

网络安全事件处置报告

事件基本信息	来源	<input checked="" type="checkbox"/> 监控系统， <input type="checkbox"/> 租户报障/投诉， <input type="checkbox"/> 第三方反馈， <input type="checkbox"/> 情报 节点： <u> 华南节点 </u>
	租户名称	139.9.211.51
	事件概要	客户反馈云主机 139.9.211.51 收到安全预警，请求协助排查。

一、排查主机发现异常进程正在运行；

```

www      18365  0.0  0.2 386252 21260 ?      S   Jun19  0:08  \_ php-fpm: pool www
www      8346   0.0  0.0 149820  3860 ?      S   Jun18  0:00  nginx: cache manager process
root     8351   0.0  0.0 148916   848 ?      Ss  Jun18  0:00  pure-ftpd (SERVER) VIRTUAL_ENV=/www/server/panel/puenv Pf
root     8984   0.0  0.2 721140 18500 ?      S1  01:11  0:15  ./phpguard XDG_SESSION_ID=4474 SHELL=/bin/sh USER=root Pf
root     14478  0.2  0.0 114632  3020 ?      S   15:12  0:00  sh /tmp/kow356kd XDG_SESSION_ID=4474 SHELL=/bin/sh USER=r
root     16971  209  0.0 2777548 5076 ?      S1  15:13  3:52  \_ ./phpupdate XDG_SESSION_ID=4474 SHELL=/bin/sh USER=rc
root     16997  115  0.5 979908 47828 ?      SN1 15:13  2:02  \_ ./networkmanager 15 XDG_SESSION_ID=4474 SHELL=/bin/sh
root     17061  0.0  0.0 113292  1500 ?      S   15:13  0:00  \_ bash XDG_SESSION_ID=4474 SHELL=/bin/sh USER=root PATH
root     17814  0.0  0.0 113416  1596 ?      S   15:14  0:00  \_ bash XDG_SESSION_ID=4474 SHELL=/bin/sh USER=root
root     22186  11.0 0.0 10530612 7076 ?     S1  15:15  0:00  \_ /usr/local/bin/pnscan -t512 -R 6f 73 3a 4c 65
(base) root@hmc ~#
    
```

二、异常程序正在扫描 6380, 8088, 8080 等端口；

详细分析

```

1 192.168.0.129:47012 26.181.11.94:8088 SYN_SENT -
1 192.168.0.129:43380 209.164.150.174:8080 SYN_SENT -
1 192.168.0.129:49590 60.155.226.165:1433 SYN_SENT -
1 192.168.0.129:33326 13.223.63.128:6380 SYN_SENT -
1 192.168.0.129:43476 120.186.26.247:7001 SYN_SENT -
1 192.168.0.129:33496 41.97.55.110:8088 SYN_SENT 16997/./networkmana
0 192.168.0.129:59932 217.22.30.236:80 TIME_WAIT -
1 192.168.0.129:35292 95.186.103.184:9200 SYN_SENT -
1 192.168.0.129:39578 38.37.68.209:6379 SYN_SENT 16997/./networkmana
1 192.168.0.129:39052 123.178.106.132:6380 FIN_WAIT1 -
1 192.168.0.129:50180 247.57.47.156:9200 SYN_SENT -
1 192.168.0.129:48074 153.35.185.227:8088 SYN_SENT 16997/./networkmana
0 192.168.0.129:38860 13.209.76.23:8080 TIME_WAIT -
1 192.168.0.129:39368 108.109.165.23:7001 SYN_SENT 16997/./networkmana
1 192.168.0.129:44376 189.133.146.165:7002 SYN_SENT 16997/./networkmana
0 192.168.0.129:48650 13.51.37.253:80 TIME_WAIT -
0 192.168.0.129:38092 104.77.25.209:80 TIME_WAIT -
1 192.168.0.129:45734 199.171.12.78:6380 SYN_SENT 16997/./networkmana
1 192.168.0.129:56950 103.45.117.132:9200 SYN_SENT 16997/./networkmana
1 192.168.0.129:55748 67.109.74.107:7001 SYN_SENT 16997/./networkmana
1 192.168.0.129:36464 23.112.60.224:80 SYN_SENT 16997/./networkmana
0 192.168.0.129:40878 143.204.243.0:80 TIME_WAIT -
198 192.168.0.129:45292 180.68.56.92:80 FIN_WAIT1 -
1 192.168.0.129:39700 99.178.72.207:6380 SYN_SENT -
1 192.168.0.129:55494 161.210.107.171:8080 SYN_SENT 16997/./networkmana
1 192.168.0.129:58502 240.137.201.72:7002 SYN_SENT 16997/./networkmana
1 192.168.0.129:45142 12.87.210.128:6380 SYN_SENT 16997/./networkmana
1 192.168.0.129:51294 144.85.184.91:7001 SYN_SENT 16997/./networkmana
1 192.168.0.129:41444 217.35.82.171:80 FIN_WAIT1 -
0 192.168.0.129:51040 23.108.199.220:80 ESTABLISHED 16997/./networkmana
1 192.168.0.129:51840 209.82.31.146:7001 SYN_SENT 16997/./networkmana
1 192.168.0.129:33904 160.253.161.47:8088 SYN_SENT 16997/./networkmana
0 192.168.0.129:37800 120.157.75.17:8080 CLOSE_WAIT 16997/./networkmana
1 192.168.0.129:33156 40.227.41.83:9200 SYN_SENT 16997/./networkmana
    
```

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_u2k36m4ha64usqhkktkgfgzja2o
-rw-r--r-- 1 root root 3304 Jun 21 11:20 388_og
-rw----- 1 www www 24 Jun 21 11:20 sess_6tba6rmnusspj7cqk6dfudggsi
-rw----- 1 www www 23 Jun 21 11:21 sess_49g3kt1fv5o9f4km5jsd_j35d4c
-rw----- 1 www www 24 Jun 21 11:22 sess_hcb2r1knd38okp6s9fck0eksnp
-rw----- 1 www www 23 Jun 21 11:27 sess_gummm8khi3o82ioos5fs4gjlre
-rw----- 1 www www 24 Jun 21 11:29 sess_ub63vmygy1puunfk3sfddis0idv
-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 sysconf ig
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 pnscaan
-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 #

```

	<p>五、主机存在异常密钥，请用户自行清除：</p> <pre>(base) root@hmc/usr/local/bin # strings /root/.ssh/authorized_keys ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQ9WkiJ7yQ6HcafmczDMv1RKxPdJI/oeXUWdNW1MrWiQNVKeSeSSdZ6NaYUqfSjgXUSg iQbktTo8Fhv4 wPoFBz9SAfg086 jc0M2kGUNS9JZsLJdUB9u1KxY5 I0zqG4QTgZ6LP2UuWLG7TGMpkbK7z6G8HAZx7u315+Uc82dKt I0zb/ohYSBb7pK/2QFeUa22L+4II H5DwCh3HchjtDPrAhFqGUyFZBsRZbQV1rPf sxxH2b0Lc1PMrK1o68dyk8gY8m4iZf r9ZD6xs4gAqdWtBQNIN8cvz4SI+Jv9f vayMH7f+K12yXiHN5oD9E t0u17 ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQ9WkiJ7yQ6HcafmczDMv1RKxPdJI/oeXUWdNW1MrWiQNVKeSeSSdZ6NaYUqfSjgXUSg iQbktTo8Fhv4 wPoFBz9SAfg086 jc0M2kGUNS9JZsLJdUB9u1KxY5 I0zqG4QTgZ6LP2UuWLG7TGMpkbK7z6G8HAZx7u315+Uc82dKt I0zb/ohYSBb7pK/2QFeUa22L+4II H5DwCh3HchjtDPrAhFqGUyFZBsRZbQV1rPf sxxH2b0Lc1PMrK1o68dyk8gY8m4iZf r9ZD6xs4gAqdWtBQNIN8cvz4SI+Jv9f vayMH7f+K12yXiHN5oD9E t0u17 ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQ9WkiJ7yQ6HcafmczDMv1RKxPdJI/oeXUWdNW1MrWiQNVKeSeSSdZ6NaYUqfSjgXUSg iQbktTo8Fhv4 wPoFBz9SAfg086 jc0M2kGUNS9JZsLJdUB9u1KxY5 I0zqG4QTgZ6LP2UuWLG7TGMpkbK7z6G8HAZx7u315+Uc82dKt I0zb/ohYSBb7pK/2QFeUa22L+4II H5DwCh3HchjtDPrAhFqGUyFZBsRZbQV1rPf sxxH2b0Lc1PMrK1o68dyk8gY8m4iZf r9ZD6xs4gAqdWtBQNIN8cvz4SI+Jv9f vayMH7f+K12yXiHN5oD9E t0u17 ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQ9WkiJ7yQ6HcafmczDMv1RKxPdJI/oeXUWdNW1MrWiQNVKeSeSSdZ6NaYUqfSjgXUSg iQbktTo8Fhv4 wPoFBz9SAfg086 jc0M2kGUNS9JZsLJdUB9u1KxY5 I0zqG4QTgZ6LP2UuWLG7TGMpkbK7z6G8HAZx7u315+Uc82dKt I0zb/ohYSBb7pK/2QFeUa22L+4II H5DwCh3HchjtDPrAhFqGUyFZBsRZbQV1rPf sxxH2b0Lc1PMrK1o68dyk8gY8m4iZf r9ZD6xs4gAqdWtBQNIN8cvz4SI+Jv9f vayMH7f+K12yXiHN5oD9E t0u17 (base) root@hmc/usr/local/bin #</pre> <p>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。</p>
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	<ol style="list-style-type: none"> 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