

بسمه تعالی

گزارش تحلیل باج افزار WannaPeace RansSIRIA

مقدمه :

مشاهده و رصد فضای سایبری در زمینه باج افزار، از ظهور نمونه جدیدی به نام RansSIRIA خبر می‌دهد. باج افزار RansSIRIA برای نخستین بار در تاریخ ۲۰ آوریل ۲۰۱۸ میلادی مشاهده گردید که به نظر می‌رسد جامعه کاربران پرتغالی زبان را مورد هدف قرار داده است. *مشاهدات حاکی از آن است که هدف سازندگان این باج افزار در ظاهر کمک به مردم بیگناه و جنگ زده است. سازندگان این باج افزار ادعا می‌کنند مبلغ باج جمع آوری شده از این باج افزار را صرف کمک به مردم سوریه خواهند کرد اما بررسی‌ها نشان می‌دهد این ادعایی دروغین است!!*

مشخصات فایل اجرایی :

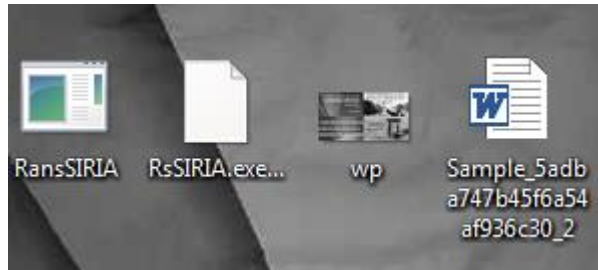
نام فایل	RsSIRIA.exe
MD۵	۵۰۷۱۷۳۲edda۳۶۸۶۶fea۶۱۷۴۱۵۰b۱۶e۲۹
SHA-۱	۷۶b۷bcbf۱۰۹۷c۶c۴۵b۵afa۰dfa۹۶۴۲۱۷۴۴۳۵۳e۲۵۰
SHA-۲۵۶	۴d۵۲۳۲ed۶۸۲۳۹۰ec۴۵۹۰۰۹۶۵۷ddda۲۲df۷d۸۲e۷۲۸۲cca۱۰۵۴۳a۸۵a۳۲d۹f۹۹a۵۳
اندازه فایل	۱.۵۸ MB
کامپایلر	Microsoft visual C# v۷.۰ / Basic .NET

فایل اجرایی این باج افزار دارای سه بخش است :

نام بخش	آنتروپی	آدرس مجازی	اندازه مجازی	اندازه خام
.text	۷.۸۱	۸۱۹۲	۱۶۱۵۱۹۲	۱۶۱۵۳۶۰
.rsrc	۲.۲۶	۱۶۳۰۲۰۸	۳۹۵۹۴	۳۹۹۳۶
.reloc	۰.۱	۱۶۷۱۱۶۸	۱۲	۵۱۲

تحلیل پویا :

نتایج حاصل از اجرای نمونه باج افزار در محیط آزمایشگاهی نشان می‌دهد که این باج‌افزار به محض اجرا، چهار فایل به نام‌های RansSIRIA ، RsSIRIA.exe.Config ، یک فایل متنی بنام log.txt (که حاوی آدرس فایل‌های رمزگذاری شده و اطلاعات دیگر می‌باشد) و همچنین تصویر پس‌زمینه‌ای که پس از رمزگذاری تغییر می‌دهد را در همان دایرکتوری قرار می‌دهد.



سپس، تصویری شبیه تصویر بازگشایی نرم افزار Microsoft Word در وسط صفحه ظاهر می شود.



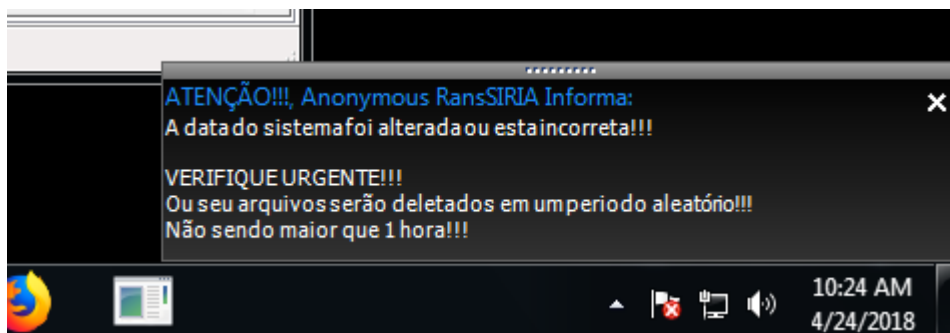
در ادامه تصویری به شکل زیر نیز ظاهر می گردد که حاوی جمله ای به زبان پرتغالی است.

Aguarde, verificando matematicamente a chave inserida...

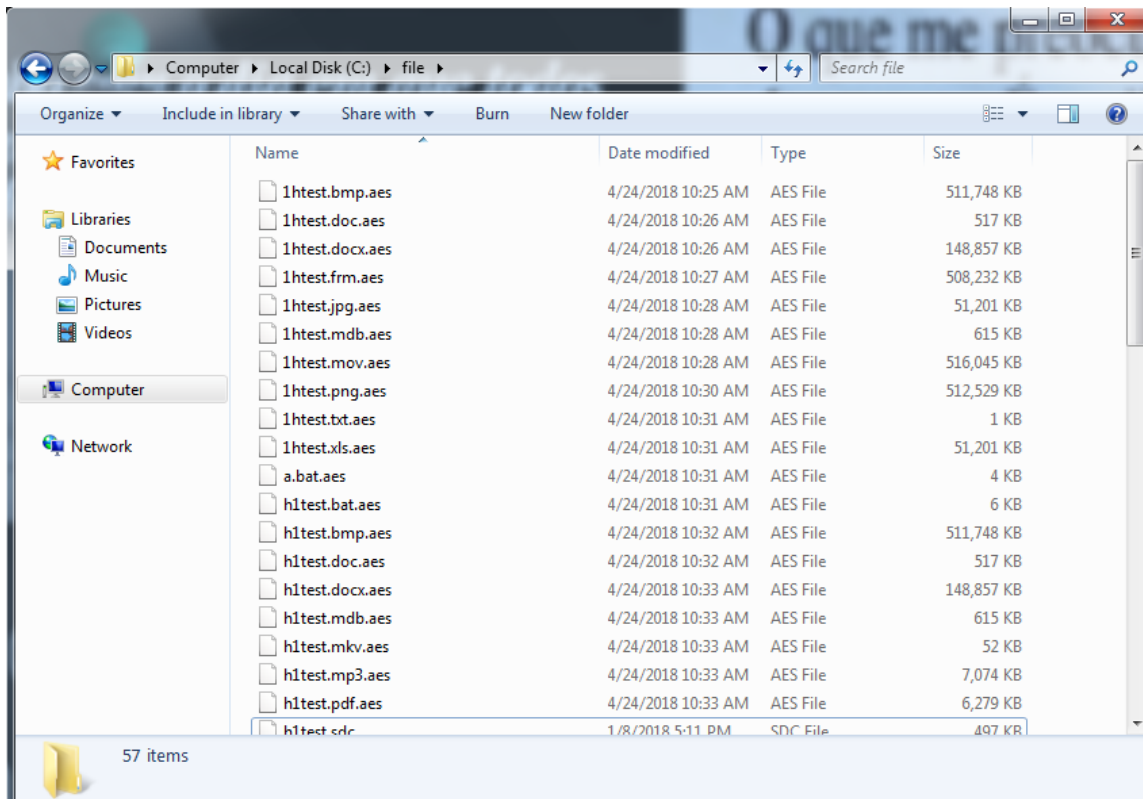
مضمون این پیغام، بررسی کلید های وارد شده است که احتمالاً منظور، کلید رمزگذاری است. پس از چند دقیقه تصویر پس زمینه به تصویر زیر تغییر کرده و پیغام باجخواهی نیز ظاهر می گردد.



همانطور که ملاحظه می کنید تصویر پس زمینه، حاوی چهار نقل قول از افراد مشهور و متفکر جهان از جمله نلسون ماندلا بوده که مضمون صلح طلبی و ترک خشونت دارند. به نظر می رسد مهاجم با این پیام ها سعی در جریحه دار کردن احساسات قربانیان و جلب اعتماد آنان را داشته است. در ادامه، مشاهده گردید که هر چند دقیقه یکبار پیامی به صورت هشدار برای ایجاد اضطراب و جلب توجه قربانی، در قسمت پایین راست صفحه نیز نمایش داده می شود.



گفتنی است که این باج افزار پس از اتمام فرآیند رمزگذاری، پسوند aes را به انتهای فایل های رمزگذاری شده، اضافه می کند. در تصویر زیر تعدادی فایل با پسوند های مختلف که توسط باج افزار RansSIRIA رمزگذاری می گردد را مشاهده می کنید.



در ادامه به بررسی پیغام باج‌خواهی می‌پردازیم.

پنجره گرافیکی پیغام باج‌خواهی این باج‌افزار با نمایش تصویر زیر گشوده می‌شود.



و پس از چند لحظه، پنجره زیر نمایان شده که حاوی مطالب مهمی در مورد باج‌افزار است.



Desculpe.., seus arquivos foram encriptados!

Permita nos apresentar como **Anonymous**, e **Anonymous** apenas.
Nós somos uma idéia. Uma idéia que não pode ser contida, perseguida nem aprisionada.

Milhares de seres humanos estão nesse momento rufigiados, feridos, com fome e sofrendo...
Todos como vítimas de uma guerra que não é nem mesmo deles!!!

Mas infelizmente apenas palavras não mudarão a situação desses seres humanos...

NÃO queremos os seus arquivos ou lhe prejudicar.... queremos apenas uma pequena contribuição...
Lembre-se..., contribuindo você não vai estar apenas recuperando os seus arquivos...
...e sim ajudando a recuperar a dignidade dessas vitimas...

Envie a sua contribuição de apenas: **0.01** Litecoins para carteira/endereço abaixo.


 **litecoin**
accepted here



 **litecoin**
accepted here

 **LSfKetPxMsu5GwdF8Tm6oKArb4eVYP8vqU**

 <-- Confirmar Contribuição

Desbloquear Arquivos --> 

Obter Litecoin

Sobre o Litecoin

Mais informações

A sua CONTRIBUIÇÃO deverá ser efetuada até
4/27/2018 2:46:46 PM
Tempo Restante
D H M S
02:23:49:11

Arquivos totalmente PERDIDOS até
5/3/2018 2:46:46 PM
Tempo Restante
D H M S
08:23:49:11

@AnonymousBr - #PAZ

محتوای این متون که به زبان پرتغالی نوشته شده بدین شرح است که ابتدا خود را ناشناس معرفی کرده و سپس از میلیون‌ها انسان که در جنگ مورد آزار، جراحت و گرسنگی قرار گرفته‌اند سخن گفته و در ادامه با بیان اینکه "با حرف چیزی تغییر نمی‌کند" اقدام خود را قدمی در جهت کمک مالی به جنگ‌زدگان بیان نموده است. سپس در متن آبی رنگ می‌خوانیم که نویسندگان این باج‌افزار قصد نابودی فایل‌ها را ندارند و فقط برای کمک به جنگ‌زدگان تلاش می‌کنند !!!

همانطور که در تصویر مشخص است، مبلغ باج یا به اصطلاح سهم قربانی برای کمک، ۰.۰۱ لایت کوین در نظر گرفته شده و آدرس کیف پول لایت کوین نیز در پایین پنجره قرار داده شده است. همچنین در سمت چپ دو شمارنده وجود دارد که یکی از آن‌ها به مدت ۳ روز و شمارنده بعدی به مدت ۹ روز می‌باشد. شمارنده اول (۳ روز) مهلت پرداخت ۰.۰۱ لایت کوین به مهاجم بوده و شمارنده دوم (۹ روز) مهلتی برای سالم باقی ماندن فایل‌های قربانی است و اگر قربانی تا ۹ روز مبلغ باج را نپردازد، فایل‌ها برای همیشه حذف خواهند شد.

پس از کلیک بر روی علامت قفل سبز رنگ، صفحه جدیدی گشوده می‌شود که در تصویر زیر قابل مشاهده است:

در این بخش، قربانی باید ایمیل خود را برای ارتباط با مهاجم در فیلد اول وارد نماید. در فیلد دوم، امکان کمک بیشتر به جنگ‌زدگان وجود دارد که فیلد سمت راست مقدار کمک مالی و سمت چپ شماره حساب باید وارد شود. همچنین در فیلد سوم، قربانی امکان بیان انتقادات و پیشنهادات خود را نیز داراست.

در بخش دیگری از پیغام باج‌خواهی، صفحه‌ای مشابه پیغام باج‌خواهی باج‌افزارهای دیگر قرار دارد مبنی بر اینکه چه اتفاقی افتاده است و تهدید قربانی در صورت عدم پرداخت باج و همچنین راهنمایی قربانی درباره پرداخت باج چگونه انجام می‌گیرد.

Seus ARQUIVOS importantes foram CRIPTOGRAFADOS!!!

Muitos de seus documentos, fotos, vídeos, bancos de dados e outros arquivos não podem mais ser acessados sem uma CHAVE de descriptação VÁLIDA, esta que poderá ser obtida somente se a DOAÇÃO solicitada for confirmada! ...através de uma e-mail válido lhe a ENVIAREMOS em seguida. ;)

Posso RECUPERAR meus arquivos?, ...e é CONFIÁVEL?

CLARO!! Somos os Anonymous!! Somos uma legião respeitada!!! E RESPEITAMOS igualmente!!! temos a missão de que mudanças necessárias ocorram em nosso planeta!!! Usamos o nosso conhecimento apenas para causas nobres!!! portanto GARANTIMOS que você poderá recuperar todos os seus arquivos com segurança e facilidade. Mas você não tem muito tempo..., enquanto você lê esse texto milhares de seres humanos estão em situações desesperadoras! Se você necessita descriptografar seus arquivos, você precisará efetuar a doação solicitada (lembre-se que a causa é nobre...). Você tem 3 dias úteis para efetuar a doação. Depois disso, o valor será triplicado!!! Além disso, se você não efetuar a doação em 7 dias úteis não poderá mais recuperar seus arquivos para sempre!

Como DOAR?

A DOAÇÃO é aceita apenas em LITECOIN (atenção!!! não confundir com BITCOIN). Para obter mais informações, clique em <Sobre o Litecoin>.... Verifique o preço atual do Litecoin e compre alguns, caso deseje indicamos uma corretora de criptomoedas confiável no Brasil, clique em <Obter Litecoin>. Envie o valor correto para o endereço Litecoin especificado na janela principal. Após a doação, clique em <Confirmar Contribuição>. e aguarde... Uma vez que a doação for confirmada em nossos sistemas, você receberá um e-mail contendo a chave válida e poderá começar a desbloquear/descriptografar seus arquivos imediatamente ;)

Atenção!, Em alguns casos o processo para aquisição dos Litecoins pode levar horas ou até dias dependendo do processo cadastral da corretora escolhida para obtê-los, portanto aconselhamos iniciar o quanto antes o processo para adquiri-los

در ادامه، مشاهده گردید در بخشی دیگر نیز پیامی جهت اطلاعات بیشتر به قربانی نمایش داده می‌شود که در آن به جهانی بودن این حرکت اشاره شده و همچنین با بیان اینکه "ما به دنبال شهرت و مقام نیستیم" مهاجم هدف خود مبنی بر فریب کاربر را دنبال می‌کند و از قربانی درخواست می‌کند که این پیام را در پیام‌رسان WhatsApp و یا شبکه‌های اجتماعی دیگر نیز منتشر کند.

تحلیل ایستا :

پس از بررسی کدمنبع باج‌افزار RansSIRIA توسط کارشناسان این مرکز، نتایج زیر حاصل گردید :

تصویر زیر بخشی از کد را نشان می‌دهد که در آن باج‌افزار سعی در شناسایی پسوند فایل‌های رمزگذاری شده را دارد. همچنین فایل رمزگذاری شده را در قالب متنی که به عنوان log در فایل log.txt یادداشت می‌کند، قرار می‌دهد.


```
foreach (Object obj in items)
{
    string text = (string)obj;
    if (Directory.Exists(text))
    {
        bool @checked = this.chkSubFolders.Checked;
        IEnumerable<string> folderFilesPaths = text.GetFolderFilesPaths(@checked);
        foreach (string file in folderFilesPaths)
        {
            if (file.CheckExtension(this.lstEx.Text.ParseExtensions()))
            {
                if (!file.EndsWith(".aes"))
                {
                    try
                    {
                        await file.EncryptFileAsync(this.fvfv.Text);
                        this.Log(file + " Encriptado.");
                        count++;
                        if (this.chkDeleteOrg.Checked)
                        {
                            Delete.DeleteFile(file);
                        }
                        this.lblsystemtype.Text = file;
                        goto IL_24C;
                    }
                }
            }
        }
    }
}
```

پس از گذشت لحظاتی، آدرسی در مرورگر وب گشوده می‌شود که در آن صفحه ای حاوی تصاویر کودکان سوری به نمایش گذاشته شده است. سپس لینک دیگری متعلق به یک ویدیو گشوده می‌شود که در آن تصاویری احساسی از یک دختر بچه (احتمالاً اروپایی) نمایش داده می‌شود که در آرامش و امنیت به سر برده و به مرور دچار جنگ و مشکلات ناشی از آن می‌گردد. این لینک‌ها در کد منبع این باج‌افزار یافت شد که در زیر تصویری از کد آن قابل ملاحظه است.

```
Directory.GetCurrentDirectory()
}) + "\\Chrome.lnk";
if (File.Exists(text ?? ""))
{
    File.Delete(text);
}
Process.Start("https://goo.gl/qNxDFP");
```

```
this.gbLog.Visible = false;
this.Log(string.Format("RansSIRIA Done!! : {0} File(s) Encrypted for Many Lives.", count));
this.Text = "@Anonymous - RansSIRIA";
string text3 = Path.Combine(new string[]
{
    Directory.GetCurrentDirectory()
}) + "\\log.txt";
if (!File.Exists(text3 ?? ""))
{
    StreamWriter streamWriter2 = new StreamWriter(text3 ?? "", true);
    streamWriter2.WriteLine(this.txtLog.Text);
    streamWriter2.Close();
}
this.lbl131.Text = "done";
Process.Start("https://www.youtube.com/watch?v=pPlnxIzt8gE");
base.Close();
}
if (count == 0)
{
    this.pnlBtns.Visible = false;
    this.pdn.Visible = false;
    this.gbLog.Visible = false;
}
```

بررسی ها نشان می دهد که باج افزار RansSIRIA با توجه به دامنه یافت شده در تصویر زیر، احتمالاً سعی در شناسایی موقعیت جغرافیایی قربانی را دارد.

```
this.webBrowser3.Url = new Uri("https://www.geoiptool.com/", UriKind.Absolute);
```

همچنین دامنه زیر نیز مورد بررسی قرار گرفت.

```
this.webBrowser4.Url = new Uri("http://domain707.tk/", UriKind.Absolute);
```

این دامنه دارای صفحه ساده‌ای همراه با پیام خاصی است که با شعارهای این باج‌افزار همسو می‌باشد.

Be the change you want to see in the world

garaz.zeboreb

همانطور که در تصویر بالا مشاهده می‌کنید، عبارت "garaz.zeboreb" دیده می‌شود که پس از بررسی‌های بیشتر، یک آدرس پست الکترونیکی با همین نام یافت شد.

```
this.textBox15.Text = "garaz.zeboreb@aol.com";
```

توابع مورد استفاده :

- ADVAPI۳۲.dll
- C:\WINDOWS\Microsoft.NET\Framework\v۴.۰.۳۰۳۱۹\mscorlib.dll
- SHLWAPI.dll
- C:\WINDOWS\Microsoft.NET\Framework\v۴.۰.۳۰۳۱۹\clr.dll
- mscoree.dll
- ntdll
- rpcrt۴.dll

- C:\WINDOWS\assembly\NativeImages_v4.0.30319_32\mscorlib\cece9d0256e18427b64587ba690605d4\mscorlib.ni.dll
- AdvApi32.dll
- HookSwitchHookEnabledEvent
- C:\WINDOWS\system32\MSCTF.dll
- C:\WINDOWS\Microsoft.NET\Framework\v4.0.30319\culture.dll
- ole32.dll
- C:\WINDOWS\Microsoft.NET\Framework\v4.0.30319\mscorlib.dll
- kernel32.dll
- C:\WINDOWS\Microsoft.NET\Framework\v4.0.30319\clrjit.dll
- C:\WINDOWS\assembly\NativeImages_v4.0.30319_32\System\7169c473071af03077b1cd2a9c1dbcbe\System.ni.dll
- C:\WINDOWS\assembly\NativeImages_v4.0.30319_32\System.Drawing\cad0df97be252ddb8a846b61f26a4dd\System.Drawing.ni.dll
- C:\WINDOWS\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\039d68cb3f0e971d7d4fa92dc6a259bf\System.Windows.Forms.ni.dll
- uxtheme.dll
- user32.dll
- imm32.dll
- comctl32.dll
- gdi32.dll
- advapi32.dll
- C:\WINDOWS\Microsoft.NET\Framework\v4.0.30319\mscorrc.dll
- NTDLL.DLL
- 996E.exe
- C:\WINDOWS\Microsoft.NET\Framework\v4.0.30319\diasymreader.dll

کلیدهای رجیستری زیر نیز در فرآیند این باج افزار گشوده شده‌اند:

- \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-۱-۵-۲۱-۱۴۸۲۴۷۶۵۰۱-۱۶۴۵۵۲۲۳۹-۱۴۱۷۰۰۱۳۳۳-۵۰۰\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\KERNEL۳۲.dll
- \Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\GDI۳۲.dll
- \Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\USER۳۲.dll
- \Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\Secur۳۲.dll
- \Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\RPCRT۴.dll
- \Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\ADVAPI۳۲.dll
- \Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\msvcrt.dll
- \Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\WS۲HELP.dll
- \Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\WS۲_۳۲.dll
- \Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\SHLWAPI.dll
- \Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\PSAPI.DLL
- \Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\winime۳۲.dll
- \Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\mscoree.dll
- \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\mscoree.dll\CheckAppHelp
- \Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\IMM۳۲.DLL
- \Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\USP۱۰.dll
- \Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\LPK.DLL
- \Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\MSVCR۱۰۰_CLR۰۴۰۰.dll
- \Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\clr.dll

- \REGISTRY\MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\۹۹۶E.exe\RpcThreadPoolThrottle
- \REGISTRY\MACHINE\Software\Policies\Microsoft\Windows NT\Rpc
- \Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\ole۳۲.dll
- \Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\mscorlib.ni.dll
- \Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\MSCTF.dll
- \Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\culture.dll
- \Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\nlssorting.dll
- \Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\clrjit.dll
- \Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\uxtheme.dll
- \Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\System.ni.dll
- \Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\System.Drawing.ni.dll
- \Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\System.Windows.Forms.ni.dll
- \Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\comctl۳۲.dll
- \Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\VERSION.dll
- \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AeDebug
- \REGISTRY\MACHINE\SOFTWARE\Policies\Microsoft\Windows\Windows Error Reporting\DebugApplications
- \REGISTRY\USER\S-۱-۵-۲۱-۱۴۸۲۴۷۶۵۰-۱-۱۶۴۵۵۲۲۳۳۹-۱۴۱۷۰۰-۱۳۳۳-۵۰۰\SOFTWARE\Policies\Microsoft\Windows\Windows Error Reporting\DebugApplications
- \REGISTRY\USER\S-۱-۵-۲۱-۱۴۸۲۴۷۶۵۰-۱-۱۶۴۵۵۲۲۳۳۹-۱۴۱۷۰۰-۱۳۳۳-۵۰۰\SOFTWARE\Policies\Microsoft\PCHealth\ErrorReporting
- \REGISTRY\MACHINE\SOFTWARE\Policies\Microsoft\PCHealth\ErrorReporting
- \REGISTRY\MACHINE\SOFTWARE\Microsoft\PCHealth\ErrorReporting\ShowUI
- \REGISTRY\MACHINE\SOFTWARE\Microsoft\PCHealth\ErrorReporting\DoReport
- \Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\diasymreader.dll

نتایج حاصل از بررسی ها نشان می دهد که این باج افزار با تنظیم کلید رجیستری زیر، پس از هر بار راه اندازی مجدد رایانه، خود را نیز اجرا می کند.

```
string name = "Software\Microsoft\Windows\CurrentVersion\Run";
```

همچنین قطعه کدی نیز یافت شد که احتمالاً عملکرد این قطعه کد استتفا قرار دادن بعضی دایرکتوری‌ها در هنگام رمزگذاری است.

```
// Token: 0x0600009D RID: 157 RVA: 0x000E3B8 File Offset: 0x000C5B8
public static IEnumerable<string> GetFolderFilesPaths(this string folder, bool followSubDirs = true)
{
    List<string> list = new List<string>();
    if (!Directory.Exists(folder.Replace("Windows", "").Replace("windows", "").Replace("WINDOWS", "").Replace("program
files", "").Replace("Program Files", "").Replace("ProgramData", "").Replace("Program Files (x86)", "").Replace("program
files (x86)", ""))))
    {
```

تحلیل ترافیک شبکه :

تحلیل‌ها نشان می‌دهد که باج افزار RansSIRIA پس از اجرا، ارتباطات گسترده‌ای را با شبکه جهانی وب برقرار می‌سازد. لیست کامل این ارتباطات در جداول زیر آمده است.

55	4.513936	158.69.67.193	192.168.56.15	TLSv1	113	Change Cipher Spec, Encrypted Handshake Message
56	4.599780	159.203.146.126	192.168.56.15	TLSv1	113	Change Cipher Spec, Encrypted Handshake Message
57	4.789413	192.168.56.15	158.69.67.193	TCP	54	63542 → 443 [ACK] Seq=457 Ack=5568 Win=65640 Len=0
58	4.805987	158.69.67.193	192.168.56.15	TLSv1	113	[TCP Spurious Retransmission], Change Cipher Spec, Encrypted Handshake Message
59	4.806039	192.168.56.15	158.69.67.193	TCP	66	[TCP Dup ACK 57#1] 63542 → 443 [ACK] Seq=457 Ack=5568 Win=65640 Len=0 SLE=5509 SRE=5568
60	4.889570	192.168.56.15	159.203.146.126	TCP	54	63541 → 443 [ACK] Seq=261 Ack=3259 Win=65640 Len=0
61	4.897105	159.203.146.126	192.168.56.15	TLSv1	113	[TCP Spurious Retransmission], Change Cipher Spec, Encrypted Handshake Message
62	4.897150	192.168.56.15	159.203.146.126	TCP	66	[TCP Dup ACK 60#1] 63541 → 443 [ACK] Seq=261 Ack=3259 Win=65640 Len=0 SLE=3200 SRE=3259
63	5.794193	208.113.168.89	192.168.56.15	TCP	60	80 → 63540 [FIN, ACK] Seq=1551 Ack=325 Win=16384 Len=0
64	5.794276	192.168.56.15	208.113.168.89	TCP	54	63540 → 80 [ACK] Seq=325 Ack=1552 Win=65700 Len=0
65	8.163861	192.168.56.15	8.8.8.8	DNS	78	Standard query 0xcbae A ocsip.usertrust.com
66	8.168669	8.8.8.8	192.168.56.15	DNS	94	Standard query response 0xcbae A ocsip.usertrust.com A 178.255.83.1

درخواست های DNS

دامنه	آدرس آی پی	کشور
www.taringa.net	۱۰۴.۱۶.۱۲۸.۶۵	ایالات متحده امریکا
ssl.gstatic.com	۱۷۲.۲۱۷.۲۳.۹۹	ایالات متحده امریکا
srv.buysellads.com	۱۸۸.۱۶۶.۱۲۲.۱۴۰	هلند
s۳.buysellads.com	۲۳.۱۱۱.۹.۲۲	ایالات متحده امریکا
platform.twitter.com	۱۹۹.۹۶.۵۷.۶	ایالات متحده امریکا
pagead۲.google syndication.com	۲۱۶.۵۸.۲۰۵.۱۹۴	ایالات متحده امریکا
ocsp.pki.goog	۱۷۲.۲۱۷.۲۲.۷۸	ایالات متحده امریکا
ocsp.int-x۳.letsencrypt.org	۲.۱۸.۲۱۲.۵۶	اتحادیه اروپا
ocsp.comodoca۴.com	۲.۱۷.۱۲۲.۲۲۴	اتحادیه اروپا
o۱.t۲۶.net	۱۰۴.۱۶.۱۲۹.۶۵	ایالات متحده امریکا
maxcdn.bootstrapcdn.com	۲۰۵.۱۸۵.۲۱۶.۱۰	ایالات متحده امریکا
isrg.trustid.ocsp.identrust.com	۲.۱۸.۲۱۲.۷۳	اتحادیه اروپا

domainY۰Y.tk	۱۹۵.۲۰.۳۴.۱۱۱	هلند
dolarhoje.com	۱۵۹.۲۰۳.۱۴۶.۱۲۶	ایالات متحده امریکا
d۳b۴n۳yyoc۸n۵۹.cloudfront.net	۵۲.۸۵.۱۷۷.۱۰۵	ایالات متحده امریکا
d۲۸۲ykz۶vx۰۱th.cloudfront.net	۵۲.۸۵.۱۷۷.۱۲۸	ایالات متحده امریکا
code.jquery.com	۶۹.۱۶.۱۷۵.۱۰	ایالات متحده امریکا
cdn.adfront.org	۲۳.۱۱۱.۹.۲۲	ایالات متحده امریکا
cas.criteo.com	۱۷۸.۲۵۰.۰.۷۱	فرانسه
ajax.googleapis.com	۱۷۲.۲۱۷.۲۳.۱۳۸	ایالات متحده امریکا
adservice.google.de	۲۱۶.۵۸.۲۰۵.۱۹۴	ایالات متحده امریکا

میزبان هایی که با آن ها ارتباط برقرار کرده است :

آدرس آی پی	شماره پورت	نام کشور
۱۶۷.۱۱۴.۴۶.۰	۸۰ TCP	کانادا
۱۷۲.۲۱۷.۲۲.۶۷	۴۴۳ TCP	ایالات متحده امریکا
۴۶.۱۰۱.۴۴.۶۱	۴۴۳ TCP	هلند
۱۰۴.۱۶.۲۵۳.۶۴	۴۴۳ TCP	ایالات متحده امریکا
۱۸۵.۶۰.۲۱۶.۱۹	۴۴۳ TCP	ایرلند
۲.۱۷.۱۲۲.۲۲۴	۸۰ TCP	اتحادیه اروپا
۱۷۲.۲۱۷.۲۲.۷۷	۴۴۳ TCP	ایالات متحده امریکا
۱۷۲.۲۱۷.۱۶.۲۰۰	۴۴۳ TCP	ایالات متحده امریکا
۱۰۴.۱۶.۱۳۲.۶۵	۴۴۳ TCP	ایالات متحده امریکا

شناسایی :

این باج افزار در هنگام نگارش این گزارش، توسط ۳۶ آنتی ویروس معتبر در سامانه VirusTotal قابل شناسایی است.

Ad-Aware	⚠ Trojan.GenericKD.30629268	AegisLab	⚠ Troj.W32.Generictc
ALYac	⚠ Trojan.Ransom.RansSIRIA	Arcabit	⚠ Trojan.Generic.D1D35D94
Avast	⚠ Win32:Malware-gen	AVG	⚠ Win32:Malware-gen
Avira	⚠ TR/Ransom.mmmuvq	BitDefender	⚠ Trojan.GenericKD.30629268
CrowdStrike Falcon	⚠ malicious_confidence_60% (W)	Cylance	⚠ Unsafe
Cyren	⚠ W32/Trojan.PXTR-6197	Emsisoft	⚠ Trojan.GenericKD.30629268 (B)
Endgame	⚠ malicious (moderate confidence)	eScan	⚠ Trojan.GenericKD.30629268
ESET-NOD32	⚠ a variant of MSIL/Filecoder.MI	F-Secure	⚠ Trojan.GenericKD.30629268
Fortinet	⚠ W32/Generic.MI!tr	GData	⚠ Trojan.GenericKD.30629268
Ikarus	⚠ Trojan-Ransom.FileCoder	K7AntiVirus	⚠ Trojan (0052b27f1)
K7GW	⚠ Trojan (0052b27f1)	Kaspersky	⚠ HEUR:Trojan.Win32.Generic
Malwarebytes	⚠ Trojan.MalPack	MAX	⚠ malware (ai score=98)
McAfee	⚠ Artemis!5071732EDDA3	McAfee-GW-Edition	⚠ BehavesLike.Win32.BadFile.tc
Palo Alto Networks	⚠ generic.ml	Panda	⚠ Trj/GdSda.A
Qihoo-360	⚠ Win32/Trojan.5a2	Sophos AV	⚠ Mal/Generic-5
Sophos ML	⚠ heuristic	Symantec	⚠ Trojan.Gen.2
Tencent	⚠ Win32.Trojan.Generic.Stkb	TrendMicro	⚠ TROJ_GEN.R00EC0WDK18
TrendMicro-HouseCall	⚠ TROJ_GEN.R00EC0WDK18	ZoneAlarm	⚠ HEUR:Trojan.Win32.Generic