بسمه تعالی

گزارش تحلیل باج افزار Spartacus

مقدمه :

رصد فضای سایبری در حوزه باج‌افزار، از ظهور نمونه جدیدی به نام Spartacus خبر می‌دهد. شواهد حاکی از آن است که احتمالاً نام این باج افزار از سریالی به همین نام الهام گرفته شده است. بر اساس گزارشات بدست آمده، فعالیت این باج‌افزار از اواسط ماه آوریل سال ۲۰۱۸ میلادی آغاز گردیده و به نظر می‌رسد تمرکز آن بیشتر بر روی کاربران انگلیسی زبان می‌باشد. *بررسی های صورت گرفته توسط کارشناسان این مرکز نشان می دهد باج افزار Spartacus و باج افزارهای Satyr و BlackRouter که تقریباً همزمان شروع به فعالیت نموده اند، هر سه از خانواده باج‌افزارهای Crypto می‌باشند.* نکته‌ای که در مورد پیغام باج‌خواهی این باج‌افزار به چشم می خورد این است که مبلغ باج متغیر بوده و بر اساس روش ارتباط گیری قربانی با مهاجم تعیین خواهد شد.

مشخصات فایل اجرایی :

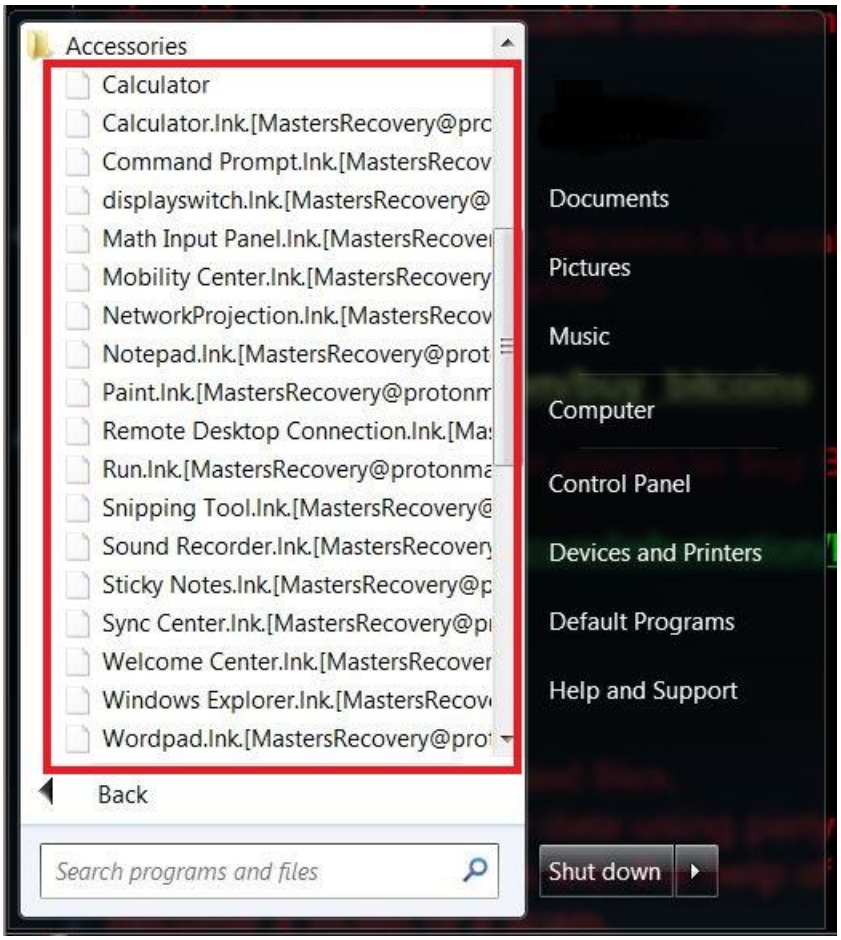
نام فایل	Spartacus.exe, SF.exe
اندازه	۹۴.۵۰ KB (۹۶۷۶۸ bytes)
SHA-۱	a۰۱۲۹۴ffd۵۴۱۲۲۹۷۱۸۹۴۸e۱۷f۷۹۱۶۹۴efb۵۹۶۱۲۳
SHA-۲۵۶	ef۲۵bdbcf۰۵fa۴۷۸df۳ddc۵f۴f۷۱۷c۰۷۰e۴۴۳da۰۴cfc۵۹۰d۴۴۴۰۹c۸۱۵f۲۳۷cb۳
MD۵	۲۵dee۲e۷۰c۹۳۱f۳fa۸۳۲a۵b۱۸۹۱۱۷ce۸
کامپایلر	Microsoft visual C# v۷.۰ / Basic .NET

فایل اجرایی این باج افزار دارای چهار بخش است :

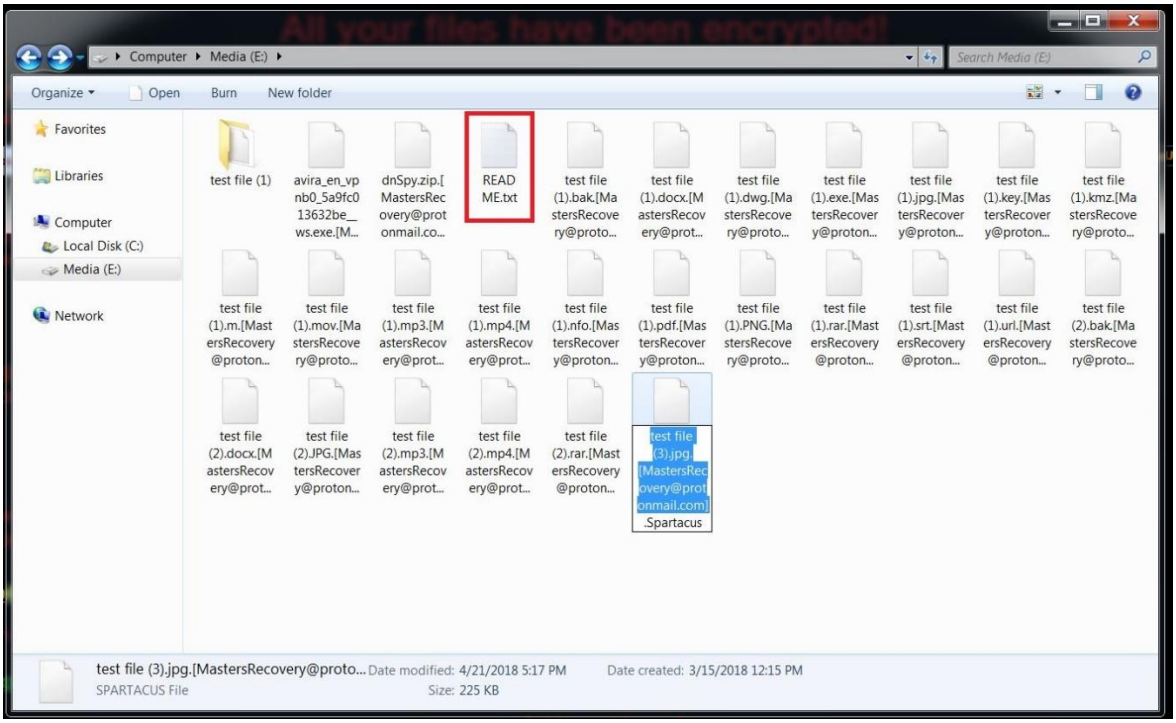
نام بخش	آنتروپی	آدرس مجازی	اندازه مجازی	اندازه خام
.text	۶.۲۳	۸۱۹۲	۹۲۹۰۰	۹۳۱۸۴
.sdata	۶.۶۳	۱۰۶۴۹۶	۴۸۸	۵۱۲
.rsrc	۳.۹۹	۱۱۴۶۸۸	۱۴۰۰	۱۵۳۶
.reloc	۰.۱	۱۲۲۸۸۰	۱۲	۵۱۲

تحلیل پویا :

برای بررسی عمیق‌تر باج افزار Spartacus فایل اجرایی آن را در محیط آزمایشگاهی اجرا کردیم تا عملکرد آن را از نزدیک مورد بررسی قرار دهیم. نتایج حاصل از این بررسی نشان داد باج‌افزار مورد اشاره، فایل‌های موجود در پوشه‌هایی خاص، بدون در نظر گرفتن پسوند آن‌ها و با استفاده از الگوریتم‌های رمزنگاری AES و RSA ۲۰۴۸ بیتی، رمزگذاری می‌کند. پس از رمزگذاری موفقیت‌آمیز فایل‌ها، دسکتاپ سیستم قربانی با به نمایش در آمدن پیغام باج‌خواهی قفل شده و به صورت مستقیم دسترسی به دسکتاپ وجود ندارد. این باج-افزار اغلب ابزارهای کاربردی ویندوز از جمله Calculator ، Snipping Tools ، Sound Recorder و ... را نیز رمزگذاری می کند که منجر به ایجاد اختلال در عملکرد صحیح سیستم عامل می گردد.



تصویر زیر نشان‌دهنده فایل‌های رمزگذاری شده توسط باج‌افزار Spartacus می‌باشد :

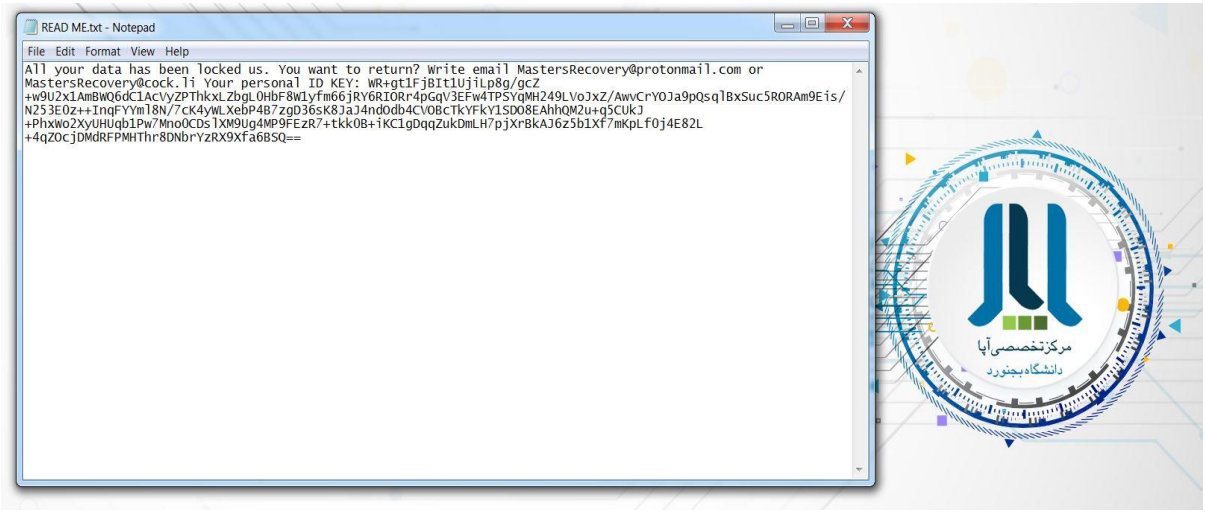


همانطور که در تصویر قابل مشاهده است، پس از رمزگذاری فایل‌ها به انتهای آن‌ها، ایمیل برقراری ارتباط با مهاجم و پسوندی همنام با نام باج‌افزار اضافه می‌شود. همچنین یک فایل متنی با فرمت TXT در هر پوشه‌ای که فایل‌های رمزگذاری شده وجود دارد، ایجاد می‌شود که حاوی ایمیل‌های برقراری ارتباط با مهاجم و شناسه منحصر به فرد قربانیان می‌باشد.

در تصویر زیر پیغام باج خواهی باج‌افزار Spartacus را مشاهده می‌کنید :

بر اساس پیغام باج خواهی، مهاجم اعلام می‌کند که تمام فایل‌های قربانی رمزگذاری شده و در صورت تمایل برای رمزگشایی آن‌ها، می بایست یک ایمیل به همراه کد شخصی موجود در پیغام باج‌خواهی برای وی به آدرس ایمیل MastersRecovery@protonmail.com ارسال نماید. ضمناً در صورت عدم ارسال پاسخ طی ۲۴ ساعت، ایمیل جایگزین به آدرس MastersRecovery@cock.li نیز تعبیه شده است. همچنین مهاجم اعلام نموده که قربانی، مبلغ باج را از طریق کیف پول بیت‌کوین پرداخت نماید اما مبلغ مشخصی برای پرداخت تعیین نشده است. این مبلغ پس از ارتباط گیری با مهاجم از طریق ایمیل‌های ذکر شده مشخص می‌شود که به نظر می‌رسد با توجه به نحوه پرداخت، مبلغ باج‌خواهی متغیر باشد. در ضمن این امکان برای قربانی در نظر گرفته شده که قبل از پرداخت مبلغ باج، تعداد ۵ فایل با حجم کمتر از ۱۰ مگابایت که شامل محتوای ارزشمند از جمله پایگاه داده و فایل‌های پشتیبان نباشد را برای رمزگشایی ارسال نماید. البته توصیه اکید ما به قربانیان باج افزارها در چنین مواقعی این است که هیچگاه به این پیام ها اعتماد نکرده و در صورت وجود فایل‌های پشتیبان، از آن‌ها برای بازگرداندن فایل‌ها استفاده نمایند. در غیر این صورت از ابزارهای رمزگشایی که ممکن است وجود داشته باشند، برای رمزگشایی فایل‌ها استفاده نمایند.

در ادامه، مشاهده گردید در صورتی که قربانی سیستم خود را ری‌استارت نماید، پیغام باج‌خواهی بسته می-شود و یک فایل متنی به فرمت TXT که در تصویر زیر قابل مشاهده است، به وی نشان داده می‌شود که شامل متنی حاوی ایمیل مهاجم و شناسه منحصربفرد مخصوص قربانی می‌باشد.

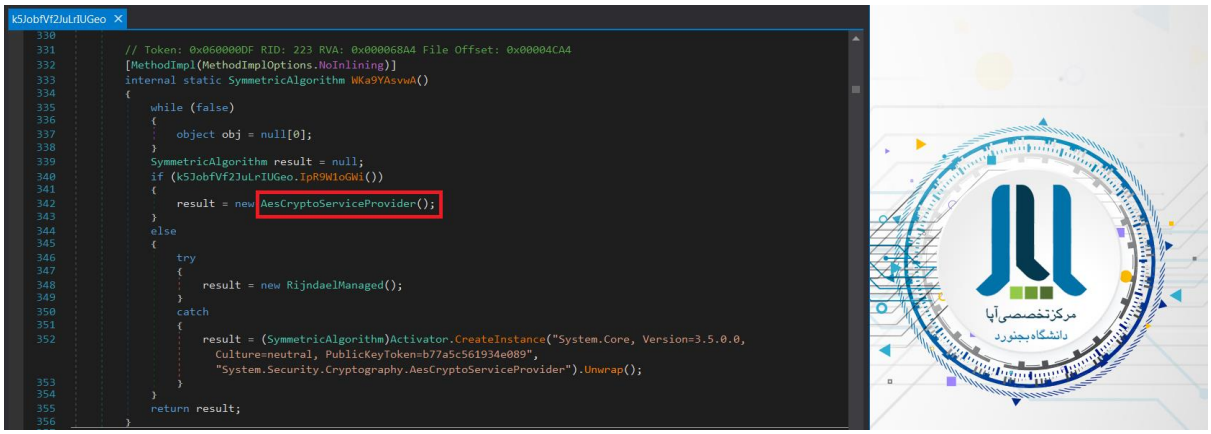


پس از بررسی‌های انجام شده روش مشخصی برای ورود این باج‌افزار یافت نشد اما کارشناسان بر این باورند مانند اکثر باج‌افزارها از روش‌هایی مانند هرزنامه‌ها، فایل‌های مخرب و به روز رسانی‌های جعلی، قربانیان را مورد حمله قرار دهد.

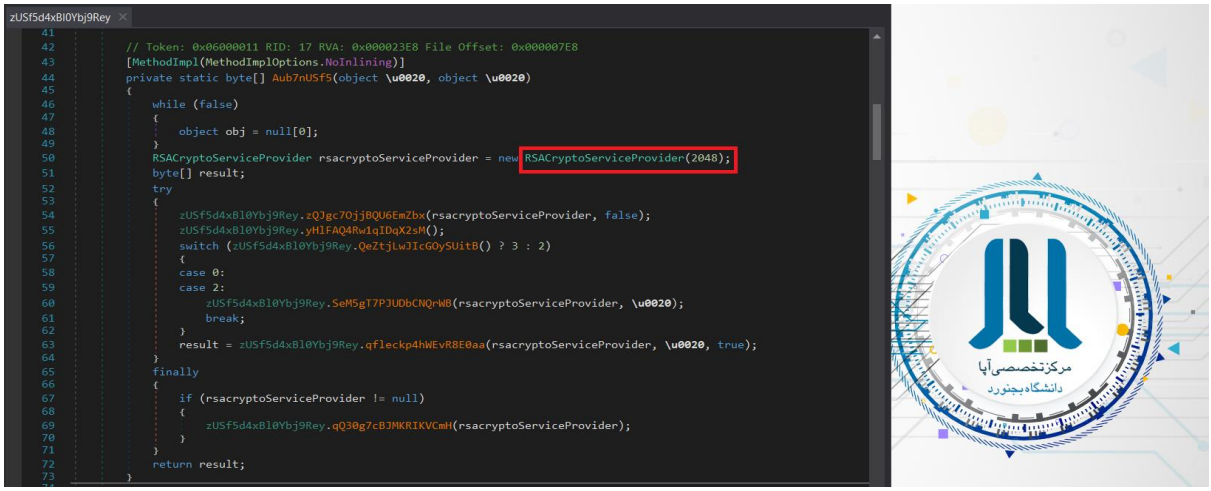
تحلیل ایستا :

پس از تحلیل کد فایل اجرایی باج افزار توسط کارشناسان این مرکز، نتایج زیر حاصل گردید :

همانطور که پیش تر نیز اشاره شد باج‌افزار Spartacus از الگوریتم‌های رمزنگاری AES و RSA ۲۰۴۸ بیتی برای رمزگذاری فایل‌ها استفاده می‌نماید که تصاویر زیر به خوبی گویای این مسئله هستند.



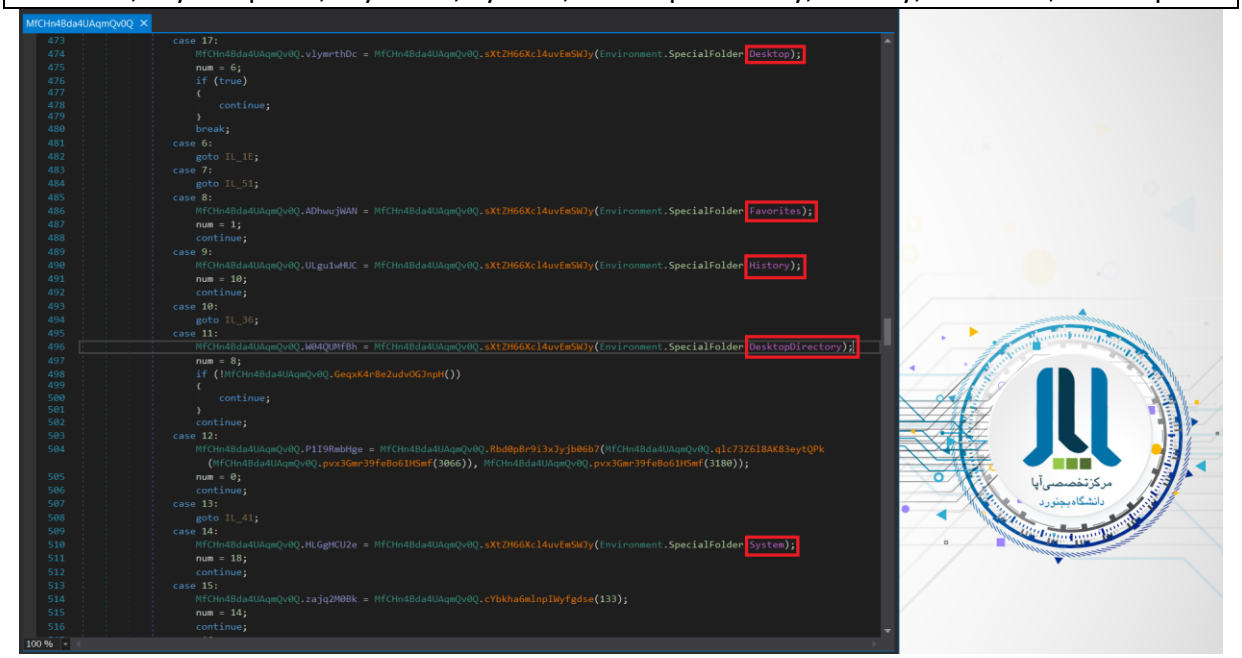
الگوریتم رمزنگاری AES استفاده شده توسط باج‌افزار Spartacus



الگوریتم رمزنگاری RSA ۲۰۴۸ بیتی استفاده شده توسط باج‌افزار Spartacus

بررسی‌ها نشان می‌دهد که باج افزار Spartacus فایل‌های موجود در دایرکتوری‌های خاص را رمزگذاری کند و پس از اتمام فرآیند رمزگذاری، به انتهای تمام فایل‌های موجود در آن دایرکتوری‌ها، عبارت ".MastersRecovery@protonmail.com.Spartacus" اضافه می گردد. این دایرکتوری ها عبارتند از :

Personal, MyComputer, MyMusic, System, DesktopDirectory, History, Favorites, Desktop

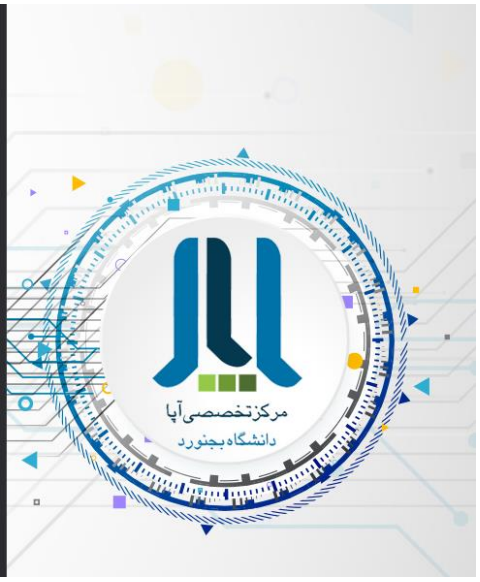


نتایج بدست آمده از تحلیل ها نشان می دهد که باجافزار Spartacus از تابعی به نـام Form۱ بـرای نمـایش پیغام باج‌خواهی و تنظیمات مربوط به آن استفاده می‌کند. این باجافزار در پیغام باج‌خواهی خود یک شناسـه منحصربفرد برای هر قربانی تولید می‌کند که در تصویر زیر نشان داده شده است.

```
KeyGenerator
11  public class KeyGenerator
12  {
13      // Token: 0x060000A4 RID: 164 RVA: 0x00005770 File Offset: 0x00003B70
14      [MethodImpl(MethodImplOptions.NoInlining)]
15      public static string GetUniqueKey(int maxSize)
16      {
17          while (false)
18          {
19              object obj = null[0];
20          }
21          int num = 8;
22          if (!KeyGenerator.CGGrC46Nf05rLkM1xa8())
23          {
24          }
25          StringBuilder stringBuilder;
26          for (;;)
27          {
28              byte[] array;
29              int num2;
30              char[] array2;
31              switch (num)
32              {
33              case 0:
34                  array = new byte[1];
35                  num = 11;
36                  if (!true)
37                  {
38                      goto IL_1AD;
39                  }
40                  continue;
41              case 1:
42                  break;
43              case 2:
44                  goto IL_1AD;
45              case 3:
46              case 5:
47                  goto IL_C2;
48              case 4:
49                  goto IL_143;
50              case 6:
51                  num2 = 0;
52                  goto IL_153;
53              case 7:
54                  goto IL_169;
55              case 8:
56                  array2 = KeyGenerator.m8KMDc6AugOhLJV7i58(KeyGenerator.Cw5BKm6fUmxCNyyg7yR(3208));
57                  num = 0;
58                  if (!KeyGenerator.RVugQU6MSfy7plpSby3())
59                  {
60                      goto Block_4;
61                  }
62                  continue;
```

اما همانطور که در بالا اشاره شد این باج‌افزار پس از اجرا، Desktop سیستم قربانی را قفل می‌نماید و امکان دسترسی مستقیم به آن وجود ندارد. قطعه کدی که در تصویر زیر مشاهده می‌نمایید مربوط به انجام این فرایند می‌باشد.

```
RunOnlyOneClass
10  namespace SF
11  {
12      // Token: 0x02000003 RID: 3
13      public static class RunOnlyOneClass
14      {
15          // Token: 0x06000001 RID: 1
16          [DllImport("user32.dll", EntryPoint = "SetForegroundWindow")]
17          [return: MarshalAs(UnmanagedType.Bool)]
18          private static extern bool PSB9vpF0Y(IntPtr \u0020);
19
20          // Token: 0x06000002 RID: 2
21          [DllImport("user32.dll", EntryPoint = "ShowWindow",
              SetLastError = true)]
22          internal static extern int Bhrk3V38S(int \u0020, int \u0020);
23
24          // Token: 0x06000003 RID: 3 RVA: 0x00002050 File Offset:
              0x00000450
25          [MethodImpl(MethodImplOptions.NoInlining)]
26          public static bool ChekRunProgramm(string UniqueValue)
27          {
28              while (false)
29              {
30                  object obj = null[0];
31              }
32              int num;
33              if (!RunOnlyOneClass.RLn5MnP5LJaIopERgC())
34              {
35                  num = 4;
```



سایر نتایج بدست آمده از تحلیل کد باج افزار :

باج‌افزار Spartacus فقط از کتابخانه ویندوزی زیر به همراه یک تابع از آن، استفاده می‌کند.

mscoree.dll
_CorExeMain

بر اساس بررسی‌های صورت گرفته، این باج‌افزار در مجموع سه فرایند را ایجاد می‌کند که در زیر به همراه دستوراتی که اجرا می‌کنند، قابل مشاهده است.

```
Spartacus.exe

cmd.exe  /c vssadmin.exe delete shadows /all /quiet

vssadmin.exe delete shadows /all /quiet
```

هدف از ایجاد این فرایندها حذف shadow copy های ویندوز می‌باشد که امکان بازیابی فایل‌ها میسر نباشد.

پس از بررسی‌های انجام شده مشخص گردید باج‌افزار Spartacus فایل‌های زیر را در مسیرهای مشخص شده باز می‌کند :

```
C:\Documents and Settings\Administrator\money.doc
C:\Documents and Settings\Administrator\Application Data\Adobe\Acrobat\9.0\AdobeSysFnt09.lst
C:\Documents and Settings\Administrator\Favorites\Desktop.ini
C:\Documents and Settings\Administrator\Application Data\Adobe\Acrobat\9.0\SharedDataEvents
C:\Documents and Settings\Administrator\ntuser.ini
C:\Documents and Settings\Administrator\Application Data\Adobe\Acrobat\9.0\UserCache.bin
C:\Documents and Settings\Administrator\Application Data\Adobe\Acrobat\9.0\JavaScripts\glob.js
C:\Documents and Settings\Administrator\Application Data\Adobe\Acrobat\9.0\JavaScripts\glob.settings.js
C:\READ ME.txt
C:\Documents and Settings\Administrator\Application Data\Macromedia\Flash
Player\#SharedObjects\EEY47AFV\admaster.com.cn\admck.sol
C:\Documents and Settings\Administrator\Application Data\Macromedia\Flash
Player\#SharedObjects\EEY47AFV\macromedia.com\redirectSO.sol
C:\Documents and Settings\Administrator\Application Data\Macromedia\Flash
Player\macromedia.com\support\flashplayer\sys\settings.sol
C:\DiskD\READ ME.txt
C:\Documents and Settings\Administrator\Application Data\Macromedia\Flash
Player\macromedia.com\support\flashplayer\sys\#admaster.com.cn\settings.sol
C:\DiskX\READ ME.txtC:\WINDOWS\system32\cmd.exe
C:\WINDOWS\system32\advapi32.dll
C:\WINDOWS\system32\rpcrt4.dll
C:\WINDOWS\system32\secur32.dll
C:\WINDOWS\system32\shimeng.dll
C:\WINDOWS\AppPatch\AcGenral.dll
C:\WINDOWS\system32\winmm.dll
C:\WINDOWS\system32\ole32.dll
C:\WINDOWS\system32\oleaut32.dll
C:\WINDOWS\system32\msacm32.dll
```

C:\Documents and Settings\Administrator\Application Data\Microsoft\CryptnetUrlCache\Content\2BF68F4714092295550497DD56F57004
C:\DocumentsandSettings\Administrator\ApplicationData\Microsoft\CryptnetUrlCache\Content\60E31627FDA0A46932B0E5948949F2A5
C:\WINDOWS\WINDOWSSHELL.MANIFEST
C:\DocumentsandSettings\Administrator\ApplicationData\Microsoft\CryptnetUrlCache\Content\62B5AF9BE9ADC1085C3C56EC07A82BF6
C:\DocumentsandSettings\Administrator\ApplicationData\Microsoft\CryptnetUrlCache\Content\8DFDF057024880D7A081AFBF6D26B92F
C:\WINDOWS\system32\conime.exe
C:\Documents and Settings\Administrator\Application Data\Microsoft\Internet Explorer\brndlog.bak
C:\Documents and Settings\Administrator\Application Data\Microsoft\Internet Explorer\brndlog.txt
C:\Documents and Settings\Administrator\Application Data\Microsoft\Internet Explorer\Desktop.htt
C:\DocumentsandSettings\Administrator\ApplicationData\Microsoft\InternetExplorer\QuickLaunch\desktop.iniC:\WINDOWS\system32\vssadmin.exe

فایل‌های نوشته شده:

C:\Documents and Settings\Administrator\Application Data\Adobe\Acrobat\9.0\SharedDataEvents
C:\Documents and Settings\Administrator\Application Data\Adobe\Acrobat\9.0\UserCache.bin
C:\Documents and Settings\Administrator\Application Data\Adobe\Acrobat\9.0\JavaScripts\glob.js
C:\Documents and Settings\Administrator\Application Data\Adobe\Acrobat\9.0\JavaScripts\glob.settings.js
C:\READ ME.txt
C:\Documents and Settings\Administrator\Application Data\Macromedia\Flash Player\#SharedObjects\EEY47AFV\admaster.com.cn\admck.sol
C:\DiskD\READ ME.txt
C:\Documents and Settings\Administrator\Application Data\Microsoft\Internet Explorer\brndlog.bak
C:\Documents and Settings\Administrator\Application Data\Microsoft\Internet Explorer\brndlog.txt
C:\Documents and Settings\Administrator\Application Data\SogouExplorer\datapack1
C:\Documents and Settings\Administrator\Application Data\SogouExplorer\datapack2
C:\Documents and Settings\Administrator\Application Data\SogouExplorer\datapack3
C:\Documents and Settings\Administrator\Application Data\SogouExplorer\Dynamark.db
C:\Documents and Settings\Administrator\Application Data\SogouExplorer\Extension.db
C:\Documents and Settings\Administrator\Application Data\SogouExplorer\Favorite2.dat
C:\Documents and Settings\Administrator\Application Data\SogouExplorer\FormData.dat
C:\Documents and Settings\Administrator\Application Data\SogouExplorer\HistoryUrl.db
C:\Documents and Settings\Administrator\Application Data\SogouExplorer\MCPattern.db
C:\Documents and Settings\Administrator\Cookies\administrator@sogou[2].txt
C:\Documents and Settings\Administrator\Cookies\administrator@sohu[1].txt
C:\Documents and Settings\Administrator\Local Settings\Application Data\GDIPFONTCACHEV1.DAT
C:\Documents and Settings\Administrator\Local Settings\Application Data\Adobe\Acrobat\9.0\Cache\AcroFnt09.lst
C:\Documents and Settings\Administrator\Local Settings\Application Data\Adobe\Acrobat\9.0\Updater\updater.log
C:\Documents and Settings\Administrator\Local Settings\Application Data\Adobe\Color\ACECache10.lst
C:\Documents and Settings\Administrator\Templates\amipro.sam
C:\Documents and Settings\Administrator\Templates\excel.xls
C:\Documents and Settings\Administrator\Templates\excel4.xls
C:\Documents and Settings\Administrator\Templates\lotus.wk4
C:\Documents and Settings\Administrator\Templates\powerpnt.ppt
C:\Documents and Settings\Administrator\Templates\presenta.shw
C:\Documents and Settings\Administrator\Templates\quattro.wb2

C:\Documents and Settings\Administrator\Templates\sndrec.wav
C:\Documents and Settings\Administrator\Templates\winword.doc
C:\Documents and Settings\Administrator\Templates\winword2.doc
C:\Documents and Settings\Administrator\UserData\index.dat
C:\Documents and Settings\Administrator\UserData\KL238XQ7\www.skycn[1].xml
C:\Documents and Settings\Administrator\UserData\OH67GPIF\www.skycn[1].xml

فایل‌های حذف شده:

C:\Documents and Settings\Administrator\CMB\PB40\SysData\Cert.db
C:\Documents and Settings\Administrator\CMB\PB40\SysData\CertApply.db
C:\Documents and Settings\Administrator\CMB\PB40\SysData\Certv01.db
C:\Documents and Settings\Administrator\CMB\PB40\SysData\Certv01.db~
C:\Documents and Settings\Administrator\CMB\PB40\SysData\SysCfg.ini
C:\Documents and Settings\Administrator\CMB\PB40\SysData\SysConfig.db
C:\Documents and Settings\Administrator\CMB\PB40\SysData\User.db
C:\Documents and Settings\Administrator\CMB\PB40\SysData\Userv01.db
C:\Documents and Settings\Administrator\CMB\PB40\SysData\Userv01.db~
C:\Documents and Settings\Administrator\Cookies\administrator@sogou[2].txt
C:\Documents and Settings\Administrator\Cookies\administrator@sohu[1].txt
C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\C1OS62RY\collect_111220[2].htm
C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\IUKHR8T2\collect_111220[1].htm
C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\IUKHR8T2\collect_111220[2].htm
C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\IUKHR8T2\grid-narrow-compressed[1].htm
C:\Documents and Settings\Administrator\Recent\system32.lnk
C:\Documents and Settings\Administrator\Recent\wscui.cpl.lnk
C:\Documents and Settings\Administrator\Templates\excel4.xls
C:\Documents and Settings\Administrator\Templates\lotus.wk4
C:\Documents and Settings\Administrator\Templates\powerpnt.ppt
C:\Documents and Settings\Administrator\Templates\presenta.shw
C:\Documents and Settings\Administrator\Templates\quattro.wb2
C:\Documents and Settings\Administrator\Templates\sndrec.wav
C:\Documents and Settings\Administrator\Templates\winword.doc
C:\Documents and Settings\Administrator\Templates\winword2.doc
C:\Documents and Settings\Administrator\UserData\index.dat
C:\Documents and Settings\Administrator\Application Data\SogouExplorer\datapack1
C:\Documents and Settings\Administrator\Application Data\SogouExplorer\datapack2
C:\Documents and Settings\Administrator\Application Data\SogouExplorer\datapack3
C:\Documents and Settings\Administrator\Application Data\SogouExplorer\Dynamark.db
C:\Documents and Settings\Administrator\Application Data\SogouExplorer\Extension.db
C:\Documents and Settings\Administrator\Application Data\SogouExplorer\Favorite2.dat
C:\Documents and Settings\Administrator\Application Data\SogouExplorer\FormData.dat
C:\Documents and Settings\Administrator\Application Data\SogouExplorer\HistoryUrl.db
C:\Documents and Settings\Administrator\Application Data\SogouExplorer\MCPattern.db
C:\Documents and Settings\Administrator\Application Data\SogouExplorer\Misc.db
C:\Documents and Settings\Administrator\Application Data\SogouExplorer\p4p.db
C:\Documents and Settings\Administrator\Application Data\SogouExplorer\rk.dat
C:\Documents and Settings\Administrator\CMB\PB40\SysData\Cert.db

C:\Documents and Settings\Administrator\CMB\PB40\SysData\CertApply.db
C:\Documents and Settings\Administrator\CMB\PB40\SysData\Certv01.db
C:\Documents and Settings\Administrator\CMB\PB40\SysData\Certv01.db~
C:\Documents and Settings\Administrator\CMB\PB40\SysData\SysCfg.ini
C:\Documents and Settings\Administrator\CMB\PB40\SysData\SysConfig.db
C:\Documents and Settings\Administrator\CMB\PB40\SysData\User.db
C:\Documents and Settings\Administrator\CMB\PB40\SysData\Userv01.db
C:\Documents and Settings\Administrator\CMB\PB40\SysData\Userv01.db~
C:\Documents and Settings\Administrator\Cookies\administrator@sogou[2].txt
C:\Documents and Settings\Administrator\Cookies\administrator@sohu[1].txt

تغییرات رجیستری:

کلیدهای رجیستری زیر توسط باج‌افزار در سیستم عامل باز می‌شوند:

\REGISTRY\MACHINE\SOFTWARE\Policies\Microsoft\Windows\Safer\CodeIdentifiers\LogFileName
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\cmd.exe
\REGISTRY\USER\S-1-5-21-1482476501-1645522239-1417001333-500\Software\Policies\Microsoft\Windows\System
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Command Processor\AutoRun
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\vssadmin.exe
\REGISTRY\MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\vssadmin.exe\RpcThreadPoolThrottle
\REGISTRY\MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\cmd.exe\RpcThreadPoolThrottle
\REGISTRY\USER\S-1-5-21-1482476501-1645522239-1417001333-500\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\262144\Paths
\REGISTRY\USER\S-1-5-21-1482476501-1645522239-1417001333-500\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\262144\Hashes
\REGISTRY\USER\S-1-5-21-1482476501-1645522239-1417001333-500\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\262144\UrlZones
\Registry\Machine\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\262144\Paths
\Registry\Machine\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\262144\Hashes
\Registry\Machine\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\262144\UrlZones
\REGISTRY\MACHINE\SOFTWARE\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{dc971ee5-44eb-4fe4-ae2e-b91490411bfc}\HashAlg
\REGISTRY\MACHINE\SOFTWARE\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{dc971ee5-44eb-4fe4-ae2e-b91490411bfc}\ItemSize
\REGISTRY\MACHINE\SOFTWARE\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{dc971ee5-44eb-4fe4-ae2e-b91490411bfc}\SaferFlags
\REGISTRY\USER\S-1-5-21-1482476501-1645522239-1417001333-500\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\Startup
\Registry\MACHINE\System\CurrentControlSet\Control\Session Manager\AppCertDlls
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\Apphelp.dll
\REGISTRY\MACHINE\SOFTWARE\Policies\Microsoft\Windows\Safer\CodeIdentifiers\AuthenticodeEnabled
\Registry\Machine\Software\Policies\Microsoft\Windows\Safer\LevelObjects
\REGISTRY\MACHINE\SOFTWARE\Policies\Microsoft\Windows\Safer\CodeIdentifiers\Levels
\Registry\Machine\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Paths
\REGISTRY\USER\S-1-5-21-1482476501-1645522239-1417001333-500\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\Personal
\REGISTRY\USER\S-1-5-21-1482476501-1645522239-1417001333-500\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\Local Settings

\REGISTRY\MACHINE\Software\Policies\Microsoft\Windows\System
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\uxtheme.dll
\REGISTRY\USER\S-1-5-21-1482476501-1645522239-1417001333-500\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\Desktop
\REGISTRY\USER\S-1-5-21-1482476501-1645522239-1417001333-500\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\Favorites
\REGISTRY\USER\S-1-5-21-1482476501-1645522239-1417001333-500\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\My Music
\REGISTRY\USER\S-1-5-21-1482476501-1645522239-1417001333-500\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\History
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\996E.exe
\Registry\MACHINE\System\CurrentControlSet\Control\SafeBoot\Option
\Registry\Machine\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers
\REGISTRY\MACHINE\SOFTWARE\Policies\Microsoft\Windows\Safer\CodeIdentifiers\TransparentEnabled
\REGISTRY\USER\S-1-5-21-1482476501-1645522239-1417001333-500\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\mscoreei.dll
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\ntdll.dll
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\KERNEL32.dll
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\GDI32.dll
HKLM\System\CurrentControlSet\Control\Session Manager
HKLM\System\CurrentControlSet\Control\Session Manager
HKLM\System\CurrentControlSet\Control\Nls\Sorting\Versions
HKLM\System\CurrentControlSet\Control\Nls\Sorting\Versions
HKLM\System\CurrentControlSet\Control\SafeBoot\Option
HKLM\System\CurrentControlSet\Control\Srp\GP\DLL
HKCU\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers
HKLM\SOFTWARE\Microsoft\.NETFramework\Policy\v۴.۰
HKLM\Software\Microsoft\.NETFramework
HKLM\System\CurrentControlSet\Control\Error
HKLM\System\CurrentControlSet\Control\Error

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 Spartacus نشدیم.

شناسایی :

در حال حاضر یعنی در زمان نگارش این گزارش، تعداد ۴۶ مورد از ۶۸ آنتی‌ویروس معتبر دنیا قادر به تشخیص آلودگی این باج‌افزار در سامانه VirusTotal شده‌اند.

Ad-Aware	Trojan.GenericKD.40189340	AegisLab	Troj.Ransom.W32.Crypren!c
AhnLab-V3	Trojan/Win32.Crypren.C2465616	ALYac	Trojan.Ransom.Spartacus
Antiy-AVL	Trojan[Ransom]/Win32.Crypren	Arcabit	Trojan.Generic.D2653D9C
Avast	Win32:Malware-gen	AVG	Win32:Malware-gen
Avira	TR/Ransom.odaei	AVware	Trojan.Win32.Generic!BT
BitDefender	Trojan.GenericKD.40189340	CAT-QuickHeal	Trojan.Occamy
Comodo	UnclassifiedMalware	CrowdStrike Falcon	malicious_confidence_100% (W)
Cylance	Unsafe	Cyren	W32/Trojan.RRUP-6464
DrWeb	Trojan.Encoder.25098	Emsisoft	Trojan.GenericKD.40189340 (B)
eScan	Trojan.GenericKD.40189340	ESET-NOD32	MSIL/Filecoder.MT
F-Secure	Trojan.GenericKD.40189340	Fortinet	W32/Crypren.AEII!tr
GData	Trojan.GenericKD.40189340	Ikarus	Trojan-Ransom.Spartacus
K7AntiVirus	Trojan (0052d79c1)	K7GW	Trojan (0052d79c1)
Kaspersky	Trojan-Ransom.Win32.Crypren.aeii	Malwarebytes	Ransom.Spartacus
McAfee	RDN/Ransom	McAfee-GW-Edition	RDN/Ransom
Microsoft	Trojan:Win32/Occamy.B	Palo Alto Networks	generic.ml
Panda	Trj/GdSda.A	Qihoo-360	Win32/Trojan.Ransom.f9b
SentinelOne	static engine - malicious	Sophos AV	Mal/Generic-S
Sophos ML	heuristic	Symantec	Trojan.KillDiskmens
Tencent	Win32.Trojan.Crypren.Hsta	TrendMicro	Ransom_STACUS.THDAFAH
TrendMicro-HouseCall	Ransom_STACUS.THDAFAH	VIPRE	Trojan.Win32.Generic!BT
ViRobot	Trojan.Win32.Z.Crypren.96768	Webroot	W32.Trojan.GenKD
Yandex	Trojan.Crypren!AkeYVfpKhN8	ZoneAlarm	Trojan-Ransom.Win32.Crypren.aeii