50_5f9fe710-99e6-4c04-be62-a7f1b8b321d1
%WINDIR%\decode.key
C:\how to restore files.txt
<REM_DRIVE>:\how to restore files.txt

کلیدهای رجیستری تنظیم شده :

<HKLM>\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\\decrypt
<HKLM>\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\\notepad++
<HKLM>\SOFTWARE\Microsoft\Windows\CurrentVersion\DateTime\\notepad++
<HKLM>\SOFTWARE\Microsoft\Windows\CurrentVersion\DateTime\\cXVxvj0xUv
<HKLM>\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\\PromptOnSecureDesktop
<HKLM>\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\\EnableLUA
<HKLM>\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\\ConsentPromptBehaviorAdmin
<HKCU>\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Personal
<HKCU>\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{289bc201-4726-11e5-8ac9-806d6172696f}\\BaseClass
<HKCU>\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{6a9759b0-c6f5-11e6-92ae-0800279ec8ab}\\BaseClass
<HKCU>\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{b80a4ef0-1b58-11e8-82aa-806d6172696f}\\BaseClass
<HKCU>\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{289bc200-4726-11e5-8ac9-806d6172696f}\\BaseClass
<HKCU>\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{941eacb0-337b-11e6-929c-080027188e55}\\BaseClass
<HKLM>\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Common Documents
<HKCU>\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Desktop
<HKLM>\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Common Desktop
<HKCU>\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Local AppData
<HKCU>\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\\ProxyBypass
<HKCU>\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\\IntranetName
<HKCU>\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\\UNCAsIntranet
<HKLM>\SOFTWARE\Microsoft\Windows\CurrentVersion\DateTime\\notepad++
<HKLM>\SOFTWARE\Microsoft\Windows\CurrentVersion\DateTime\\-3-lZ2BOGX
<HKCU>\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{6519f560-5ee1-11e8-9b5a-806d6172696f}\\BaseClass
<HKLM>\SYSTEM\CURRENTCONTROLSET\SERVICES\kmixer\Enum\Count
<HKLM>\SYSTEM\CURRENTCONTROLSET\SERVICES\kmixer\Enum\NextInstance
<HKLM>\SOFTWARE\Microsoft\Windows\CurrentVersion\DateTime\\notepad++
<HKLM>\SOFTWARE\Microsoft\Windows\CurrentVersion\DateTime\\rJaiOPyBDy
<HKCU>\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{4c0eebc0-1b5a-11e8-a9e8-806d6172696f}\\BaseClass

تحلیل ترافیک شبکه :

پس از بررسی ترافیک شبکه، متوجه هیچ گونه درخواست DNS و تلاش برای برقراری ارتباط با میزبـان در نقطه‌ی جغرافیایی خاص توسط باج‌افزار LockCrypt(.BI_D) نشدیم.

شناسایی :

در حال حاضر یعنی در زمان نگارش این گزارش تعداد ۵۰ مورد از ٦٧ آنتی ویروس و آنتی بدافزار موجـود در سامانه VirusTotal قادر به شناسایی این باج افزار بوده وآن را حذف یا غیرفعال می‌کنند.

Ad-Aware	Generic.Ransom.LockCrypt.A486ED9E	AegisLab	Troj.W32.Antiav!c
ALYac	Trojan.Ransom.LockCrypt	Antiy-AVL	Trojan/Win32.AntiAV
Arcabit	Generic.Ransom.LockCrypt.A486ED9E	Avast	FileRepMalware
AVG	FileRepMalware	Avira	TR/AD.RansomHeur.mulkg
AVware	BehavesLike.Win32.Malware.wsc (mx-v)	Babable	Malware.HighConfidence
Baidu	Win32.Trojan.WisdomEyes.16070401....	BitDefender	Generic.Ransom.LockCrypt.A486ED9E
CAT-QuickHeal	Trojan.Killav	Comodo	UnclassifiedMalware
CrowdStrike Falcon	malicious_confidence_90% (W)	Cybereason	malicious.75a679
Cylance	Unsafe	Cyren	W32/Trojan.YDYH-3133
DrWeb	Trojan.MulDrop8.25554	Emsisoft	Generic.Ransom.LockCrypt.A486ED9E (B)
Endgame	malicious (high confidence)	eScan	Generic.Ransom.LockCrypt.A486ED9E
ESET-NOD32	a variant of Win32/Filecoder.NPA	F-Secure	Generic.Ransom.LockCrypt.A486ED9E
Fortinet	W32/Filecoder.NPA!tr	GData	Generic.Ransom.LockCrypt.A486ED9E
Ikarus	Trojan-Ransom.FileCoder	Jiangmin	Trojan.AntiAV.aly
K7AntiVirus	Trojan (005255be1)	K7GW	Trojan (005255be1)
Kaspersky	HEUR:Trojan.Win32.AntiAV	MAX	malware (ai score=99)
McAfee	Artemis!3CF87E475A67	McAfee-GW-Edition	BehavesLike.Win32.Dropper.lm
Microsoft	Trojan:Win32/Killav	NANO-Antivirus	Trojan.Win32.AntiAV.fddgmt
Palo Alto Networks	generic.ml	Panda	Trj/GdSda.A
Qihoo-360	Win32/Trojan.Anti.afe	Sophos AV	Mal/Generic-S
Sophos ML	heuristic	Symantec	Ransom.Troldesh
Tencent	Win32.Trojan.Generic.Lpca	TrendMicro	TROJ_FRS.VSN01F18
TrendMicro-HouseCall	TROJ_FRS.VSN01F18	VBA32	BScope.Trojan.Invader
VIPRE	BehavesLike.Win32.Malware.wsc (mx-v)	Webroot	W32.Malware.Gen
Yandex	Trojan.AntiAV!M5gU7nOYN/4	ZoneAlarm	HEUR:Trojan.Win32.AntiAV