**原文作者**：Mayana Pereira, Shaun Coleman, Bin Yu, Martine DeCock, Anderson Nascimento

**原文标题**：Dictionary Extraction and Detection of Algorithmically Generated Domain Names in Passive DNS Traﬃc

**原文会议**：RAID2018 (CCF B类)

**原文链接**：<http://faculty.washington.edu/mdecock/papers/mpereira2018a.pdf>

**主要内容**：提出了基于字典进行DGA域名检测的方法

**论文笔记作者**：Carrie

第一章

第一章介绍了相关背景知识，首先是C2和DGA；然后介绍了Dictionary-based DGAs(generate domains by concatenating word from a dictionary)。然后作者提出，通过IP等信息检测AGD的方法数据较难获取，耗时较多，难以及时地检测出新产生的Dictionary-based DGA,提出了从literature角度取考虑的思想。

第二章

第二章介绍了已有的进行DGA域名检测的相关工作，一般都是字符特征与域名相关特征(IP等)相结合。然后作者提出目前开始有通过神经网络进行恶意域名检测的做法;最后，再次说明了Dictionary-based DGAs，它产生的域名更像人类正常创造的域名。

第三章

本文方法在建模时基于域名中的词建立了Word Graph，因此此章介绍了Word Graph的相关概念，具体包括Path,Cycle,Cycle Basis, Average Shortest-path length和 connected component，具体可见paper,重要概念(eg.connected component)在后文用到的地方进行了解释。

第四章

第四章通过实施步骤介绍了WordGraph Method的具体内容，WordGraph Method方法在实施过程中，具体包括如下：

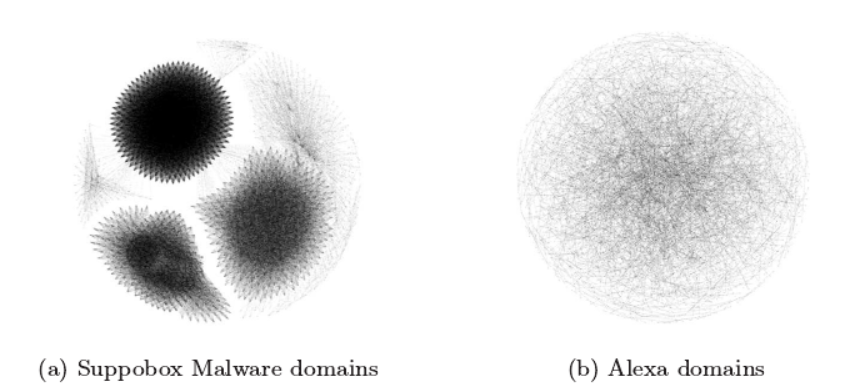
1.Extracting words(其实这并不是第一步，但这是一步基础操作，因此放在第一项介绍):

Extracting words是对域名集合中的域名提取words,这里对words的定义是，至少两次出现在二级域名中的m(m>=3)个字符组成的子串。例如当D={facetype.com, facetime.com, bedtime.com,faceboard.com, bedboard.com, bedding.com}时,所得到的words={face,time,bed,board,facet}。

2.Construction the graph

假设C是域名集合，首先根据TLD将域名分为若干个集合Ci，每个集合定义一个图Gi，Gi中的节点是对Ci 进行extract words的结果,且如果两个word出现在同一个域名里，则在这两个word的节点之间存在一条边 (这里要注意，根据TLD划分的原因是因为发现DGAs的TLD值分布在有限的几个TLD,且根据TLD划分能够限制图的大小。)。在得到Gi后，引入connected component G的概念，记作G’: a subgraph in which any two vertices are connected to each other by paths, and which is connected to no additional vertices in G.(中文翻译和很难准确，因此直接引用原文)，对每个Gi进行操作获取G’。

3. 作者对已知的良性域名(AlexaTop)和DGA域名(从DGArchice获取)进行WordGraph构建后发现，良性域名与恶意域名所构建的WordGraph的结构是不同的，从图中观察发现，每个malicious dictionary中的词都可能被用于构建多个不同的域名。



4. Feature vector construction:

基于域名集合得到的G和G’,对G’进行特征提取,具体包括：

1）Dmean: Average vertex degree of G’

2） Dmax: Maximum vertex degree of G’

3） Cardinality of cycle basis set of G’

4） CV: C/|V |, where V is the set of vertices of G’

5） ASPL: Average shortest-path length of G’ (ASPL计算公式具体见paper)

5. Graph based Dictionary Finding: 对于已知性质的域名集合Ctrain,通过以上步骤得到Gi与the connected component of Gi；然后，提取特征，训练决策树分类器；

6. Domain Classification：根据以上步骤，得到detected dictionaries。对于一个待检测域名，如果它包含至少两个属于已发现的malicious dictionary的word，且它的TLD与构架出该malicious dictionary的Ci的TLD相同，则认为他是恶意的。

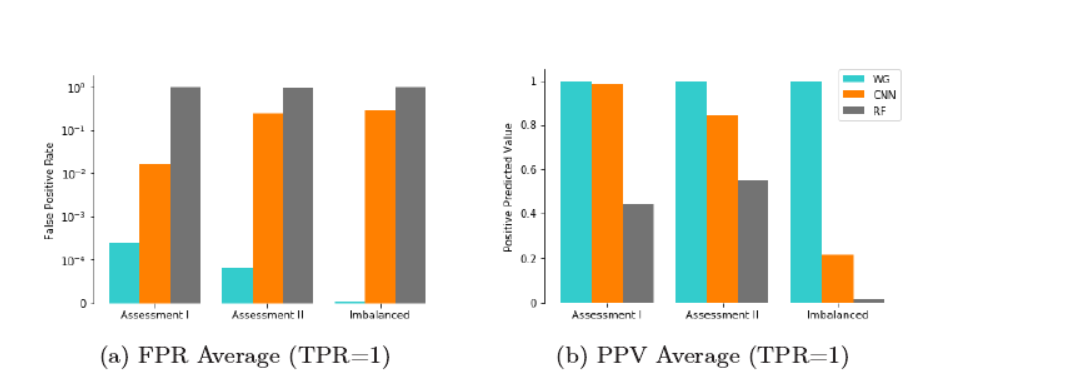
第五、六章：实验与结果

作者通过与两种模型的对比实验来对WordGraph方法进行评估。

第一种对比是Random Forest模型，选取了常见的用于DGA检测的11种lexical features进行建模，构建分类器；

第二种是卷积神经网络，网络的输入是原始的域名字符串，这些字符串在网络种将通过embedding转化为128维的向量。

作者选取了PPV, TPR, FPR三个指标进行评估，在基于Ground Truth data测试时，得到如下结果：



个人总结创新点如下：

1. 提出了WordGraph的构建，较之传统的对域名进行分析的语义特征，这一是一种新的思路；
2. 不是直接判定域名是否恶意，而是先发现了DGA dictionary，然后基于字典进行域名性质的判定。