恶意域名检测研究与应用综述

王媛媛 吴春江 刘启和 谭 浩 周世杰
(电子科技大学信息与软件工程学院 四川 成都 610054)

摘 要 目前,网络安全问题层出不穷,特别是近年来以域名为依托的攻击,如勒索软件、垃圾邮件、DDos 攻击等,成为网络安全威胁的重要表现形式。以域名攻击技术为主要攻击方式的网络威胁,经历了从传统的机器学习的检测方法到主流的深度学习检测方法的转变。发现神经网络能够很好地自学习恶意域名特征,并能提供更高的检测率。但随着检测技术的不断提高,攻击者提出了更智能的 DGA 域名来规避神经网络的检测,在后续的基于这些 DGA 变体的检测成为目前域名检测技术的主要研究方向。随着生成对抗网络在域名检测方面的应用,Anderson 等提出利用 GAN 来生成对抗样本提高检测,为域名的检测发展提出新的发展方向。最后,总结域名检测的发展概况及其存在的问题,并对域名检测的可发展点做出展望。

关键词 DGA 算法 恶意域名 检测技术 模型 深度学习

中图分类号 TP393.08 **文献标识码** A DOI: 10.3969/j.issn.1000-386x.2019.09.053

OVERVIEW OF MALICIOUS DOMAIN NAME DETECTION AND APPLICATION

Wang Yuanyuan Wu Chunjiang Liu Qihe Tan Hao Zhou Shijie
(*School of Information and Software Engineering, University of Electronic Science and Technology, Chengdu 610054, Sichuan, China*)

Abstract At present, network security issues are emerging, especially in recent years, domain-based attacks, such as ransomware, spam, DDos attacks, etc., have become an important manifestation of cyber security threats. The network threat with domain name attack technology as the main attack mode has experienced a transition from the traditional machine learning detection method to the mainstream deep learning detection method. It is found that the neural network can self-learn the malicious domain name feature and provide a higher detection rate. However, with the continuous improvement of detection technology, attackers have proposed smarter DGA domain names to avoid the detection of neural networks. The subsequent detection based on these DGA variants has become the main research direction of domain name detection technology. With the application of the anti-network in domain name detection, Anderson et al. proposed to use GAN to generate anti-sample detection, which proposed a new development direction for the development of domain name detection. Finally, we summarized the development of domain name detection and its existing problems, and prospected the development of domain name detection.

Keywords DGA algorithm Malicious domain name Detection technology Model Deep learning

0 引 言

域名系统协议是互联网的重要组成部分,它将难以记忆的互联网协议地址映射到易于记忆的域名[1-2]。大量的网络服务依赖于域名服务来展开。由于域名系统并不对依托于其开展的服务行为进行检测,DNS 服务被滥用于各种恶意活动:传播恶意软件、促进命令和控制(Command and Control,C&C)服务器[3]通信,发送垃圾邮件、托管诈骗和网络钓鱼网页[4]等。

恶意软件控制器或僵尸程序利用恶意软件进行各种未经授权的恶意活动。为了成功实现其目标,恶意

收稿日期:2019-01-16。四川省重大专项(2018GZDZX0006,2017GZDZX0002,2018GZDZX0007)。**王媛媛**,硕士生,主研领域:网络安全。**吴春江**,博士生。**刘启和**,副教授。**谭浩**,副教授。**周世杰**,教授。

软件与命令和控制中心的连接至关重要。因此,以恶意域名解析的连接方式成为网路恶意攻击的主要手段。所谓恶意域名解析,是指用户的正常 DNS 解析请求解析到他人的服务器上或是攻击者的恶意服务器上,而被解析的服务器上实际没有相应的站点[5]。以域名为依托的网络攻击方式的发展变化如图 1 所示。

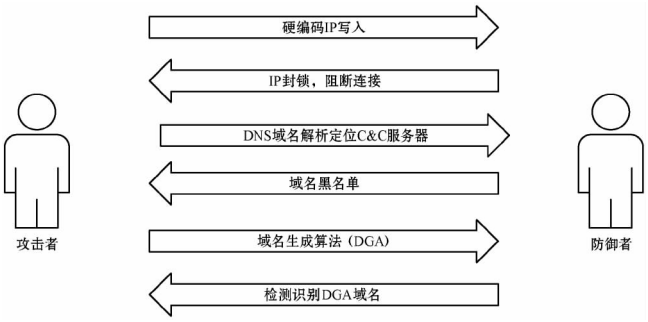

图 1　域名攻击发展变化

最初,攻击者通过对恶意软件(如僵尸网络程序)内部的 IP 地址进行硬编码,建立了与 C&C 中心的通信通道。当恶意软件的可疑 IP 被发现,网络安全管理员就可以针对 IP 进行流量阻断,以阻止恶意软件与攻击者的连接。为了应对 IP 封锁,攻击者使用 DNS 域名解析来定位 C&C 服务器。通过将注册的域名写入恶意程序中,然后恶意程序利用域名解析得到攻击者的命令控制服务器 C&C 的 IP 地址,以进行连接通信。即使 IP 地址被查了出来,攻击者通过更换域名的 IP 地址就可以继续保持与恶意程序的通信[6]。但这种方式不能抵抗安全人员逆向分析的域名黑名单,为应对黑名单的域名防御机制,攻击者引入域名算法生成技术,利用特定的域名生成算法(Domain Generation Algorithms,DGA),生成大量域名用于自身的组织和控制。攻击者从算法生成的大量域名中,选取几十个或几百个域名进行注册来掩护真正的 C&C 服务器的域名。而网络安全管理员为应对 DGA 域名,也相应提出了基于 DGA 域名的检测方法。

使用 DGA 的优势在于模糊了控制服务器的节点位置,该方法的灵活性还让网络安全管理员无法阻止所有可能的域名,并且注册一些域名对攻击者来说成本很低。利用 DGA 域名实施的攻击是网络安全中重要的攻击形式。因此,捕获由恶意软件生成的域名已成为信息安全的核心主题。

1　域名生成算法

域名生成算法是指通过输入的随机种子,利用加密算法,比如 MD5、异或操作等,生成一系列的伪随机字符串[7],即域名列表。攻击者通过与恶意软件共享 DGA 的随机种子,知道对方可能使用的域名,然后使用这些域名不断尝试连接直到连接成功。DGA 使用的随机种子主要分为三类: 时间无关和确定性种子,时间依赖性和确定性种子以及时间依赖性和非确定性种子。随着 DGA 域名的僵尸网络的检测方法在不断地改进与完善,但在检测已有的 DGA 域名的同时,新的 DGA 家族变体也在出现。迄今为止,基于 360netlab 公开的 DGA 域名家族共有 40 个。

由于 DGA 家族众多,这里我们主要介绍几类常用的 DGA 域名。表 1 中列出了 5 类常见 DGA 家族域名的样例。

表 1　常见 DGA 域名实例

DGA	Example domain names
Conficker	ydqtkptuwsa. org bnnkqwzmy. biz glrmwqh. net
Cryptolocker	nvjwoofansjbh. ru qgrkvevybtvckik. org eqmbcmgemghxbcj. co. uk
Ramnit	knpqxlxcwtlvgrdyhd. com nvlyffua. com hgyudheedieibxy. com
symmi	veeswaehsisa. ddns. net uhbacoinm. ddns. net baugkoosdui. ddns. net
suppobox	sharmainewestbrook. net tablethirteen. net childrencatch. net

Conficker[8-9]是针对 Microsoft Windows 操作系统的计算机蠕虫,最初于 2008 年末被发现。它使用 Windows 操作系统软件中的缺陷和对管理员密码的字典攻击在形成僵尸网络时传播。几乎所有以 Conficker 为依托的高级恶意软件技术都已被研究人员所熟知,但这种病毒的综合使用使得它难以根除。

CryptoLocker[10]勒索软件攻击是一种针对运行 Microsoft Windows 的计算机的木马,它通过受感染的电子邮件附件以及现有的 Gameover Zeus[11]僵尸网络传播。它使用 DGA 从英文字母表 a ~ y 中随机选取生成字符串长度为 12 至 15 的二级域名,每周大约生成 1 000 个域名。

Ramnit[12]是一种类似 Zeus 的恶意软件。它使用 DGA 与其 C2 服务器通信。感染后,样本开始快速连续地对许多不同的域进行 DNS 查询。DGA 使用随机数生成器首先通过均匀地选择 8 到 19 个字符之间的长度来确定第二级域的长度。接下来,DGA 通过从“a”到“x”统一选取字母来确定第二级域(字母“z”不

能被选中),然后附加静态顶级域“.com”。

与著名的 conficker 相比,symmi[13] 的所有随机方面都是真正的伪随机,它通过当前的日期和编码常量,利用随机数生成器生成种子。它包含三级域名,在第三级域中,除字母“j”之外,从元音和辅音中随机交替的挑选字母,因此随后的字母总是来自其他字符类,这样选取的字符组成的域名几乎是可读的。生成第三级域后,DGA 会附加配置的第二级和顶级字符串,如“.ddns.net”。

Suppobox[14] 与现有的大部分 DGA 都是利用伪随机字符串生成的域名家族不同,它利用英文单词列表,从英文单词列表中随机选择两个单词连接在一起生成恶意域名。

随着针对 DGA 检测技术的不断提高,传统的 DGA 技术的复杂性从简单的随机绘制字符的方法到尝试模拟真实域中的字符或单词分布的方法。例如:ramnit 使用从随机种子开始的乘法、除法和模数的组合来创建域名; symmi 为了能够生成几乎可发音的域名,随机交替选择元音或辅音类。另一方面,suppobox 通过连接两个伪随机选择的英语词典单词来创建域。

2 DGA 域名检测的研究与应用

DGA 的灵活性及低成本使恶意软件大量利用 DGA 来生成恶意域名以连接控制和命令服务器。为针对以 DGA 生成的域名的检测研究最先是从 DGA 生成算法入手的。文献[15]通过逆向恶意样本的 DGA 算法,提前抢注域名来控制恶意软件与 C&C 通信。虽然逆向技术可以深入了解恶意样本采用的域名生成算法以及对域名的使用机制,但这种方法所消耗的人力资源过大且应用受限。因此后续在异常域名检测识别方面研究主要包括基于网络流量上下文特征提取的机器学习方法的检测、基于无特征提取的深度学习方法的检测和基于附加条件的深度学习方法的检测。

2.1 基于特征提取的机器学习方法的检测

通过特征提取的恶意域名检测方法主要分为两类:一是根据域名字符统计特征的检测,二是根据 DNS 流量信息的检测。

2.1.1 域名字符统计特征的检测

域名在构造上可以分为主机名和域名(包含顶级域名和可能存在的二级和三级域名)。由于域名部分数据相对固定,变化较少,因此大部分对域名的研究处理是针对主机名的处理,以下提及的域名都是指域名的主机名。

利用合法域名与 DGA 域名在字符分布上有明显的差异,Davuth 等[16] 以域名的 bigram 作为特征,通过人工阈值的方式过滤出现频率较低的 bigram,采用支持向量机分类器检测随机域名。Yadav 等[17] 通过查看同一组 IP 地址的所有域中的 unigram 和 bigram 特征分布,查找算法生成的域名的固有模式来检测 DNS 流量中的域名。在域名长度上,Mowbray 等[18] 在域名查询服务中通过使用不寻常的字符串长度分布来检测恶意域名。王红凯等[19] 提出了一种基于随机森林的随机域名检测方法。该方法以人工提取的域名长度、域名字符信息熵分布,元音辅音比、有意义的字符比率等特征来构建随机森林模型训练分类,实现对随机域名的检测。随后 Agyepong 等[20] 也利用算法生成域名与正常域名的字符分布的不同,分别利用域名 K-L 距离、编辑距离、Jaccard 系数分别作为特征向量的识别效果。除了利用域名传统定量的域名特征之外,文献[21]使用分词算法将域名分割成单个词,来扩展特征集的大小以提高检测恶意域名的能力。

2.1.2 DNS 流量信息的检测

在 DNS 流量分析上面,文献[22]提出了一种依赖于 fast-flux 僵尸网络的三个特征:委托代理模式、恶意活动的执行者和硬件性能,来检测 Web 服务是否被 fast-flux 僵尸网络实时托管。Bilge 等[23] 介绍了一个名为 Exposure 的系统,它利用 DNS 分析技术来检测涉及恶意活动的域,通过从 DNS 流量中提取 15 个特征来描述 DNS 名称的不同属性以及查询它们的方式。与之前的 DNS 流量分析不同,Antonakakis 等[24] 通过分析因名称错误响应的域名的 DNS 查询,也称为 NXDOMAIN 响应,即不存在 IP 地址的域名,并设计了一个名为 Pleisdes 的系统来检测 DGA 生成的域。它主要利用由 DGA 生成的域名中,只有相对较少的域名成功解析为 C&C 服务器的地址的特点。当 Pleiades 找到一组 NXDOMAIN 时,它应用统计学习技术构建 DGA 模型,然后用它来检测用同一种 DGA 算法的受感染的主机,并检测与 DGA 看起来类似的活动域名,因为其有可能指向僵尸网络 C&C 服务器的地址。Pleiades 具有能够发现和建模新的 DGA 而无需劳动密集型恶意软件逆向工程的优势。另外 Pleiades 通过监控本地网络中的 DNS 流量来实现这些目标,而无需大规模部署先前工作所需的 DNS 分析工具。文献[25]也通过分析 NXDOMAIN 响应来检测 DGA 域名。此外,文献[26-27]通过 DNS 数据源及其丰富度、数据分析方法以及评估策略和度量,对近年来使用 DNS 数据的恶意域名检测技术的一般框架分类,并就 DNS 领域下的检测提出了一些挑战:大规模的真实 DNS 数据日志很少公开可

用,恶意域的特征弹性以及缺少评估的具体方案。

通过网络的 DNS 流量的上下文信息及域名的统计特征对潜在的 DGA 分类有一定的成果,但是这些不能满足实时检测和预防的现实安全应用的需求。为满足实时检测的要求,诸多的实时方法都使用手工挑选的特征(例如: 熵、字符串长度、元音比、辅音比等) 。机器学习模型,例如随机深林分类器[19] 就是比较典型的一个。然而,这些依赖人工提取特征检测方法存在着误报率较高、整体检测率低的问题。主要原因有两方面: 一方面,大多数现有的基于网络的僵尸网络检测方法仅限于数据包检测级别,大多数方法也主要关注网络流的部分特征,不能完全表征僵尸网络的异常行为; 另一方面,僵尸网络与时俱进,利用先进的思想和技术来逃避检测。特别是为了应对人工提取的特征检测,攻击者可以设计新的 DGA 算法以绕过某些固定的特征。随着检测技术的不断发展,僵尸网络变得越来越复杂和智能化,在一定程度上表现出复杂性和对抗性,这使得网络安全形势依然严峻。

2.2　基于无特征提取的深度学习方法的检测

在以往依赖手工提取的特征来检测恶意域名有两个主要的缺点: 手工提取的特征容易规避,手工提取特征耗时。Antonakakis 等[28] 提出了无特征的实时技术隐马尔可夫模型(HMM) 。但 HMM 在检测 DGA 方面表现不佳。深度学习方法是传统机器学习机制的复杂模型,具有将输入信息提取为最佳特征表示的巨大能力,在语音识别和图像识别领域取得了显著的成果,也为恶意域名检测技术提供了一个全新的思路。近年的多数研究采用深度学习方法,如文献[29]提出了一种基于 word-hashing 技术的深度学习网络对域名进行分类,其不仅避免了手工提取特征还发现了传统统计方法无法发现的特征。接下来我们介绍两种主要的神经网络模型在恶意域名检测上的应用。

2.2.1　RNN 在域名检测的应用

循环神经网络[30] (RNN) 因其能捕获序列之间有意义的时间关系被应用于各种自然语言任务中。因此,初期主要应用循环神经网络、递归神经网络来检测伪域名。但 RNN 在长链操作中易导致梯度消失问题,不具备学习长期依赖信息的能力。LSTM[31-32] 在 RNN 的基础上增加一个状态信息使其能够学习长期依赖信息,在长时间的学习模式方面非常擅长文本和言语处理,因此被广泛应用。Woodbridge 等[33] 利用长短期记忆网络实现对 DGA 的实时预测,而无需上下文信息或手动创建的特征。其模型框架如图 2 所示,包括一个嵌入层,一个基本上用作特征提取器的 LSTM 层以及一个逻辑回归分类器。基于 RNN 的 DGA 检测模型都是类似于此模型框架。另外其所提出的技术可以准确地执行多种分类,从而能够将 DGA 生成的域归属于特定的 DGA 家族。

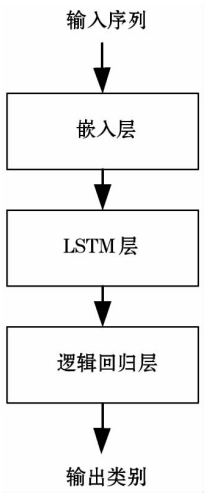

图 2　基于 LSTM 的 DGA 域名检测模型

Yu 等[34] 为了比较深度学习方法的优势,以传统的机器学习方法中比较有效的基于特征构建的随机森林模型作为基准实验,利用 LSTM 网络和 CNN 网络进行域名检测分类比较。在整体检测率上,CNN 和 LSTM 模型相对于随机森林有突出的表现,但在个别 DGA 上表现不佳。存在的原因大概有两方面: 一是因数据不平衡导致检测率低或识别误差大; 二是传统的 DGA 和基于字典的 DGA 之间存在偏差的样本分布。为解决 DGA 家族中个体识别率低,Tran 等[35] 提出了一种改进的成本敏感的 LSTM 算法来应对 DGA 域名数据多类不平衡的问题,相对原始敏感 LSTM 算法,具有较高的准确率。

之后,Vinayakumar 等[36] 也比较了几种常见的神经网络模型。他们对递归神经网络(RNN) 、身份-递归神经网络(I-RNN) 、长期短期记忆(LSTM) 、卷积神经网络(CNN) 和卷积神经网络长短期内存(CNN-LSTM) 体系结构五类神经网络进行实验比较。结果表明,深度学习方法,特别是递归神经网络系列和混合网络显示出优越的性能,最高检测率分别为 0.994 5 和 0.987 9。主要原因是深度学习方法具有捕获层次特征提取和序列输入中的长期依赖性的固有机制。

以循环神经网络为基本框架的检测模型对随机性高的 DGA 域名检测准确率高,但对随机性低的 DGA 域名识别率低,导致对正常域名产生较高的误报。因此,此类网络在低随机性和基于字典的 DGA 域名成为其未来的主要发展点。

2.2.2　GAN 在域名检测的应用

Goodfellow 等[37] 在 2014 年提出的生成对抗网络

(GAN) 是一种深度学习[38]模型,为生成模型提供了一个新的框架。它借鉴博弈论中的纳什均衡思想[39],使生成器和鉴别器相互学习以生成模拟数据。生成器捕获实际数据的分布,而鉴别器估计样本来自训练集的概率。Anderson 等[40]利用了生成对抗网络的思想,构建了基于深度学习的 DGA 域名生成对抗样本方法。在一系列的对抗轮回中,生成器学习生成检测器越来越难以检测的域名。相反地,检测器通过更新其参数以提高检测。其提出的生成对抗网络是基于预先训练的自动编码器(编码器 + 解码器),其中自动编码器先在 Alexa 的一百万个域中训练,以生成看起来更像真实域名的域。然后在生成对抗网络中竞争性地重新组装编码器和解码器,模型框架大致如图 3 所示。由于编解码器是预训练好的,因此,在对抗训练中,只训练生成模型的生成层和判别模型的逻辑回归层。最后用随机森林 DGA 分类器来验证生成的对抗样本的表现力。

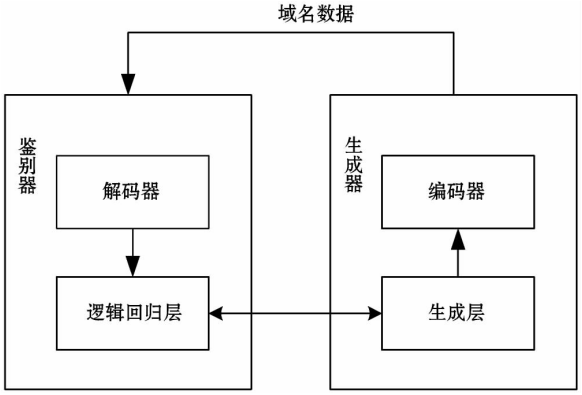

图 3 基于生成对抗网络的域名对抗样本生成模型

虽然在基于人工特征提取的随机森林 DGA 分类器上,对抗样本表现良好,但实验对比较少,只验证了在随机森林模型上的检测效果。之后,文献[41]也采用了 GAN 的思想来生成恶意域名对抗样本,不同之处在于编码器部分的设计,后者设计了基于的 Ascall 编码方式定义域名编、解码器对域名字符进行向量映射及逆映射,然后将处理好的数据输入对抗网络。接着用生成的样本与真实的数据的检测率作对比实验,以验证生成的对抗样本的有效性。

然而,我们知道 GAN 在自然图像分类处理上取得了较好的成果,但是朴素 GAN 在处理像序列这种离散数据上存在两个问题:一是生成器难以传递梯度更新;二是鉴别器难以评估非常完整的序列。因此由于域名数据的序列性,利用 GAN 生成域名数据应用上的研究较少。

在 GAN 研究应用上,大多数研究更多地关注生成模型,如图像超分辨率[42]、文本到图像合成[43],图像到图像翻译和语音增强[44]等。与其他的 GAN 变体不同,文献[45]将视角放在了鉴别器上,提出了一种基于生成对抗网络的僵尸网络检测增强框架,该网络通过生成器连续生成“假”样本,并扩展标记的数量,以帮助原始模型进行僵尸网络检测和分类。

2.3 基于附加条件的深度学习方法的检测

单纯的深度学习的检测方法在应对越来越智能的 DGA 域名上的表现不佳,为此后面的研究都在深度学习方法的基础上增加了附加条件以提高检测率。

LSTM 在域名很长时,很难学会合理的表达,因此文献[46]提出了一个结合注意机制的 LSTM 模型。该模型将注意力集中在域中更重要的子串并改善域的表达,并在 DGA 检测中实现更好的性能,尤其是对于长域。在二元分类中,其误报率分别低至 1.29% 和假负率 0.76%。陈立皇等[47]也提出了一种基于注意力机制的深度学习模型,不同的是,他们提出一种域名的多字符随机性提取方法,提升了识别低随机 DGA 域名的有效性。Satoh 等[48]通过词法分析和 Web 搜索来估计域名随机性,但该方法对域名长度较短时,无法区分,不包含在字典中的域名会被误判。

为了逃避应用神经网络的检测技术,恶意域名已升级为多个单词的组合来欺骗神经网络的检测。为此,Curtin 等[49]提出了 smash 分数来评估 DGA 域名像英文单词的程度,然后设计了一种新的模型:递归神经网络架构与域注册信息的组合。虽然实验在对 matsnu 和 suppobox 这种看起来像自然域名的家族的检测效果好,但是在那些看起来不像自然域名 DGA 系列表现效果欠佳。

3 结 语

以互联网为依托的经济贸易圈日益增大,网络信息安全成为了近年来关注的热点。以域名欺骗技术为首的网络攻击方式也在不断更新迭代。通过国内外在恶意域名特别是算法生成的域名上的检测研究分析,在恶意域名检测的对抗环境中,恶意软件从简单的利用域名生成算法生成伪随机字符串的域名来和控制与命令服务器连接,发展到为躲避神经网络检测的更智能化的域名,即由英语单词构成的域名。与之对抗的,网络安全研究人员也从手工提取域名字符特征、DNS 流量特征的机器学习方法发展到利用神经网路自动学习特征的转变和改进来提高模型的检测率与性能。

大多数研究是基于域名字符特征的规律来识别合法域名与伪域名。由于 DGA 域名生成算法在不断地更新,新的 DGA 家族变体在不断涌现,特别是目前对由英语单词拼接的域名检测上效果不佳。DGA 家族

因其算法实现不同,不同家族生成的域名数据量不一,导致训练数据过少、识别率低等问题。虽然有研究提出了解决多类不平衡的算法,在一定程度上提高了检测率,但没有从根本上解决数据源的问题。另外现有的检测模型都是基于某一类问题而提出的,例如文献[49]提出的检测模型只针对像 matsnu 这样难以检测的家族,而在一般 DGA 家族的检测表现欠佳。针对以上问题,DGA 域名的检测可以从以下三方面展开研究:

(1) DGA 域名变体的研究　DGA 域名变体生成的域名大多数为了躲避基于字符特征的模型检测,利用英语单词列表随机生成。虽然这类伪域名从马尔可夫模型或是 n-gram 分布的角度来看,都和正常域名没有太大的区别。但是通过观察这些域名可以看出域名的长度与正常域名相差较大,以及这些域名都是由几个毫无关联的单词拼凑而成,因此可以针对这两个角度对这类域名检测。

(2) 恶意域名对抗样本的生成方法研究　现有的伪随机域名生成方式大概分为两类: 一类是通过逆向工程等手段破解 DGA 生成算法,还原 DGA 算法生成伪随机域名,但这类生成的域名大都具有固定模式,在有限数据集上训练的模型缺乏对新的 DGA 变体的预测。另一类就是通过生成对抗网络来生成对抗样本,文献[21]利用 GAN 生成了域名的对抗样本,并用实验证明了对抗样本在充当恶意域名数据及预测未知 DGA 家族上有可观的表现。但由于 GAN 主要是处理连续数据,对离散序列数据的上表现较差,所以针对文本序列数据处理,文献[50]提出了 SeqGAN(Sequence Generative Adversarial) 来解决朴素 GAN 在离散数据处理上的问题,并在语言文本上[51]有不错的表现。相信未来通过 SeqGAN 生成的域名对抗样本会有更高的质量。

因此,研究 DGA 恶意域名对抗样本的生成方法有助于预测未来可能出现的 DGA 变体域名。另外,通过训练恶意域名对抗样本也有益于解决由于 DGA 家族存在数据不平衡导致恶意域名检测识别差的问题。

(3) 恶意域名的检测模型　基于现有的检测模型,如何设计一个高效的检测模型是一个难点,因为伪域名越来越智能化,可以逃避一般的神经网络模型的检测。同时如何将模型设计成为一个既可以作为单独的模型,也可以作为更大的 DGA 检测系统的一部分,还可以包含网络流量,运用到实时的网络安全系统中也是未来的可发展点。

参 考 文 献

[1] Mockapetris P V. Domain Names: Concepts and Facilities [S]. RFC1034, 1987.

[2] Mockapetris P V. Domain Names: Implementation and Specification [S]. RFC1035, 1987.

[3] 郭晓军. 面向 DGA 类型 Bot 的命令控制通信过程研究[J]. 网络安全技术与应用, 2017(8) : 48 - 49.

[4] Amin R M, Ryan J J C H, van Dorp J R. Detecting Targeted Malicious Email [J]. IEEE Security and Privacy Magazine, 2012, 10(3) : 64 - 71.

[5] Choi H, Lee H, Lee H, et al. Botnet Detection by Monitoring Group Activities in DNS Traffic [C]//Proceedings of the 7th IEEE International Conference on Computer and Information Technology. IEEE, 2007: 715 - 720.

[6] 朱迦南. 基于 DNS 日志数据的异常域名检测研究[D]. 成都: 电子科技大学, 2018.

[7] Stone G B, Cova M, Cavallaro L, et al. Your botnet is my botnet: analysis of a botnet takeover [C]//Proceedings of the 16th ACM Conference on Computer and Communications Security. New York: ACM, 2009.

[8] Conficker [OL]. https://en.wikipedia.org/wiki/Conficker.

[9] Damballa. Top-5 most prevalent DGA-based crimeware families [EB/OL]. https://www.damballa.com/downloads/r_pubs/WP_DGAs-in-the-Hands-of-Cyber-Criminals.pdf.

[10] Cryptolocker victims to get files back for free [OL]. BBC News, 2014 - 08 - 06.

[11] Brian Krebs. 'Operation Tovar' Targets 'Gameover' ZeuS Botnet, CryptoLocker Scourge [OL]. Krebs on Security. 6, 2014.

[12] Bader J. The dga of ramnit [OL]. https://johannesbader.ch/2014/12/the-dga-of-ramnit/.

[13] Bader J. The dga of symmi [OL]. https://johannesbader.ch/2015/01/the-dga-of-symmi/.

[14] Geffner J. End-to-end analysis of a domain generating algorithm malware family [C]//RSA Conference 2014, 2014.

[15] Stone-Gross B, Cova M, Cavallaro L, et al. Your Botnet is My Botnet: Analysis of a Botnet Takeover [C]//Proceedings of the 16th ACM conference on Computer and communications security. ACM, 2009: 635 - 647.

[16] Davuth N, Kim S R. Classification of malicious domain names using support vector machine and bi-gram method [J]. International Journal of Security & Its Applications, 2013, 7(1) : 51 - 58.

[17] Yadav E, Reddy A K K, Reddy A L N, et al. Detecting algorithmically generated malicious domain names [C]//Acm Sigcomm Conference on Internet Measurement. DBLP, 2010.

[18] Mowbray M, Hagen J. Finding domain-generation algorithms by looking at length distribution [C]//IEEE International Symposium on Software Reliability Engineering Workshops. USA: IEEE, 2014: 395 - 400.

[19] 王红凯, 张旭东, 杨维永, 等. 基于随机森林的 DGA 域名检测方法: 中国, CN105577660A [P]. 2016 - 05 - 11.

[20] Agyepong E, Buchanan W J, Jones K. Detection of Algo-

rithmically Generated Malicious Domain [C]//International Conference of Advanced Computer Science & Information Technology. 2018.

[21] Wang W, Shirley K. Breaking Bad: Detecting malicious domains using word segmentation [C]//Proceedings of the 9th Workshop on Web 2.0 Security and Privacy(W2SP) , 2015.

[22] Hsu C H, Huang C Y, Chen K T. Fast-flux bot detection in real time [C]//International Conference on Recent Advances in Intrusion Detection. Springer-Verlag, 2010.

[23] Bilge L, Kirda E, Kruegel C, et al. EXPOSURE: Finding Malicious Domains Using Passive DNS Analysis [C]//Proceedings of the Network and Distributed System Security Symposium, NDSS 2011, 2011.

[24] Antonakakis M, Perdisci R. From throw-away traffic to bots: detecting the rise of DGA-based malware [C]//Usenix Conference on Security Symposium. 2012.

[25] Zhou Y L, Li Q S, Miao Q D, et al. DGA-Based Botnet Detection Using DNS Traffic [J]. Journal of Internet Services and Information Security, 2013,3(3/4) : 116 - 123.

[26] Yury Z, Issa K, Ting Y, et al. A Survey on Malicious Domains Detection through DNS Data Analysis [J]. ACM Computing Surveys, 2018, 51(4) : 1 - 36.

[27] Sadegh T, Amine B, Chadi A, et al. Detecting Internet Abuse by Analyzing Passive DNS Traffic: A Survey of Implemented Systems [J]. IEEE Communications Surveys & Tutorials, 2018,20(4) : 3389 - 3415.

[28] Antonakakis M, Perdisci R, Dagon D, et al. Building a Dynamic Reputation System for DNS [C]//Usenix Conference on Security. USENIX Association, 2010.

[29] 赵科军,葛连升,秦丰林,等. 基于 word-hashing 的 DGA 僵尸网络深度检测模型 [J]. 东南大学学报(自然科学版) ,2017,47(S1) : 30 - 33.

[30] Graves A. Sequence Transduction with Recurrent Neural Networks [J]. Computer Science, 2012, 58(3) : 235 - 242.

[31] Graves A. Long Short-Term Memory [M]//Supervised Sequence Labelling with Recurrent Neural Networks. 2012.

[32] Gers F A, Schmidhuber J, Cummins F. Learning to Forget: Continual Prediction with LSTM [J]. Neural Computation, 2000, 12(10) : 2451 - 2471.

[33] Woodbridge J, Anderson H S, Ahuja A, et al. Predicting Domain Generation Algorithms with Long Short-Term Memory Networks [EB]. eprint arXiv: 1611. 00791, 2016.

[34] Yu B, Gray D L, Pan J, et al. Inline DGA Detection with Deep Networks [C]//IEEE International Conference on Data Mining Workshops. IEEE, 2017.

[35] Tran D, Mac H, Tong V, et al. A LSTM based framework for handling multiclass imbalance in DGA botnet detection [J]. Neurocomputing, 2018, 275: 2401 - 2413.

[36] Vinayakumar R, Soman K P, Poornachandran P, et al. Evaluating deep learning approaches to characterize and classify the DGAs at scale [J]. Journal of Intelligent & Fuzzy Systems, 2018, 34(3) : 1265 - 1276.

[37] Goodfellow I J, Pouget-Abadie J, Mirza M, et al. Generative Adversarial Nets [C]//Proceedings of the 27th International Conference on Neural Information Processing Systems-Volume 2. MIT Press, 2014: 2672 - 2680.

[38] Goodfellow I J, Bengio Y, Courville A. Deep learning [M]. The MIT Press, 2016.

[39] Ratliff L J, Burden S A, Sastry S S. Characterization and computation of local Nash equilibria in continuous games [C]//2013 51st Annual Allerton Conference on Communication, Control, and Computing(Allerton) . IEEE, 2013.

[40] Anderson H S, Woodbridge J, Filar B. DeepDGA: Adversarially-Tuned Domain Generation and Detection [C] //Acm Workshop on Artificial Intelligence & Security. ACM, 2016.

[41] 袁辰. 基于对抗模型的恶意域名检测方法的研究与实现 [D]. 北京: 北京建筑大学,2018.

[42] Ledig C, Theis L, Huszar F, et al. Photo-Realistic Single Image Super-Resolution Using a Generative Adversarial Network [EB]. Eprint arXiv: 1609. 04802, 2016.

[43] Reed S, Akata Z, Yan X, et al. Generative adversarial text to image synthesis [C]//International Conference on International Conference on Machine Learning. 2016.

[44] Isola P, Zhu J Y, Zhou T, et al. Image-to-Image Translation with Conditional Adversarial Networks [EB]. Eprint arXiv: 1611. 07004, 2016.

[45] Yin C, Zhu Y, Liu S, et al. An enhancing framework for botnet detection using generative adversarial networks [C]// International Conference on Artificial Intelligence & Big Data. 2018.

[46] Chen Y, Zhang S, Liu J, et al. Towards a Deep Learning Approach for Detecting Malicious Domains [C]//IEEE International Conference on Smart Cloud(SmartCloud) , IEEE, 2018.

[47] 陈立皇,程华,房一泉. 基于注意力机制的 DGA 域名检测算法 [J]. 华东理工大学学报(自然科学版) ,2019,45(3) : 478 - 485.

[48] Satoh A, Nakamura Y, Nobayashi D, et al. Estimating the Randomness of Domain Names for DGA Bot Callbacks [J]. IEEE Communications Letters, 2018,22(7) : 1378 - 1381.

[49] Curtin R R, Gardner A B, Grzonkowski S, et al. Detecting DGA domains with recurrent neural networks and side information [EB]. Eprint arXiv: 1810. 02023, 2018.

[50] Yu L, Zhang W, Wang J, et al. SeqGAN: Sequence Generative Adversarial Nets with Policy Gradient [C]//Proceedings of the Thirty-First AAAI Conference on Artificial Intelligence(AAAI-17) . 2017: 2852 - 2858.

[51] Pascual S, Bonafonte A, Serrà J. SEGAN: Speech Enhancement Generative Adversarial Network [EB]. Eprint arXiv: 1703. 09452, 2017.