باسمه تعالی

تحلیل فنی باج‌افزار LanRan v۲

مقدمه :

مشاهده و رصد فضای سایبری در زمینه باج‌افزار، از شروع فعالیت نمونه جدیدی از خانواده‌ی باج‌افزار LanRan v۲ خبر می‌دهد. این باج‌افزار نسخه جدیدی از باج‌افزار LanRan می باشد که از ترکیب دو باج‌افزار LanRan و njRat بدست آمده است. هر دوی این باج‌افزارها از خانواده HiddenTear می باشند. باج‌افزار مورد اشاره پس از رمزگذاری فایل‌ها پسوند LanRan۲.۰.۵. را به انتهای فایل‌های رمزگذاری شده اضافه می‌کند. بررسی‌ها نشان می‌دهد که فعالیت این باج‌افزار در اوایل ماه جولای سال ۲۰۱۸ میلادی شروع شده و به نظر می‌رسد تمرکز آن بیشتر بر روی کاربران انگلیسی زبان می‌باشد. این باج‌افزار از الگوریتم رمزنگاری AES استفاده میکند.

مشخصات فایل اجرایی :

نام فایل	get.exe KryptoTrojaner.exe njRAT v۸.٤ Pro.exe ee٥ebb٧١٤٠٥d٥٠٠٠٥٢٠٧٦c٨e١٨٨٥٥٥٥de٩٤١٤٤٥٤٨٣٩e٩c٢٦a٢٧٤٦b١cc٩٧fe٧ef._exe
MD٥	e١٦٨٣٩٢٠٦٦c٦d٠٠c٦de٦b٧١c٨٢adcdb٣
SHA-١	٠١٤efbc٦f٧ef١٥cf٤٦٦d٦١٥e٠b٩٣٥٥١٢٠aef٢c٢d
SHA-٢٥٦	ee٥ebb٧١٤٠٥d٥٠٠٠٥٢٠٧٦c٨e١٨٨٥٥٥٥de٩٤١٤٤٥٤٨٣٩e٩c٢٦a٢٧٤٦b١cc٩٧fe٧ef
اندازه فایل	٢٠٩ KB
کامپایلر / پکر	Microsoft Visual C# v٧.٠ / Basic .NET (managed)

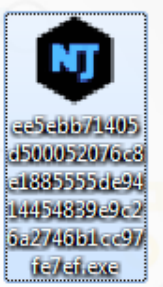
فایل اجرایی این باج‌افزار دارای چهار بخش است :

نام بخش	آنتروپی	آدرس مجازی	اندازه مجازی	اندازه خام
.text	٧.٤	٨١٩٢	١٥١٥٥٦	١٥٢٠٦٤
.sdata	٦.٦١	١٦٣٨٤٠	٤٨٨	٥١٢
.rsrc	٥.٤٩	١٧٢٠٣٢	٥٩٨٤٨	٥٩٩٠٤
.reloc	٠.٠٨	٢٣٧٥٦٨	١٢	٥١٢

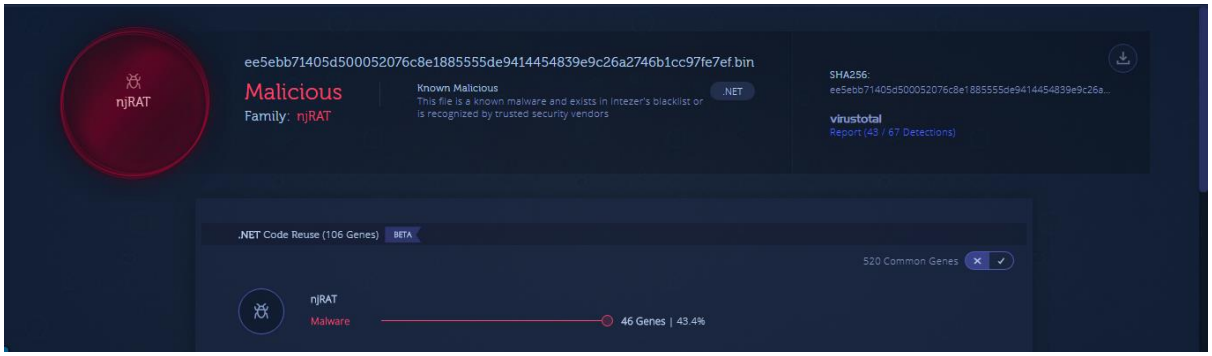
تحلیل پویا :

برای بررسی عمیق‌تر باج‌افزار LanRan v۲ فایل اجرایی آن را در محیط آزمایشگاهی اجرا کردیم تا عملکرد باج‌افزار را از نزدیک مورد بررسی قرار دهیم.

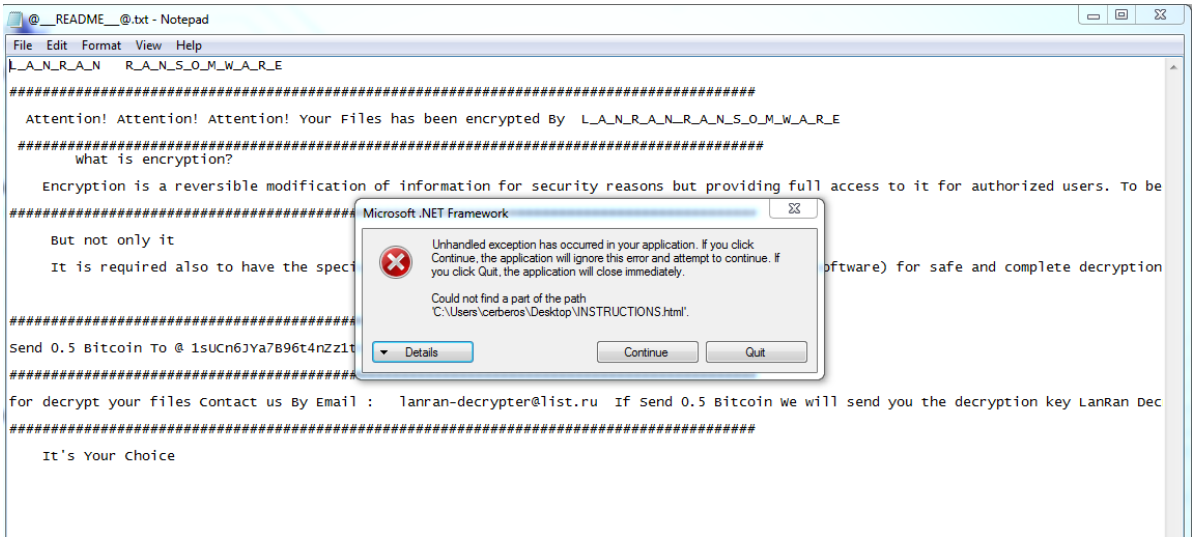
آیکن باج‌افزار مربوطه به شکل شش ضلعی زیر می باشد که به نظر می رسد حروف NJ به همان نام والدش یعنی njRat باز میگردد :



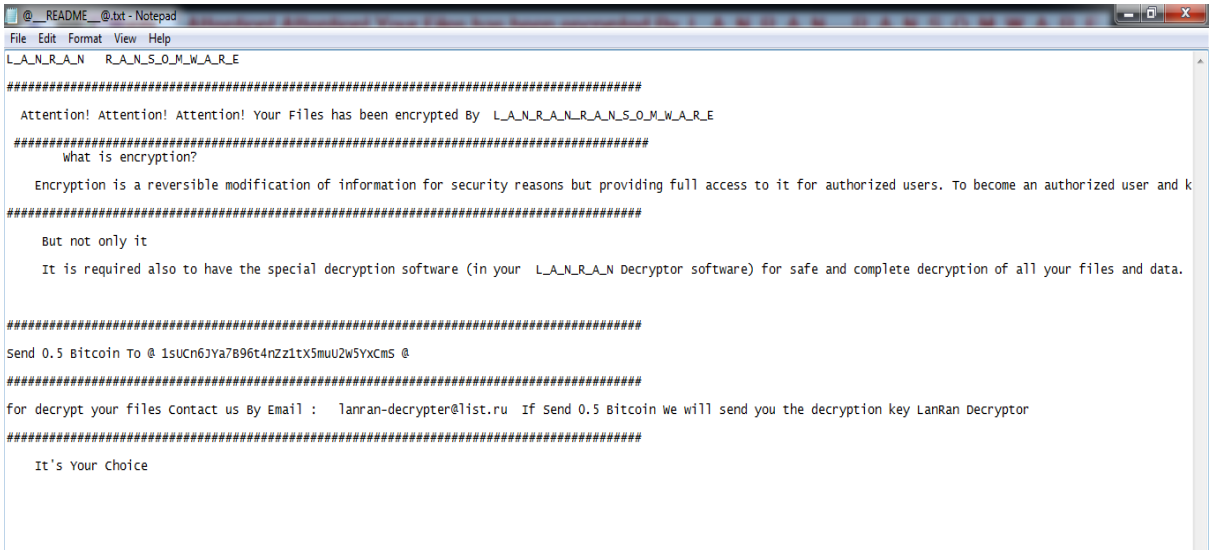
همانطور که در تصویر زیر قابل مشاهده است، ٤٣.٤ ٪ مشابه والد خود یعنی njRat می‌باشد :



پس از اجرای باج‌افزار پیغام باج خواهی تحت عنوان @___README___@.txt به همراه خطای Microsoft.NET Framework گشوده می‌شود:

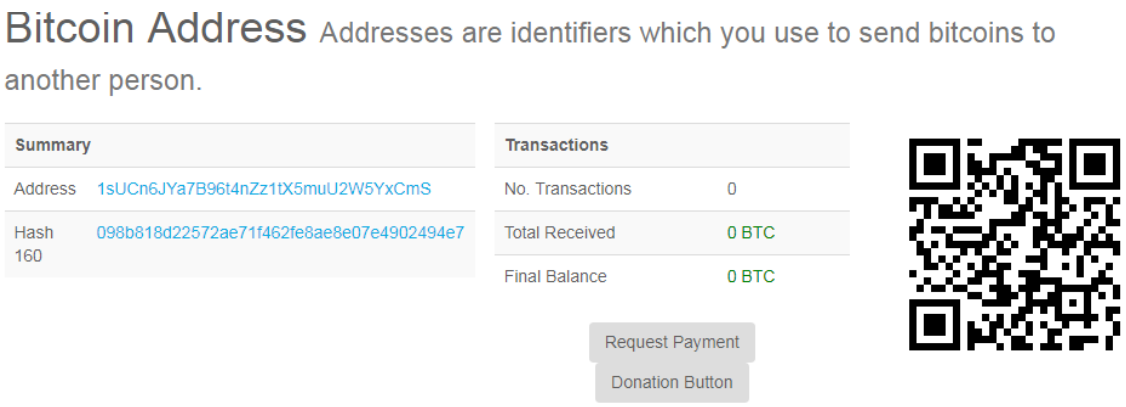


تصویر زیر پیغام باج‌خواهی باج‌افزار LanRan V۲ را نشان می دهد که بر روی پس زمینه سیستم قربانی مستقر شده است :

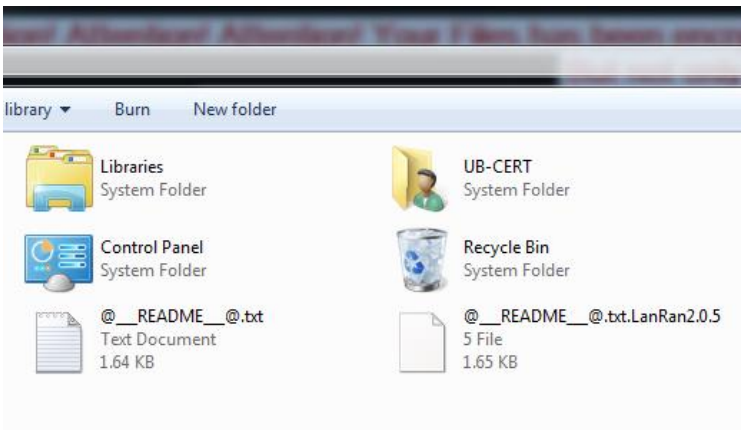


بر اساس پیغام باج‌خواهی که در ابتدا توضیحاتی درباره مفهوم رمزگذاری فایل ها داده شده، تنها راه چاره، دریافت نرم افزار رمزگشا معرفی شده است. در ادامه قربانی باید برای رمزگشایی فایل‌ها مبلغ ۰.۵ بیت‌کوین را به آدرس کیف پول ۱sUCn٦JYaVB٩٦t٤nZz١tX٥muU٢W٥YxCmS که در پیغام باج خواهی ذکر شده است بفرستد. راه ارتباط با باجگیر نیز آدرس ایمیل LanRan٢-decrypter@list.ru تعیین شده است. ضمناً مهلتی برای پرداخت باج نیز تعیین نشده است.

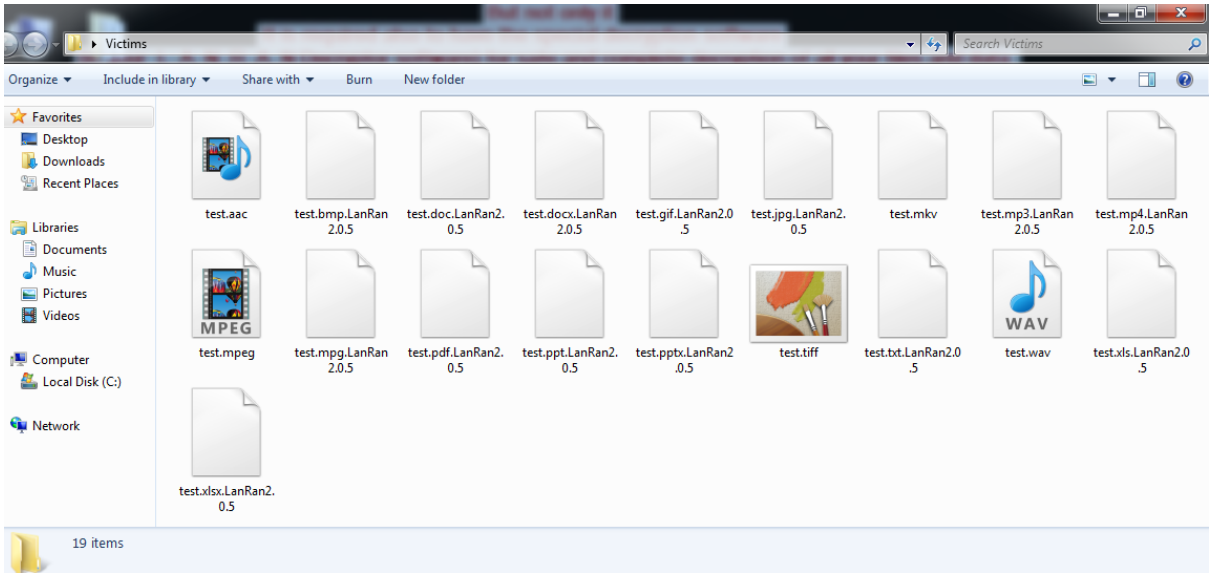
طبق بررسی‌های انجام شده، در حال حاضر کیف پول مربوط به این باج‌افزار تراکنشی نداشته است.



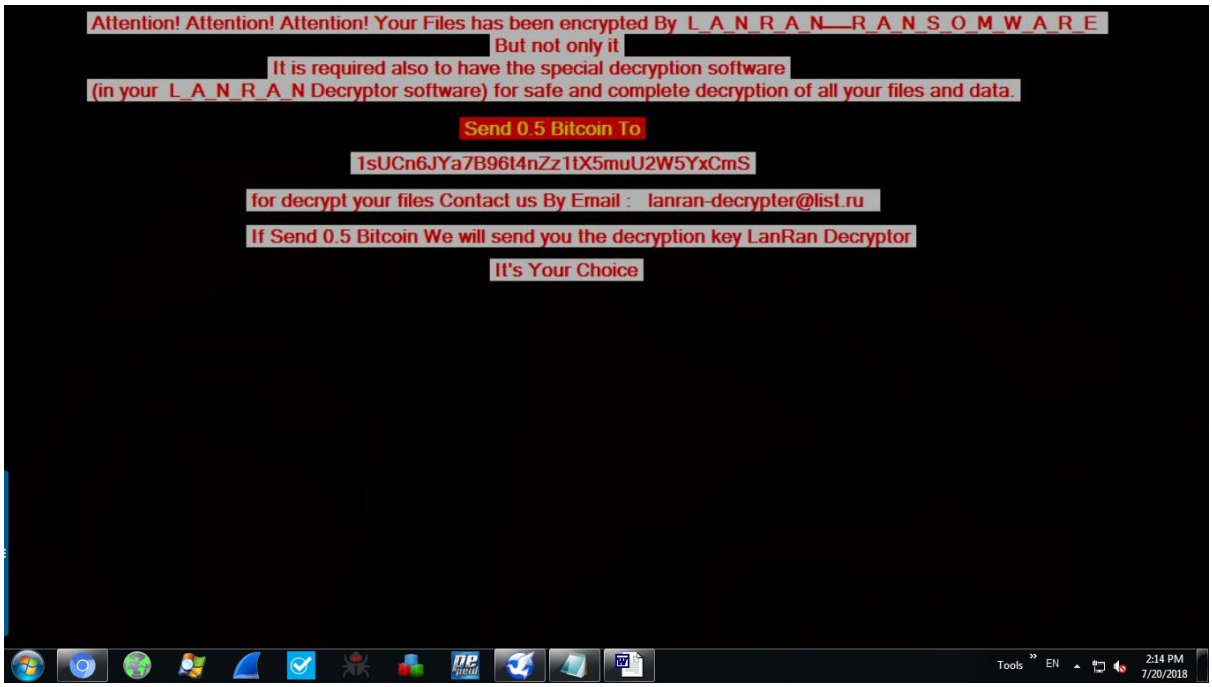
این باج‌افزار پس از رمزگذاری پسوند LanRan۲.۰.۵. را به انتهای فایل‌های رمزگذاری شده اضافه می‌کند و حتی پیغام باج‌خواهی خود را نیز رمزگذاری می‌کند.



تصویر زیر نشان‌دهنده فایل‌های رمزگذاری شده توسط این باج‌افزار می‌باشد:

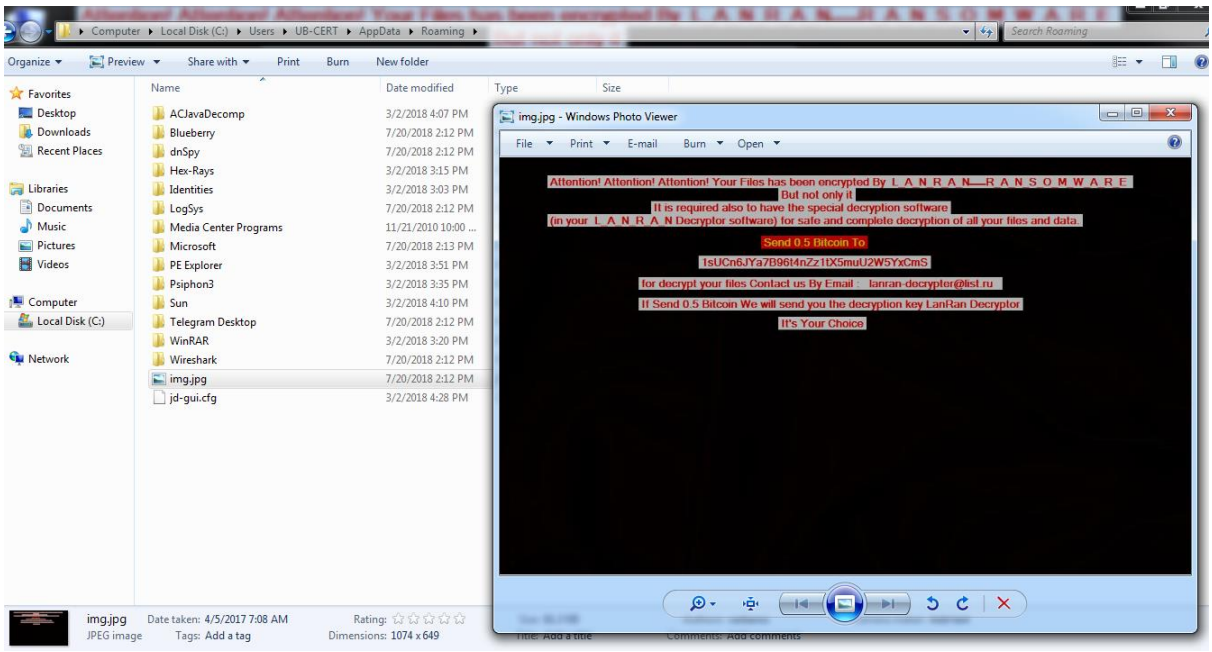


فایل های رمزگذاری شده عموما فایل های آفیس, پی دی اف , پایگاه داده, تصاویر , موسیقی , ویدئو و.... می باشند. در ادامه، تصویر پس زمینه سیستم قربانی توسط باج‌افزار تغییر پیدا می کند.

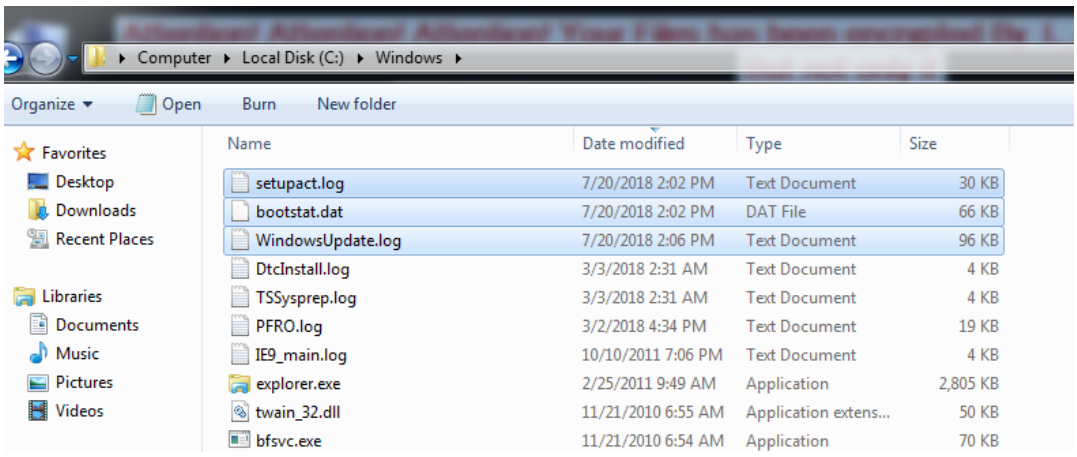


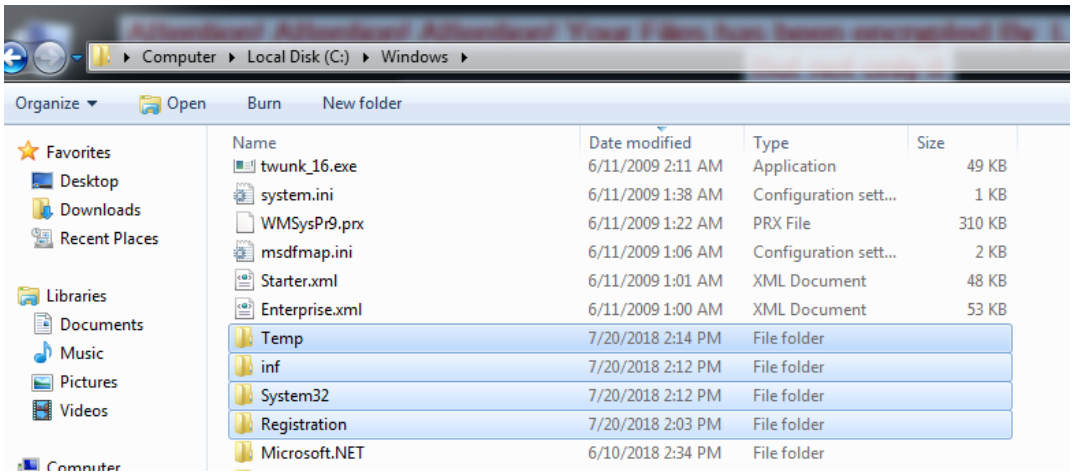
محتویات تصویر فوق همانند محتویات ذکر شده در پیغام باج خواهی بوده با این تفاوت که توضیحاتی در رابطه با فرآیند رمزگذاری در آن دیده نمی‌شود.

این تصویر به نام img.jpg در مسیر AppData سیستم قربانی قرار گرفته است:

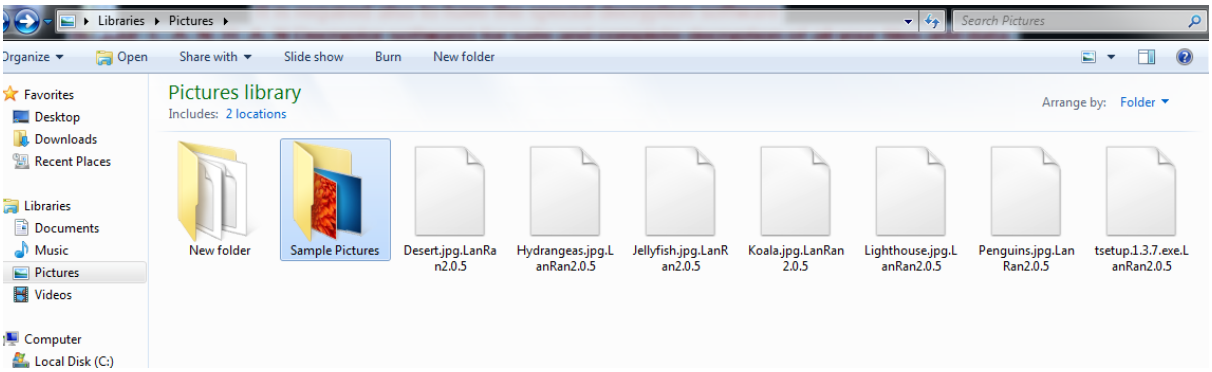


در تصاویر زیر فایل های اضافه شده و تغییر یافته در مسیر درایو سیستم عامل و پوشه Windows را مشاهده می کنید :





طبق بررسی ها انجام شده، باج‌افزار فایل‌های موجود در دایرکتوری‌های Pictures ، Music و ... را رمزگذاری نمی کند :



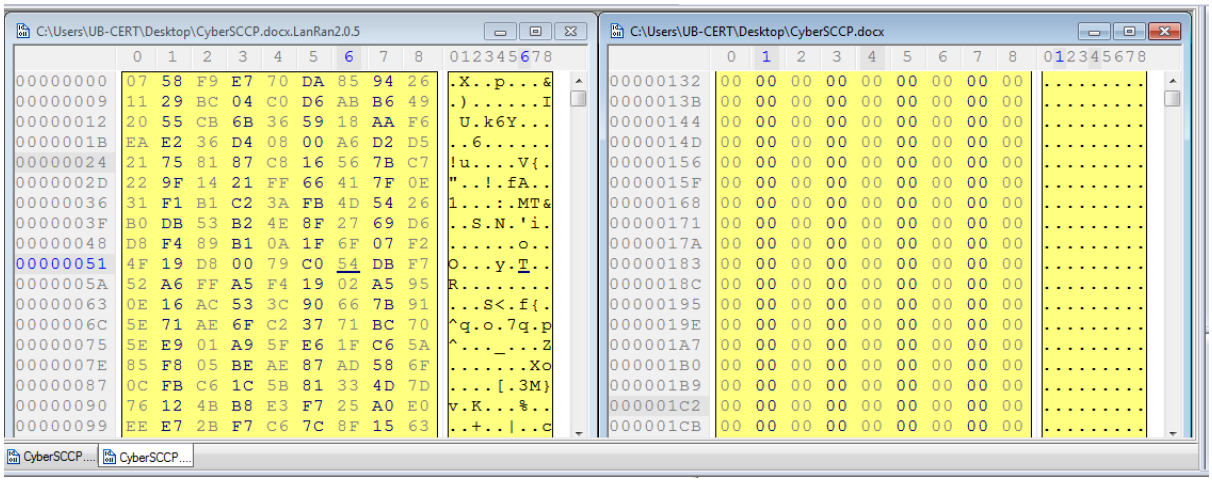
همچنین محتویات فولدر Downloads , Recycle bin نیز رمزگذاری نمی شوند.

طبق بررسی‌های صورت گرفته اکثر آنتی‌ویروس‌های معتبر، این باج‌افزار را به عنوان یک تروجان شناسایی نموده‌اند. لذا احتمال نفوذ باج‌افزار به سیستم از راه های متداول نیز مانند هرزنامه‌ها وجود دارد.

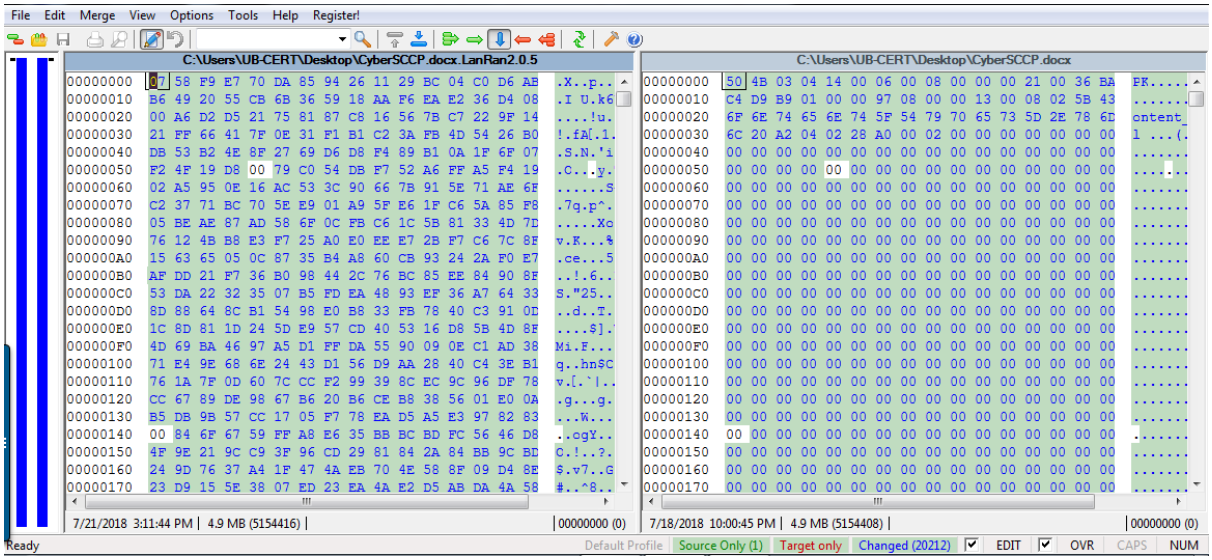
تحلیل ایستا:

پس از تحلیل کد باج‌افزار LanRan V۲ به نتایج زیر دست پیدا کردیم.

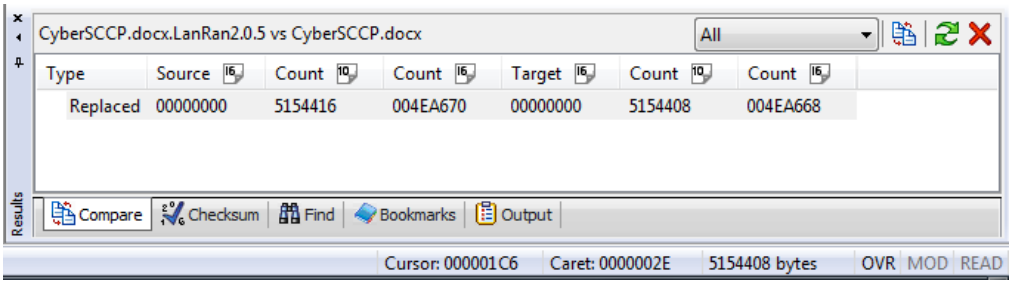
مقایسه نمونه فایل، قبل و بعد از رمزگذاری :



بعد از رمزگذاری، به فایل نمونه، ده ها برابر مقدار اولیه فایل اضافه شد.



تعداد بایت های جایگزین شده ی نمونه فایل بعد از رمزگذاری:



بر اساس قطعه کد زیر، بـاج‌افـزار نسـخه هـای Volume Shadow Copy را از سیسـتم قربـانی حـذف می‌کند. این عمل بازگردانی فایل‌ها را با مشکل مواجه می‌کند.

```
AppDomain
831         this.InternalSetPrivateBinPath(string.Empty);
832     }
833
834     // Token: 0x060004D4 RID: 1236 RVA: 0x0001142F File Offset: 0x0001042F
835     [Obsolete("AppDomain.ClearShadowCopyPath has been deprecated. Please investigate the use of AppDomainSetup.ShadowCopyDirectories
          instead. http://go.microsoft.com/fwlink/?linkid=14202")]
836     [SecurityPermission(SecurityAction.LinkDemand, ControlAppDomain = true)]
837     public void ClearShadowCopyPath()
838     {
839         this.InternalSetShadowCopyPath(string.Empty);
840     }
841
842     // Token: 0x060004D5 RID: 1237 RVA: 0x0001143C File Offset: 0x0001043C
843     [Obsolete("AppDomain.SetCachePath has been deprecated. Please investigate the use of AppDomainSetup.CachePath instead. http://
          go.microsoft.com/fwlink/?linkid=14202")]
844     [SecurityPermission(SecurityAction.LinkDemand, ControlAppDomain = true)]
845     public void SetCachePath(string path)
846     {
847         this.InternalSetCachePath(path);
848     }
849
850     // Token: 0x060004D6 RID: 1238 RVA: 0x00011445 File Offset: 0x00010445
851     [SecurityPermission(SecurityAction.LinkDemand, ControlAppDomain = true)]
852     public void SetData(string name, object data)
853     {
854         this.SetDataHelper(name, data, null);
855     }
856
857     // Token: 0x060004D7 RID: 1239 RVA: 0x00011450 File Offset: 0x00010450
858     [SecurityPermission(SecurityAction.LinkDemand, ControlAppDomain = true)]
```

طبق نتایج بدست آمده، باج‌افزار LanRan v۲.۰ از طریق قطعه کد زیر اقدام به تولید دامنه های تصادفی و سپس ارتباطگیری با سرور کنترل و فرمان (C & C) خود می‌کند. تصاویر زیر الگوریتم ایجاد دامنه (DGA) باج‌افزار مورد اشاره را نشان می‌دهند.

```
700             }
701             try
702             {
703                 objectHandle = appDomain.CreateInstance(fullName, fullName2);
704             }
705             finally
706             {
707                 if (impersonationContext != null)
708                 {
709                     impersonationContext.Undo();
710                 }
711                 if (objectHandle == null)
712                 {
713                     AppDomain.Unload(appDomain);
714                 }
715             }
716             HostingEnvironment hostingEnvironment = (objectHandle != null) ? (objectHandle.Unwrap() as HostingEnvironment) : null;
717             if (hostingEnvironment == null)
718             {
719                 throw new SystemException(SR.GetString("Cannot_create_HostEnv"));
720             }
721             IConfigMapPathFactory configMapPathFactory = appHost.GetConfigMapPathFactory();
722             hostingEnvironment.Initialize(this, appHost, configMapPathFactory, hostingParameters);
723             return hostingEnvironment;
```

```
1710        // Token: 0x0600050E RID: 1294 RVA: 0x000122B0 File Offset: 0x000112B0
1711        public static AppDomain CreateDomain(string friendlyName, Evidence securityInfo, string appBasePath, string appRelativeSearchPath,
              bool shadowCopyFiles, AppDomainInitializer adInit, string[] adInitArgs)
1712        {
1713            AppDomainSetup appDomainSetup = new AppDomainSetup();
1714            appDomainSetup.ApplicationBase = appBasePath;
1715            appDomainSetup.PrivateBinPath = appRelativeSearchPath;
1716            appDomainSetup.AppDomainInitializer = adInit;
1717            appDomainSetup.AppDomainInitializerArguments = adInitArgs;
1718            if (shadowCopyFiles)
1719            {
1720                appDomainSetup.ShadowCopyFiles = "true";
1721            }
1722            return AppDomain.CreateDomain(friendlyName, securityInfo, appDomainSetup);
1723        }
```

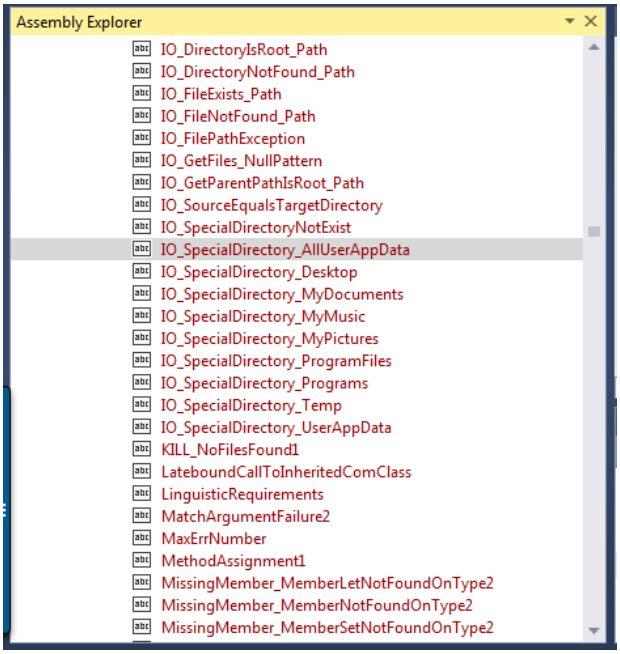
```
79
80      // Token: 0x060024E2 RID: 9442 RVA: 0x000935F8 File Offset: 0x000925F8
81      [SecurityPermission(SecurityAction.Assert, Flags = SecurityPermissionFlag.ControlAppDomain)]
82      private void CreateAppDomain()
83      {
84          bool flag = false;
85          RuntimeHelpers.PrepareConstrainedRegions();
86          try
87          {
88              try
89              {
90              }
91              finally
92              {
93                  Monitor.Enter(AutoWebProxyScriptWrapper.s_AppDomains.SyncRoot);
94                  flag = true;
95              }
96              if (AutoWebProxyScriptWrapper.s_CleanedUp)
97              {
98                  throw new InvalidOperationException(SR.GetString("net_cant_perform_during_shutdown"));
99              }
100             if (AutoWebProxyScriptWrapper.s_AppDomainInfo == null)
101             {
102                 AutoWebProxyScriptWrapper.s_AppDomainInfo = new AppDomainSetup();
103                 AutoWebProxyScriptWrapper.s_AppDomainInfo.DisallowBindingRedirects = true;
104                 AutoWebProxyScriptWrapper.s_AppDomainInfo.DisallowCodeDownload = true;
105                 NamedPermissionSet namedPermissionSet = new NamedPermissionSet("__WebProxySandbox", PermissionState.None);
106                 namedPermissionSet.AddPermission(new SecurityPermission(SecurityPermissionFlag.Execution));
107                 ApplicationTrust applicationTrust = new ApplicationTrust();
108                 applicationTrust.DefaultGrantSet = new PolicyStatement(namedPermissionSet);
109                 AutoWebProxyScriptWrapper.s_AppDomainInfo.ApplicationTrust = applicationTrust;
110             }
111             AppDomain appDomain = AutoWebProxyScriptWrapper.s_ExcessAppDomain;
112             if (appDomain != null)
113             {
114                 TimerThread.GetOrCreateQueue(0).CreateTimer(new TimerThread.Callback(AutoWebProxyScriptWrapper.CloseAppDomainCallback),
                      appDomain);
115                 throw new InvalidOperationException(SR.GetString("net_cant_create_environment"));
116             }
```

```
117             this.appDomainIndex = AutoWebProxyScriptWrapper.s_NextAppDomainIndex++;
118             try
119             {
120             }
121             finally
122             {
123                 AutoWebProxyScriptWrapper.s_ExcessAppDomain = AppDomain.CreateDomain("WebProxyScript", null,
                      AutoWebProxyScriptWrapper.s_AppDomainInfo);
124                 try
125                 {
126                     AutoWebProxyScriptWrapper.s_AppDomains.Add(this.appDomainIndex, AutoWebProxyScriptWrapper.s_ExcessAppDomain);
127                     this.scriptDomain = AutoWebProxyScriptWrapper.s_ExcessAppDomain;
128                 }
129                 finally
130                 {
131                     if (object.ReferenceEquals(this.scriptDomain, AutoWebProxyScriptWrapper.s_ExcessAppDomain))
132                     {
133                         AutoWebProxyScriptWrapper.s_ExcessAppDomain = null;
134                     }
135                     else
136                     {
137                         try
138                         {
139                             AutoWebProxyScriptWrapper.s_AppDomains.Remove(this.appDomainIndex);
140                         }
141                         finally
142                         {
143                             TimerThread.GetOrCreateQueue(0).CreateTimer(new TimerThread.Callback
                                (AutoWebProxyScriptWrapper.CloseAppDomainCallback), AutoWebProxyScriptWrapper.s_ExcessAppDomain);
144                         }
145                     }
146                 }
147             }
148         }
149         finally
150         {
151             if (flag)
152             {
153                 Monitor.Exit(AutoWebProxyScriptWrapper.s_AppDomains.SyncRoot);
154             }
155         }
```

همانطور که اشاره شد باج‌افزار LanRan v۲.۰ از الگوریتم رمزنگاری AES برای رمزگذاری فایل‌ها استفاده می‌کند که در تصویر زیر نشان داده شده است :

```
66
67      // Token: 0x06000423 RID: 1059 RVA: 0x0001539C File Offset: 0x0001439C
68      internal static byte[] AESKeyWrapEncrypt(byte[] rgbKey, byte[] rgbWrappedKeyData)
69      {
70          int num = rgbWrappedKeyData.Length >> 3;
71          if (rgbWrappedKeyData.Length % 8 != 0 || num <= 0)
72          {
73              throw new CryptographicException(SecurityResources.GetResourceString("Cryptography_Xml_KW_BadKeySize"));
74          }
75          ICryptoTransform cryptoTransform = new RijndaelManaged
76          {
77              Key = rgbKey,
78              Mode = CipherMode.ECB,
79              Padding = PaddingMode.None
80          }.CreateEncryptor();
81          if (num == 1)
82          {
83              byte[] array = new byte[SymmetricKeyWrap.s_rgbAES_KW_IV.Length + rgbWrappedKeyData.Length];
84              Buffer.BlockCopy(SymmetricKeyWrap.s_rgbAES_KW_IV, 0, array, 0, SymmetricKeyWrap.s_rgbAES_KW_IV.Length);
85              Buffer.BlockCopy(rgbWrappedKeyData, 0, array, SymmetricKeyWrap.s_rgbAES_KW_IV.Length,
                    rgbWrappedKeyData.Length);
86              return cryptoTransform.TransformFinalBlock(array, 0, array.Length);
87          }
88          byte[] array2 = new byte[num + 1 << 3];
89          Buffer.BlockCopy(rgbWrappedKeyData, 0, array2, 8, rgbWrappedKeyData.Length);
```

لیست دایرکتوری هایی که باید رمزگذاری شده و یا نباید رمزگذاری شوند در تصویر زیر نشان داده است :



برای نمونه فولدر My Pictures نباید رمزگذاری شود :

```
33      // Token: 0x17000081 RID: 129
34      // (get) Token: 0x06000222 RID: 546 RVA: 0x0000AA28 File Offset: 0x00009A28
35      public static string MyPictures
36      {
37          get
38          {
39              return SpecialDirectories.GetDirectoryPath(Environment.GetFolderPath
                  (Environment.SpecialFolder.MyPictures), "IO_SpecialDirectory_MyPictures");
40          }
41      }
```

و فولدر دسکتاپ باید رمزگذاری شود:

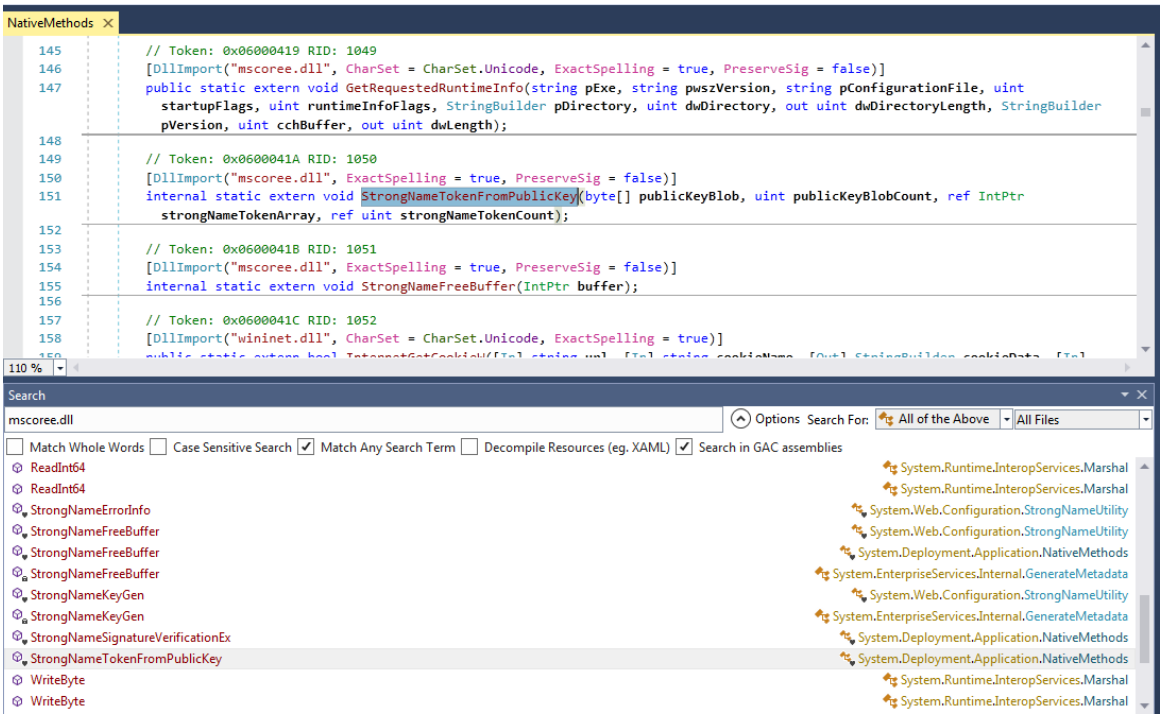
```
43      // Token: 0x17000082 RID: 130
44      // (get) Token: 0x06000223 RID: 547 RVA: 0x0000AA48 File Offset: 0x00009A48
45      public static string Desktop
46      {
47          get
48          {
49              return SpecialDirectories.GetDirectoryPath(Environment.GetFolderPath
                  (Environment.SpecialFolder.Desktop), "IO_SpecialDirectory_Desktop");
50          }
51      }
```

این باج‌افزار از کتابخانه‌های ویندوزی به همراه توابعی از هرکدام از کتابخانه‌ها استفاده می‌کند که در تصویر زیر قابل مشاهده است. همچنین لیست کامل این کتابخانه‌ها به همراه توابع مورد استفاده نیز در ادامه‌ی متن آمده است:

mscoree.dll

CorExeMain_

نمونه های استفاده از این کتابخانه در کد باج‌افزار:



بر اساس بررسی‌های صورت گرفته، باج‌افزار LanRan V۲ پس از اجرا، فرایندهای زیر را ایجاد می‌کند :

KryptoTrojaner.bin.exe (PID: ۲۵۵۲)

- *anRan.exe (PID: ۲۳۲۰)*
- *unsom.exe (PID: ۲۵٤۰)*
- *notepad.exe %USERPROFILE%\Desktop\@___README___@.txt (PID: ۲۵۵٦)*

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 باج‌افزار LanRan V۲ نشدیم.

خروجی سامانه VirusTotal :

در حال حاضر تعداد ۵۱ مورد از ٦٨ آنتی ویروس و آنتی بدافزار موجود در سامانه VirusTotal قادر به شناسایی این باج‌افزار بوده وآن را حذف یا غیرفعال می‌کنند.

Ad-Aware	Trojan.Generic.21071577	AegisLab	Troj.Ransom.W32.Gen!c
AhnLab-V3	Trojan/Win32.Ryzerlo.C2592008	ALYac	Trojan.Ransom.LanRan
Antiy-AVL	Trojan[Ransom]/Win32.AGeneric	Arcabit	Trojan.Generic.D14186D9
Avast	Win32:Malware-gen	AVG	Win32:Malware-gen
Avira	TR/Dropper.MSIL.Gen	AVware	Trojan.Win32.Generic!BT
Baidu	Win32.Trojan.WisdomEyes.16070401....	BitDefender	Trojan.Generic.21071577
CAT-QuickHeal	Trojan.Fuerboos	Comodo	.UnclassifiedMalware
CrowdStrike Falcon	malicious_confidence_100% (W)	Cybereason	malicious.066c6d
Cylance	Unsafe	Cyren	W32/Trojan.SUVH-4420
DrWeb	Trojan.Encoder.10598	Emsisoft	Trojan.Generic.21071577 (B)
Endgame	malicious (high confidence)	eScan	Trojan.Generic.21071577
ESET-NOD32	a variant of MSIL/TrojanDropper.Agent.CER	F-Secure	Trojan.Generic.21071577
Fortinet	MSIL/Agent.CER!tr	GData	Trojan.Generic.21071577
Ikarus	Worm.MSIL.Bladabindi	K7AntiVirus	Trojan (004de14c1)
K7GW	Trojan (004de14c1)	Kaspersky	Trojan-Ransom.Win32.Gen.dnu

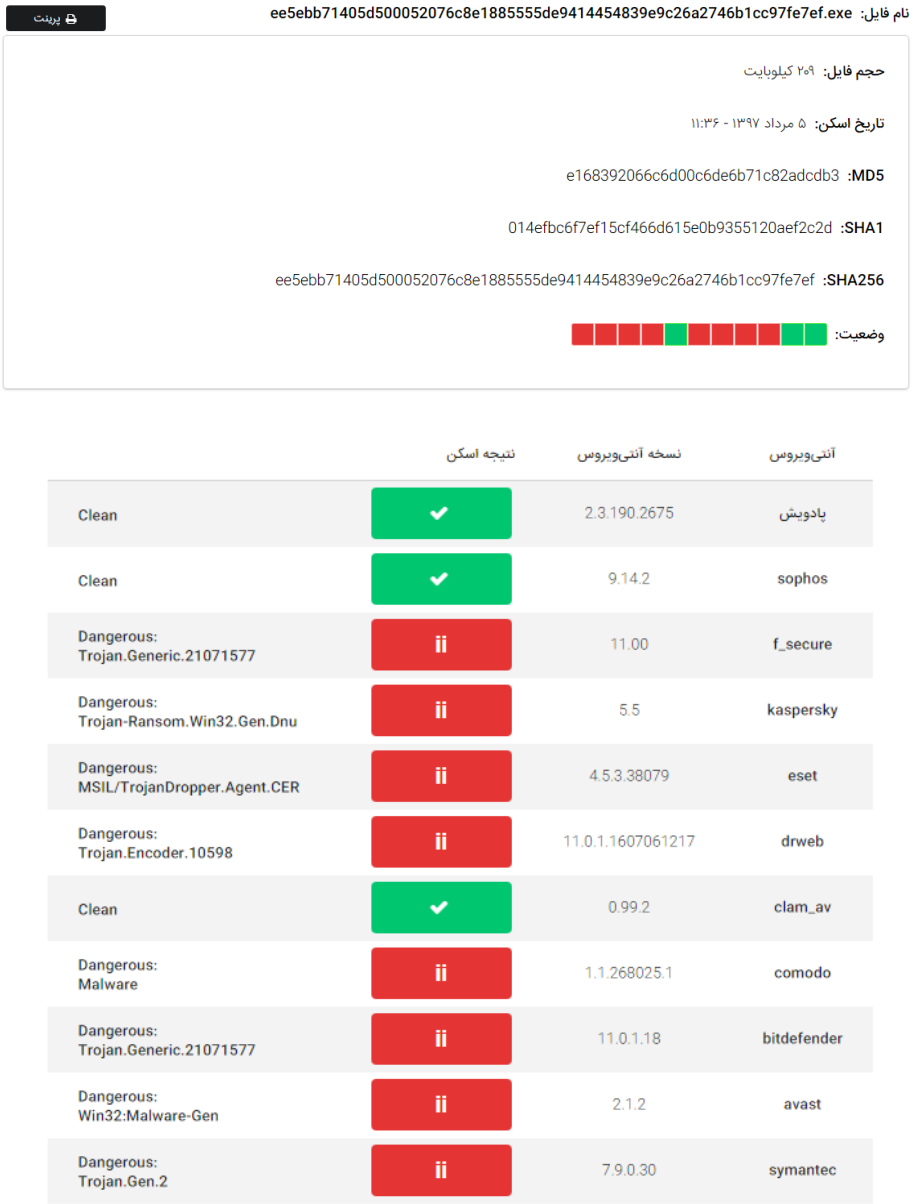
MAX	malware (ai score=100)	McAfee	Artemis!E168392066C6
McAfee-GW-Edition	BehavesLike.Win32.Generic.dh	Microsoft	Ransom:MSIL/Ryzerlo.A
NANO-Antivirus	Trojan.Win32.Agent.enriky	Palo Alto Networks	generic.ml
Panda	Trj/GdSda.A	Qihoo-360	Win32/Trojan.Generic.b4c
Rising	Dropper.Generic!8.35E (CLOUD)	SentinelOne	static engine - malicious
Sophos AV	Troj/Cryptear-M	Sophos ML	heuristic
Symantec	Trojan.Gen.2	Tencent	Win32.Trojan.Gen.Ahxw
TrendMicro	TROJ_DROPPER.FBFAL	TrendMicro-HouseCall	TROJ_DROPPER.FBFAL
VBA32	Hoax.Gen	VIPRE	Trojan.Win32.Generic!BT
Webroot	W32.Trojan.Gen	Yandex	Trojan.DR.Agent!opuTkJ9HRCo
ZoneAlarm	Trojan-Ransom.Win32.Gen.dnu	Avast Mobile Security	Clean

نتایج بدست آمده از اجرای باج‌افزار بر روی سیستم دارای آنتی‌ویروس بومی پادویش :

بر اساس آزمایشات صورت گرفته، قبل از اجرای باج‌افزار فایل اجرایی آن را توسط آنتی‌ویروس پادویش پویش کردیم که قادر به شناسایی باج‌افزار نبود. پس از اجرای باج‌افزار نیز موفق به شناسایی آن نشد.

خروجی سامانه ویروس‌کاو مرکز ماهر :

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



پرینت

نام فایل: ee5ebb71405d500052076c8e1885555de9414454839e9c26a2746b1cc97fe7ef.exe

حجم فایل: ۲۰۹ کیلوبایت

تاریخ اسکن: ۵ مرداد ۱۳۹۷ - ۱۱:۳۶

MD5: e168392066c6d00c6de6b71c82adcdb3

SHA1: 014efbc6f7ef15cf466d615e0b9355120aef2c2d

SHA256: ee5ebb71405d500052076c8e1885555de9414454839e9c26a2746b1cc97fe7ef

وضعیت:

آنتی‌ویروس	نسخه آنتی‌ویروس	نتیجه اسکن	
پادویش	2.3.190.2675	✔	Clean
sophos	9.14.2	✔	Clean
f_secure	11.00	ii	Dangerous: Trojan.Generic.21071577
kaspersky	5.5	ii	Dangerous: Trojan-Ransom.Win32.Gen.Dnu
eset	4.5.3.38079	ii	Dangerous: MSIL/TrojanDropper.Agent.CER
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: Trojan.Generic.21071577
avast	2.1.2	ii	Dangerous: Win32:Malware-Gen
symantec	7.9.0.30	ii	Dangerous: Trojan.Gen.2