某客户CAS平台中毒导致网络中断排查案例（一）

薛泰吉 2014-12-22 发表

某客户CAS平台中毒导致网络中断排查案例（一）

一、 问题描述：

某客户CAS平台在运行一段时间后突然导致整网网络中断，断开CAS平台网络后网络立刻恢复。

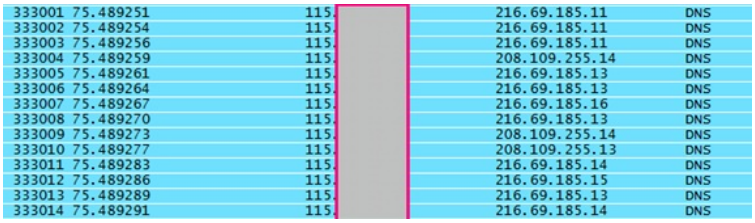
二、 组网环境

CAS平台组网采用UIS，网络模块为B6300XLG，CAS平台部署零存储。客户整网直接使用公网地址，二层网络，出口防火墙未做安全策略，CVK直接使用公网地址接入网络。

三、 过程分析：

1、将CAS平台及零存储环境恢复，接入网络，复现断网情况。

2、复现网络中断情况时，在接入交换机连接B6300XLG的下联口和某个CVK上进行抓包。对报文进行分析，发现有大量以CVK地址为源地址，以公网地址为目的地址的DNS请求报文。



333001	75.489251	115.	216.69.185.11	DNS
333002	75.489254	115.	216.69.185.11	DNS
333003	75.489256	115.	216.69.185.11	DNS
333004	75.489259	115.	208.109.255.14	DNS
333005	75.489261	115.	216.69.185.13	DNS
333006	75.489264	115.	216.69.185.13	DNS
333007	75.489267	115.	216.69.185.16	DNS
333008	75.489270	115.	216.69.185.13	DNS
333009	75.489273	115.	208.109.255.14	DNS
333010	75.489277	115.	208.109.255.13	DNS
333011	75.489283	115.	216.69.185.14	DNS
333012	75.489286	115.	216.69.185.15	DNS
333013	75.489289	115.	216.69.185.13	DNS
333014	75.489291	115.	216.69.185.14	DNS

CAS正常开局过程中是没有配置DNS地址的，于是检查CVK节点下/etc/resolv.conf文件，发现该文件被修改并添加了DNS地址，并且CVK节点root密码过于简单，于是怀疑CAS平台系统被攻击。

```
root@cvknode-2:~# cat /etc/resolv.conf
# Dynamic resolv.conf(5) file for glibc resolver(3) generated by resolvconf(8)
#     DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
nameserver 8.8.8.8
nameserver 8.8.4.4
root@cvknode-2:~# ssh cvknode-3
Warning: Permanently added 'cvknode-3,115.*.*.*' (ECDSA) to the list of known hosts.
```

3、使用ps –ef查询每台CVK节点的进程发现可疑进程

```
root      3180     1  0 10:50 ?        00:00:14 /etc/.SSH2
root      3182     1  0 10:50 ?        00:00:14 /etc/.SSHH2
root      2066     1  0 14:35 ?        00:00:02 /etc/sfewfesfs
root      1855     1 14 14:35 ?        00:07:55 /etc/whitptabil
root      1857     1 15 14:35 ?        00:09:01 /etc/smarvtd
root      1861     1  0 14:35 ?        00:00:01 /etc/gfhjrtfyhuf
root      1880     1 15 14:35 ?        00:09:00 /etc/gdmorpen
root      3659  3584  0 10:50 ?        00:00:00 /tmp/.sshdd1418611830
root      3660  3659  0 10:50 ?        00:01:29 /tmp/.sshdd1418611830
root      3661  3659  0 10:50 ?        00:00:00 /tmp/.sshdd1418611830
root      3663  3659  0 10:50 ?        00:00:04 /tmp/.sshdd1418611830
root      3676  3594  0 10:50 ?        00:00:00 /tmp/.sshhdd1418611830
root      3678  3676  0 10:50 ?        00:00:19 /tmp/.sshhdd1418611830
root      3680  3676  0 10:50 ?        00:00:00 /tmp/.sshhdd1418611830
root      3681  3676  0 10:50 ?        00:00:05 /tmp/.sshhdd1418611830
root     64191     1  0 14:34 ?        00:00:01 /etc/gfhjrtfyhuf
```

查询每个CVK节点的目录下的文件，发现在相应的目录下多了上述可疑进程的文件，并且使用cat命令显示该文件的结果是乱码刷屏。

查询每个节点rc.local文件，发现这些可疑进程是开机自启动。

```
root@cvknode-1:/etc# cat rc.local
#!/bin/sh -e
# rc.local
```

```
# This script is executed at the end of each multiuser runlevel.
# Make sure that the script will "" on success or any other
# value on error.
# In order to enable or disable this script just change the execution
# bits.
# By default this script does nothing.
touch /var/run/h3c_cas_cvk
/usr/bin/set-printk-console 2
exit 0
cd /tmp;./sfewfesfs
cd /tmp;./gfhjrtfyhuf
cd /tmp;./rewgtf3er4t
cd /tmp;./fdsfsfvff
cd /tmp;./smarvtd
cd /tmp;./whitptabil
cd /tmp;./gdmorpen
cd /etc;./sfewfesfs
cd /etc;./gfhjrtfyhuf
cd /etc;./rewgtf3er4t
cd /etc;./fdsfsfvff
cd /etc;./smarvtd
cd /etc;./whitptabil
cd /etc;./gdmorpen
```

4、通过上网查询相关资料，确认所有CVK节点被攻击，中了sfewfesfs病毒，该病毒相应进程会使CPU占用率瞬间达到300%多，向网络发送大量报文，导致网络阻塞。

```
top - 16:33:27 up  5:46,  2 users,  load average: 2.03, 1.30, 1.29
Tasks: 520 total,   6 running, 512 sleeping,   0 stopped,   2 zombie
Cpu(s):  4.2%us, 30.1%sy,  0.0%ni, 62.7%id,  0.0%wa,  3.0%hi,  0.0%si,  0.0%st
Mem:  16391908k total, 10569696k used,  5822212k free,   440204k buffers
Swap:  8803324k total,        0k used,  8803324k free,   846476k cached

  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
56794 root      20   0  339m  29m    0 S  393  0.2  11:58.88 whitptabil
56620 root      20   0  340m  29m    0 S  392  0.2  15:53.49 smarvtd
54572 root      20   0 4933m 1.6g 5344 S   16 10.3  32:37.23 kvm
54196 root      20   0 9044m 1.6g 5348 S   11 10.4  35:54.12 kvm
  167 root      20   0     0    0    0 S    2  0.0   0:13.16 ksoftirqd/6
  248 root      20   0     0    0    0 S    2  0.0   0:11.84 ksoftirqd/22
    3 root      20   0     0    0    0 S    2  0.0   0:53.44 ksoftirqd/0
  147 root      20   0     0    0    0 S    2  0.0   0:12.15 ksoftirqd/2
  142 root      20   0     0    0    0 S    1  0.0   0:11.73 ksoftirqd/1
  157 root      20   0     0    0    0 S    1  0.0   0:12.08 ksoftirqd/4
  233 root      20   0     0    0    0 S    1  0.0   0:16.91 ksoftirqd/19
  198 root      20   0     0    0    0 S    1  0.0   0:09.14 ksoftirqd/12
 5917 root      20   0 2217m 374m 2696 S    1  2.3   7:25.67 lichd
 5979 root      20   0 2217m 376m 2708 S    1  2.4   7:26.81 lichd
 6094 root      20   0 2289m 383m 2908 S    1  2.4   6:17.24 lichd
 6229 root      20   0 2360m 377m 2716 S    1  2.4  17:57.36 lichd
```

四、 解决方法：

1、 备份所有虚拟机磁盘镜像和配置信息，重新部署CAS平台及零存储，部署时使用较复杂的root密码，包含大小写，数字和特殊的字符信息。

2、 增加防火墙，在防火墙上做好安全策略，使CAS平台与外界网络完全隔开。由于客户网络为公网地址，在做好安全策略前，CAS平台先不接入网络。

3、 由于客户虚拟机分配的也是公网地址，也有可能中毒，建议客户检查虚拟机。