

[逆向][Writeup]ISG2015 flagfinder - .NET程序逆向

转载

[weixin_34355715](#) 于 2017-02-16 11:35:00 发布 53 收藏

原文链接: <http://www.cnblogs.com/gsharpsh00ter/p/6404940.html>

版权

这个题目同样是一道.NET的逆向题，.NET的逆向方法在之前的博文中已经介绍过，这里不做重复的说明。本题的源程序可以在我的github上下载: <https://github.com/gsharpsh00ter/reverse>

0x01 逆向

flagfinder为.NET编译的PE文件，用dnSpy反编译后，得到如下源码：

```
1 using System;
2 using System.IO;
3 using System.Linq;
4 using System.Security.Cryptography;
5 using System.Threading;
6 using Microsoft.VisualBasic.CompilerServices;
7
8 namespace flagfinder
9 {
10     // Token: 0x02000007 RID: 7
11     [StandardModule]
12     internal sealed class Module1
13     {
14         // Token: 0x06000012 RID: 18 RVA: 0x000020D4 File Offset: 0x000002D4
15         [STAThread]
16         //遍历所有驱动器上的所有文件
17         public static void Main()
18         {
19             DriveInfo[] drives = DriveInfo.GetDrives();
20             checked
21             {
22                 for (int i = 0; i < drives.Length; i++)
23                 {
24                     DriveInfo driveInfo = drives[i];
25                     if (driveInfo.IsReady)
26                     {
27                         Module1.SearchDir(driveInfo.RootDirectory);
28                     }
29                 }
30             }
31         }
32
33         // Token: 0x06000013 RID: 19 RVA: 0x0000210C File Offset: 0x0000030C
34         public static void SearchDir(DirectoryInfo dir)
35         {
36             checked
37             {
38                 try
39                 {
40                     FileInfo[] files = dir.GetFiles();
41                     for (int i = 0; i < files.Length; i++)
42                     {
43                         FileInfo file = files[i];
```

```

44         //对于每一个文件，会进行检查，找到符合条件的文件会打印flag
45         Module1.CheckFile(file);
46     }
47     DirectoryInfo[] directories = dir.GetDirectories();
48     for (int j = 0; j < directories.Length; j++)
49     {
50         dir = directories[j];
51         Module1.SearchDir(dir);
52     }
53 }
54 catch (Exception expr_49)
55 {
56     ProjectData.SetProjectError(expr_49);
57     Console.WriteLine("Unable to search: " + dir.FullName);
58     ProjectData.ClearProjectError();
59 }
60 }
61 }
62
63 // Token: 0x06000014 RID: 20 RVA: 0x00002198 File Offset: 0x00000398
64 public static void CheckFile(FileInfo file)
65 {
66     try
67     {
68         Console.WriteLine("Analyzing " + file.FullName + " ...");
69         //此处为判断条件，文件内容的MD5为指定值后会计算sha256哈希值，并打印flag
70         MD5CryptoServiceProvider mD5CryptoServiceProvider = new MD5CryptoServiceProvider();
71         if (mD5CryptoServiceProvider.ComputeHash(file.OpenRead()).SequenceEqual(Module1.target))
72         {
73             SHA256CryptoServiceProvider sha256CryptoServiceProvider = new
SHA256CryptoServiceProvider();
74             Console.WriteLine("We've found the flag on your hard drive:");
75             Console.WriteLine("ISG{" +
BitConverter.ToString(sha256CryptoServiceProvider.ComputeHash(file.OpenRead())).ToLower() + "}");
76             Environment.Exit(0);
77         }
78         Thread.Sleep(100);
79     }
80     catch (Exception expr_81)
81     {
82         ProjectData.SetProjectError(expr_81);
83         Console.WriteLine("Unable to read: " + file.FullName);
84         ProjectData.ClearProjectError();
85     }
86 }
87
88 // Token: 0x04000006 RID: 6
89 private static byte[] target = new byte[]
90 {
91     108,
92     203,
93     97,
94     69,
95     90,
96     216,
97     146,
98     25,
99     144,
100    43,
101    50

```

```

101         58,
102         246,
103         10,
104         154,
105         45,
106         28
107     };
108 }
109 }

```

0x02 分析

程序逻辑比较简单，运行后会遍历驱动器上的所有文件，并对每一个文件进行检查。如果某个文件的内容经过MD5哈希后是指定的值(target)，则该文件为flag文件，此时会计算器sha256的哈希值，并打印flag。

显然我们不太可能根据已有的MD5值去逆向破解出文件的内容。可以用google查一下对应的MD5值。在<http://www.herdprotect.com/a2cmd.exe-12fc1578b371d0847bf158eefb36f85f42cb9fb3.aspx>这个页面，我们发现相关的信息：

Overview	
Analysis	a2cmd.exe
File Details	Emsisoft Anti-Malware
Programs (1)	Emsisoft GmbH
	This is installed with Emsisoft Internet Security.
File name:	a2cmd.exe
Publisher:	Emsisoft GmbH (signed and verified)
Product:	Emsisoft Anti-Malware
Description:	Command Line Scanner
Version:	9.0.0.4570
MD5:	6ccb61455ad89219902b3af60a9a2d1c
SHA-1:	12fc1578b371d0847bf158eefb36f85f42cb9fb3
SHA-256:	4cbce92e74fc64dba2b0c5194dd54bf7d694d37fc758572f46bd5b3b8a0c1a80

MD5: 6ccb61455ad89219902b3af60a9a2d1c

Sha256: 4cbce92e74fc64dba2b0c5194dd54bf7d694d37fc758572f46bd5b3b8a0c1a80

这应该是一个恶意文件的MD5值，虽然我们没有该文件，但是没关系，我们已经得到了sha256的哈希值，根据程序逻辑，我们已经可以自己打印flag了。

打印flag的python代码如下：

```

1  #!/usr/bin/python2
2
3  #targets = [108, 203, 97, 69, 90, 216, 146, 25, 144, 43, 58, 246, 10, 154, 45, 28]
4  md5="6ccb61455ad89219902b3af60a9a2d1c"
5  sha256="4cbce92e74fc64dba2b0c5194dd54bf7d694d37fc758572f46bd5b3b8a0c1a80"
6  flag="ISG{"
7
8  for i in range(0, len(sha256), 2):
9      flag = flag + sha256[i:i+2] + "-"
10 flag += "}"
11 flag = flag.replace("-}", "}")
12 print flag

```

运行结果如下：

```
选择C:\WINDOWS\system32\cmd.exe
F:\ctf\reverse\0ctf2015-flagfinder>
F:\ctf\reverse\0ctf2015-flagfinder>flagfinder.py
ISG{4c-bc-e9-2e-74-fc-64-db-a2-b0-c5-19-4d-d5-4b-f7-d6-94-d3-7f-c7-58-57-2f-46-bd-5b-3b-8a-0c-1a-80}
F:\ctf\reverse\0ctf2015-flagfinder>
```

Flag为:

ISG{4c-bc-e9-2e-74-fc-64-db-a2-b0-c5-19-4d-d5-4b-f7-d6-94-d3-7f-c7-58-57-2f-46-bd-5b-3b-8a-0c-1a-80}

转载于:<https://www.cnblogs.com/gsharpsh00ter/p/6404940.html>