

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。

3	2021/258	09:35:37.424797	192.168.144.130	192.168.144.1	DNS	81 Standard query 0x49f6 A update.googleapis.com
4	2021/258	09:35:39.425106	192.168.144.130	192.168.144.1	DNS	81 Standard query 0x49f6 A update.googleapis.com
5	2021/258	09:35:43.430747	192.168.144.130	192.168.144.1	DNS	81 Standard query 0x49f6 A update.googleapis.com
6	2021/258	09:35:46.708414	192.168.144.130	192.168.144.1	DNS	88 Standard query 0x98e6 A asia.zcoin.miningpoolhub.com
7	2021/258	09:35:47.721376	192.168.144.130	192.168.144.1	DNS	88 Standard query 0x98e6 A asia.zcoin.miningpoolhub.com
8	2021/258	09:35:48.735244	192.168.144.130	192.168.144.1	DNS	88 Standard query 0x98e6 A asia.zcoin.miningpoolhub.com
9	2021/258	09:35:50.751237	192.168.144.130	192.168.144.1	DNS	88 Standard query 0x98e6 A asia.zcoin.miningpoolhub.com
10	2021/258	09:35:51.562316	Vmware_63:8e:89	Vmware_c0:00:01	ARP	42 Who has 192.168.144.1? Tell 192.168.144.130
11	2021/258	09:35:51.562411	Vmware_c0:00:01	Vmware_63:8e:89	ARP	60 192.168.144.1 is at 00:50:56:c0:00:01
12	2021/258	09:35:52.898454	192.168.144.130	192.168.144.1	DNS	85 Standard query 0x8f00 A teredo.ipv6.microsoft.com
13	2021/258	09:35:53.902621	192.168.144.130	192.168.144.1	DNS	85 Standard query 0x8f00 A teredo.ipv6.microsoft.com
14	2021/258	09:35:54.760193	192.168.144.130	192.168.144.1	DNS	88 Standard query 0x98e6 A 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。

42	2021/258	09:36:21.133979	192.168.144.130	192.168.144.1	DNS	81	Standard query 0xf0b3 A update.googleapis.com
43	2021/258	09:36:23.141953	192.168.144.130	192.168.144.1	DNS	81	Standard query 0xf0b3 A update.googleapis.com
44	2021/258	09:36:27.153153	192.168.144.130	192.168.144.1	DNS	81	Standard query 0xf0b3 A update.googleapis.com
45	2021/258	09:36:32.350786	192.168.144.130	192.168.144.1	DNS	88	Standard query 0x80dc A asia.zcoin.miningpoolhub.
46	2021/258	09:36:33.360436	192.168.144.130	192.168.144.1	DNS	88	Standard query 0x80dc A asia.zcoin.miningpoolhub.
47	2021/258	09:36:34.378165	192.168.144.130	192.168.144.1	DNS	88	Standard query 0x80dc A asia.zcoin.miningpoolhub.
48	2021/258	09:36:36.386189	192.168.144.130	192.168.144.1	DNS	88	Standard query 0x80dc A asia.zcoin.miningpoolhub.
51	2021/258	09:36:40.402972	192.168.144.130	192.168.144.1	DNS	88	Standard query 0x80dc A asia.zcoin.miningpoolhub.
52	2021/258	09:36:47.249968	192.168.144.130	192.168.144.1	DNS	85	Standard query 0x32ef A teredo.ipv6.microsoft.com
53	2021/258	09:36:48.260755	192.168.144.130	192.168.144.1	DNS	85	Standard query 0x32ef A teredo.ipv6.microsoft.com
54	2021/258	09:36:49.272089	192.168.144.130	192.168.144.1	DNS	85	Standard query 0x32ef A teredo.ipv6.microsoft.com

User Datagram Protocol, Src Port: 60643, Dst Port: 53	
Source Port:	60643
Destination Port:	53
Length:	54
Checksum:	0xf90b [unverified]
[Checksum Status:	Unverified]
[Stream index:	10]

Domain Name System (query)	
Transaction ID:	0x80dc
Flags:	0x0100 Standard query
Questions:	1
Answer RRs:	0
Authority RRs:	0
Additional RRs:	0
Queries	

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

恶意

微步情报

asia.zcoin.miningpoolhub.com

工具 | 计算机和互联网 | Umbrella 100w+ | Alexa 100w+ | 查看历史排名

相关URL 0

解析IP数 37

注册时间 2014-01-27 01:25:05

域名服务商 GoDaddy.com, LLC

通信样本 3

子域名数 452

过期时间 2024-01-27 01:25:05

域名注册邮箱 -

Graph

用户标

评论 (0)

矿池

公共矿池

2018-11-06发现, 2021-07-16更新

微步情报

2 条微步情报, 1条 公共矿池、1条 矿池 相关。

发现时间	更新时间	情报内容	状态
2018-11-06	2021-07-16	矿池 公共矿池	有效
2017-03-22	2017-03-22	白名单	过期

相关情报

403 条可疑/恶意情报, 其中 通信样本 2个、解析IP 2个、相关域名 399个。

通信样本(2)

解析IP(2)

相关域名(399)

样本	扫描时间	多引擎检出	木马家族和类型	威胁等级
eb7362a40ae29817cc0d369aa15f21e...	2021-07-16 07:09:50	14/25	CoinMiner Trojan	1 恶意
fd81c0a514e0b0d24b648361393147d...	2021-07-16 07:09:48	13/25	Priou BrowserModifier	1 恶意

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。

⚠ 经微步云沙箱检测该文件为恶意

文件名称: eb7362a40ae29817_LoveCloud.exe

SHA256: eb7362a40ae29817cc0d369aa15f21eac4655a5199b52c1ea74c46ada309cf3f

运行环境: win7_sp1_enx86_office2013

提交时间: 2019-09-10 08:33:07

样本标签: Trojan CoinMiner encrypt_algorithm PE32 lang_english

EXE x86

100分 ?

处置建议

重新分析

报告

PCAP

样本

收藏

🔍 多引擎检出率 14 / 25

API 接口

反病毒引擎

检测结果 (最近检测时间: 2021-07-16 07:09:50)

江民 (JiangMin)

Trojan.Generic.bkbpf

360 (Qihoo 360)

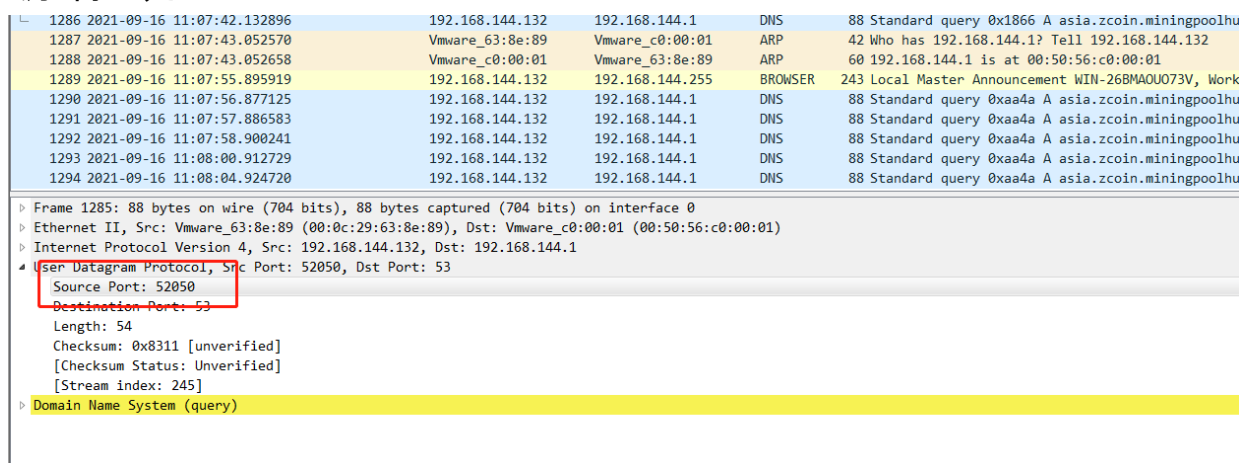
Win32/Miner.RitMiner.HwsRnLOA

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。

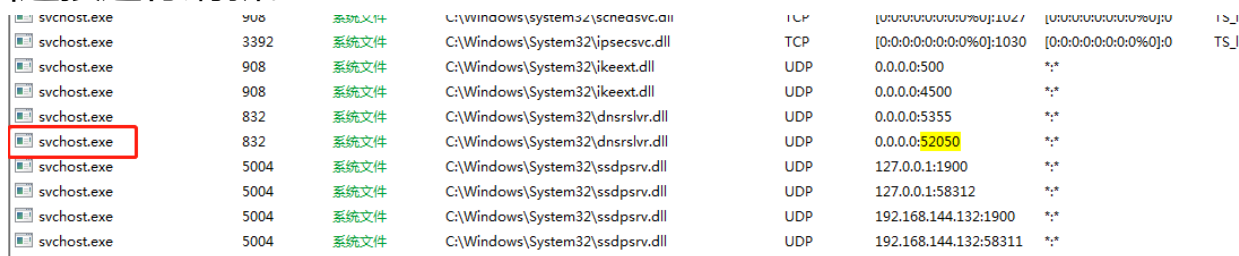


2、火绒剑使用

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。

svchost.exe	756	0	Mi
svchost.exe	832	0	Mi
svchost.exe	852	0	Mi
svchost.exe	884	0	Mi
svchost.exe	908	0	Mi
notepad++.exe	1080	1080	Do
nessus-service.exe	1088	1088	Te
spoolsv.exe	1140	0	Mi
svchost.exe	1176	0	Mi
WVSScheduler.exe	1308	1308	
mysqld.exe	1316	1316	
taskhost.exe	1460	0	Mi
taskeng.exe	1672	0	Mi
SecurityInput.exe	1732	1732	北
SecurityInputService.exe	1792	1792	北

进程	任务组	线程	TCP/IP
协议	本地地址	远程地址	
UDP	0.0.0.0:5355	0.0.0.0:0	
UDP	0.0.0.0:55343	0.0.0.0:0	
UDP	0.0.0.0:0	0.0.0.0:0	

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

```

1 192.168.144.131 asia.zcoin.miningpoolhub.com
2 192.168.144.131 windows10.microsoft.com
3

```

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

```

C:\Users\Administrator>netstat -no
活动连接
 协议 本地地址           外部地址           状态           PID
  TCP  127.0.0.1:1658      127.0.0.1:1659      ESTABLISHED     5392
  TCP  127.0.0.1:1659      127.0.0.1:1658      ESTABLISHED     5392
  TCP  127.0.0.1:1664      127.0.0.1:1665      ESTABLISHED     5392
  TCP  127.0.0.1:1665      127.0.0.1:1664      ESTABLISHED     5392
  TCP  192.168.144.131:1687 192.168.144.131:20581 SYN_SENT         5004
C:\Users\Administrator>netstat -no

```

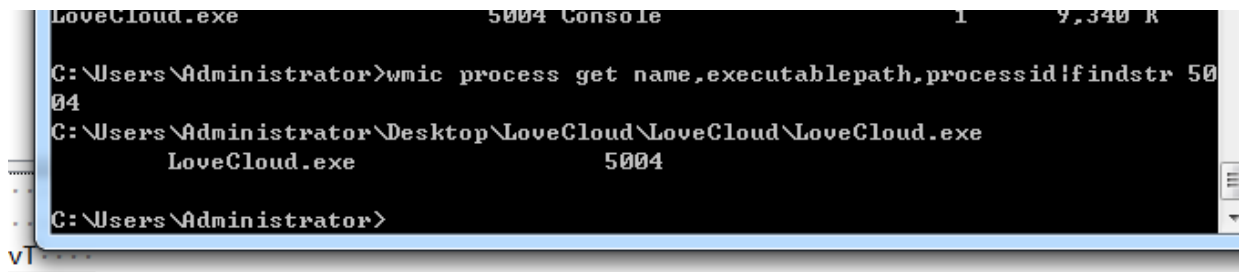
跟进5004 pid进程， tasklist | findstr 5004，发现是lovecloud.exe的程序，通过网上查看发现该程序确实一个挖矿木马

```

C:\Users\Administrator>tasklist | findstr 5004
LoveCloud.exe           5004 Console           1           9,340 K
C:\Users\Administrator>

```

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



```
LoveCloud.exe 5004 Console 1 9,340 K
C:\Users\Administrator>wmic process get name,executablepath,processid|findstr 5004
C:\Users\Administrator\Desktop\LoveCloud\LoveCloud.exe
LoveCloud.exe 5004
C:\Users\Administrator>
```

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dnssrslvr.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>

```
>
C:\Users\Administrator\Desktop\LoveCloud\LoveCloud\upx-3.96-win64\upx-3.96-win64
>upx.exe -d LoveCloud.exe

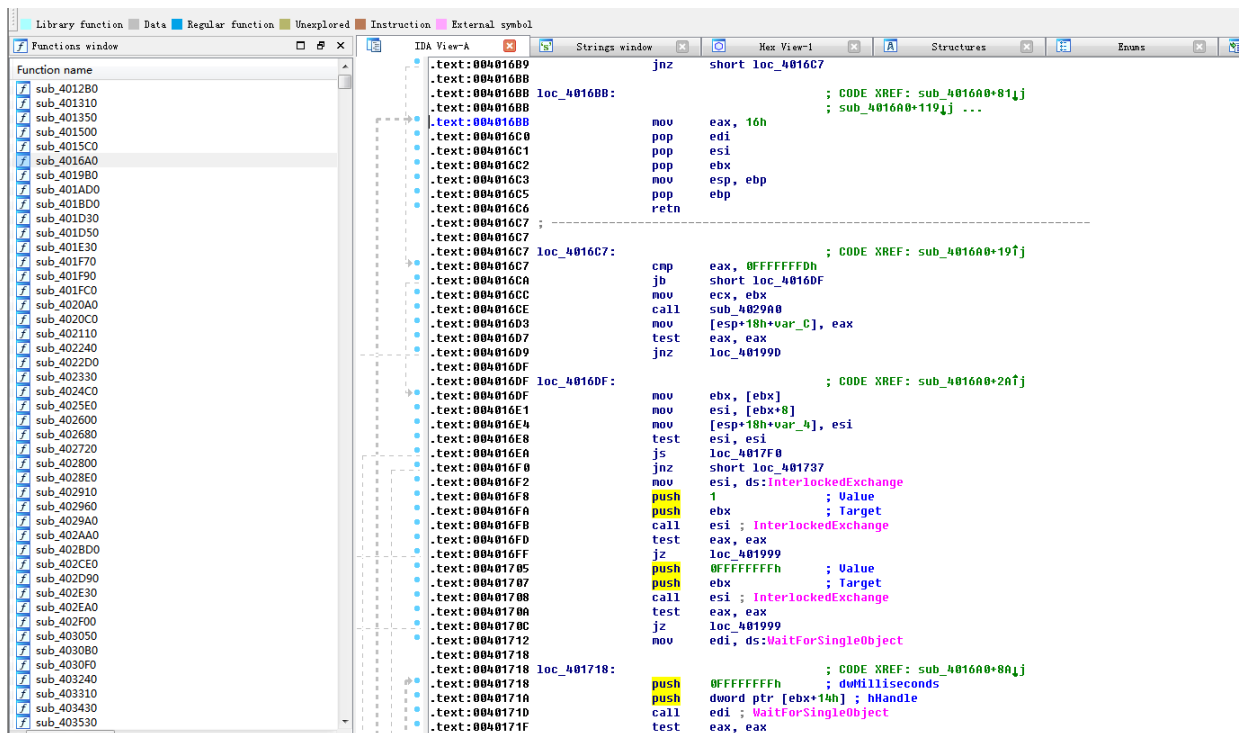
      Ultimate Packer for eXecutables
      Copyright (C) 1996 - 2020
UPX 3.96w      Markus Oberhumer, Laszlo Molnar & John Reiser   Jan 23rd 2020

File size      Ratio      Format      Name
-----
1178624 <-    444928    37.75%    win32/pe    LoveCloud.exe

Unpacked 1 file.

C:\Users\Administrator\Desktop\LoveCloud\LoveCloud\upx-3.96-win64\upx-3.96-win64
```

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。

