SRSniffer 和 SuperScan 学习报告

stormlin 2017-06-04

* [1. SRSniffer](file:///D:\Program%20Files%20(x86)\Microsoft%20VS%20Code\resources\app\out\vs\workbench\parts\html\browser\webview.html#1-srsniffer)
  + [1.1 测试过程](file:///D:\Program%20Files%20(x86)\Microsoft%20VS%20Code\resources\app\out\vs\workbench\parts\html\browser\webview.html#11-%E6%B5%8B%E8%AF%95%E8%BF%87%E7%A8%8B)
  + [1.2 测试结果](file:///D:\Program%20Files%20(x86)\Microsoft%20VS%20Code\resources\app\out\vs\workbench\parts\html\browser\webview.html#12-%E6%B5%8B%E8%AF%95%E7%BB%93%E6%9E%9C)
* [2. SuperScan 与 Nmap](file:///D:\Program%20Files%20(x86)\Microsoft%20VS%20Code\resources\app\out\vs\workbench\parts\html\browser\webview.html#2-superscan-%E4%B8%8E-nmap)
  + [2.1 SuperScan 测试结果](file:///D:\Program%20Files%20(x86)\Microsoft%20VS%20Code\resources\app\out\vs\workbench\parts\html\browser\webview.html#21-superscan-%E6%B5%8B%E8%AF%95%E7%BB%93%E6%9E%9C)
  + [2.2 Nmap 测试结果](file:///D:\Program%20Files%20(x86)\Microsoft%20VS%20Code\resources\app\out\vs\workbench\parts\html\browser\webview.html#22-nmap-%E6%B5%8B%E8%AF%95%E7%BB%93%E6%9E%9C)

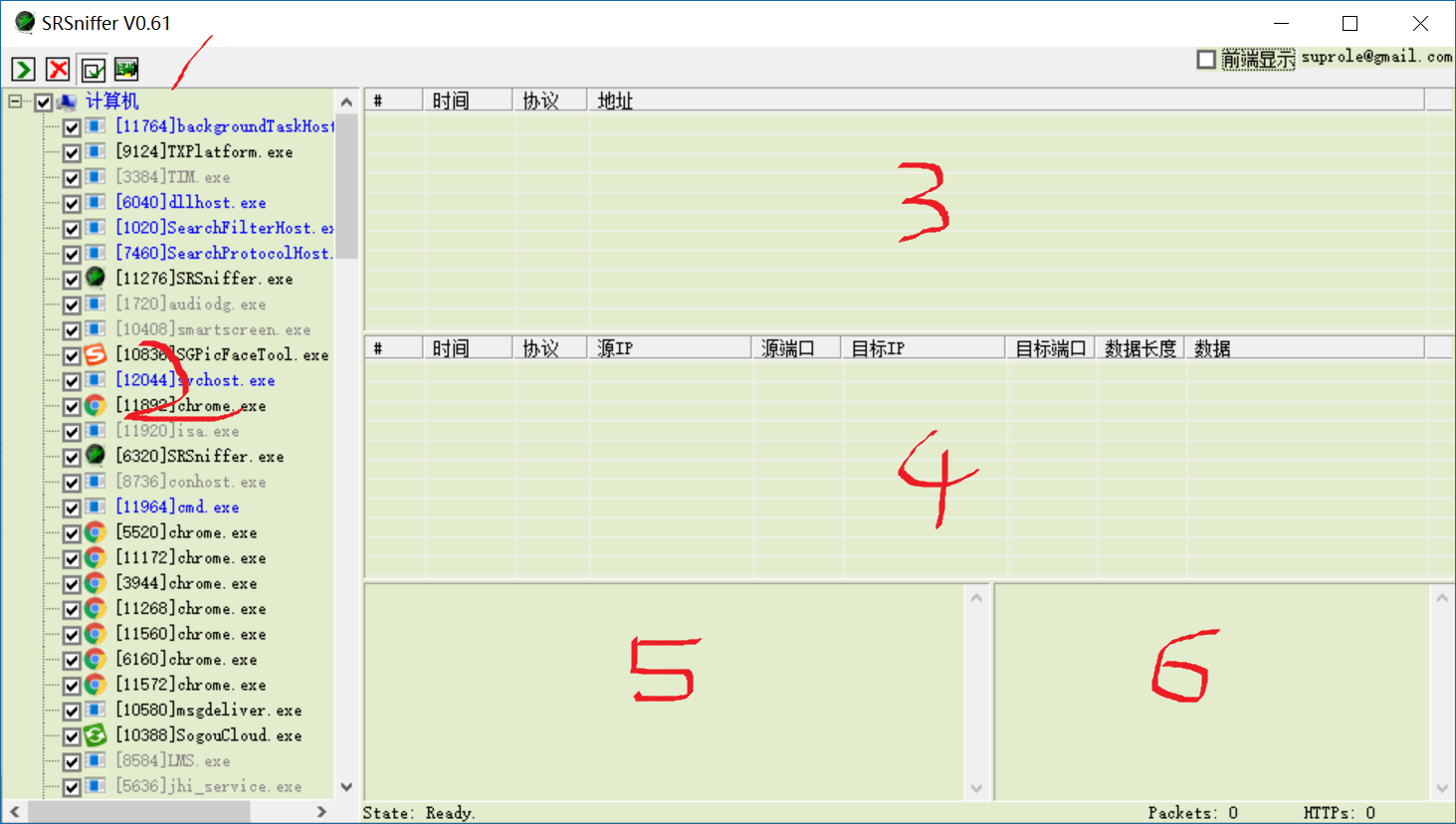
1. SRSniffer

网传用户在参加了 360 杀毒的云安全计划之后，它就会在后台上传用户电脑中的“可疑文件（Scan Suspicious File）”。但对于“可疑文件的”的定义，360 官方并没有提供详细的定义。

本次实验通过使用 SRSniffer 来抓取系统中所有包，并分析其中的 360 链接，以确认其是否会在后台上传用户数据，。

1.1 测试过程

在互联网上下载 SRSniffer V0.61 绿色版。下载完成后在主机中以管理员用户启动软件。



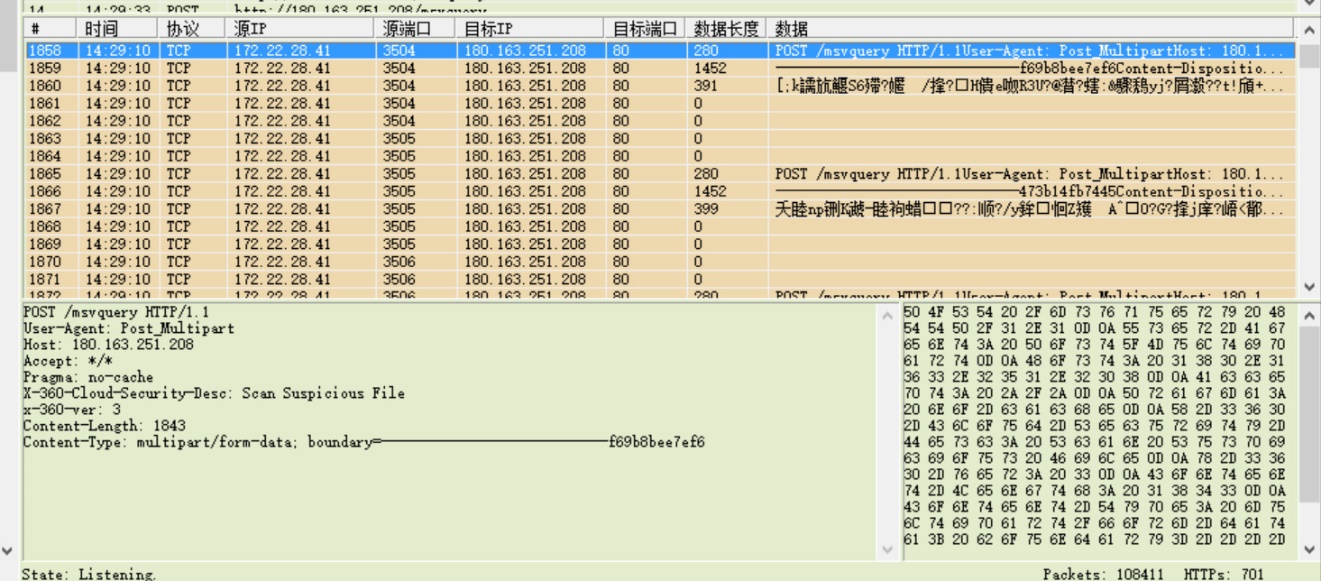
图一 SRSniffer 的启动界面

软件的界面较为简单，一共分为 6 块。

1. 第一块为工具栏，其上的按钮依次为“开始/停止 监听”、“清除所有数据”、“勾选新进程”和“切换监听网卡”；
2. 第二块为进程列表，可以在这一块勾选需要监听的进程；
3. 第三块为按照时间和目的主机地址排序的会话列表；
4. 第四块为按包排序的详细结果区；
5. 第五块为包内容的文本显示区；
6. 第六块为包内容的十六进制显示区。

1.2 测试结果

经过分析，我们发现 360 杀毒的确会向其内部服务器发送一些数据。



图二 360 杀毒向内部服务器发送的数据包

从图中的数据包我们可以发现，接收方服务器的 IP 为：180.163.251.208。但这个服务器已经对接受的数据包进行了过滤：由于抓包结果显示对方端口号为 80，故我们也在浏览器中范围此 IP，但是对方返回“403 Forbidden”。

以下为发送方发出的第一个包。

POST /msvquery HTTP/1.1

User-Agent: Post\_Multipart

Host: 180.163.251.208

Accept: \*/\*

Pragma: no-cache

X-360-Cloud-Security-Desc: Scan Suspicious File

x-360-ver: 3

Content-Length: 1843

Content-Type: multipart/form-data; boundary=----------------------------f69b8bee7ef6

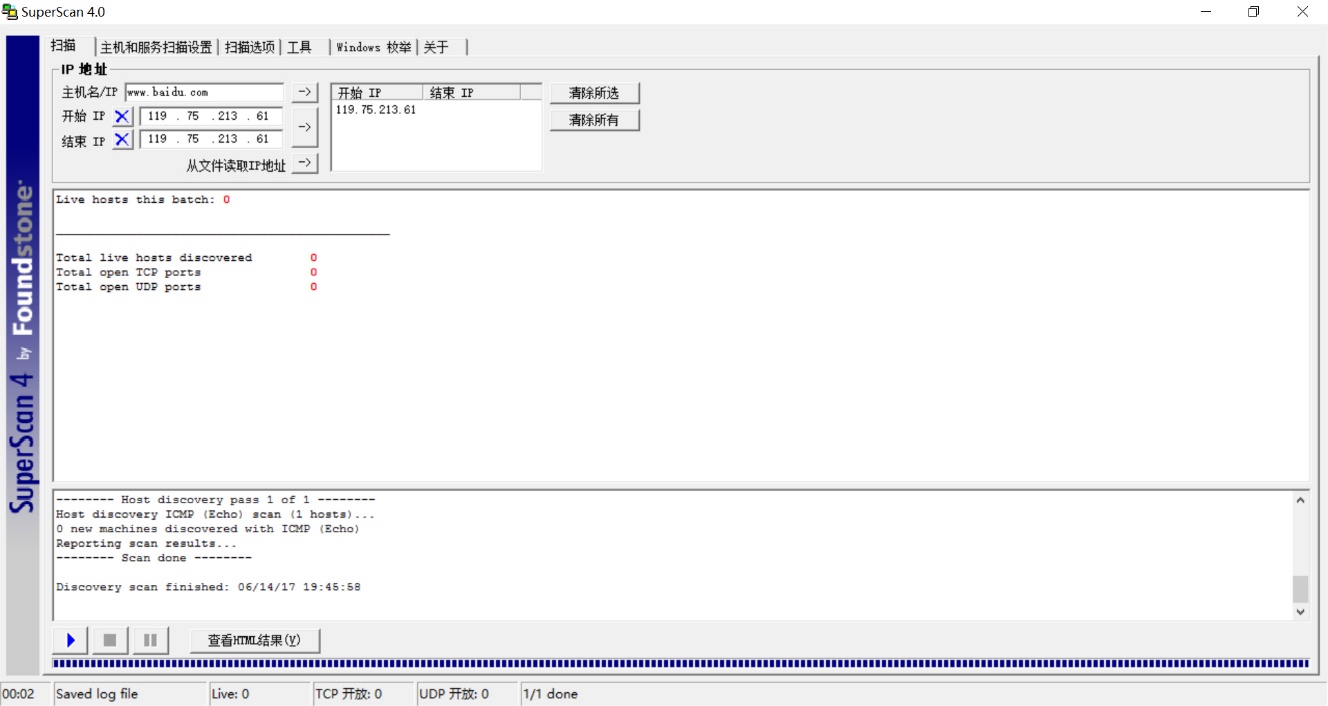
但由于我们不清楚数据中的格式，也不能确定包中的数据是否为源数据，故无法还原出原始数据。故在此提醒用户，参加云安全计划时要谨慎选择。

2. SuperScan 与 Nmap

2.1 SuperScan 测试结果

在下载 SuperScan V4.0 之后，我们在测试主机上以管理员权限打开软件。在“主机名/IP”一栏中填入百度的网址。

但是由于位置原因，此 SuperScan 不能获取到任何结果（见）



图三 无法获取到 SuperScan 的测试结果

2.2 Nmap 测试结果

由于无法通过 SuperScan 获取测试结果，我们在本次试验中引入了比 SuperScan 更加先进、更加简便易用的 Nmap 来作为我们的扫描测试软件。



图四 Nmap 测试结果

本次端口扫描测试选择了百度的主机（119.75.216.20）作为目标主机。

根据获得的扫描结果，我们发现目标主机只开放了 80（http）和 443（https）两个端口。并无其他多余端口。证明对方有一定安全意识。