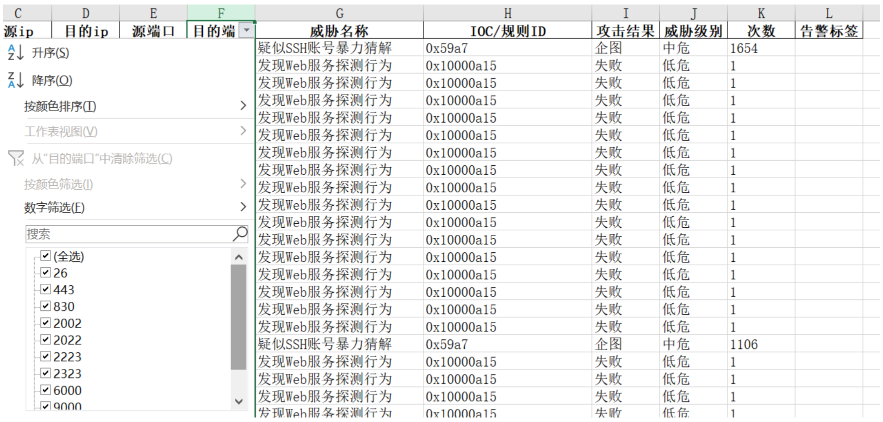
License Server操作系统被异常攻击的经验案例

AD-NET解决方案　统一数字底盘　**路康**　2024-04-15 发表

问题描述

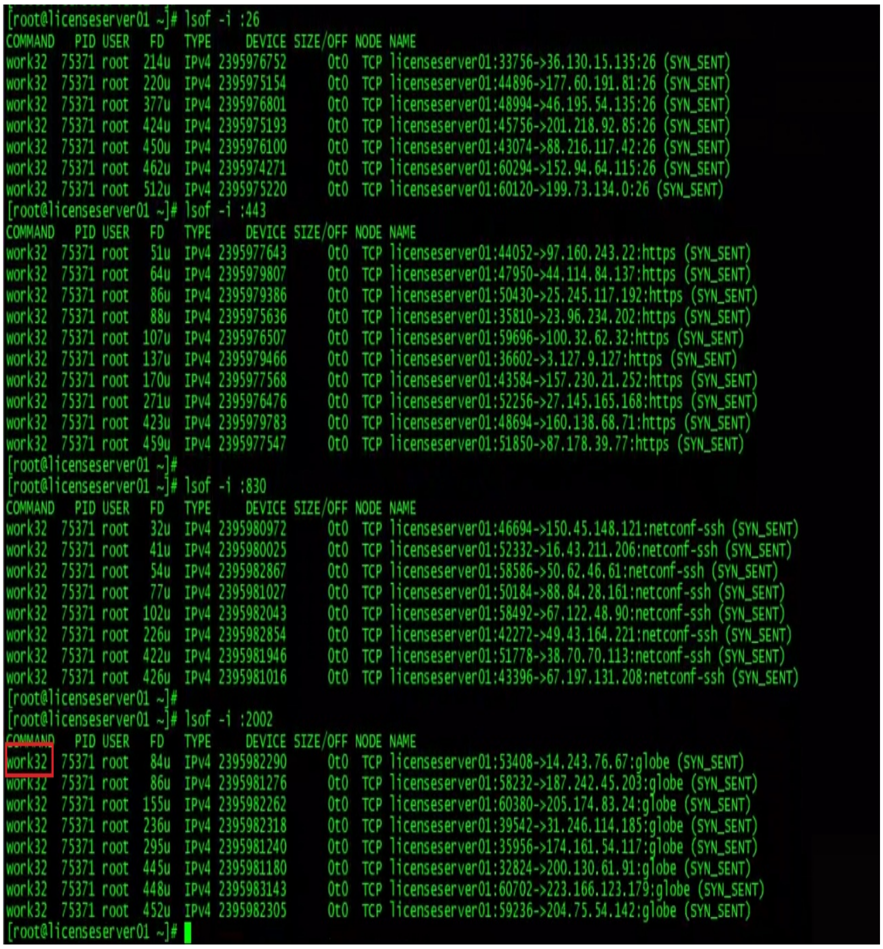
现场使用License Server自带iso安装操作系统，HA部署License Server，外部安全设备检测到被两个宿主机IP地址攻击。攻击的端口信息如下：



C	D	E	F	G	H	I	J	K	L
源ip	目的ip	源端口	目的端	威胁名称	IOC/规则ID	攻击结果	威胁级别	次数	告警标签
				疑似SSH账号暴力猜解	0x59a7	企图	中危	1654	
				发现Web服务探测行为	0x10000a15	失败	低危	1	
				发现Web服务探测行为	0x10000a15	失败	低危	1	
				发现Web服务探测行为	0x10000a15	失败	低危	1	
				发现Web服务探测行为	0x10000a15	失败	低危	1	
				发现Web服务探测行为	0x10000a15	失败	低危	1	
				发现Web服务探测行为	0x10000a15	失败	低危	1	
				发现Web服务探测行为	0x10000a15	失败	低危	1	
				发现Web服务探测行为	0x10000a15	失败	低危	1	
				发现Web服务探测行为	0x10000a15	失败	低危	1	
				发现Web服务探测行为	0x10000a15	失败	低危	1	
				发现Web服务探测行为	0x10000a15	失败	低危	1	
				发现Web服务探测行为	0x10000a15	失败	低危	1	
				发现Web服务探测行为	0x10000a15	失败	低危	1	
				发现Web服务探测行为	0x10000a15	失败	低危	1	
				发现Web服务探测行为	0x10000a15	失败	低危	1	
				发现Web服务探测行为	0x10000a15	失败	低危	1	
				疑似SSH账号暴力猜解	0x59a7	企图	中危	1106	
				发现Web服务探测行为	0x10000a15	失败	低危	1	
				发现Web服务探测行为	0x10000a15	失败	低危	1	
				发现Web服务探测行为	0x10000a15	失败	低危	1	
				发现Web服务探测行为	0x10000a15	失败	低危	1	

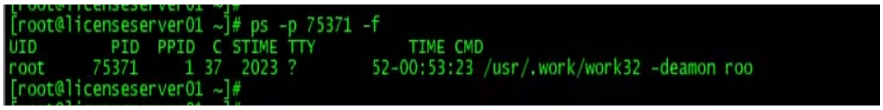
过程分析

1. 登录到操作系统后台，使用“lsof -i :[port]”命令查询端口所属进程信息，发现均为"work32"进程，PID为75371。

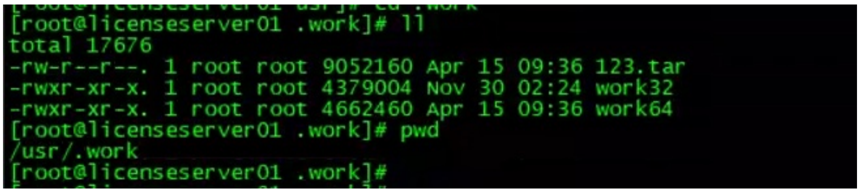


```
[root@licenseserver01 ~]# lsof -i :26
COMMAND   PID USER   FD   TYPE     DEVICE SIZE/OFF NODE NAME
work32  75371 root  214u  IPv4 2395976752      0t0  TCP licenseserver01:33756->36.130.15.135:26 (SYN_SENT)
work32  75371 root  220u  IPv4 2395975154      0t0  TCP licenseserver01:44896->177.60.191.81:26 (SYN_SENT)
work32  75371 root  377u  IPv4 2395976801      0t0  TCP licenseserver01:48994->46.195.54.135:26 (SYN_SENT)
work32  75371 root  424u  IPv4 2395975193      0t0  TCP licenseserver01:45756->201.218.92.85:26 (SYN_SENT)
work32  75371 root  450u  IPv4 2395976100      0t0  TCP licenseserver01:43074->88.216.117.42:26 (SYN_SENT)
work32  75371 root  462u  IPv4 2395974271      0t0  TCP licenseserver01:60294->152.94.64.115:26 (SYN_SENT)
work32  75371 root  512u  IPv4 2395975220      0t0  TCP licenseserver01:60120->199.73.134.0:26 (SYN_SENT)
[root@licenseserver01 ~]# lsof -i :443
COMMAND   PID USER   FD   TYPE     DEVICE SIZE/OFF NODE NAME
work32  75371 root   51u  IPv4 2395977643      0t0  TCP licenseserver01:44052->97.160.243.22:https (SYN_SENT)
work32  75371 root   64u  IPv4 2395979807      0t0  TCP licenseserver01:47950->44.114.84.137:https (SYN_SENT)
work32  75371 root   86u  IPv4 2395979386      0t0  TCP licenseserver01:50430->25.245.117.192:https (SYN_SENT)
work32  75371 root   88u  IPv4 2395975636      0t0  TCP licenseserver01:35810->23.96.234.202:https (SYN_SENT)
work32  75371 root  107u  IPv4 2395976507      0t0  TCP licenseserver01:59696->100.32.62.32:https (SYN_SENT)
work32  75371 root  137u  IPv4 2395979466      0t0  TCP licenseserver01:36602->3.127.9.127:https (SYN_SENT)
work32  75371 root  170u  IPv4 2395977568      0t0  TCP licenseserver01:43584->157.230.21.252:https (SYN_SENT)
work32  75371 root  271u  IPv4 2395976476      0t0  TCP licenseserver01:52256->27.145.165.168:https (SYN_SENT)
work32  75371 root  423u  IPv4 2395979783      0t0  TCP licenseserver01:48694->160.138.68.71:https (SYN_SENT)
work32  75371 root  459u  IPv4 2395977547      0t0  TCP licenseserver01:51850->87.178.39.77:https (SYN_SENT)
[root@licenseserver01 ~]#
[root@licenseserver01 ~]# lsof -i :830
COMMAND   PID USER   FD   TYPE     DEVICE SIZE/OFF NODE NAME
work32  75371 root   32u  IPv4 2395980972      0t0  TCP licenseserver01:46694->150.45.148.121:netconf-ssh (SYN_SENT)
work32  75371 root   41u  IPv4 2395980025      0t0  TCP licenseserver01:52332->16.43.211.206:netconf-ssh (SYN_SENT)
work32  75371 root   54u  IPv4 2395982867      0t0  TCP licenseserver01:58586->50.62.46.61:netconf-ssh (SYN_SENT)
work32  75371 root   77u  IPv4 2395981027      0t0  TCP licenseserver01:50184->88.84.28.161:netconf-ssh (SYN_SENT)
work32  75371 root  102u  IPv4 2395982043      0t0  TCP licenseserver01:58492->67.122.48.90:netconf-ssh (SYN_SENT)
work32  75371 root  226u  IPv4 2395982854      0t0  TCP licenseserver01:42272->49.43.164.221:netconf-ssh (SYN_SENT)
work32  75371 root  422u  IPv4 2395981946      0t0  TCP licenseserver01:51778->38.70.70.113:netconf-ssh (SYN_SENT)
work32  75371 root  426u  IPv4 2395981016      0t0  TCP licenseserver01:43396->67.197.131.208:netconf-ssh (SYN_SENT)
[root@licenseserver01 ~]#
[root@licenseserver01 ~]# lsof -i :2002
COMMAND   PID USER   FD   TYPE     DEVICE SIZE/OFF NODE NAME
work32  75371 root   84u  IPv4 2395982290      0t0  TCP licenseserver01:53408->14.243.76.67:globe (SYN_SENT)
work32  75371 root   86u  IPv4 2395981276      0t0  TCP licenseserver01:58232->187.242.45.203:globe (SYN_SENT)
work32  75371 root  155u  IPv4 2395982262      0t0  TCP licenseserver01:60380->205.174.83.24:globe (SYN_SENT)
work32  75371 root  236u  IPv4 2395982318      0t0  TCP licenseserver01:39542->31.246.114.185:globe (SYN_SENT)
work32  75371 root  295u  IPv4 2395981240      0t0  TCP licenseserver01:35956->174.161.54.117:globe (SYN_SENT)
work32  75371 root  445u  IPv4 2395981180      0t0  TCP licenseserver01:32824->200.130.61.91:globe (SYN_SENT)
work32  75371 root  448u  IPv4 2395983143      0t0  TCP licenseserver01:60702->223.166.123.179:globe (SYN_SENT)
work32  75371 root  452u  IPv4 2395982305      0t0  TCP licenseserver01:59236->204.75.54.142:globe (SYN_SENT)
[root@licenseserver01 ~]#
```

2. 使用“ps -p 75371 -f”命令确认异常进程具体目录为“/usr/.work/work32”。



```
[root@licenseserver01 ~]# ps -p 75371 -f
UID        PID  PPID  C STIME TTY          TIME CMD
root     75371     1 37  2023 ?        52-00:53:23 /usr/.work/work32 -deamon roo
[root@licenseserver01 ~]#
```



```
[root@licenseserver01 .work]# ll
total 17676
-rw-r--r--. 1 root root 9052160 Apr 15 09:36 123.tar
-rwxr-xr-x. 1 root root 4379004 Nov 30 02:24 work32
-rwxr-xr-x. 1 root root 4662460 Apr 15 09:36 work64
[root@licenseserver01 .work]# pwd
/usr/.work
[root@licenseserver01 .work]#
```

3. 经H3Linux操作系统以及License Server研发确认，正常环境不存在/usr/.work目录，以及这些异常端口均与License Server无关，参考互联网相关案例，怀疑是挖矿病毒。

解决方法

建议现场进行授权卸载迁移，重装操作系统后，使用卸载码重新激活授权。