**网络攻击追踪溯源：**

旨在利用各种手段追踪网络攻击的发起者。相关技术提供了定位攻击源和攻击路径，针对性反制或抑制网络攻击，以及网络取证能力。传统攻击溯源方法是通过单个组织的技术力量，获取局部的攻击相关信息，无法构建完整的攻击链条，一旦攻击链中断，往往会使得前期大量的溯源工作变得毫无价值。

目前所提出的恶意代码溯源分析与研究工作。其基本思路是：

* **同源分析：**利用恶意样本间的同源关系发现溯源痕迹，并根据它们出现的前后关系判定变体来源。目的是判断不同的恶意代码是否源自同一套恶意代码或是否由同一个作者、团队编写，其是否具有内在关联性、相似性。从溯源目标上来看，可分为**恶意代码家族溯源**、**作者溯源**。
  + - * + **家族溯源：**家族变体是已有恶意代码在不断的对抗或功能进化中生成的新型恶意代码，针对变体的家族溯源是通过提取其特征数据及代码片段，分析它们与已知样本的同源关系，进而推测可疑恶意样本的家族。

例如，Kinable等人提取恶意代码的系统调用图，采用图匹配的方式比较恶意代码的相似性，识别出同源样本，进行家族分类。

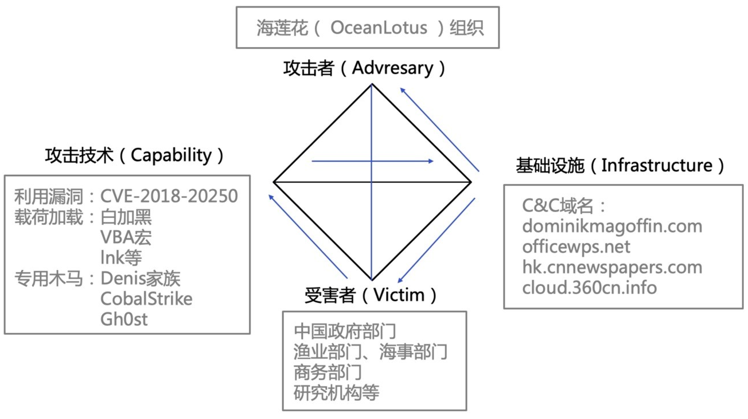
* + - * + **作者溯源：**恶意代码作者溯源即通过分析和提取恶意代码的相关特征，定位出恶意代码作者特征，揭示出样本间的同源关系，进而溯源到已知的作者或组织。

例如，Gostev等通过分析Stuxnet与Duqu所用的驱动文件在编译平台、时间、代码等方面的同源关系，实现了对它们作者的溯源。2015年，针对中国的某APT攻击采用了至少4种不同的程序形态、不同编码风格和不同攻击原理的木马程序，潜伏3年之久，最终360天眼利用多维度的“大数据”分析技术进行同源性分析，进而溯源到“**海莲花**”黑客组织。

**海莲花（APT32）**

海莲花，又称APT32、OceanLotus。攻击目标包括中国海事机构、海域建设部门、科研院所和航运企业，后扩展到几乎所有重要的组织机构，并持续活跃至今。

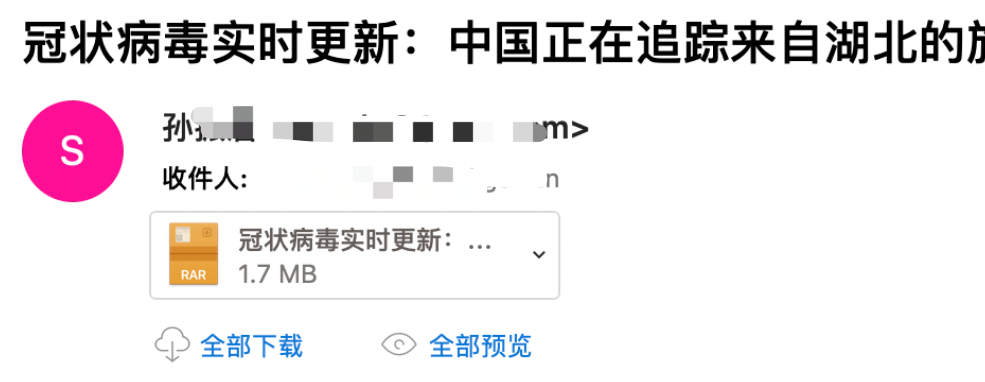
**常用攻击方法：**

* 构造诱饵文件欺骗用户点击
* 利用钓鱼邮件攻击，钓鱼关键字为新冠疫情相关信息等
* 采用恶意文件投递的鱼叉攻击
* 带有VBA宏病毒的Office文档
* 专用木马（Denis家族、CobalStrike、Gh0st）

**攻击手段：**

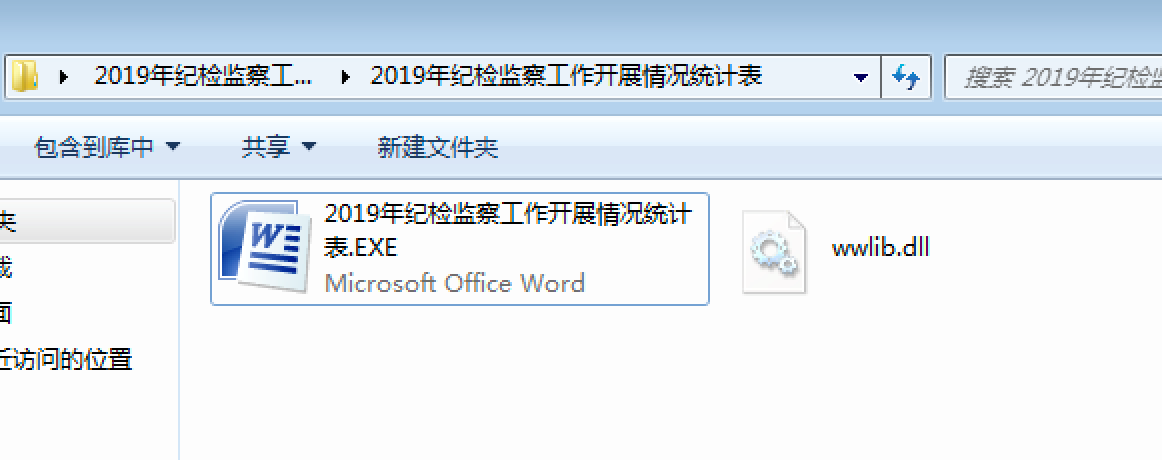
鱼叉邮件的附件含有恶意宏Word文件、捆绑后的文档图标的可执行文件、快捷方式文件、HTA文件等。入侵成功后通过一些内网渗透工具扫描渗透内网并横向移动，入侵重要服务器，植入Denis家族木马进行持久化控制。通过横向移动和渗透拿到域控或者重要的服务器权限，通过对这些重要机器的控制来设置水坑、利用第三方工具并辅助渗透。横向移动过程中还会使用一些逃避杀软检测的技术：包括白利用技术、PowerShell混淆技术等。

**诱导文档初始攻击：**

恶意文件投递的方式依然是最常用的鱼叉攻击的方式，近来钓鱼关键字主要是过武汉人员行程、新冠疫情相关信息等，相关的邮件如下。此外，投递钓鱼邮件的账号有网易邮箱，包括126邮箱和163邮箱。

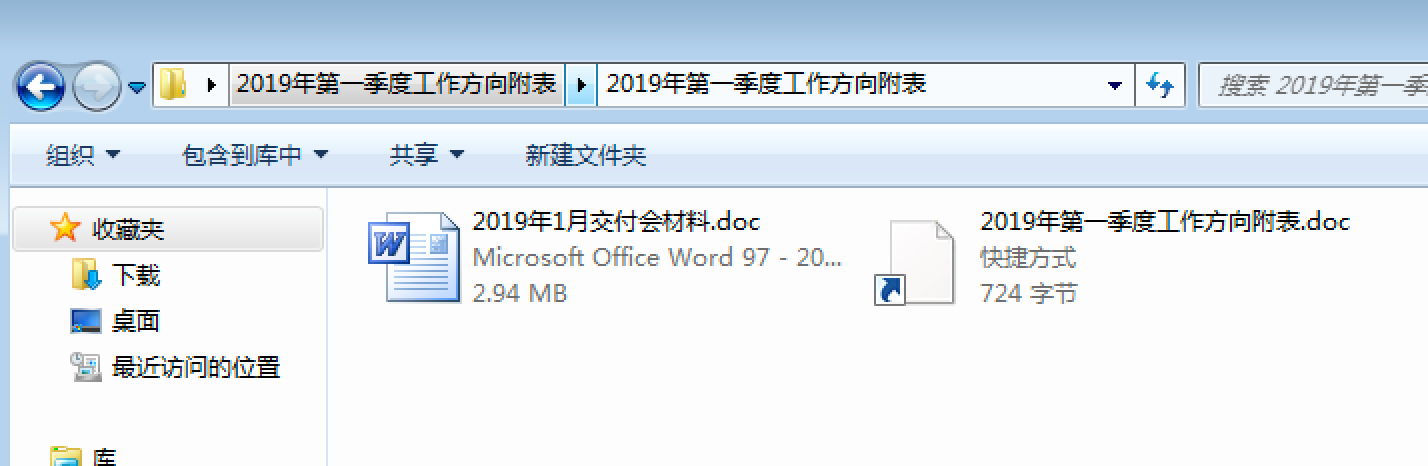
投递的恶意诱饵类型众多，包括白加黑、lnk、doc文档、带有WinRARACE（CVE-2018-20250）漏洞的压缩包等，之后的攻击中还新增了伪装为word图标的可执行文件、chm文件等。

1. **白加黑诱饵：**

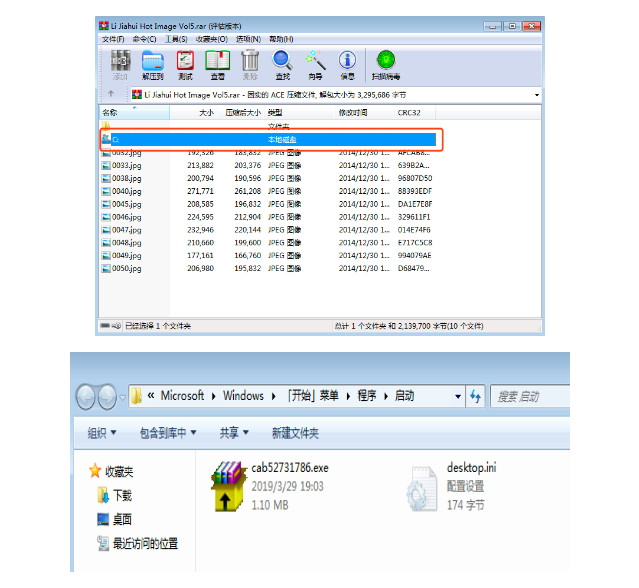
病毒伪装成一个DLL文件，伪装为Word图标的可执行文件启动的同时，病毒DLL也会被加载启动（也叫DLL劫持）。使用DLL侧加载技术来执行载荷，通俗的讲就是白加黑执行。

1. 带宏的恶意office文档

所谓的宏，利用一段程序代码,进行一系列的操作。自动连续完成。最终提取资源文件，进行解密。得到最终的rat在内存中展开，查找Createlnstance函数地址，最终将配置信息传入调用该函数，利用https进行通讯。



1. **带有WinRAR ACE（CVE-2018-20250）漏洞的压缩包**

解压文件时，它会自动加载恶意程序至C盘自启动目录并运行。