باسمه تعالی

تحلیل فنی باج افزار PDB Fake

مقدمه :

مشاهده و رصد فضای سایبری در زمینه باج‌افزار، از شروع فعالیت نمونه جدیدی به نام PDB Fake خبر می‌دهد. بررسی‌ها نشان می‌دهد که فعالیت این باج‌افزار در تاریخ ۳۱ ماه ژوئیه سال ۲۰۱۸ میلادی شروع شده است و طبق تحقیقات صورت گرفته برخی از آنتی‌ویروس‌های معتبر آن را از خانواده باج‌افزار Razy تشخیص داده‌اند. طبق مشاهدات انجام شده این باج‌افزار در حال حاضر قادر به رمزگذاری فایل‌ها نمی‌باشد و طبق بررسی‌های صورت گرفته بر روی کدمنبع آن متوجه وجود نواقصی در آن شدیم که احتمال می‌دهیم این باج‌افزار در حال توسعه باشد. همچنین طبق تحقیقات صورت گرفته متوجه انتشار این باج‌افزار از آدرس زیر شدیم :

http://aka[.]ms/ioavtest

مشخصات فایل اجرایی :

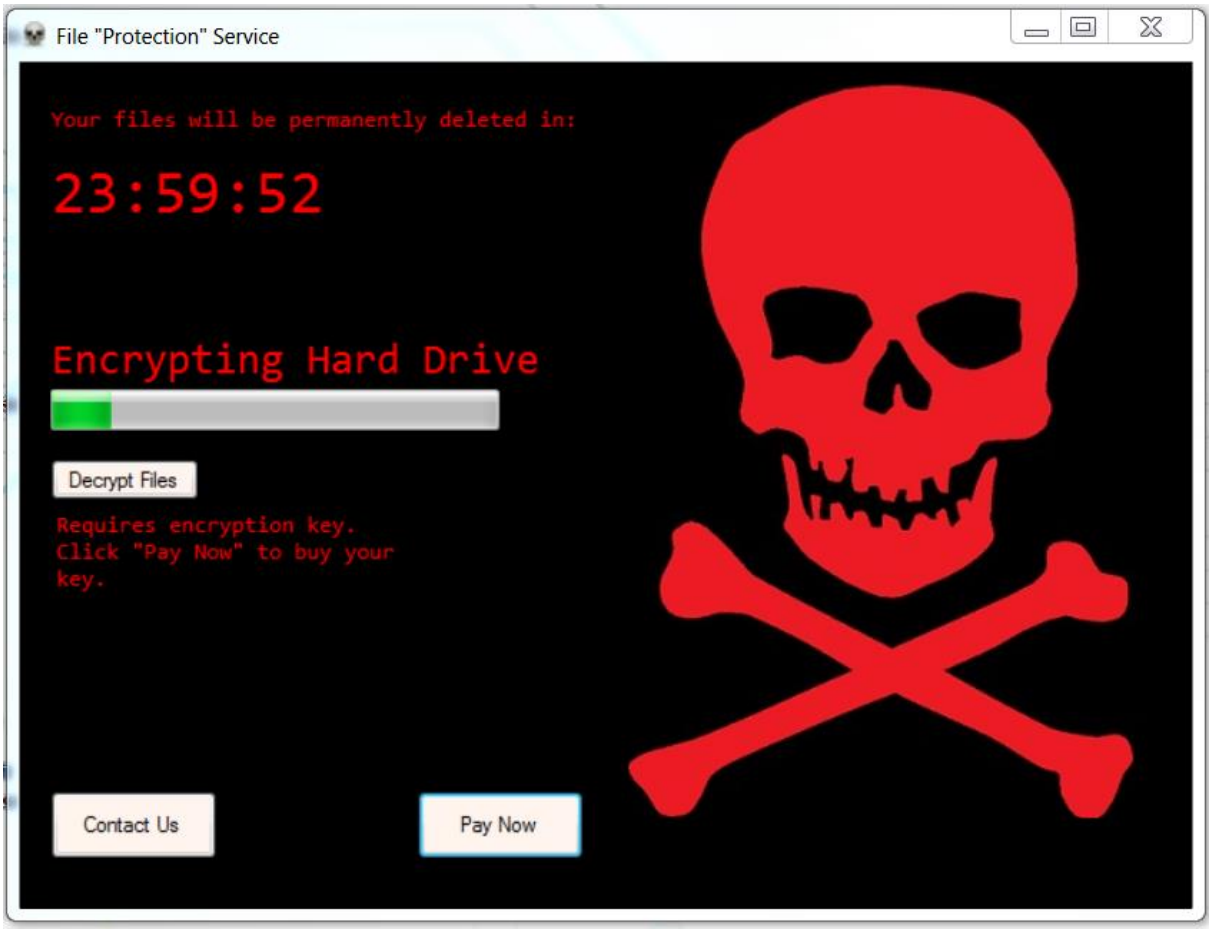
نام فایل	validatecloud.exe
MD۵	٦٣f٩٤٧٨b٥db٠e٠٠٩cb٠de٦a٢fc٤a١ce٢
SHA-١	ce٢b١٥١ac٧b٥e٥dc٨٣٨e٩٠٥efb٣٢٠b٢٠٤١٧٨٩٦٧٧
SHA-٢٥٦	٨٢٠ffafecae٧١a٠٥٠٤٦٢٨cdc٧٤cb٤a٣e٨٢٣f٦١cca٥٤ab٥٠٥c٩٣٣٦d٧٧ba٨eb٠٣b
اندازه فایل	١٢٠.٥٦ KB
کامپایلر	Microsoft visual C# v٧.٠ / Basic .NET

فایل اجرایی این باج افزار دارای سه بخش است :

نام بخش	آنتروپی	آدرس مجازی	اندازه مجازی	اندازه خام
.text	٥.٨٤	٨١٩٢	١٢٠٥٣٢	١٢٠٨٣٢
.rsrc	٤.١١	١٣١٠٧٢	١٤٦٨	١٥٣٦
.reloc	٠.١	١٣٩٢٦٤	١٢	٥١٢

تحلیل پویا :

برای بررسی عمیق‌تر باج‌افزار PDB Fake، 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، فقط پنجره‌ی زیر را به نمایش می‌گذارد و قادر به رمزگذاری فایل‌ها نمی‌باشد و قربانیان به راحتی می‌توانند با بستن این پنجره و اسکن نمودن سیستم خود با آخرین به‌روزسانی یکی از آنتی‌ویروس‌های معتبر از خطرات احتمالی این باج‌افزار رهایی یابند.



طبق پیغام موجود در این پنجره مهاجمین مدعی شده‌اند که فایل‌های قربانیان را رمزگذاری نموده‌اند و طی ۲٤ ساعت و در صورت عدم پرداخت مبلغ باج‌خواهی، آن‌ها را حذف خواهند نمود که همانطور که اشاره نمودیم چنین چیزی صحت ندارد و طی بررسی‌هایی که بر روی کدمنبع باج‌افزار انجام داده‌ایم شاهد این بوده‌ایم که کدمنبع آن دارای نواقصی می‌باشد و قادر به رمزگذاری فایل‌ها نمی‌باشد.

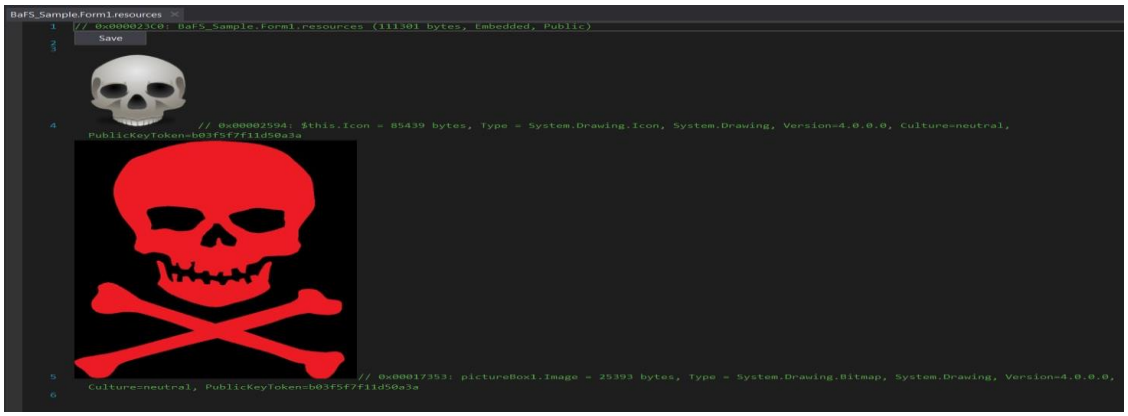
طبق مشاهدات صورت گرفته، هنگام اجرای باج‌افزار PDB Fake به طور میانگین از ۲ الی ۳ درصد ظرفیت CPU، و ۵ الی ۱۰ درصد ظرفیت حافظه (RAM) استفاده می‌گردد و به نظر می‌رسد علت پایین بودن عدد مربوط به ظرفیت CPU، عدم رمزگذاری فایل‌ها می‌باشد.

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 PDB Fake به نتایج زیر دست پیدا کردیم.

تصویر زیر مربوط به تصویر موجود در پنجره‌ی مربوط به پیغام باج‌خواهی می‌باشد :



قطعه کد زیر مربوط به تابع Form۱() می‌باشد که توابع مختلف را جهت اجرای باج‌افزار فراخوانی می‌کند :

```
Form1
using System;
using System.ComponentModel;
using System.Drawing;
using System.Globalization;
using System.Windows.Forms;

namespace BaFS_Sample
{
    // Token: 0x02000002 RID: 2
    public class Form1 : Form
    {
        // Token: 0x06000001 RID: 1 RVA: 0x00002050 File Offset: 0x00000250
        public Form1()
        {
            this.InitializeComponent();
            this.label2.Text = "Encrypting Hard Drive";
            this.progressBarTimer.Tick += this.timer1_tick;
            this.progressBarTimer.Interval = 100;
            this.progressBarTimer.Enabled = true;
            this.progressBarTimer.Start();
            this.countDown.AddHours(24.0);
            this.label1.Text = this.countDown.ToString("HH:mm:ss", this.ci);
            this.label1.Update();
            this.countdowntimer.Tick += this.timer2_tick;
            this.countdowntimer.Interval = 10;
            this.countdowntimer.Enabled = true;
            this.countdowntimer.Start();
            this.progressBar1.Minimum = 1;
            this.progressBar1.Maximum = 1000;
            this.progressBar1.Step = 1;
        }
```

قطعه کد زیر مربوط به توابع لازم جهت ایجاد پنجره‌ی پیغام باج‌خواهی می‌باشد :

Form1

```
86
87          // Token: 0x0600000B RID: 11 RVA: 0x000021FC File Offset: 0x000003FC
88          private void InitializeComponent()
89          {
90              this.components = new Container();
91              ComponentResourceManager componentResourceManager = new ComponentResourceManager(typeof(Form1));
92              this.pictureBox1 = new PictureBox();
93              this.progressBarTimer = new Timer(this.components);
94              this.button1 = new Button();
95              this.label1 = new Label();
96              this.label2 = new Label();
97              this.progressBar1 = new ProgressBar();
98              this.countdowntimer = new Timer(this.components);
99              this.label3 = new Label();
100             this.button2 = new Button();
101             this.button3 = new Button();
102             this.textBox1 = new TextBox();
103             ((ISupportInitialize)this.pictureBox1).BeginInit();
104             base.SuspendLayout();
105             this.pictureBox1.Image = (Image)componentResourceManager.GetObject("pictureBox1.Image");
106             this.pictureBox1.Location = new Point(340, 12);
107             this.pictureBox1.Name = "pictureBox1";
108             this.pictureBox1.Size = new Size(303, 434);
109             this.pictureBox1.TabIndex = 0;
110             this.pictureBox1.TabStop = false;
111             this.progressBarTimer.Enabled = true;
112             this.progressBarTimer.Interval = 5000;
113             this.progressBarTimer.Tick += this.timer1_tick;
114             this.button1.BackColor = Color.SeaShell;
115             this.button1.FlatAppearance.BorderColor = Color.Red;
116             this.button1.FlatAppearance.MouseDownBackColor = Color.FromArgb(255, 255, 192);
117             this.button1.Location = new Point(222, 408);
118             this.button1.Name = "button1";
119             this.button1.Size = new Size(93, 38);
120             this.button1.TabIndex = 1;
121             this.button1.Text = "Pay Now";
122             this.button1.UseVisualStyleBackColor = false;
123             this.button1.Click += this.button1_Click;
124             this.label1.AutoSize = true;
125             this.label1.BackColor = Color.Black;
126             this.label1.Font = new Font("Consolas", 26.25f, FontStyle.Regular, GraphicsUnit.Point, 0);
127             this.label1.ForeColor = Color.Red;
128             this.label1.Location = new Point(10, 52);
```

100 %

قطعه کد زیر مربوط به توابع مربوط به دکمه‌های مختلف موجود بر روی پنجره‌ی پیغام باج‌خواهی می‌باشد و همانطور که مشاهده می‌گردد هیچ گونه دستورالعمل خاصی برای انجام وجود ندارد و در صورت کلیک بر روی آن‌ها هیچ اتفاقی رخ نمی‌دهد :

Form1

```
32
33          // Token: 0x06000002 RID: 2 RVA: 0x0000217B File Offset: 0x0000037B
34          private void timer1_tick(object sender, EventArgs e)
35          {
36              this.progressBar1.PerformStep();
37          }
38
39          // Token: 0x06000003 RID: 3 RVA: 0x00002188 File Offset: 0x00000388
40          private void timer2_tick(object sender, EventArgs e)
41          {
42              this.countDown = this.countDown.AddMilliseconds(-7.0);
43              this.label1.Text = this.countDown.ToString("HH:mm:ss", this.ci);
44              this.label1.Update();
45          }
46
47          // Token: 0x06000004 RID: 4 RVA: 0x000021DB File Offset: 0x000003DB
48          private void button1_Click(object sender, EventArgs e)
49          {
50          }
51
52          // Token: 0x06000005 RID: 5 RVA: 0x000021DB File Offset: 0x000003DB
53          private void label2_Click(object sender, EventArgs e)
54          {
55          }
56
57          // Token: 0x06000006 RID: 6 RVA: 0x000021DB File Offset: 0x000003DB
58          private void progressBar1_Click(object sender, EventArgs e)
59          {
60          }
61
62          // Token: 0x06000007 RID: 7 RVA: 0x000021DB File Offset: 0x000003DB
63          private void label1_Click(object sender, EventArgs e)
64          {
65          }
66
67          // Token: 0x06000008 RID: 8 RVA: 0x000021DB File Offset: 0x000003DB
68          private void label3_Click(object sender, EventArgs e)
69          {
70          }
71
72          // Token: 0x06000009 RID: 9 RVA: 0x000021DB File Offset: 0x000003DB
73          private void label4_Click(object sender, EventArgs e)
74          {
75          }
76
77          // Token: 0x0600000A RID: 10 RVA: 0x000021DD File Offset: 0x000003DD
78          protected override void Dispose(bool disposing)
79          {
80              if (disposing && this.components != null)
81              {
82                  this.components.Dispose();
```

100 %

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

mscoree.dll
_CorExeMain

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 PDB Fake نشدیم.

خروجی سامانه VirusTotal :

در حال حاضر تعداد ٤٦ مورد از ٦٨ آنتی ویروس و آنتی بدافزار موجود در سامانه VirusTotal قادر به شناسایی این باج افزار بوده وآن را حذف یا غیرفعال می‌کنند.

Ad-Aware	Gen:Variant.Razy.267354	AegisLab	Troj.Ransom.Msil.Agent!c
ALYac	Trojan.Ransom.Filecoder	Antiy-AVL	Trojan/Win32.BTSGeneric
Arcabit	Trojan.Razy.D4145A	Avast	FileRepMalware
AVG	FileRepMalware	AVware	Trojan.Win32.Generic!BT
BitDefender	Gen:Variant.Razy.267354	CAT-QuickHeal	Trojan.Skeeyah
ClamAV	Win.Trojan.Agent-6637915-0	CrowdStrike Falcon	malicious_confidence_80% (D)
Cybereason	malicious.b5db0e	Cyren	W32/Trojan.OKAA-0429
Emsisoft	Gen:Variant.Razy.267354 (B)	ESET-NOD32	MSIL/Hoax.FakeFilecoder.CX
F-Secure	Gen:Variant.Razy.267354	Fortinet	W32/Agent.AAZ!tr
GData	Gen:Variant.Razy.267354	Ikarus	Trojan.SuspectCRC
Jiangmin	Trojan.MSIL.irzh	K7AntiVirus	Riskware (0040eff71)
K7GW	Riskware (0040eff71)	Kaspersky	Trojan-Ransom.MSIL.Agent.aaz
Malwarebytes	Ransom.FileLocker	MAX	malware (ai score=98)
McAfee	Trojan-FPHR!63F9478B5DB0	McAfee-GW-Edition	Trojan-FPHR!63F9478B5DB0
Microsoft	Trojan:Win32/Occamy.C	NANO-Antivirus	Trojan.Win32.Ransom.ffzjwk
Palo Alto Networks	generic.ml	Panda	Trj/GdSda.A
Qihoo-360	Win32/Trojan.7c5	Rising	Ransom.Agent!8.6B7 (CLOUD)
SentinelOne	static engine - malicious	Sophos AV	Mal/Generic-S
Symantec	Trojan.Gen.2	Tencent	Msil.Trojan.Agent.Wqnh
TrendMicro	Ransom_SKULL.THHOGAH	TrendMicro-HouseCall	Ransom_SKULL.THHOGAH
VBA32	Trojan.Skeeyah	VIPRE	Trojan.Win32.Generic!BT
ViRobot	Trojan.Win32.Z.Razy.123456	Webroot	W32.Trojan.Gen
Yandex	Trojan.Agent!NzqLD5jb45g	ZoneAlarm	Trojan-Ransom.MSIL.Agent.aaz

خروجی سامانه ویروس‌کاو مرکز ماهر :

در حال حاضر تعداد ۸ 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 Honest_Sample_5b6da20fcb4ca54ad0ca7eb9.exe

آنتی‌ویروس	نسخه آنتی‌ویروس	نتیجه اسکن	
پادویش	2.3.190.2675	✔	Clean
sophos	9.14.2	✔	Clean
f_secure	11.00	ii	Dangerous: Gen:Variant.Razy.267354
kaspersky	5.5	ii	Dangerous: Trojan-Ransom.MSIL.Agent.aaz
eset	4.5.3.38333	ii	Dangerous: MSIL/Hoax.FakeFilecoder.CX
drweb	11.0.1.1607061217	✔	Clean
clam_av	0.99.2	ii	Dangerous: Win.Trojan.Agent-6637915-0
comodo	1.1.268025.1	ii	Dangerous: Malware
bitdefender	11.0.1.18	ii	Dangerous: Gen:Variant.Razy.267354
avast	2.1.2	ii	Dangerous: MSIL:Agent-DRN
symantec	7.9.0.30	ii	Dangerous: Trojan.Gen.2