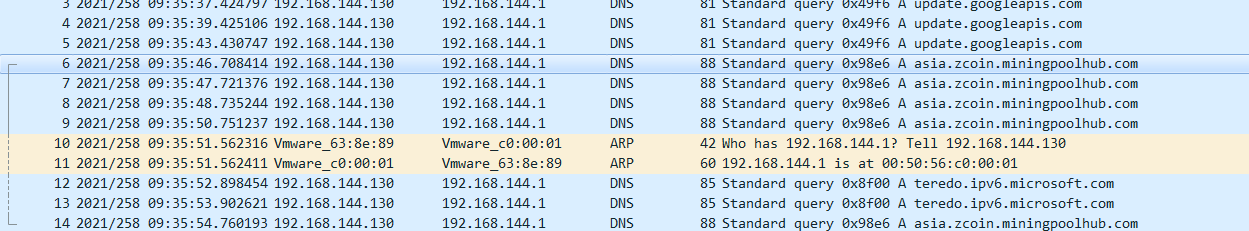
**置顶：**

**铭记九一八，永志不忘，奋勇向前！！**

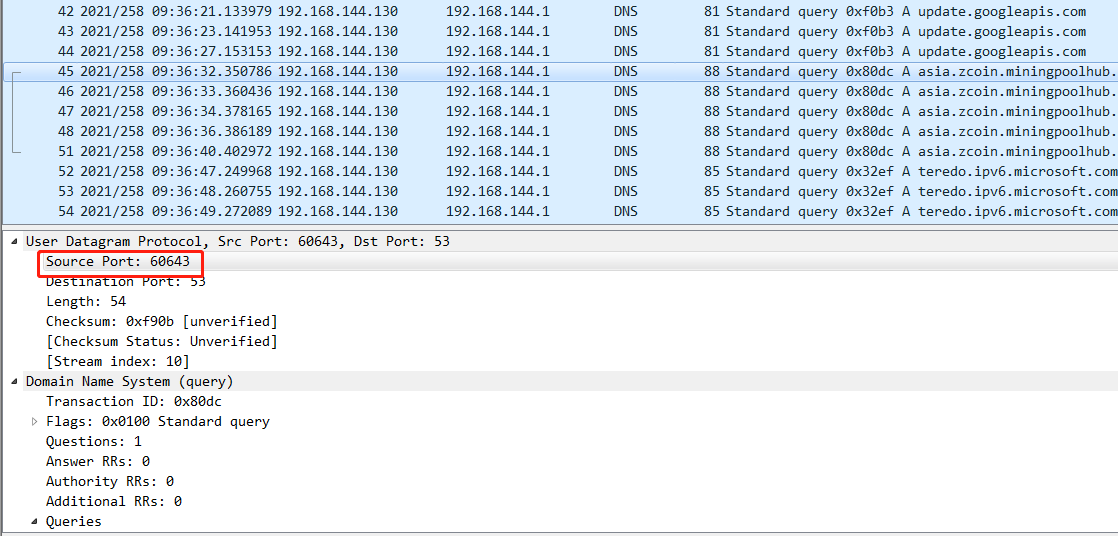
一、事件描述

最近遇到过一个挖矿木马，在应急的时候没有能做到快速响应，尽快定位恶意文件位置，所以事后进行重新整理分析，以便在发生类似事件时进行尽快锁定恶意文件。

某台主机被安全设备监测到一直在向另外一台服务器发送dns的请求数据，在请求的数据包中发现一个疑似矿池地址的域名，于是猜测该主机感染挖矿木马，随后对该主机开展应急工作。首先对系统服务、端口连接情况、开机启动项、任务计划等常规内容进行排查，并没有发现异常的程序。通过wireshark抓取数据包，发现确实存在异常dns请求，本地运行恶意软件，wireshark拦截数据流量包如下，从数据包中可清楚地发现该矿池地址：asia.zcoin.miningpoolhub.com。



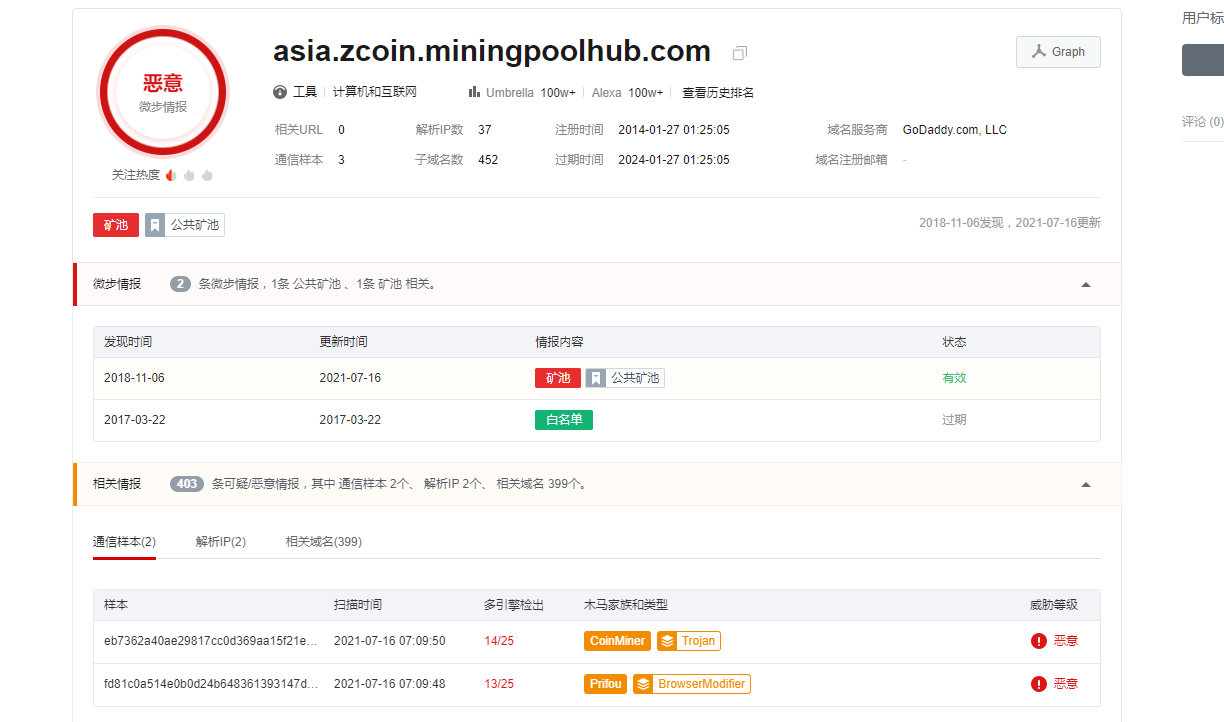
通过对流量数据包进行分析，发现数据包的源端口一直在发生变化，无法定位到具体的发包进程，到此为止，就陷入僵局，所以此处想重点说下如何通过数据流量包定位异常进程。



动态文件监测往往是一种很有效的恶意文件排查方法，一旦锁定进程的pid就能利用wmic process get name,executablepath,processid |findstr pid 迅速抓出文件的，wrishark抓包工具只是对数据流量进行提取，但是无法直接定位到进程，多数的恶意程序在进行发送数据流量时，基本都在变换源端口，所以更是给确定进程id增加难度，那如何进行pid定位呢，可尝试如下方法：

1、威胁情报平台匹配

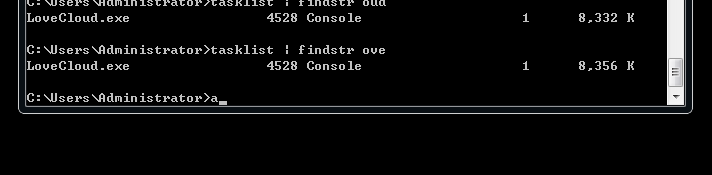
对于挖矿类的病毒木马，数据流量中往往会携带矿池域名，可去威胁情报平台去做匹配，如此处发现的asia.zcoin.miningpoolhub.com，可放到微步在线进行域名匹配，匹配结果如下



可通过查看样本详细信息，来辅助查看本地的恶意文件，如本次发现的挖矿木马，威胁平台上存在一个lovecloud的木马文件，可去搜索本地是否存在类似的软件。

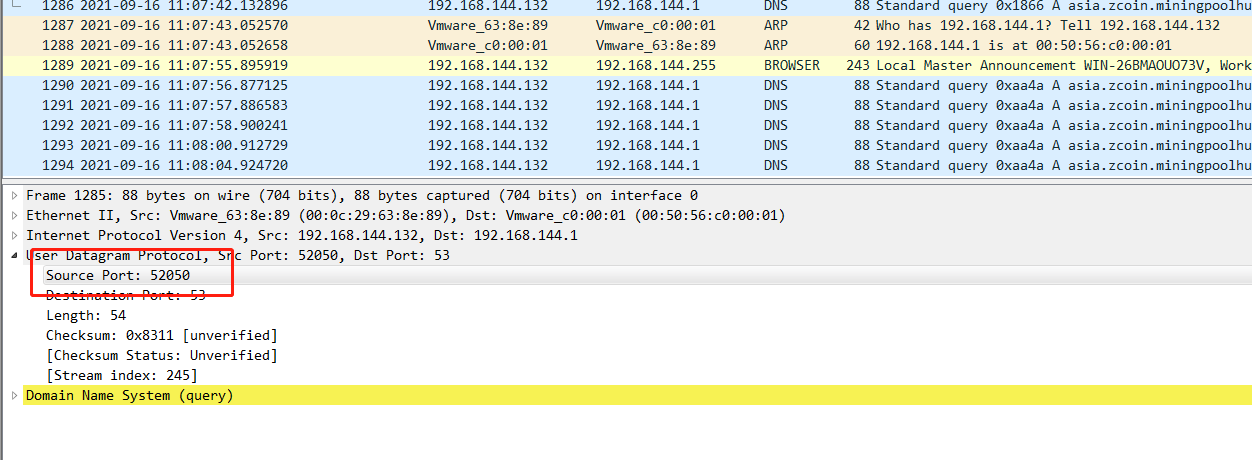


通过tasklist进行模糊匹配tasklist | findstr ove，可看到进程中确实存在一个lovecloud的进程，通过特征匹配去发现恶意文件也是种方法。

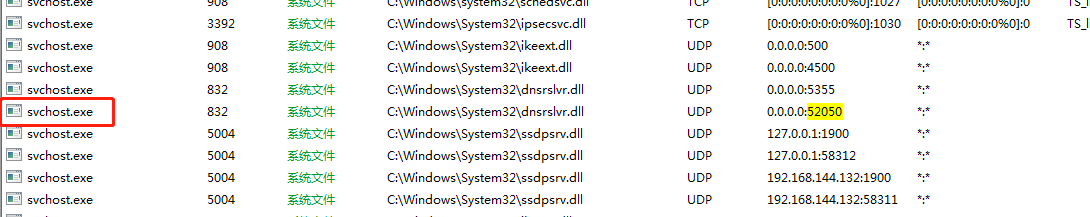


2、火绒剑使用

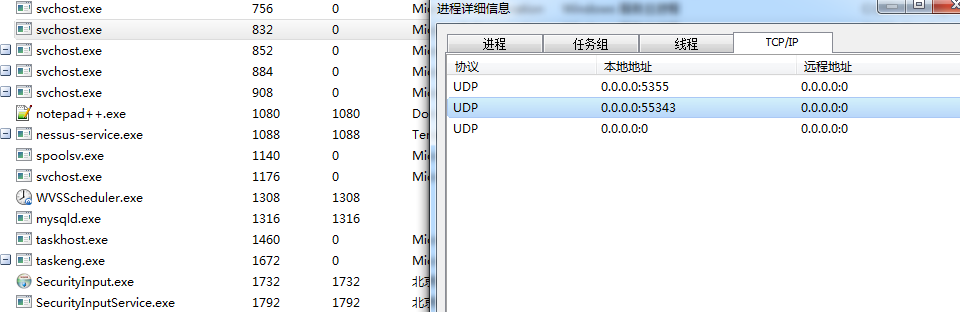
火绒剑还是非常好用的，虽然当时也用到火绒剑但是由于不是很熟悉，导致没有做到快速定位，其实通过wrishark和火绒剑配合使用就能很快找到请求进程。通过wireshark进行实时抓包，通过wrishark找出数据包源端口为52050



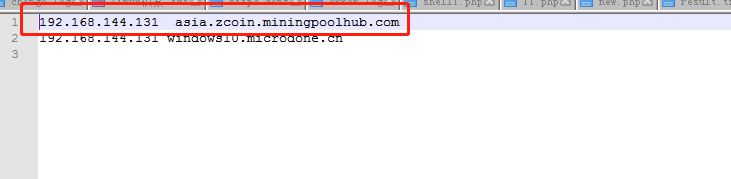
在配合火绒剑的网络实时监控功能，就可通过匹配端口的方法找到进程pid，由此可见是Svchost.exe被病毒感染，一直在发送含有矿池地址的dns请求，由于数据包是一直在实时发送的，所以要随时对火绒剑的网络连接进行刷新。



可进一步查看该进程详细信息，查看其udp的数据，与我们当前wrishark抓取的数据包源端口匹配，进一步确认该进程为发包进程，由此可见病毒程序感染了svhost.exe文件。



但是在知道svchost.exe进程，实际并无意义，此时我们依然无法确定是谁在请求矿池地址。此时抓包发现，木马会没间隔一段时间就会向该矿池地址发起一次请求，因为网络一直无法通信，所以会一直在请求该矿池地址，我们抓取的数据包中也就只有这些重复的dns请求数据包，此时可尝试修改host文件伪造该域名解析地址，修改host文件如下图



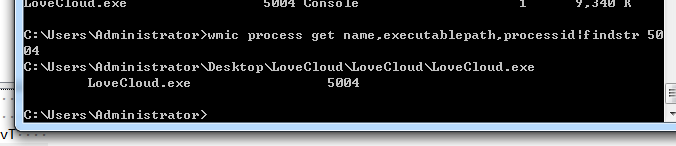
查看netstat请求发现出现一个syn\_sent tcp连接情况，由于该连接会在瞬间结束，所以需要一直刷新，跟进该pid进程



跟进5004 pid进程， tasklist | findstr 5004，发现是lovecloud.exe的程序，通过网上查看发现该程序确实一个挖矿木马



利用wmic process get name,executablepath,processid|findstr 5004，获取文件路径



利用taskkill /f /t /im 5004结束进程即可，至此，通过跟踪进程一步步慢慢发现该恶意文件的名称以及所在路径。

3、借助杀毒软件查杀

可利用杀毒软件工具进行查杀，杀毒软件还是很实用的一种方法，前提是所使用的杀毒软件能够杀的出来，杀毒软件还存在一个弊端就是，全盘查杀可能会存在扫描时间长，可能会出现等了很长时间杀软查杀结束后，仍然没有发现恶意文件的情况，此时还是建议进行人工手动排查，进行快速恶意程序定位。



二、Svchost.exe介绍

Svchost.exe文件主要是存在于“%system root%\system32”通常是在在C盘的Windows\system32这个目录下面，他是NY核心windows的重要进程，专门为系统启动各种服务的。Svchost.exe实际上是一个服务宿主，它本身并不能给用户提供任何的服务，但是可以用来运行动态链接库DLL文件，从而启动相对应的服务，每一个Svchost.exe进程可以同时启动多个服务文件。比如我们本次的lovecloud木马就是利用svchost.exe服务调用dnsrslvr.dll服务，所以病毒木马会想尽办法来利用svchost.exe，新增svchost.exe或替换该文件，那如何判断该服务是否被感染呢，具体可参考前人总结的经验，链接如下：http://security.zhiding.cn/security\_zone/2009/0424/1364792.shtml

三、命令

列举本次应急中用到的一些命令：

wrishark:

tcp.port == 80

udp.port >= 2048

tcp dst port 3128

cmd命令：

wmic process get name,executablepath,processid|findstr pid

netstat -ano |findstr "9002"

netstat -no

tasklist | findstr ""

taskkill /f /t /im pid（结束进程）

windows获取tcp连接数

netstat -an | findstr TCP | find /C "TIME\_WAIT"

netstat -an | find /C "TIME\_WAIT"

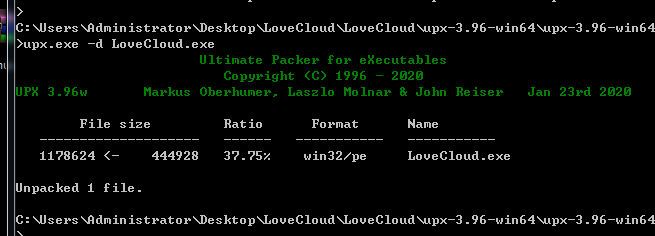
查看已经成功建立的连接：

netstat -ano | findstr "ESTABLISHED"

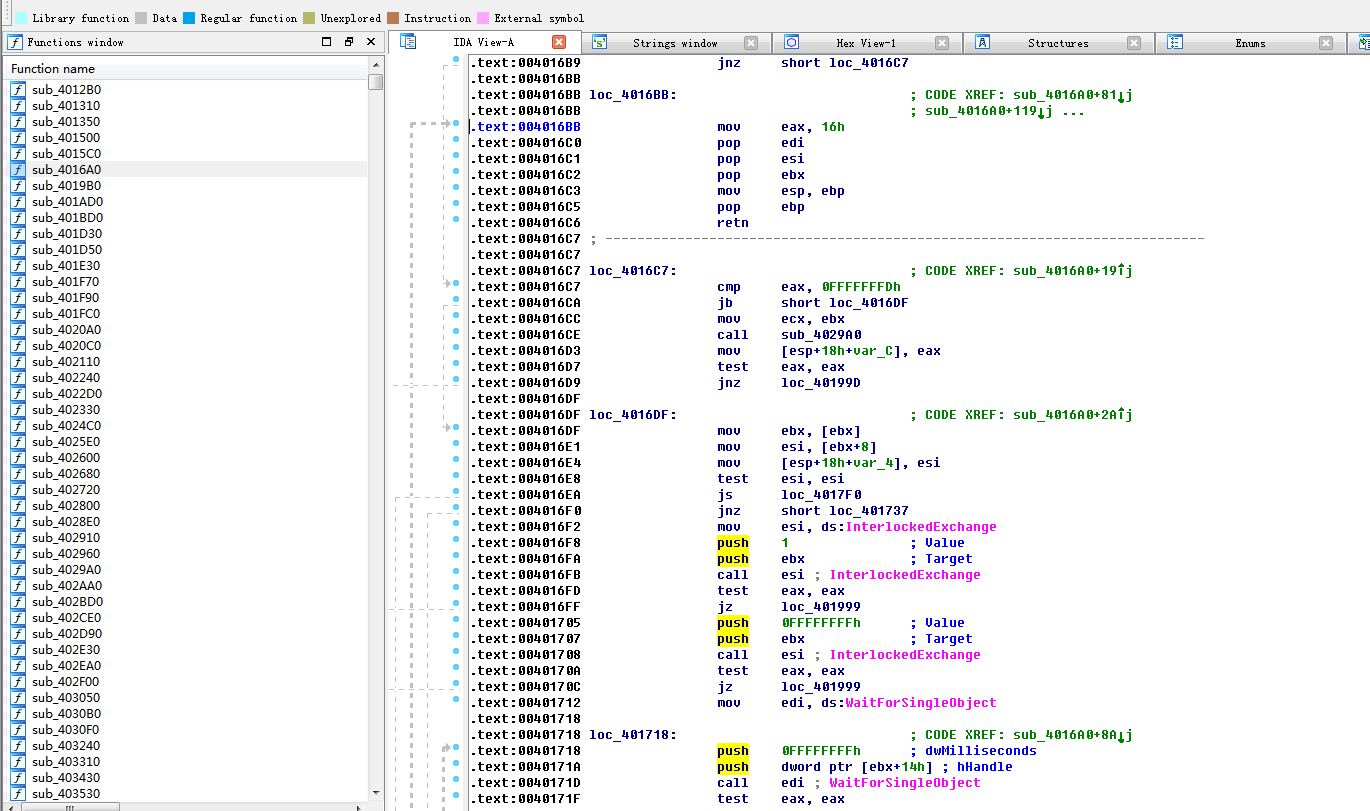
查看哪些dll被调用

tasklist /m dll

通过对lovecloud.exe分析发现，该文件采用了upx加壳，利用upx脱壳工具可成功脱壳，工具下载地址如下：<https://github.com/upx/upx/releases/tag/v3.96>



脱壳之后可对木马进行进一步逆向分析



四、小结

针对被恶意文件感染的机器，动态分析还是很有成效的，通过数据流量包进行分析，获取数据流量包特征在进行进程pid的匹配，从而获取相关文件进程，当然在配合杀毒软件进行全盘查杀不失为一种高效的方法。