

باسمه تعالی

تحلیل فنی باج افزار Sigrun

مقدمه :

مشاهده و رصد فضای سایبری در زمینه باج افزار، از شروع فعالیت نمونه جدیدی به نام Sigrun خبر می‌دهد. بررسی‌ها نشان می‌دهد فعالیت این باج افزار 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 باج افزار کاربران روسی را مورد حمله خود قرار نمی‌دهد. طبق بررسی‌های انجام شده به نظر می‌رسد باج افزار GandCrab والد این باج افزار می‌باشد. همچنین برخی از آنتی‌ویروس‌های معتبر آن را از خانواده باج افزار Razy تشخیص داده‌اند. این باج افزار از الگوریتم رمزنگاری AES برای رمزگذاری فایل‌ها استفاده می‌کند و همانند اکثر باج افزارها، پس از رمزگذاری فایل‌ها از قربانیان تقاضای بیت‌کوین می‌کند که برای اطلاع از مقدار باج درخواستی، می‌بایست از طریق ایمیل ذکر شده در پیغام باج‌خواهی با مهاجمین ارتباط برقرار نمود.

مشخصات فایل اجرایی :

نام فایل	sigrun.exe
MD۵	۴adf۹۹۴۴۴۴۵۳e۵a۳ecdc۱۹۷bf۶e۳b۰۰
SHA-۱	۶۲e۳۶c۴۰۰ad۸۳۸۴۲bf۹۵c۳e۱d۳۶۶f۲۳۱۴a۸d۰۸۳c
SHA-۲۵۶	۴۸۵۵۹۰۲۵۳ddae۰۵۱a۴b۲b۸۳۰۴۴f۷۸b۳e۲a۴a۶۷۹۷۵dc۲۹f۸۴۵۰b۹de۴۲۹d۵۳cccf
اندازه فایل	۴۷.۵ KB
کامپایلر	Borland Delphi ۳.۰

فایل اجرایی این باج افزار دارای شش بخش است :

نام بخش	آنتروپی	آدرس مجازی	اندازه مجازی	اندازه خام
.text	۶.۳۹	۴۰۹۶	۱۲۲۸۰	۱۲۲۸۸
.rdata	۴.۴۳	۱۶۳۸۴	۳۴۰۶	۳۵۸۴
.data	۲.۷۴	۲۰۴۸۰	۲۹۳۳۲	۲۹۶۹۶
.CRT	۰.۰۶	۵۳۲۴۸	۴	۵۱۲
.rsrc	۴.۷	۵۷۳۴۴	۴۸۰	۵۱۲
.reloc	۵.۳۸	۶۱۴۴۰	۷۴۰	۱۰۲۴

تحلیل پویا :

برای بررسی عمیق تر باج افزار Sigrun، 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، شروع به رمزگذاری فایل ها می کند و پس از اتمام فرایند رمزگذاری، فایل اجرایی خود را حذف می کند. این باج افزار دو فایل زیر را در کنار فایل های رمزگذاری شده و دایرکتوری های مختلف ایجاد می کند :

۱. فایل RESTORE-SIGRUN.html که شامل پیغام باج خواهی می باشد و پس از اتمام فرایند رمزگذاری فایل ها به نمایش در می آید.
۲. فایل RESTORE-SIGRUN.txt که شامل پیغام باج خواهی، ایمیل مهاجمین و کدشناسایی مربوط به قربانی می باشد.

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

```
RESTORE-SIGRUN.txt - Notepad
File Edit Format View Help
~~~~~SIGRUN 1.0 RANSOMWARE~~~~~

Attention!
All your files documents, photos, databases and other important files are encrypted and have the extension:
.sigrun
The only method of recovering files is to purchase a private key. It is on our server and only we can recover your
files.

But don't worry! You still can restore it!

In order to restore it you need to contact with us via e-mail.

-----
|Our e-mail is: sigrun_decryptor@protonmail.ch|
-----

As a proof we will decrypt 3 files for free!!

Please, attach this to your message:

94 04 00 00 e7 49 3c b5 10 99 81 91 ed 89 b0 1e
e2 e7 dc de db c2 c4 a5 6c 7a 44 3a 3c d6 cc 70
e8 12 52 b1 82 c2 5f 02 dd 3f d6 c7 b2 2e f9 cc
58 8e 9c 11 94 e7 81 e8 a3 cd f3 e0 59 90 a5 34
6d ee 1f ef f7 7e 12 63 94 c1 a7 2e 57 9c 9e 14
48 cf d8 d5 bd 21 4a aa 33 37 41 e3 76 3a cd 3c
53 a0 9b 39 63 9e 15 92 52 99 27 9d ae be 12 cc
79 04 6d 7c 4a 29 ff ad 54 87 55 10 27 3b 11 5e
73 ce 2a 96 bf d2 da 41 e4 f1 8a c6 93 75 f7 6c
fa 17 ce bb dd 46 89 c3 17 cd d4 7a 6b 18 d1 eb
9d 40 fc de dd 16 44 2f 20 a5 89 22 bf 3e 20 b5
26 f1 2b 07 c3 dd 06 02 f0 ef fd 0a 04 30 73 9f
eb 88 7d 36 73 d5 8c 65 4a 1f 29 67 de 51 86 2c
2a e8 86 30 99 e1 57 1b c5 97 18 ff 0a be b6 3d
2f 43 09 01 fd 6c 93 03 59 58 4b 6a be 19 d5 77
7b 20 7d 8a 43 ff d2 76 a3 97 eb 4e 7a e4 37 15
d6 43 65 1e d0 c8 79 06 48 98 5c 64 b7 03 d3 00
68 fb d5 ee 05 fa ce e6 28 be 20 59 9c 63 e2 b4
32 4f a0 62 5b 3c bb ec b4 75 2d 02 6c ee 8f f4
c0 86 af 31 f2 23 00 fb 86 68 b0 4f 42 4c b4 d0
cf 1a 8d ce 73 80 02 68 96 df 65 2e 0f a3 8e b6
c7 3c 7d 23 33 ef d7 9f 13 52 dd de a3 c3 f7 f0
3b 18 3c 7c f2 91 ee aa bf 7e 8d d4 9f 73 67 0e
d4 10 68 e3 e6 fd 72 85 11 30 69 b8 63 cd 9d 2c
60 a0 36 e6 dc 81 e3 f2 d4 22 8f f1 68 79 e4 81
a2 c0 21 8d 3a 86 00 9e 6d 7f db 74 f0 1a cc 60
b4 f5 1d e0 f9 9d f5 69 a4 26 85 9d 98 a4 ba e6
8a 1d 84 2c 5d 45 91 be c3 f0 1f 6d 28 58 4d a1
4f 39 25 82 d2 57 49 d4 83 10 cd 4f 5d 85 1c 7d
bb 5c a0 ba 87 34 d9 6f f0 39 79 08 0a a3 6b cf
21 0a 2f 61 74 ef 07 b9 f3 30 c5 5c 6a 83 5c d2
a8 01 98 c7 61 00 1c fd d8 31 e3 3b c8 1a a9 41
58 c2 0b 69 48 96 99 e6 35 73 db 2e 1b 7a 48 6e
17 a8 83 dd 35 f6 e8 ed d7 d4 bb 44 42 9f cb 75
7c c3 9f 54 c0 57 ff da 54 93 bc fc f8 81 8f b1
5d 0a 6b 19 95 ac d3 e2 4c 5c 21 ec 6c 58 90 32
72 6d c9 18 13 7d b3 54 1c 19 11 ae e8 b9 f3 52
66 f3 17 77 75 10 50 73 8c 39 76 ea 80 42 c9 74
52 a3 a3 94 cc f7 55 a8 ab 5c ad 57 f1 ac 29 82
```

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

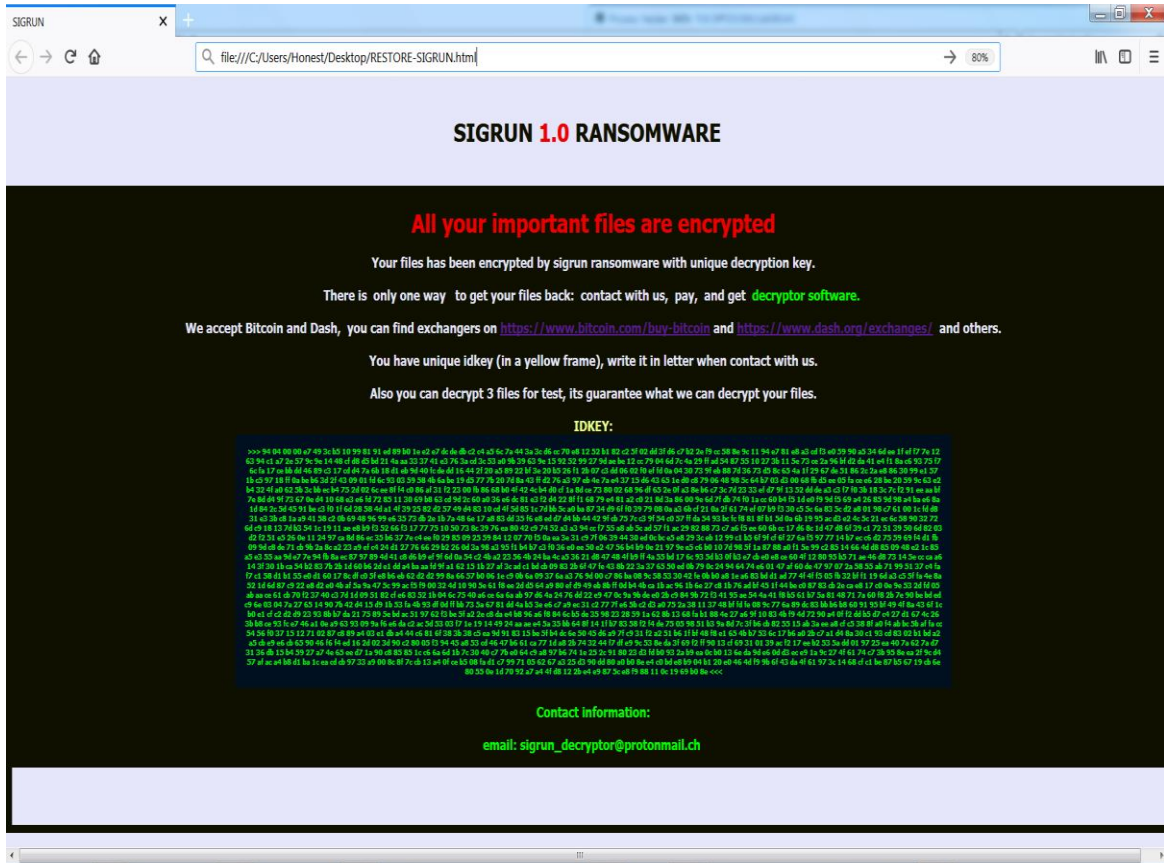
ProgramData, IETldCache, Program Files, All Users, Local Settings, Windows, Tor Browser, Boot

تصویر زیر نشان‌دهنده فایل‌های رمزگذاری شده توسط این باج‌افزار می‌باشد.

Name	Date modified	Type	Size
RESTORE-SIGRUN.html	5/29/2018 3:19 PM	Firefox HTML Doc...	27 KB
dnSpy.zip.sigrun	5/29/2018 3:19 PM	SIGRUN File	23,553 KB
test file (1).bak.sigrun	5/29/2018 3:19 PM	SIGRUN File	84 KB
test file (1).docx.sigrun	5/29/2018 3:19 PM	SIGRUN File	13 KB
test file (1).dwg.sigrun	5/29/2018 3:19 PM	SIGRUN File	115 KB
test file (1).jpg.sigrun	5/29/2018 3:19 PM	SIGRUN File	405 KB
test file (1).kmz.sigrun	5/29/2018 3:19 PM	SIGRUN File	2 KB
test file (1).m.sigrun	5/29/2018 3:19 PM	SIGRUN File	2 KB
test file (1).mov.sigrun	5/29/2018 3:19 PM	SIGRUN File	1,537 KB
test file (1).mp3.sigrun	5/29/2018 3:19 PM	SIGRUN File	6,233 KB
test file (1).mp4.sigrun	5/29/2018 3:19 PM	SIGRUN File	48,438 KB
test file (1).nfo.sigrun	5/29/2018 3:19 PM	SIGRUN File	3 KB
test file (1).pdf.sigrun	5/29/2018 3:19 PM	SIGRUN File	511 KB
test file (1).PNG.sigrun	5/29/2018 3:19 PM	SIGRUN File	13 KB
test file (1).rar.sigrun	5/29/2018 3:19 PM	SIGRUN File	72,216 KB
test file (1).srt.sigrun	5/29/2018 3:19 PM	SIGRUN File	66 KB
test file (1).url.sigrun	5/29/2018 3:19 PM	SIGRUN File	1 KB
test file (2).bak.sigrun	5/29/2018 3:19 PM	SIGRUN File	91 KB
test file (2).docx.sigrun	5/29/2018 3:19 PM	SIGRUN File	540 KB
test file (2).JPG.sigrun	5/29/2018 3:19 PM	SIGRUN File	135 KB
test file (2).mp3.sigrun	5/29/2018 3:19 PM	SIGRUN File	4,070 KB
test file (2).mp4.sigrun	5/29/2018 3:19 PM	SIGRUN File	801 KB
test file (2).rar.sigrun	5/29/2018 3:19 PM	SIGRUN File	29,909 KB
test file (3).jpg.sigrun	5/29/2018 3:19 PM	SIGRUN File	227 KB
RESTORE-SIGRUN.txt	5/29/2018 3:19 PM	Text Document	12 KB

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 باج‌افزار **sigrun** را نشان می‌دهد.



بر اساس پیغام باج‌خواهی، یک کد شناسایی منحصر بفرد 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		Transactions	
Address	1FgTcDK9vuiPTgUXfBodCLYpipcwwfmwGY	No. Transactions	0
Hash 160	a10831a89062743abf15156864c4bb1beba630f9	Total Received	0 BTC
Tools	Related Tags - Unspent Outputs	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 راه‌های 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.

قبل از رمزگذاری

بعد از رمزگذاری

File Comparison

Type	Offset (Source)	Offset (Dest)	Size
Modified	0	0	4,051,723
Inserted	4,051,723	4,051,723	520
Modified	4,051,723	4,052,243	2,329,860

مربوط به پسوند اضافه شده به انتهای فایلها

قطعه کد زیر مربوط به تابع آغاز فعالیت باج افزار می باشد :

```

.text:00402420 ;----- SUBROUTINE -----
.text:00402420
.text:00402420 ; Attributes: noreturn bp-based frame
.text:00402420
.text:00402420 start public start
.text:00402420      push    ebp
.text:00402421      mov     ebp, esp
.text:00402423      and    esp, 0FFFFFFFh
.text:00402426      push  esi
.text:00402427      push  esi
.text:00402428      call   ds:GetCommandLine
.text:0040242E      push  0 ; dwProcessId
.text:00402430      push  0 ; BinheritedHandle
.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:0040244D ;-----
.text:0040244D loc_40244D: call sub_402150 ; CODE XREF: start+23fj
.text:00402452      test   eax, eax
.text:00402454      jz     short loc_40245B
.text:00402456      call   sub_402000
.text:0040245B ;-----
.text:0040245B loc_40245B: call sub_401FB0 ; CODE XREF: start+34fj
.text:0040245D      test   eax, eax
.text:00402460      jnz    short loc_40246B
.text:00402462      push  eax
.text:00402465      call   ds:ExitProcess
.text:0040246B ;-----
.text:0040246B loc_40246B: call ds:SetErrorMode ; CODE XREF: start+42fj
.text:0040246D      ; uMode
.text:00402473      mov    esi, ds:InitializeCriticalSection
.text:00402479      push  offset CriticalSection ; lpCriticalSection
.text:0040247E      call  esi ; InitializeCriticalSection
.text:00402485      call  offset stru_40C240 ; lpCriticalSection
.text:00402487      call  esi ; InitializeCriticalSection
.text:0040248C      push  offset stru_40C268 ; lpCriticalSection
.text:0040248E      call  esi ; InitializeCriticalSection
.text:00402499      mov    esi, ds>DeleteCriticalSection
.text:0040249E      push  offset CriticalSection ; lpCriticalSection
.text:004024A0      call  esi ; DeleteCriticalSection
.text:004024A5      call  offset stru_40C240 ; 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_402000
.text:004024CB start
.text:004024CB      endp

```


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

```

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 باج افزار فایل های موجود در دایرکتوری هایی خاص را رمزگذاری نمی کند
قطعه کد زیر صحت این موضوع را بیان می کند :

```

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 ( SHGetSpecialFolderPath(0, v4, 42, 0) && sub_403480(v3, (int)v4) )
1773             {
1774                 *(_DWORD *)v7 = 1;
1775             }
1776             else if ( !SHGetSpecialFolderPath(0, v4, 43, 0) || !sub_403480(v3, (int)v4)
1777                 && !SHGetSpecialFolderPath(0, v4, 36, 0) || !sub_403480(v3, (int)v4)
1778                 && !SHGetSpecialFolderPath(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 ( lstrcmplw(v5, L"desktop.ini")
1824         && lstrcmplw(v5, L"autorun.inf")
1825         && lstrcmplw(v5, L"ntuser.dat")
1826         && lstrcmplw(v5, L"iconcache.db")
1827         && lstrcmplw(v5, L"bootsect.bak")
1828         && lstrcmplw(v5, L"boot.ini")
1829         && lstrcmplw(v5, L"ntuser.dat.log")
1830         && lstrcmplw(v5, L"thumbs.db")
1831         && lstrcmplw(v5, L"RESTORE-SIGRUN.html")
1832         && lstrcmplw(v5, L"RESTORE-SIGRUN.txt")
1833         && lstrcmplw(v5, L"ntldr")
1834         && lstrcmplw(v5, L"NTDETECT.COM") )
1835         result = lstrcmplw(v5, L"Bootfont.bin") == 0;
1836     else
1837         result = 1;
1838     return result;
1839 }
1840
1841 //----- (00403000) -----

```

بر اساس قطعه کد زیر، باج‌افزار 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     wprintfW(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 باج افزار 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 ; DATA XREF: .rdata:__IMPORT_DESCRIPTOR_KERNEL32To
.rdata:00404780 off_404780 dd rva word_404948
.rdata:00404784 dd rva word_404958
.rdata:00404788 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_404A36
.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_404AF8
.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_404B48
.rdata:004047F8 dd rva word_404B58
.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_404974
.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_40487C
.rdata:0040483C dd rva word_40486C
.rdata:00404840 dd rva word_404D32
.rdata:00404844 dd 0
.rdata:00404848 ; Import names for MPR.dll
.rdata:00404848 ; DATA XREF: .rdata:__IMPORT_DESCRIPTOR_MPRTo
.rdata:00404848 off_404848 dd rva word_404D16
.rdata:0040484C dd rva word_404D06
.rdata:00404850 dd rva word_404CF6
.rdata:00404854 dd 0
.rdata:00404858 ; Import names for SHELL32.dll
.rdata:00404858 ; DATA XREF: .rdata:__IMPORT_DESCRIPTOR_SHELL32To
.rdata:00404858 off_404858 dd rva word_404CD0
.rdata:0040485C dd rva word_404CC0
.rdata:00404860 dd 0
.rdata:00404864 ; Import names for USER32.dll
.rdata:00404864
00003BD8 004047D8: .rdata:004047D8

```

MPR.DLL	SHELL۳۲.dll	USER۳۲.dll
WNetCloseEnum	ShellExecuteW	wsprintfW
WNetEnumResourceW	SHGetSpecialFolderPath	
WNetOpenEnumW		

ADVAPI۳۲.dll	KERNEL۳۲.dll	KERNEL۳۲.dll	KERNEL۳۲.dll	KERNEL۳۲.dll
CryptAcquireContextW	CloseHandle	IstrcatW	GetCommandLineA	VerifyVersionInfoW
CryptDestroyKey	CreateFileW	IstrcmpiW	GetComputerNameW	VerSetConditionMask
CryptEncrypt	CreateThread	IstrcmpW	GetDriveTypeA	VirtualAlloc
CryptExportKey	DeleteCriticalSection	IstrcpyA	GetDriveTypeW	VirtualFree
CryptGenKey	EnterCriticalSection	IstrcpyW	GetLastError	VirtualLock
CryptGetKeyParam	ExitProcess	IstrlenW	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
 - [explore.exe](#) -nohome
 - [explore.exe](#) SCODEF:۳۳۲۰ CREDAT:۷۹۸۷۳
 - [cmd.exe](#) /c timeout -c ۵ & del "C:\Sigrun.exe /f /q
 - [timeout.exe](#) timeout -c ۵

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:

```

IDA View-A
Hex View-1
Structures
Enums

.sub_4020D0:
.text: 004020D0 ; ===== S U B R O U T I N E =====
.text: 004020D0 ; Attributes: noreturn
.text: 004020D0
.text: 004020D0 sub_4020D0 proc near ; CODE XREF: start+361p
.text: 004020D0 ; start+AB1p
.text: 004020D0 push esi
.text: 004020D1 mov esi, ds:VirtualAlloc
.text: 004020D7 push edi
.text: 004020D8 push 4 ; FlProtect
.text: 004020DA push 3000h ; FlAllocationType
.text: 004020DF push 400h ; dwSize
.text: 004020E4 push 0 ; lpAddress
.text: 004020E6 call esi ; VirtualAlloc
.text: 004020E8 push 4 ; FlProtect
.text: 004020EA push 3000h ; FlAllocationType
.text: 004020EF push 400h ; dwSize
.text: 004020F4 push 0 ; lpAddress
.text: 004020F6 mov edi, eax
.text: 004020F8 call esi ; VirtualAlloc
.text: 004020FA mov esi, eax
.text: 004020FC test edi, edi
.text: 004020FE jz short loc_402139
.text: 00402100 push 200h ; nSize
.text: 00402105 push edi ; lpFilename
.text: 00402106 push 0 ; hModule
.text: 00402108 call ds:GetModuleFileNameW
.text: 0040210E test esi, esi
.text: 00402110 jz short loc_402139
.text: 00402112 push edi
.text: 00402113 push offset aCTimeoutC5DelS ; "/c timeout -c 5 & del \"%s\" /f /q"
.text: 00402118 push esi ; LPWSTR
.text: 00402119 call ds:wprintfW
.text: 0040211F add esp, 0Ch
.text: 00402122 push 0 ; nShowCmd
.text: 00402124 push 0 ; lpDirectory
.text: 00402126 push esi ; lpParameters
.text: 00402127 push offset File ; "cmd.exe"
.text: 0040212C push offset Operation ; "open"
.text: 00402131 push 0 ; hwnd
.text: 00402133 call ds:ShellExecuteW
.text: 00402139 loc_402139: ; CODE XREF: sub_4020D0+2E1j
.text: 00402139 ; sub_4020D0+401j
.text: 00402139 push 0 ; uExitCode
.text: 0040213B call ds:ExitProcess
.text: 0040213B sub_4020D0 endp

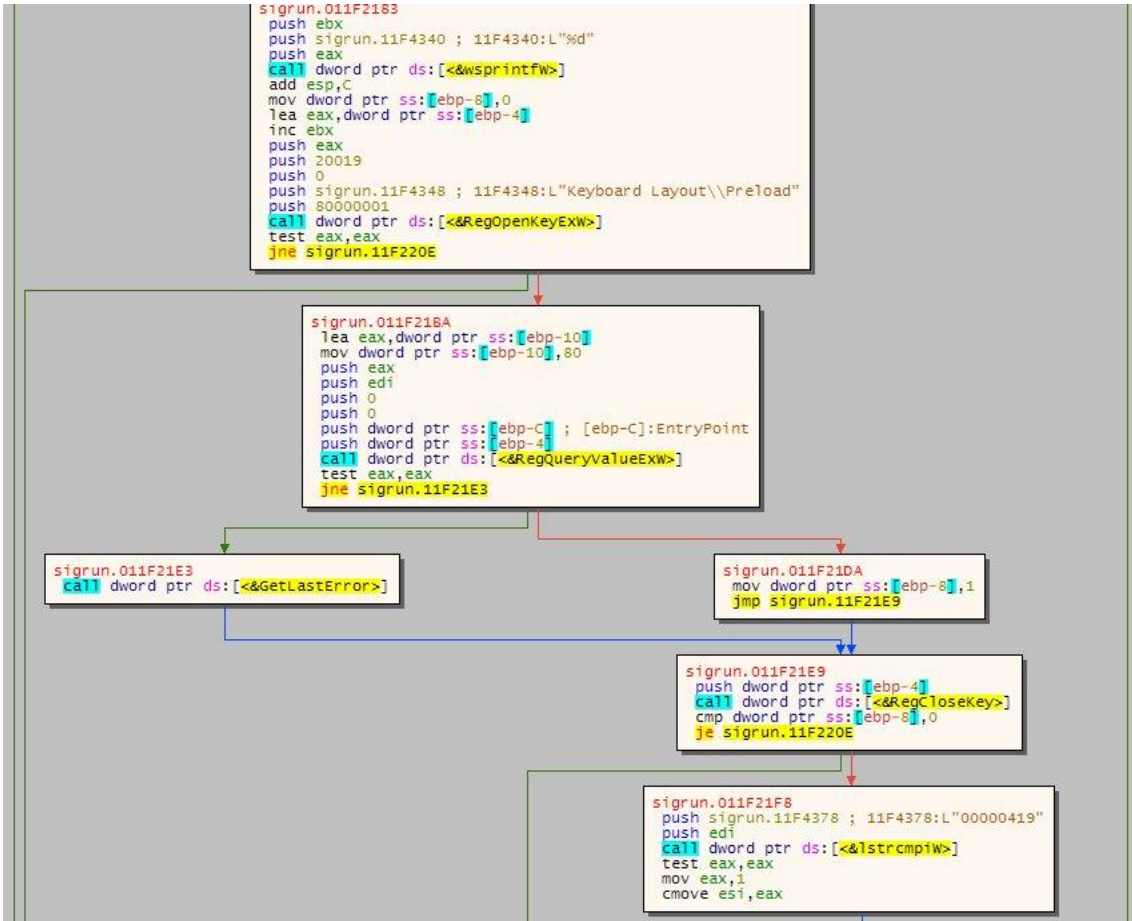
```

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

```
485590253ddae051a4b2b83044f78b3e2a4a67975dc29f8450b9de429d53ccfc.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 ( RegOpenKeyEx(HKEY_CURRENT_USER, L"SOFTWARE\\Valkyrie\\data", 0, 0x20019u, &phkResult) )
737     {
738         result = 0;
739     }
740     else
741     {
742         cbData = 0;
743         if ( !RegQueryValueEx(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 ( !RegQueryValueEx(phkResult, L"public", 0, 0, v6, &cbData) )
750             {
751                 v8 = 0;
752                 RegQueryValueEx(phkResult, L"KeyData", 0, 0, 0, &v8);
753                 if ( v8 < 0xA04 )
754                     v2 = RegQueryValueEx(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 باج افزار کاربران روسی زبان را مورد حمله قرار

نمی دهد.



کلیدهای رجیستری زیر توسط باج افزار به سیستم اضافه می شود :

HKLM\SYSTEM\ControlSet\services\VSS\Diag\SwProvider_{b09e7137-7b9f-4925-af10-51abd70b20d5}

HKLM\SYSTEM\CurrentControlSet\services\VSS\Diag\SwProvider_{b09e7137-7b9f-4925-af10-51abd70b20d5}

HKU\S-1-5-21-549034115-1014311591-3115137102-1000\Software\Classes\Applications

HKU\S-1-5-21-549034115-1014311591-3115137102-1000\Software\Classes\Applications\updater.exe

HKU\S-1-5-21-549034115-1014311591-3115137102-1000\Software\Valkyrie

HKU\S-1-5-21-549034115-1014311591-3115137102-1000\Software\Valkyrie\data

مقدار رجیستری تنظیم شده :

\REGISTRY\USER\S-1-5-21-14124765011645522391417001333500\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 ۶۶ آنتی ویروس و آنتی بدافزار موجود در سامانه VirusTotal قادر به شناسایی این باج‌افزار بوده و آن 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/CryptXPACK.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	Ikarus	⚠ Riskware (0040eff71)
Ikarus	⚠ Riskware (0040eff71)	Kaspersky	⚠ Trojan-Ransom.Win32.Cryptor.bsj
Malwarebytes	⚠ Ransom.SigRun	MAX	⚠ malware (ai score=95)
McAfee	⚠ Generic.dtf	McAfee-GW-Edition	⚠ BehavesLike.Win32.Adware.ConvertAd...
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