باسمه تعالی

تحلیل فنی باج‌افزار The Brotherhood

مقدمه :

مشاهده و رصد فضای سایبری در زمینه باج‌افزار، از شروع فعالیت نمونه جدیدی از خانواده‌ی باج‌افزار HiddenTear به نام The Brotherhood خبر می‌دهد. بررسی‌ها نشان می‌دهد که فعالیت این باج‌افزار در اوایل ماه ژوئیه سال ۲۰۱۸ میلادی شروع شده و به نظر می‌رسد تمرکز آن بیشتر بر روی کاربران انگلیسی زبان می‌باشد. این باج‌افزار از الگوریتم رمزنگاری AES در حالت CBC - ۲۵۶ بیتی برای رمزگذاری فایل‌ها استفاده می‌کند و تنها تمام فایل‌های موجود در پوشه‌ی Documents ویندوز را رمزگذاری می‌کند. این باج-افزار همانند اکثر باج‌افزارها، پس از رمزگذاری فایل‌ها از قربانیان تقاضای بیت‌کوین می‌کند و به نظر می‌رسد در حال توسعه باشد.

مشخصات فایل اجرایی :

نام فایل	RansomWare.exe
MD۵	۲۳d۸۲۸۳۵c۲۵۷a۱۶۲f۵۷۰۲۷۰۰۸bfed۷۱۶
SHA-۱	۳۵۷d۰۵۹۰۳cdc۱۰٤cd٤ba٦٦٦ca۸ffbb۸ed۹٦٦۳۱ae
SHA-۲۵٦	۷c٦٦۸۳۳a۸۹ee۰۹٦۲٦۳۵۳۳a۲ff۰۷c۲۵۱۰۵٤b۹f۷a۳۳٤۱f٤۱bbd٦b۷f۰۹۸۸۵۷b٦a۷a
اندازه فایل	۲۷۳ KB

فایل اجرایی این باج‌افزار دارای سه بخش است :

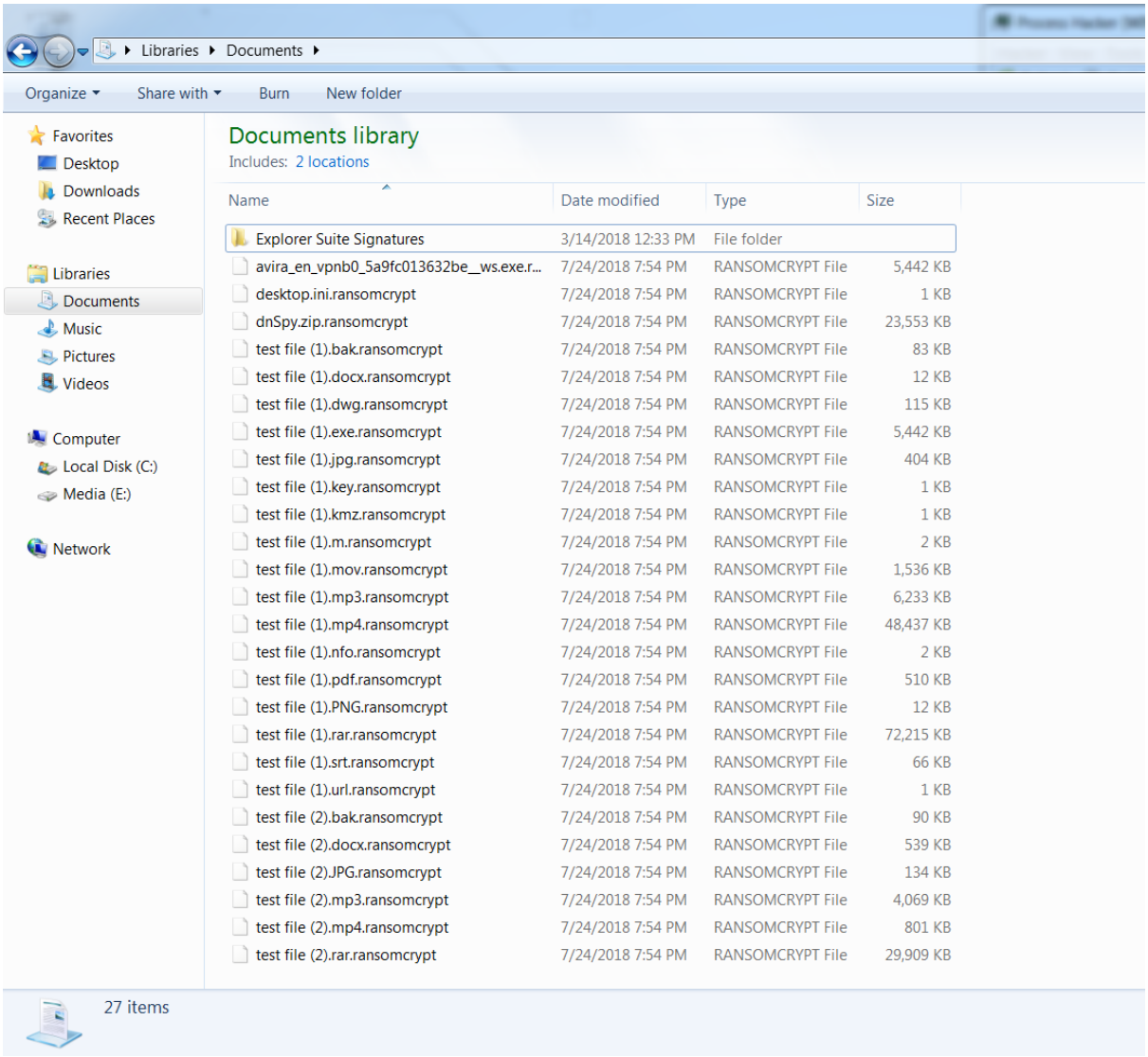
نام بخش	آنتروپی	آدرس مجازی	اندازه مجازی	اندازه خام
.text	٤.۰۳	۸۱۹۲	۲۷٦۹۰۰	۲۷٦۹۹۲
.rsrc	٤.۱	۲۸٦۷۲۰	۱٤۸٤	۱۵۳٦
.reloc	۰.۱	۲۹٤۹۱۲	۱۲	۵۱۲

تحلیل پویا :

برای بررسی عمیق‌تر باج‌افزار The Brotherhood، 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، شروع به رمزگذاری تمام فایل‌های موجود در پوشه‌ی Documents ویندوز می‌کند و پس از اتمام فرایند رمزگذاری، یک تصویر که شامل پیغام باج‌خواهی می‌باشد را بر روی Desktop قرار می‌دهد. سپس فرایند مربوط به باج‌افزار پایان می‌یابد. تصویر زیر مربوط به پیغام باج‌خواهی این باج‌افزار می‌باشد :

بر اساس پیغام باج‌خواهی، مهاجمین اعلام کرده اند که تمام فایل‌ها را رمزگذاری نموده‌اند و قربانیان جهت رمزگشایی فایل‌ها می بایست مبلغ هنگفت ۱۰۰ بیت‌کوین را به کیف پول بیت‌کوین به آدرس ۲٤fAcfdYasU٩٧٥qwFGyesl٤٥eH٦٣cNuCZP انتقال دهند و در صورت عدم پرداخت این مبلغ تا ساعت ۱٦:۳۰ عصر همان روز، مهاجمین فایل ها را از بین خواهند برد. در واقع این متن شبیه به یک شوخی می‌باشد زیرا طبق بررسی‌های انجام شده چنین آدرسی جهت پرداخت مبلغ باج‌خواهی وجود ندارد، همچنین در متن پیغام باج‌خواهی هیچ راهی برای برقراری ارتباط با مهاجمین ذکر نشده است.

تصویر زیر نشان‌دهنده فایل‌های رمزگذاری شده توسط این باج‌افزار می‌باشد و همانطور که قابل مشاهده است پس از رمزگذاری فایل‌ها پسوند ransomcrypt. به انتهای فایل‌ها اضافه می‌شود.

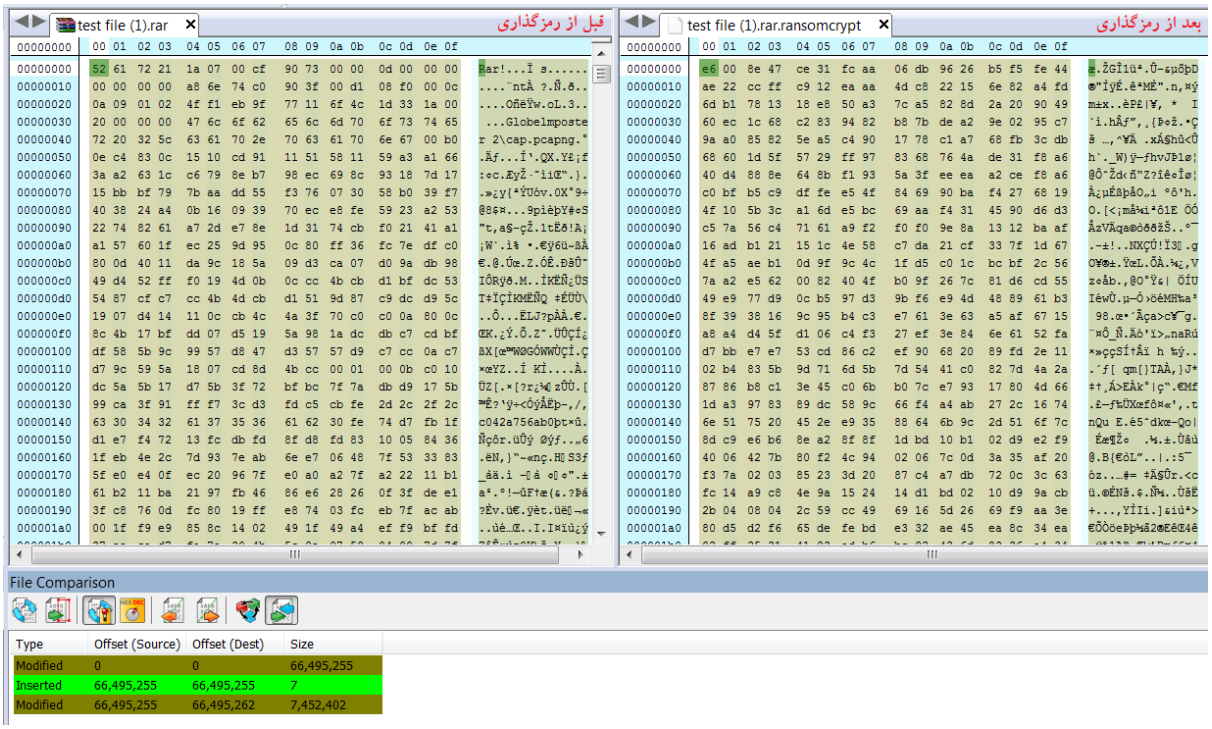


بر اساس بررسی‌های انجام شده اکثر آنتی‌ویروس‌های معتبر، این باج‌افزار را به عنوان یک تروجان شناسایی نموده‌اند. لذا احتمال نفوذ باج‌افزار به سیستم از راه‌های متداول از جمله هرزنامه‌ها وجود دارد.

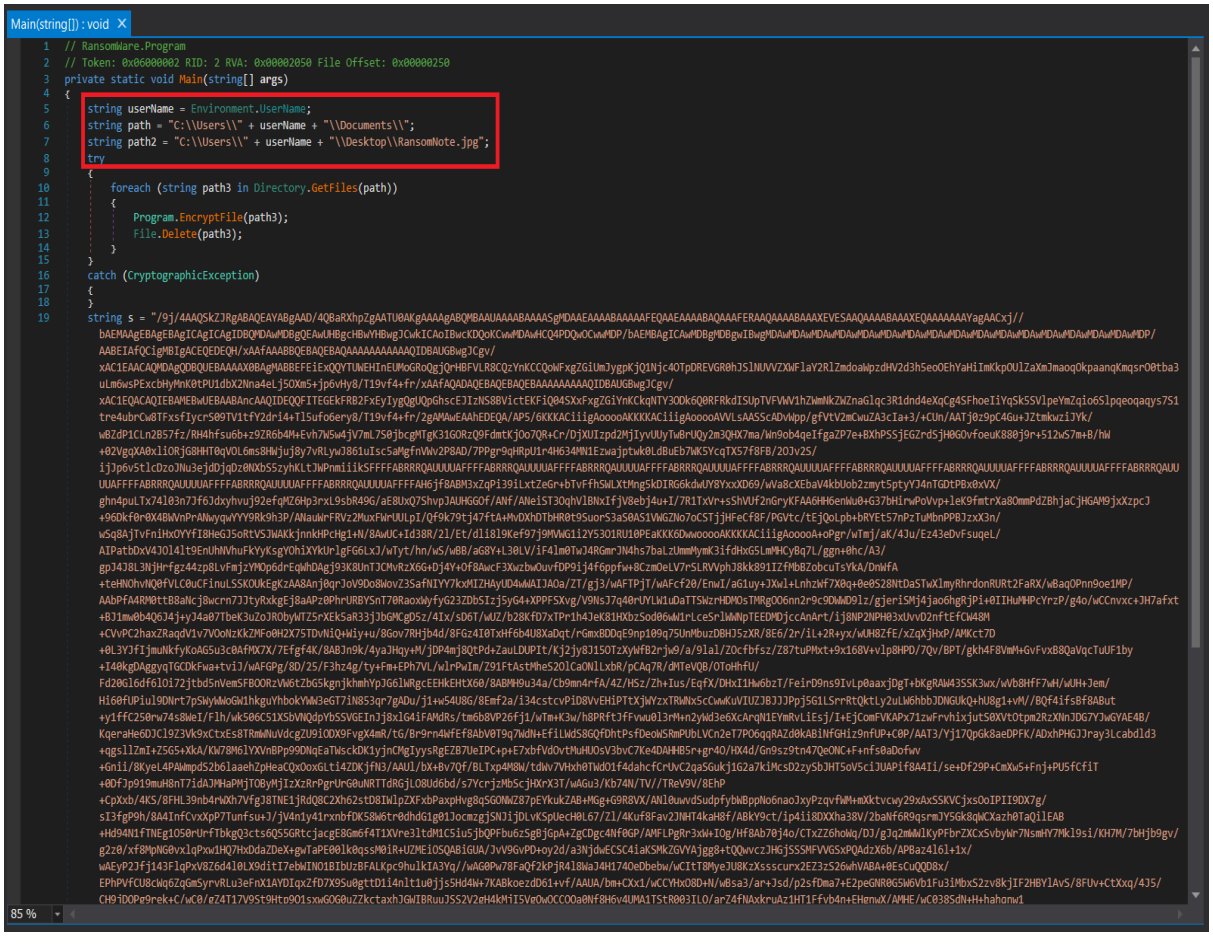
تحلیل ایستا:

پس از تحلیل کد باج‌افزار The Brotherhood 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 The Brotherhood ساختار فایل‌ها را پس از رمزگذاری به طور کامل تغییر می‌دهد. تصویر زیر نمونه‌ای از تغییرات ساختار فایل‌ها را نشان می‌دهد :



تصویر زیر تابع Main() باج‌افزار را نشان می‌دهد که دایرکتوری مورد هدف باج‌افزار و دایرکتوری که تصویر پیغام باج‌خواهی را در آن قرار می‌دهد مشخص شده است :



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

```
AES_Encrypt(byte[], byte[]) : byte[]
// RansomWare.Program
// Token: 0x06000004 RID: 4 RVA: 0x00002140 File Offset: 0x00000340
public static byte[] AES_Encrypt(byte[] bytesToBeEncrypted, byte[] passwordBytes)
{
    byte[] array = null;
    byte[] salt = new byte[]
    {
        1,
        2,
        3,
        4,
        5,
        6,
        7,
        8
    };
    byte[] result;
    using (MemoryStream memoryStream = new MemoryStream())
    {
        using (RijndaelManaged rijndaelManaged = new RijndaelManaged())
        {
            rijndaelManaged.KeySize = 256;
            rijndaelManaged.BlockSize = 128;
            Rfc2898DeriveBytes rfc2898DeriveBytes = new Rfc2898DeriveBytes(passwordBytes, salt, 1000);
            rijndaelManaged.Key = rfc2898DeriveBytes.GetBytes(rijndaelManaged.KeySize / 8);
            rijndaelManaged.IV = rfc2898DeriveBytes.GetBytes(rijndaelManaged.BlockSize / 8);
            rijndaelManaged.Mode = CipherMode.CBC;
            using (CryptoStream cryptoStream = new CryptoStream(memoryStream, rijndaelManaged.CreateEncryptor(), CryptoStreamMode.Write))
            {
                cryptoStream.Write(bytesToBeEncrypted, 0, bytesToBeEncrypted.Length);
                cryptoStream.Close();
            }
            array = memoryStream.ToArray();
        }
        result = array;
    }
    return result;
}
```

قطعه کد زیر مربوط به فرایند رمزگذاری فایل‌ها و اضافه نمودن پسوند ransomcrypt. به انتهای فایل‌ها می‌باشد :

```
EncryptFile(string) : void
// RansomWare.Program
// Token: 0x06000003 RID: 3 RVA: 0x000020EC File Offset: 0x000002EC
public static void EncryptFile(string path)
{
    string s = "asjkdhjskdfhvdsjkvhdkjnvdjksvdshseuvnhdsjksdfhdksvmdofjdsiogjovkdovkd123243t4t4kjlv";
    byte[] bytesToBeEncrypted = File.ReadAllBytes(path);
    byte[] array = Encoding.UTF8.GetBytes(s);
    array = SHA256.Create().ComputeHash(array);
    byte[] bytes = Program.AES_Encrypt(bytesToBeEncrypted, array);
    string path2 = path + ".ransomcrypt";
    File.WriteAllBytes(path2, bytes);
}
```

قطعه کد زیر مربوط به استفاده باج‌افزار از کتابخانه ویندوزی می‌باشد :

```
SystemParametersInfo(uint, uint, string, ui...
// RansomWare.Program
// Token: 0x06000001 RID: 1
[DllImport("user32.dll", CharSet = CharSet.Auto)]
private static extern int SystemParametersInfo(uint action, uint uParam, string vParam, uint winIni);
```

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

mscoree.dll
_CorExeMain

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

- RansomWare.exe

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 The Brotherhood نشدیم.

خروجی سامانه VirusTotal :

در حال حاضر تعداد ۵۰ مورد از ٦٧ آنتی ویروس و آنتی بـدافزار موجـود در سـامانه VirusTotal قـادر بـه شناسایی این باج‌افزار بوده وآن را حذف یا غیرفعال می‌کنند.

Ad-Aware	Gen:Heur.Ransom.MSIL.1	AegisLab	Troj.W32.Generic!c
ALYac	Trojan.Ransom.Brotherhood	Antiy-AVL	Trojan/Win32.AGeneric
Arcabit	Trojan.Ransom.MSIL.1	AVG	FileRepMalware
Avira	TR/Ransom.rkuyq	AVware	Trojan.Win32.Generic!BT
Baidu	Win32.Trojan.WisdomEyes.16070401....	BitDefender	Gen:Heur.Ransom.MSIL.1
CAT-QuickHeal	Trojan.IGENERIC	ClamAV	Win.Trojan.Agent-6599973-0
CrowdStrike Falcon	malicious_confidence_100% (D)	Cybereason	malicious.5c257a
Cylance	Unsafe	Cyren	W32/Trojan.EGLR-5991
DrWeb	Trojan.Encoder.25645	Emsisoft	Gen:Heur.Ransom.MSIL.1 (B)
Endgame	malicious (high confidence)	eScan	Gen:Heur.Ransom.MSIL.1
ESET-NOD32	a variant of MSIL/Filecoder.NV	F-Secure	Gen:Heur.Ransom.MSIL.1
Fortinet	MSIL/Filecoder.D716!tr.ransom	GData	Win32.Trojan-Ransom.Filecoder.P@gen
Ikarus	Trojan-Ransom.FileCoder	K7AntiVirus	Trojan (005361a51)
K7GW	Trojan (005361a51)	Kaspersky	HEUR:Trojan.Win32.Generic
Malwarebytes	Trojan.FileCryptor	MAX	malware (ai score=96)
McAfee	Artemis!23D82835C257	McAfee-GW-Edition	Artemis!Trojan
Microsoft	Trojan:Win32/Occamy.B	NANO-Antivirus	Trojan.Win32.Encoder.feqngv
Palo Alto Networks	generic.ml	Panda	Trj/GdSda.A
Qihoo-360	Win32/Trojan.Ransom.935	Rising	Trojan.Generic!8.C3 (CLOUD)
SentinelOne	static engine - malicious	Sophos AV	Mal/Generic-S
Sophos ML	heuristic	Symantec	Trojan Horse
Tencent	Win32.Trojan.Generic.Hrzc	TrendMicro	Ransom_BHOOD.THGODAH
TrendMicro-HouseCall	Ransom_BHOOD.THGODAH	VBA32	TScope.Trojan.MSIL
VIPRE	Trojan.Win32.Generic!BT	Webroot	W32.Ransom.Gen
Yandex	Trojan.Agent!wRgAEFT7174	ZoneAlarm	HEUR:Trojan.Win32.Generic

خروجی سامانه ویروس‌کاو 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 وآن را حذف یا غیرفعال می‌کنند.

نتیجه اسکن Sample_5b3e10e08983e342a8553390.bin

آنتی‌ویروس	نسخه آنتی‌ویروس	نتیجه اسکن	
پادویش	2.3.190.2675	✔	Clean
sophos	9.14.2	✔	Clean
f_secure	11.00	ii	Dangerous: Gen:Heur.Ransom.MSIL.1
kaspersky	5.5	i	Suspicious: HEUR:Trojan.Win32.Generic
eset	4.5.3.38183	ii	Dangerous: MSIL/Filecoder.NV
drweb	11.0.1.1607061217	ii	Dangerous: Trojan.Encoder.25645
clam_av	0.99.2	ii	Dangerous: Win.Trojan.Agent-6599973-0
comodo	1.1.268025.1	✔	Clean
bitdefender	11.0.1.18	ii	Dangerous: Gen:Heur.Ransom.MSIL.1
avast	2.1.2	✔	Clean
symantec	7.9.0.30	ii	Dangerous: Trojan Horse