站连续 3 次排名前 1 万且在 *JSERNET_DNS* 中出现过的域名,同时去除曾经在黑名单中出现过的域名.合法域名集一共包含 5 438 个二级域名对象,其中包含 161 个 CDN 二级域名对象.

恶意域名集 *Malicious_Domain_Set*:选取僵尸网络[23,24]、钓鱼网站[25]、垃圾邮件[26]和恶意软件[23,24]等黑名单中出现过、并且在 *JSERNET_DNS* 中出现过的域名.为保证恶意样本集的干净,进一步删除 Alex 网站 3 次排名前 100 万的域名.恶意域名集一共包含 5 533 个二级域名对象,其中,僵尸网络二级域名对象 2 846 个、钓鱼网站二级域名对象 663 个、垃圾邮件二级域名对象 937 个、其他恶意软件二级域名对象 1 087 个.

3.2 准确率

对于 DNS 流量检测算法而言,设计和实现的关键在于检测所依据的测度和采用的分类算法.目前,关于分类算法的研究无论是有监督的机器学习算法还是无监督的聚类或者分类算法都相当成熟.因而,测度的选取成为当前各 DNS 流量检测算法关注的重点.表 1 中,与本文 DAOS 系统在检测目标、数据源和实验环境上相似的工作有 Notos[19],Exposure[20,21]和 Kopis[15],它们都是针对上层 DNS 流量的通用域名检测算法,都使用了域名访问活动特征和资源记录特征,此外,3 项先前的工作还增加了域名字面特征和黑名单证据特征.

Table 1 The list of DNS traffic detection algorithms

表 **1** DNS 流量检测算法列表

项目/人名	测度集(括号中的数字代表具体测度个数)	检测算法
Notos[19]	①域名字面特征(17);②资源记录 *A* 特征(18);③黑名单证据(6).	有监督机器学习
Exposure[20,21]	①域名字面特征(2);②资源记录 *A* 及 *TTL* 特征(17);③DNS 查询时间分布(7).	有监督机器学习(C4.5)
Kopis[15]	①DNS 查询者 RDNS 的空间分布及用户规模(13+10);②黑名单证据(9).	有监督机器学习(随机森林)
DAOS(本文)	①依赖性,即,DNS 查询用户的空间、时间分布特征(7); ②使用位置,即,资源记录 *A*,*NS* 及 *TTL* 特征(6).	有监督机器学习(多分类器)

DAOS 从依赖性和使用位置两个方面,一共提出 13 个测度.为了证明该测度集的重要性,本文基于相同的标准数据集和分类算法,分别选用 4 项工作中不同的测度集 C_1~C_4,比较它们的检测准确率,具体实验过程如下:首先,选取标准域名集 *Good_Domain_Set* 和 *Malicious_Domain_Set* 中标记过合法/恶意的二级域名作为观测对象集 O;其次,基于 DNS 数据 *JSERNET_DNS* 和 NetFlow 数据 *JSERNET_NETFLOW*,根据文献中测度集 C_i 的具体定义,统计每个二级域名对象的测度组;而后,统一使用单个 C4.5 分类器对标记过的二级域名对象集进行分类,有监督的机器学习方法需要提供训练集和测试集,本文采用十字交叉验证法,将域名对象集 O 划分成 10 份,每次选 9 份训练 1 份测试,最终得到的检测结果为这 10 次的平均结果;最后,从检测准确率、假阳性和假阴性 3 个方面比较 4 个测度集相应的检测结果.这里有两点需要说明:(1) 只关注域名访问活动特征和资源记录特征两方面的测度,由于域名字面特征检测精度不高,证据特征过多依赖外界黑名单的正确性,DAOS 现阶段并未考虑这两方面的特征测度,但是下阶段仍然可以增加它们作为辅助测度,因此算法比较时,出于公平性的考虑,Notos,Exposure 和 Kopis 这 3 项工作也不计算域名字面特征和黑名单证据特征;(2) 多分类器虽然在时间开销上优于单分类器(降低 20%),但是在检测准确率上相差不大(准确率只有 0.2%的增加),因此,该节对于所有测度集都使用单个 C4.5 分类器进行分类.

如图 14 所示,DAOS 虽然只使用了 13 个测度,却具有最高的检测精度(准确率 93.7%,假阳性 1.7%,假阴性 4.6%).为了探查其原因,本文基于表 1 给出的测度集进行分析.

- 首先,Notos 关注资源记录 *A* 的地理位置分布和逻辑归属分布,但是忽略了访问活动特征;而 Kopis 观测域名访问活动中,DNS 查询者“RDNS”的空间分布和用户规模,却未使用资源记录特征.与之相比,DAOS 结合了域名的访问活动特征和资源记录特征,因而检测精度具有较大幅度的提升:比 Notos 准确率提高 9.5%,假阳性降低 7.4%,假阴性降低 2.1%;比 Kopis 准确率提高 8.3%,假阳性减少 5.6%,假阴性也降低 2.7%;
- 其次,Exposure 虽然也综合了访问活动特征和资源记录特征,但是只观察资源记录 *A* 以及 *TTL* 的空间分布特征,只测量访问活动中 DNS 查询的时间分布特征;而 DAOS 全面分析了资源记录 *A*,*NS* 以及 *TTL*

的时间和空间分布特征,并借助流数据间接测量用户访问活动的时间和空间分布特征;

- 另外,实际观察发现:平均每个域名的查询用户数有 340 个,而 RDNS 数只有 210 个.即,从用户视角可以比 RDNS 视角更好地观测访问活动特征.因此,DAOS 比 Exposure 拥有更高的检测精度(准确率上升 2.8%,假阳性减少 2.8%,假阴性不变);
- 最后,值得说明的是:Notos 使用了 18 个测度,Exposure 使用了 24 个测度,Kopis 使用了 23 个测度;而本文通过使用测度选择算法 CFS,只选取了 13 个测度,大概只有它们的一半.

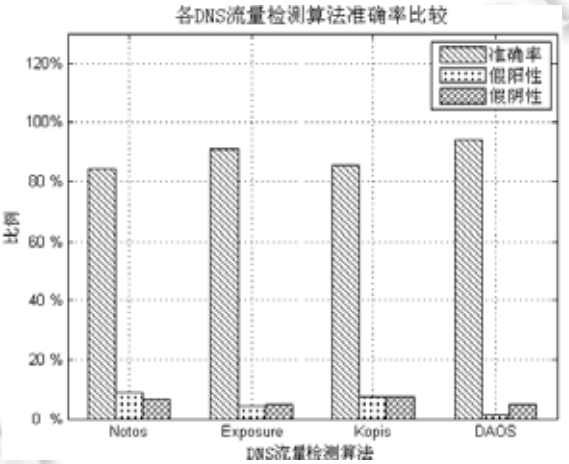


Fig.14 Accuracy comparison of these DNS traffic detection algorithms

图 14 各 DNS 流量检测算法准确率比较

实验结果表明:本文从依赖性和使用位置两个方面提出的两组特征测度,要优于现有检测算法所使用的域名访问活动特征测度和资源记录特征测度.因而,可以改进和补充现有检测算法中的测度,提高主干网 DNS 流量实时检测的精度.

3.3 影响因子

恶意域名的识别,需要事先观察和统计该域名对象的 DNS 活动特征.一般而言,观测的时间越长,检测的准确率越高;观测的时间越短,检测的准确率也会相对下降.即,准确率和观测时间长度此消彼长.如何根据用户对检测实时性的需求选择两者间合适的平衡点,是需要研究的一个重点.

本节重复第 3.2 节中的实验过程,保持数据集、测度集(13 个测度)和多分类算法不变,调节测度统计的时间窗口长度(2 小时、4 小时、8 小时、16 小时、1 天、2 天、1 星期),即,每个域名对象需要持续观测的时间长度.而后,同样使用十字交叉验证法,从准确率、假阳性和假阴性这 3 个方面评估算法的检测精度.如图 15 所示:随着观测时间窗口长度的增加,算法的检测准确率确实有所增加,但增幅不大;与此同时,假阳性和假阴性也稍有减少.

当观测时间长度从 2 小时增加到 1 星期后,检测准确率从 90.5%上升到 93.9%(增加 3.4%),假阳性从 2.9%下降到 1.3%(减少 1.6%),假阴性也从 6.6%下降到 4.8%(减少 1.8%).结果表明:DAOS 具有较高的实时检测能力,经过 2 个小时的实时监测,就能达到 90.5%的准确率.若用户期望获得较高的准确率,则需要适当延长域名观测的时间长度.

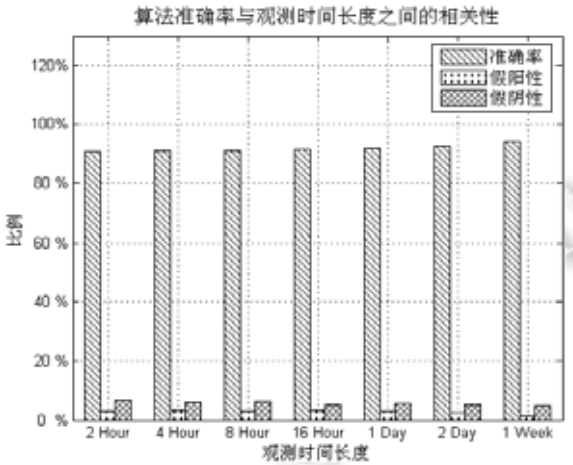


Fig.15 Correlation between theobservation intervaland the algorithm's detection accuracy

图 15 算法准确率与观测时间长度之间的相关性

3.4 实用性测试

为了验证 DAOS 检测算法的实用性,本文在中国教育科研网江苏省网边界的一个接入点路由器上,实时采集流经的 DNS 流量和 NetFlow 流记录数据,同时转发给后端 DAOS 检测服务器.DAOS 系统运行前,设定时间窗口长度为 2 小时,同时选用第 3.1 节中的两个标准域名列表 *Good_Domain_Set* 和 *Malicious_Domain_Set* 作为最初的训练样本集.DAOS 实际运行过程中包含 3 个重要环节:首先,当标准域名列表发生变更时,系统在接下来的一个时间片内,需要重新统计标准域名列表中所有标记域名的测度值,生成新的训练样本集;其次,DAOS 维护着一张二级域名列表,当出现新的二级域名对象时,才统计其测度值,并使用多分类器和训练样本集进行分类;最后,系统定期从检测结果中,选择置信度较大的二级域名对象,更新标准域名列表,实现 DAOS 算法的自学习.

从 2015 年 6 月 1 日~6 月 30 日,平均每天新出现的二级域名对象有 2.89 万个,而 DAOS 每天检测到的可疑二级域名对象有 2 852 个,一个月共发现 8.57 万个可疑域名对象.为了验证检测结果的准确率,采用抽样检测的方法,通过统计抽样样本的准确率来评估整个检测结果集的准确率.本文选用千分之一的抽样比例,从可疑域名对象集中随机抽出 857 个二级域名样本,通过查询在线黑名单[23−26]和可疑文件分析服务网站 VirusTotal[29],或者手工验证的方法确定样本类别.其中,出现在钓鱼网站[23]中的域名有 1 个,出现在恶意域名黑名单[23,24]中的域名有 3 个,DGA 域名有 22 个.VirusTotal 确定为恶意的域名有 31 个,安全的域名有 53 个.另外,有 179 个域名未经注册,有 137 个域名所辖网站包含色情、赌博和恶意销售等内容,75 个域名所辖网站无效、过期或者正在维护中,224 个域名在一个月内的活跃时间长度不足 1 小时,还有 132 个域名无法进行确认.

此外,针对上述 75 个无效、过期和正在维护中的域名网站进行追踪分析:首先,这 75 个域名网站在原始 DNS 数据中存在正确的解析响应报文,能够提取出域名映射的 IP 地址;同时,在流测量数据中也可以找到这些 IP 地址的通信会话信息,说明它们当时都活跃着.但是现在进行手工检测发现,这些域名网站都不再提供正常服务.其中,2 个网站长期处于维护中,47 个域名已经过期超过 3 个月;剩余 26 个网站无响应.通常情况下,一个合法网站是不会停止服务、不续费域名以及长期进行维护的.为了验证这一假设,本文关注 2015 年 6 月 Alex 网站排名前 2 万名中的 1 万个网站(绕过知名网站),发现其中 96.5%的网站在 2016 年 9 月还活跃着.也就是说,这 75 个域名网站如果是合法网站的话,则 1 年后至少应该有 72 个网站能够正常提供服务.另一方面,恶意网站存活时间都不长.如图 5 所示,生命周期长度超过 85 天的恶意域名不超过 5%.换句话说,这 75 个域名网站如果是恶意网站的话,则 1 年后最多只有 4 个网站还能够正常提供服务.最后,综合两方面的假设分析可知,这 75 个域名网站是恶意网站,置信度超过 95%.

综上所述,若除去无法确认的 132 个域名,则剩余 725 个域名.其中,能够确认的安全域名有 53 个,即误报率至少为 7.3%.而能够确认的恶意域名有 269 个(包括 4 个黑名单域名,22 个 DGA 域名,31 个 VirusTotal 确认的恶

意域名,137 个色情、赌博和恶意销售网站,75 个无效、过期和正在维护中的网站).考虑到合法域名的生命周期长度基本上都超过 1 天,且正常情况下,未经注册的域名是不应该出现在 DNS 报文中,若把 224 个活跃时间长度不足 1 小时的域名以及 179 个未经注册的域名也看成恶意域名,则 DAOS 检测准确率可以达到 92.7%.这与第 3.3 节中统计时间窗口设定为 2 小时的准确率 90.5%和误报率 2.9%相符,说明 DAOS 在实际运行时也能保证较高的实时性和检测精度.

4 总 结

为了保障 ISP 主干网运行安全,本文实时检测流经主干网边界的 DNS 交互报文,研究适用于主干网环境的上层 DNS 流量检测算法.

首先,借助主干网边界采集的流测量数据,间接获取域名与终端用户间的相互关系,来弥补 DNS 缓存机制屏蔽终端用户解析请求的不足;并在此基础上提出域名依赖性的概念,通过测量用户的空间规模和活跃度,从用户角度观察域名的外在使用情况;而后,为了提高算法的检测精度,观察资源记录 *A* 和 *NS* 中隐藏的域名使用位置信息,从域名自身角度关注其内部资源部署情况.在传统测量 IP-Flux 和 NS-Flux 特征的基础上,通过分析 CND 和 FFSN 内在的差异性,提出一组新的测度以识别混入 FFSN 中的 CDN;再者,主干网 DNS 流量检测需要对海量的域名对象进行实时或准实时地 DPI 检测.为了提高算法的检测效率,一方面按照相同的二级域名将域名划分成组,以组为单位进行检测;另一方面使用 CFS 算法选择最优测度集,并基于两个测度集提出多分类器的检测模型;最后,为了兼顾检测算法的及时性和准确率,同时关注域名的当前活动特征和相关对象的历史活动行为,使用较长时间的历史相关数据来弥补当前时间窗口长度较短导致数据不足的问题.

实验观察发现:对于某个域名对象,在不依赖于先验知识的前提下,经过两个小时的 DNS 活动监测,检测准确率可以达到 90.5%,假阳性和假阴性分别为 2.9%和 6.6%.若用户期望获得更高的检测精度,持续监测一周,准确率可以提升到 93.9%,假阳性和假阴性也能减少到 1.3%和 4.8%.同时,观察发现:在不依赖域名字面特征和黑名单先验知识的前提下,本文的 DAOS 算法与现有面向上层 DNS 流量的通用域名检测算法 Notos,Exposure 和 Kopis 相比,虽然使用最小数目的测度集,但是具有最高的检测精度.最后,在实用性测试中,当统计时间窗口设定为 2 小时时,DAOS 也能获得 92.7%的准确率和 7.3%的误报率.

综上所述,本文提出的依赖性和使用位置测度组以及多分类器模型,可以有效地用于主干网环境下的实时 DNS 流量监测;也可以作为现有算法的补充,提高它们的检测精度.

References:

[1] Levchenko K, Pitsillidis A, Chachra N, Enright B. Click trajectories: End-to-End analysis of the spam value chain. In: Butler K, ed. Proc. of the IEEE Symp. on Security and Privacy. IEEE, 2011. 431−446. [doi: 10.1109/SP.2011.24]

[2] Bot traffic report. 2015. https://www.incapsula.com/blog/bot-traffic-report-2015.html

[3] APWG phishing activity trends report. 2016. http://www.antiphishing.org/resources/apwg-reports/

[4] Schonewille A, Helmond DJV. The domain name service as an IDS [MS. Thesis]. University of Amsterdam, 2006. http://staff.science.uva.nl/~delaat/snb-2005-2006/p12/report.pdf

[5] Chatzis N, Popescu-Zeletin R. Flow level data mining of DNS query streams for email worm detection. In: Corchado E, Zunino R, Gastaldo P, Herrero A, eds. Proc. of the Int'l Workshop on Computational Intelligence in Security for Information Systems (CISIS 2008). Berlin, Heidelberg: Springer-Verlag, 2009. 186−194. [doi: 10.1007/978-3-540-88181-0_24]

[6] Chatzis N, Popescu-Zeletin R. Detection of email worm-infected machines on the local name servers using time series analysis. Journal of Information Assurance and Security, 2009,4(3):292−300.

[7] Chatzis N, Popescu-Zeletin R, Brownlee N. Email worm detection by wavelet analysis of DNS query streams. In: Dasgupta D, Zhan J, eds. Proc. of the IEEE Symp. on Computational Intelligence in Cyber Security (CICS 2009). Nashville: IEEE, 2009. 53−60. [doi: 10.1109/CICYBS.2009.4925090]

[8] Chatzis N, Brownlee N. Similarity search over DNS query streams for email worm detection. In: Awan I, ed. Proc. of the 2009 Int'l Conf. on Advanced Information Networking and Applications (AINA 2009). Bradford: IEEE, 2009. 588−595. [doi: 10.1109/AINA.2009.132]

[9] Choi H, Lee H, Kim H. Botnet detection by monitoring group activities in DNS traffic. In: Wei D, ed. Proc. of the 7th IEEE Int'l Conf. on Computer and Information Technology (CIT 2007). Fukushima: IEEE, 2007. 715−720. [doi: 10.1109/CIT.2007.90]

[10] Choi H, Lee H, Kim H. BotGAD: Detecting botnets by capturing group activities in network traffic. In: Bosch J, Clarke S, eds. Proc. of the 4th Int'l ICST Conf. on Communication System Software and Middleware (COMSWARE 2009). Dublin: ACM Press, 2009. 2–2. [doi: 10.1145/1621890.1621893]

[11] Jiang N, Cao J, Jin Y, Li LE, Zhang ZL. Identifying suspicious activities through DNS failure graph analysis. In: Gunes MH, ed. Proc. of the 18th IEEE Int'l Conf. on Network Protocols (ICNP 2010). Kyoto: IEEE, 2010. 144–153. [doi: 10.1109/ICNP.2010.5762763]

[12] Yadav S, Reddy ALN. Winning with DNS failures: Strategies for faster botnet detection. In: Rajarajan M, Piper F, eds. Proc. of the Security and Privacy in Communication Networks. London: Springer-Verlag, 2012. 446–459. [doi: 10.1007/978-3-642-31909-9_26]

[13] Lee J, Kwon J, Shin HJ, Lee H. Tracking multiple C&C botnets by analyzing DNS traffic. In: Fahmy S, ed. Proc. of the 6th IEEE Workshop on Secure Network Protocols (NPSec 2010). Kyoto: IEEE, 2010. 67–72. [doi: 10.1109/NPSEC.2010.5634445]

[14] Lee J, Lee H. GMAD: Graph-Based malware activity detection by DNS traffic analysis. Journal Computer Communications, 2014, 49(12):33–47. [doi: 10.1016/j.comcom.2014.04.013]

[15] Antonakakis M, Perdisci R, Lee W, Li NV, Dagon D. Detecting malware domains at the upper DNS hierarchy. In: Wagner D, ed. Proc. of the 20th USENIX Conf. on Security (SEC 2011). San Francisco: USENIX, 2011. 27–27.

[16] Thomas M, Mohaisen A. Kindred domains: Detecting and clustering botnet domains using DNS traffic. In: Chung CW, eds. Proc. of the 23rd Int'l Conf. on World Wide Web. New York: ACM Press, 2014. 707–712. [doi: 10.1145/2567948.2579359]

[17] Holz T, Gorecki C, Rieck K, Freiling FC. Measuring and detecting fast-flux service networks. Network and Distributed System Security Symp., 2008,1(5):487–492.

[18] Caglayan A, Toothaker M, Drapeau D, Burke D, Eaton G. Real-Time detection of fast flux service networks. In: Walter E, ed. Proc. of the 2009 Cybersecurity Applications & Technology Conf. for Homeland Security (CATCH 2009). Washington: IEEE, 2009. 285–292. [doi: 10.1109/CATCH.2009.44]

[19] Antonakakis M, Perdisci R, Dagon D, Lee W, Feamster N. Building a dynamic reputation system for DNS. In: Goldberg I, ed. Proc. of the 19th USENIX Conf. on Security (SEC 2010). Berkeley: USENIX, 2010. 18–18.

[20] Bilge L, Kirda E, Kruegel C, Balduzzi M. Exposure: Finding malicious domains using passive DNS analysis. In: Nishide T, ed. Proc. of the 18th Annual Network and Distributed System Security Symp. (NDSS 2011). Virginia: Internet Society, 2011. 195–211.

[21] Bilge L, Sen S, Balzarotti D, Kirda E, Kruegel C. Exposure: A passive DNS analysis service to detect and report malicious domains. ACM Trans. on Information and System Security (TISSEC), 2014,16(4):14–14. [doi: 10.1145/2584679]

[22] Alexa. 2015. http://www.alexa.com/topsites/

[23] DNS-BH malware domain blocklist. 2015. http://www.malwaredomains.com

[24] Malware domain list. 2015. http://www.malwaredomainlist.com

[25] PhishTank. 2015. http://www.phishtank.com

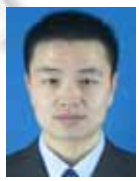
[26] Blacklist provided by joewein.net (JWSDB). 2015. http://joewein.net/spam/blacklist.htm

[27] Krishnamurthy B, Wills C, Zhang Y. On the use and performance of content distribution networks. In: Paxson V, ed. Proc. of the 1st ACM SIGCOMM Workshop on Internet Measurement (IMW 2001). New York: ACM Press, 2001. 169–182. [doi: 10.1145/505202.505224]

[28] Hall MA. Correlation-Based feature subset selection for machine learning [Ph.D. Thesis]. Hamilton: University of Waikato, 1999.

[29] VirusTotal. 2016. https://www.virustotal.com

张维维(1984－),男,江苏南通人,博士生,主要研究领域为网络安全.



刘尚东(1979－),男,博士生,CCF 专业会员,主要研究领域为网络安全.

龚俭(1957－),男,博士,教授,博士生导师,CCF 高级会员,主要研究领域为网络管理,网络安全.

胡晓艳(1985－),女,博士,讲师,CCF 专业会员,主要研究领域为网络管理,下一代互联网.