专利创新点检索报告

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 创新点名称 | 一种DGA恶意域名检测方法研究与实现【论文 陈娌砺 北方工业大学】 | | | | | | | |
| 联系人 |  | 电话 | |  | | 邮箱 |  | |
| 交底概述 | 关键词 | 恶意域名，机器学习，DGA域名，支持向量机 | | | | | | |
| 解决问题 | 域名解析系统已经发展成为了国际互联网中一个完全不可能被忽视且重要的一个关键的基础网络设施和信息服务，难以避免被域名利用者非法利用。因此域名安全检测也成为信息安全里的重要研究内容。 | | | | | | |
| 主要技术手段 | 提出了一种基于domain-flux恶意域名的异常检测的系统，结合九个主要特征，实现基于svm算法检测的恶意域名的异常检测方案。系统设计基于一个开放源代码的分词数据库，首先对域名的字符结构进行了全面的分析，并从英语域名字符组中提取了最长和可能最特殊的含义。将选取特征中连续字母最大长度改为拆词后字符串长度。基于svm法对正常域名和DGA域名之间的特征差异性关系进行了精确区分。 | | | | | | |
| 有益效果 | 该技术框架在离线训练时长、对未知DGA恶意域名家族的检测能力方面表现优秀，可以较好地满足运营商大网环境下对恶意域名的检测分析要求。 | | | | | | |
| 关联企业 | \*\*\*公司 | | | | | | |
| 以下部分将由代理人填写反馈 | | | | | | | | |
| 检索结果 | 文件编号 | | 公开号 | | 公开日期 | | | 发明名称 |
|  | |  | |  | | |  |
|  | |  | |  | | |  |
| 评价意见 | 该系统检测的是恶意域名，而本发明根据用户提供域名检测的相似域名 | | | | | | | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 创新点名称 | 一种挖掘恶意域名的方法和装置【CN109688165A】 | | | | | | | |
| 联系人 |  | 电话 | |  | | 邮箱 |  | |
| 交底概述 | 关键词 |  | | | | | | |
| 解决问题 | 提供一种挖掘恶意域名的方法和装置，以解决追踪恶意域名的问题。 | | | | | | |
| 主要技术手段 | 方法包括：获取第一恶意域名，根据第一恶意域名获取第一要素信息，根据所述第一要素信息及预设挖掘条件从预设历史信息集中获取至少一个第一域名，判断第一域名是否满足预设审核规则；若是，则确定所述第一域名为第二恶意域名。 | | | | | | |
| 有益效果 | 本申请所述的方法，通过域名服务商、域名注册时间以及与域名相关联的更新时间与已知恶意域名的关系，侦测未知恶意域名。提高网络安全。 | | | | | | |
| 关联企业 | 微步在线 | | | | | | |
| 以下部分将由代理人填写反馈 | | | | | | | | |
| 检索结果 | 文件编号 | | 公开号 | | 公开日期 | | | 发明名称 |
|  | |  | |  | | |  |
|  | |  | |  | | |  |
| 评价意见 | 该系统检测的是恶意域名，而本发明根据用户提供域名检测的相似域名 | | | | | | | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 创新点名称 | 一种基于深度学习的恶意域名识别方法、装置及电子设备【CN110008705A】 | | | | | | | |
| 联系人 |  | 电话 | |  | | 邮箱 |  | |
| 交底概述 | 关键词 |  | | | | | | |
| 解决问题 | 随着网络的普及，网络攻击日益成为严重的问题。在这些攻击中,恶意域名经常扮演着重要角色，被广泛应用到各种类型的攻击中，如钓鱼网站、垃圾邮件以及其他恶意软件。而识别恶意域名对于阻止这些攻击具有重要意义。但是目前在信息安全领域，对恶意域名的识别主要依赖安全工程师的经验去识别，随着恶意网络攻击的不断增长，采用人工方式无力应对快速增加的恶意域名识别工作，导致恶意域名识别的准确率不高。 | | | | | | |
| 主要技术手段 | 获取第一域名数据集合，并对第一域名数据集合中的识别对象进行提取操作，形成与识别对象相对应的至少一个目标特征信息；对目标特征信息进行划分形成至少一个信息单元，并确定信息单元所表征的内容；基于预设数据结构标准对信息单元所表征的内容进行处理，以生成相应的第一标准数据；将第一标准数据作为预设深度学习模型的输入，以对预设深度学习模型进行训练，并利用训练完成的预设深度学习模型针对第二域名数据集合进行恶意域名的识别。该方法能训练出具有较高识别准确度的预设深度学习模型，使用该模型即使面对海量数据也能够有效提高识别恶意域名的准确率。 | | | | | | |
| 有益效果 | 由于能够对第一域名数据集合中的识别对象进行提取操作，形成与识别对象相对应的目标特征信息，进而形成相应的信息单元，因此能够利用该信息单元对第一域名数据集合中的具体数据进行识别，从而训练出具有较高识别准确度的预设深度学习模型，使用该模型即使面对海量数据也能够有效提高识别恶意程序特别是恶意域名的准确率。 | | | | | | |
| 关联企业 | 微步在线 | | | | | | |
| 以下部分将由代理人填写反馈 | | | | | | | | |
| 检索结果 | 文件编号 | | 公开号 | | 公开日期 | | | 发明名称 |
|  | |  | |  | | |  |
|  | |  | |  | | |  |
| 评价意见 | 该系统检测的是恶意域名，而本发明根据用户提供域名检测的相似域名 | | | | | | | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 创新点名称 | 用于检测恶意网址的方法和系统【CN104766014A】 | | | | | | | |
| 联系人 |  | 电话 | |  | | 邮箱 |  | |
| 交底概述 | 关键词 |  | | | | | | |
| 解决问题 | 提供一种能够有效提高恶意网址检测能力的方案 | | | | | | |
| 主要技术手段 | 接收用户上报的URL，利用基于用户地理位置的分布式动态爬虫子系统来获取HTTP请求链。下载与所述URL关联的网页内容以获得HTTP请求链，从中提取以下至少一个维度的特征：上下游信息（302跳转次数，404页面占比，子URL是否包含广告联盟链接，子URL是否包含恶意子链接，子URL是否包含小型网站统计工具），服务器维度（是否为境外互联网协议IP地址，是否是WindowsIIS，是否采用内容分发网络CDN技术，是否是kangle服务器，是否是netbox服务器，是否是nginx服务器，是否是apache服务器，是否是多媒体视频），网页编程语言维度，时间维度，网页自身描述信息。将URL关联的网页内容渲染成图片并利用光学字符识别OCR技术提取网页文本内容，通过用隐含狄利克雷分布对网页文本内容判断URL是否为恶意网址。根据白名单执行去误报处理。 | | | | | | |
| 有益效果 |  | | | | | | |
| 关联企业 |  | | | | | | |
| 以下部分将由代理人填写反馈 | | | | | | | | |
| 检索结果 | 文件编号 | | 公开号 | | 公开日期 | | | 发明名称 |
|  | |  | |  | | |  |
|  | |  | |  | | |  |
| 评价意见 | 【高度相关】 | | | | | | | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 创新点名称 | 恶意域名检测方法、装置、设备及存储介质【CN 114024718 A】 | | | | | | | |
| 联系人 |  | 电话 | |  | | 邮箱 |  | |
| 交底概述 | 关键词 |  | | | | | | |
| 解决问题 | DNS作为互联网重要的基础设施，主要负责IP地址与域名之间的相互转换，因此，恶意域名的检测成为了网络安全防护的一道重要措施。然而，现有的基于图方法的域名检测，皆是基于静态图的检测，没有考虑域名是时刻更新的，也就没有考虑到域名操作的先后顺序，降低了在域名检测时发现恶意域名的可能性。因此，如何提高恶意域名的检测效率，是一个亟需解决的技术问题。 | | | | | | |
| 主要技术手段 | 通过构建域名关系时序图，再对域名关系时序图中的邻居节点序列进行表示学习，最后采用无监督或有监督的方式进行检测 | | | | | | |
| 有益效果 | 充分考虑了域名操作先后的关联性，增大了在域名检测时发现恶意域名的可能性，提高了恶意域名检测的效率 | | | | | | |
| 关联企业 |  | | | | | | |
| 以下部分将由代理人填写反馈 | | | | | | | | |
| 检索结果 | 文件编号 | | 公开号 | | 公开日期 | | | 发明名称 |
|  | |  | |  | | |  |
|  | |  | |  | | |  |
| 评价意见 | 本发明是针对用户提供的目标域名进行相似域名检测，该发明检测的是恶意域名并提供相应检测设备，而本发明提供方法论。 | | | | | | | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 创新点名称 | Towards quantifying visual similarity of domain names for combating typosquatting abuse【论文】 | | | | | | | |
| 联系人 |  | 电话 | |  | | 邮箱 |  | |
| 交底概述 | 关键词 |  | | | | | | |
| 解决问题 | 域名仿冒成为互联网用户和流行网站的品牌所有者的投机性和严重现象。域名仿冒者注册流行网站的类似域名，以通过显示广告、将流量重定向到第三方页面、部署网络钓鱼网站或提供恶意软件来获利。因此，在衡量分销、货币化和成本等方面的域名仿冒方面已经做了大量工作。本文没有测量域名仿冒，而是试图从异常检测的角度打击域名仿冒滥用：一个看起来非常像一个流行网站的域名是可疑的。 | | | | | | |
| 主要技术手段 | 提出了TypoPegging，一种反向查找方法，快速准确地获得给定域最相似的流行网站。提出一种新的定量方法来测量两个给定域的视觉相似性。所提出的方法基于广义的Levenshtein距离，该距离可以洞察新颖的视觉特征。然后，提供了一种有效的方法来搜索给定流行网站集上域的最大视觉相似性。基于视觉距离度量的三角形不等式和位置敏感哈希算法加速搜索过程。。 | | | | | | |
| 有益效果 | 初步结果表明，该方案在区分域名仿冒域名和普通域名方面是有效的。与线性搜索方法相比，可以将搜索过程加快几个数量级。 | | | | | | |
| 关联企业 |  | | | | | | |
| 以下部分将由代理人填写反馈 | | | | | | | | |
| 检索结果 | 文件编号 | | 公开号 | | 公开日期 | | | 发明名称 |
|  | |  | |  | | |  |
|  | |  | |  | | |  |
| 评价意见 | 【高度相关】 | | | | | | | |