助查人士调查报告

调查时间：2022 年 10 月 20 日
调查地点：AGC 公司
案件主管：网罪科行动组 1A 队
调查人员：调查员编号 76594

检取电子证物：

1) 一部 Proxmox 服务器
2) 一部桌面计算机
3) 一部流媒体服务器

现场勘查总结：

搜查人员于现场捡取一部服务器、一部员工 （Carson） 所用的桌面计算机及一部流媒体服务器。 AGC 集团 IT 部門 人员称建立服务器的同事已离职，他只是负责以浏览器登入服务器操作，对系统并不熟悉。 他只知道服务器所用的操作系统为 “Proxmox”，上面运作一个虚拟计算器。 虚拟计算机运作公司的电邮系统“Xeams”。

现场专家在初步分析后表示“Proxmox”服务器透过三个硬盘以软 RAID 建立而成，现场虽未能撷取服务器逻辑存储（Logical Storage）内容，但他认为先撷取逻辑存储内容作检验较好；桌面计算机相信被黑客入侵，分析流量纪录相信黑客取走了服务器部份档案。

警方就公司另一部流媒体服务器有以下的行动：

1. 检查流媒体服务器的配置，包括： lsblk， zpool status，详情请参阅附件一
2. 将笔记本电脑连接到因特网以进行采集过程。
3. 使用 netcat 和取证工具进行采集。 取证数码影像档为 sda.e01，sdb.e01， sdc.e01， sdd.e01 和 sde.e01 （采集文件夹名称：MediaServer\e01\）。
4. IT 人员对 2022 年 7 月 21 日 流媒体服务器的系统日志进行了备份。 他向我们提供了一份日志副本，文件名：varlog_bak_20220721.tar.gz 。

现场勘查报告完毕
调查员编号 76594

助查人士调查报告

附件一

```
user@user-PC:~$ lsblk -e7
NAME   MAJ:MIN RM   SIZE RO TYPE MOUNTPOINTS
fd0      2:0    1     4K  0 disk
sda      8:0    0    30G  0 disk
├─sda1   8:1    0     1M  0 part
├─sda2   8:2    0   513M  0 part /boot/efi
└─sda3   8:3    0  29.5G  0 part /var/snap/firefox/common/host-hunspell
                                 /
sdb      8:16   0     2G  0 disk
├─sdb1   8:17   0     2G  0 part
└─sdb9   8:25   0     8M  0 part
sdc      8:32   0     2G  0 disk
├─sdc1   8:33   0     2G  0 part
└─sdc9   8:41   0     8M  0 part
sdd      8:48   0     2G  0 disk
├─sdd1   8:49   0     2G  0 part
└─sdd9   8:57   0     8M  0 part
sde      8:64   0     2G  0 disk
├─sde1   8:65   0     2G  0 part
└─sde9   8:73   0     8M  0 part
sr0     11:0    1 126.4M  0 rom  /media/mediauser/CDROM
sr1     11:1    1  1024M  0 rom
user@user-PC:~$
```

```
user@user-PC:~$ zpool status
  pool: media0
 state: ONLINE
config:

        NAME        STATE     READ WRITE CKSUM
        media0      ONLINE       0     0     0
          mirror-0  ONLINE       0     0     0
            sdc     ONLINE       0     0     0
            sdb     ONLINE       0     0     0
          mirror-1  ONLINE       0     0     0
            sdd     ONLINE       0     0     0
            sde     ONLINE       0     0     0

errors: No known data errors
```