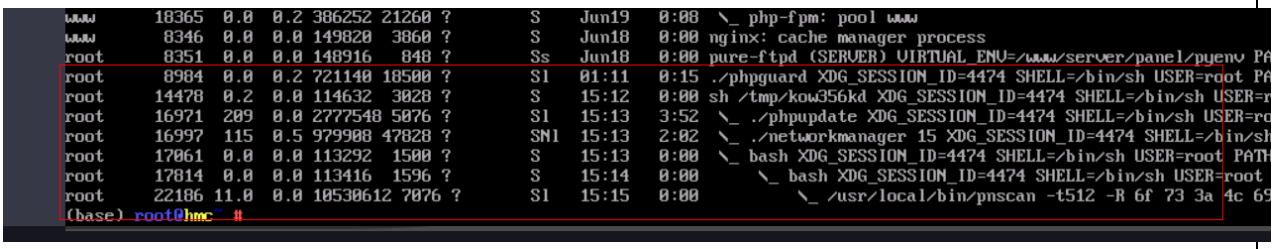
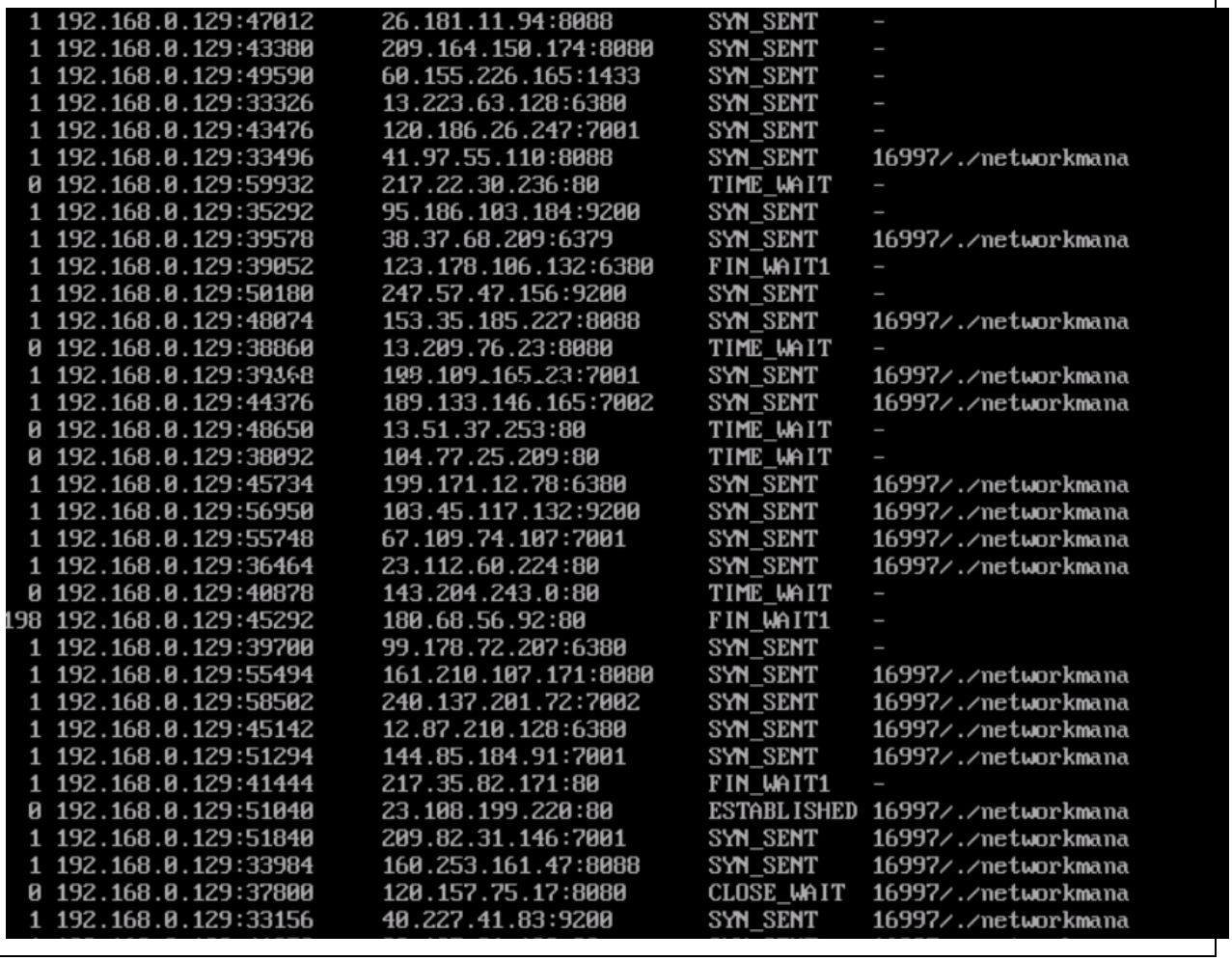
网络安全事件处置报告

<table>
<tr><td rowspan="3">事件基本信息</td><td>来源</td><td>☑监控系统， ☐租户报障/投诉，☐第三方反馈，☐情报
节点： 华南节点</td></tr>
<tr><td>租户名称</td><td>139.9.211.51</td></tr>
<tr><td>事件概要</td><td>客户反馈云主机 139.9.211.51 收到安全预警，请求协助排查。</td></tr>
<tr><td>详细分析</td><td colspan="2">一、排查主机发现异常进程正在运行；
 

二、异常程序正在扫描 6380，8088，8080 等端口；
 
</td></tr>
</table>

三、主机存在多个异常计划任务，且存在 redis 写入特征；

```
(base) root@hmc /var/spool/cron # ll -art
total 12
drwxr-xr-x. 11 root root 4096 Jun 21 11:45 ..
-rw-------   1 root root   47 Jun 21 15:13 root
drwx------.  2 root root 4096 Jun 21 15:13 .
(base) root@hmc /var/spool/cron # strings root
*/30 * * * * sh /etc/newdat.sh >/dev/null 2>&1
(base) root@hmc /var/spool/cron #
```

```
-rw-------  1 root root    0 Aug  9  2019 /etc/cron.deny
-rw-r--r--. 1 root root  451 Jun 10  2014 /etc/crontab

/etc/cron.d:
total 64
drwxr-xr-x.  2 root root  4096 Jun 21 11:45 .
drwxr-xr-x. 99 root root 12288 Jun 21 15:13 ..
-rw-r--r--   1 root root   128 Aug  9  2019 0hourly
-rw-r--r--   1 root root    92 Jun 21 01:13 admin
-rw-r--r--   1 root root    92 Jun 21 01:12 apache
-rw-------   1 root root   215 Apr  9 05:40 clamav-update
-rw-r--r--   1 root root    92 Jun 21 01:13 nginx
-rw-r--r--   1 root root    92 Jun 21 01:13 nobody
-rw-r--r--   1 root root    92 Jun 21 01:12 redis
-rw-r--r--   1 root root   892 Jun 21 14:44 root
-rw-r--r--   1 root root    92 Jun 21 01:13 user
-rw-r--r--   1 root root   182 Jun 21 01:13 web
-rw-r--r--   1 root root    92 Jun 21 01:13 www
-rw-r--r--   1 root root    92 Jun 21 01:12 www-data
```

```
(base) root@hmc /etc/cron.d # strings root
REDIS0009
        redis-ver
6.2.4
redis-bits
ctime
used-mem
aof-preamble
*/10 * * * * sh /etc/newdat.sh
*/10 * * * * sh /etc/newdat.sh
*/10 * * * * sh /etc/newdat.sh
*/10 * * * * sh /etc/newdat.sh
*/10 * * * * sh /etc/newdat.sh
*/10 * * * * sh /etc/newdat.sh
*/10 * * * * sh /etc/newdat.sh
*/10 * * * * sh /etc/newdat.sh
*/10 * * * * sh /etc/newdat.sh
*/10 * * * * sh /etc/newdat.sh
*/10 * * * * sh /etc/newdat.sh
```

四、多个路径下发现异常文件；

```
-rw-------   1 www   www       24 Jun 21 11:14 sess_u2k36m4ha64usqhktkgfg2ja2o
-rw-r--r--   1 root  root    3304 Jun 21 11:20 388_og
-rw-------   1 www   www       24 Jun 21 11:20 sess_6tba6rmnusspj7cqk6dfudgqsi
-rw-------   1 www   www       23 Jun 21 11:21 sess_49g3kt1fv5o9f4km5jsdj35d4c
-rw-------   1 www   www       24 Jun 21 11:22 sess_hcb2rlknd38okp6s9fck0eksnp
-rw-------   1 www   www       23 Jun 21 11:27 sess_qummn8khi3o82ioos5fs4gjlre
-rw-------   1 www   www       24 Jun 21 11:29 sess_ub63vmqg1puunfk3sfddis0idv
-rw-------   1 www   www       24 Jun 21 11:30 sess_2m92214va0p5jbr8ot88brs0og
-rw-r--r--   1 root  root    3985 Jun 21 11:35 677_og
-rw-r--r--   1 root  root    3833 Jun 21 11:36 62_og
-rw-r--r--   1 root  root    3833 Jun 21 11:45 636_og
-rw-r--r--   1 root  root    9570 Jun 21 12:02 315_og
-rw-r--r--   1 root  root    3815 Jun 21 12:08 795_og
-rw-r--r--   1 root  root    3833 Jun 21 12:18 529_og
-rw-r--r--   1 root  root    3833 Jun 21 13:14 218_og
-rwxr-xr-x   1 root  root   40917 Jun 21 15:12 kow356kd
-rw-r--r--   1 root  root       2 Jun 21 15:13 kdevtmpfsi
-rw-r--r--   1 root  root       2 Jun 21 15:13 redis2
drwxrwxrwt. 10 root  root  188416 Jun 21 15:14 .
-rw-r--r--   1 root  root    3833 Jun 21 15:14 162_og
(base) root@hmc/tmp # pwd
/tmp
(base) root@hmc/tmp #
```

```
-rw-r--r--.  1 root  root      688 Jun 21 11:45 group-
-rw-r--r--   1 root  root     1521 Jun 21 11:45 passwd
----------   1 root  root      868 Jun 21 11:45 shadow
-rw-r--r--   1 root  root      698 Jun 21 11:45 group
----------   1 root  root      559 Jun 21 11:45 gshadow
drwxr-xr-x   2 root  root     4096 Jun 21 11:45 clamd.d
drwxr-xr-x.  6 root  root     4096 Jun 21 11:45 sysconfig
drwxr-xr-x.  2 root  root     4096 Jun 21 11:45 logrotate.d
drwxr-xr-x.  2 root  root     4096 Jun 21 11:45 cron.d
-rw-r--r--   1 root  root    48352 Jun 21 11:45 ld.so.cache
-rwxrwxrwx   1 root  root  1472144 Jun 21 12:07 phpguard
-rw-r--r--.  1 root  root      846 Jun 21 15:12 sysctl.conf
-rw-r--r--   1 root  root        9 Jun 21 15:13 phpupdates
-rwxrwxrwx   1 root  root     3341 Jun 21 15:13 config.json
-rwxrwxrwx   1 root  root  1102480 Jun 21 15:13 phpupdate
-rwxrwxrwx   1 root  root    40917 Jun 21 15:13 newdat.sh
drwxr-xr-x. 99 root  root    12288 Jun 21 15:13 .
-rwxrwxrwx   1 root  root  1919048 Jun 21 15:13 networkmanager
-rw-r--r--   1 root  root        0 Jun 21 15:13 sshd.allow.hostguard
(base) root@hmc/etc # pwd
/etc
(base) root@hmc/etc #
```

```
lrwxrwxrwx   1 root root       12 Jun 21 01:11 redis-sentinel -> redis-server
-rwxr-xr-x   1 root root  1468080 Jun 21 01:11 masscan
dr-xr-xr-x.  2 root root    36864 Jun 21 11:45 .
-rw-r--r--   1 root root        2 Jun 21 15:14 systemd-network
-rw-r--r--   1 root root        2 Jun 21 15:14 rctlcli
-rw-r--r--   1 root root        2 Jun 21 15:14 pamdicks
-rw-r--r--   1 root root        2 Jun 21 15:14 kswaped
-rw-r--r--   1 root root        2 Jun 21 15:14 irqbalanced
-rw-r--r--   1 root root        2 Jun 21 15:14 ip6network
(base) root@hmc/usr/bin # pwd
/usr/bin
(base) root@hmc/usr/bin #
```

```
lrwxrwxrwx   1 root root      12 Jun 20 10:24 redis-sentinel -
lrwxrwxrwx   1 root root      12 Jun 20 10:24 redis-check-aof
-rwxr-xr-x   1 root root   23040 Jun 21 15:14 pnscan
-rwxr-xr-x   1 root root     132 Jun 21 15:14 ipsort
drwxr-xr-x.  2 root root    4096 Jun 21 15:14 .
(base) root@hmc/usr/local/bin # pwd
/usr/local/bin
(base) root@hmc/usr/local/bin #
```

	五、主机存在异常密钥，请用户自行清除；  总结：主机疑似因前期 redis 未授权访问漏洞导致被入侵，当前异常进程已暂协助清除，异常文件及密钥请用户自行清除，主机已确认被入侵，系统已变的不可信任，为安全起见，建议备份数据，择机重装系统，并对 redis 设置强口令，或使用安全组限制 6379 端口固定 IP 访问。
事件原因	初步判断主机疑似因前期 redis 未授权访问漏洞导致被入侵。
安全建议	1、 设置系统账号及应用账号强密码，密码包含数字、字母及特殊符号，位数 12 位以上； 强口令设置要求参照：https://bbs.huaweicloud.com/blogs/87a98385ec6411e79fc57ca23e93a89f 2、 设置安全组，关闭高危端口，或设置仅允许部分 IP 访问端口（如：22，6379 等）； 3、 定期做好数据备份，以免黑客入侵主机造成数据丢失。 4、为彻查主机和应用方面潜在的安全风险，建议使用华为云官方提供的安全体检服务进行全面的安全体检或使用主机安全服务深度防御： 企业主机安全服务参照：https://www.huaweicloud.com/product/hss.html MDR 服务参照：https://www.huaweicloud.com/product/ses.html
处理人/日期	华为云业务部网络安全中心　　2021-06-21