计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2022,31(3):129−135 [doi: 10.15888/j.cnki.csa.008367]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

DNS 的 RPZ 安全防护系统的构建、配置与验证①

戴云伟[1], 沈春苗[2]

[1](江苏省未来网络创新研究院, 南京 211111)
[2](南京师范大学 商学院, 南京 210023)
通信作者: 戴云伟, E-mail: icesandals@qq.com

摘　要: DNS (domain name system) 作为网络的重要基础服务设施, 是终端访问互联网必要的一环. 近年来, 越来越多尝试将用户通过 DNS 系统引入恶意服务器的攻击, 对互联网安全产生重要威胁. 防范与化解针对恶意域名或 IP 的访问, 如钓鱼网站、垃圾邮件、勒索软件、色情网站等, 无论是对于运营商还是网络监管机构都具有重要的现实意义. 论文阐述 RPZ (response policy zones) 的工作原理, 构建 DNS 的 RPZ 安全防护系统, 再进行相关核心软件的配置, 最后通过实验验证, 检验系统针对恶意域名和 IP 的防护效果.

关键词: DNS; RPZ; 域名攻击; 互联网安全

引用格式: 戴云伟,沈春苗.DNS 的 RPZ 安全防护系统的构建、配置与验证.计算机系统应用,2022,31(3):129–135. http://www.c-s-a.org.cn/1003-3254/8367.html

Construction, Configuration and Verification of DNS RPZ Protection System

DAI Yun-Wei[1], SHEN Chun-Miao[2]

[1](Jiangsu Future Networks Innovation Institute, Nanjing 211111, China)
[2](Business School, Nanjing Normal University, Nanjing 210023, China)

Abstract: As an important network infrastructure for service, the domain name system (DNS) is a necessary link for terminals to access the Internet. In recent years, more and more attempts have been made to trick users into malicious servers through DNS, posing a huge threat to Internet security. It is of great practical significance for both operators and network regulators to prevent and resolve access to malicious domains or IPs, including phishing websites, spam, ransomware, and pornographic websites. Therefore, this study describes the working principle of response policy zones (RPZ), builds a DNS RPZ security protection system, and then configures the related core software. The experiments are conducted on the system to verify the protection effect against malicious domains and IPs.

Key words: domain name system (DNS); response policy zones (RPZ); domain attack; Internet security

1　引言

DNS[1,2] 是互联网最重要、最基本的服务之一, 提供了方便记忆的域名与复杂的 IP 地址的相互映射. 万维网发展得如此迅速, 离不开 DNS 系统的广泛应用. 然而, 随着互联网技术的不断发展, DNS 因其协议设计的脆弱性, 成为违法分子发动网络攻击的跳板, 使互联网在可用性、安全性及完整性等方面受到严重威胁. 如何提供 DNS 防护成为 ISP (Internet service provider) 及监管机构的重要关切.

根据 EfficientIP 和 IDC 共同研究发布的“IDC 2020 Global DNS Threat Report”显示, 2019 年有 79% 的组织受到 DNS 攻击[3]. DNS 不仅仅是黑客的攻击的目标, 同时也是其实施攻击的重要手段. 最常见的 DNS 攻击类型包括[4]:

① 基金项目: 国家自然科学基金青年项目 (71903096)
收稿时间: 2021-05-13; 修改时间: 2021-06-14; 采用时间: 2021-06-24; csa 在线出版时间: 2022-01-24

(1) DNS hijacking, 域名劫持. 此类攻击手段有多种, 如攻击者通过攻击域名注册系统, 获得修改域名对应记录的权限. 一旦域名被劫持, 攻击者就可以通过篡改记录, 将用户引导至病毒网址、钓鱼网站等, 从而获得用户的敏感数据. 2010 年百度境外的 DNS 服务器被攻击, 攻击者修改了解析记录, 导致长达 11 小时的服务中断[5,6].

(2) DNS flood attack, 泛洪攻击. 这是最基本的 DNS 攻击类型之一, 在这种分布式拒绝服务 (DDoS) 中, 攻击者将攻击 DNS 服务器. 其主要目的为造成服务器过载, 使其无法继续为正常的 DNS 请求提供服务[7,8].

(3) Distributed reflection denial of service, 分布反射式拒绝服务 (DRDos). DDoS 中的一种, 此类攻击最终目的就是使用大量数据包或者大量占用带宽的请求使设备或者网络过载, 实现拒绝服务的目的. DRDos 相较于 DDoS 的攻击更为致命, 该类攻击将请求发送至正常的 DNS 服务器, 但是源地址为被攻击者的, 如此, 被攻击者将收到大量的无效响应报文, 从而资源被耗尽[9,10].

(4) Cache poisoning, 缓存投毒攻击, 最常见的 DNS 攻击之一, 一般利用系统漏洞, 攻击者尝试向 DNS 服务器的缓存中注入恶意数据, 以达到其将用户重定向到另一个远程服务器的目的[11,12].

(5) DNS tunneling, DNS 隧道攻击, 这是一种网络攻击, 通过在 DNS 响应和请求中包含恶意的应用数据, 当与 DNS 服务器建立链接以后, 攻击者向服务器传递恶意数据, 以获得控制权限[13,14].

针对 DNS 的攻击, 不少相关文献进行了研究, 如王文通等提到的从协议增强、系统增强、检测监控和去中心化的域名系统 4 个方面来应对[15]. 郝帅等针对反射放大型 DDoS 攻击, 同时对 DNS、SNMP、SSDP、NTP、Memcache 和 CLDAP 这 6 种协议存在的安全漏洞进行分析, 从受害者和服务器两个角度给出防范策略[16]. Cooney 推荐使用 CISA (cybersecurity and infrastructure security agency) 安全措施以缓解受到攻击的威胁[17] 等.

2017 年 5 月, WannaCry 蠕虫通过 MS17-010 漏洞在全球范围内感染了大量设备, 该蠕虫感染计算机后会向设备中植入勒索病毒, 导致设备中大量文件被加密. 受害者设备被黑客锁定后, 需要支付的一定价值的比特币才可解锁[18]. 而这一病毒有个关于域名的隐藏开关, 通过 RPZ 技术对特定域名的访问进行干预, 即可遏制病毒的进一步大规模传播.

现今, 无法通过某一种技术手段解决所有攻击类型, 结合 RPZ 技术设计的防护系统在一定程度上可以防范和化解域名劫持、以及不法分子试图通过 DNS 系统, 将用户引至恶意站点. 除此之外, 系统还可以辅助 ISP 控制未备案等不合法的站点被访问.

2 防护系统需求分析

目前, 多数 ISP 或者银行、电力等大型企业组织并没有部署通过干预域名解析来提升 DNS 安全的系统, 少数可能部署了域名黑名单解析功能. 但是基本上都没有部署自动化的解析干预系统, 结合运营商或者大型组织的实际情况, 整个安全防护系统需要满足以下必要功能.

(1) DNS 递归解析功能, 最核心的功能, 需要满足 ISP 用户或者大型组织内部递归解析请求, 该功能一般需要从 13 个 DNS 根服务器开始, 递归访问至授权服务器, 获取 DNS 响应结果, 并进行短时间的缓存.

(2) DNS 缓存功能, 业内常见做法是将缓存与递归分开, 该模块直接接受用户请求, 优先查找本模块内部缓存, 以响应用户. 无缓存的情况下, 会将请求转发给 DNS 递归服务器. 一般情况下, 多台缓存设备会转发至一台递归设备.

(3) DNS 安全防护功能, 当系统检测到有恶意的域名请求时, 或者 DNS 响应报文中含有恶意的 IP 地址时. 需要能够根据用户的设定返回特定结果, 如返回 NXDOMAIN, 或者返回特定的 IP 地址, 将用户重定向至警告页面.

(4) 综合管理平台, 常规功能包含设备性能监控、告警监控等. 核心功能要求协调所有设备之间的信息交互, 进行统一管理, 如数据收集、控制指令下发、控制指令反馈等.

3 DNS RPZ 技术原理

与传统的提供 DNS 解析功能的系统相比, 构建 RPZ 安全防护系统, 极大提高整个系统拦截恶意域名或者 IP 地址的效率.

RPZ 由 Paul Vixie 主导的 ISC (internet systems consortium) 机构于 2010 年提出, 目前是 IETF (Internet engineering task force) 的互联网草案[19]. 是一种针对

DNS 的网络安全解决方案, 可以防止互联网用户和系统访问到已知的恶意域名或者 IP, 可以有效地预防威胁发生, 通过阻止访问受感染或者恶意的站点, 进而阻断进一步的安全威胁. 能够主动检测到已被感染的用户, 并且防止病毒进一步扩散. 图 1 为用户通过常用的通讯软件收到包含恶意信息的链接场景下, RPZ 参与的工作过程.

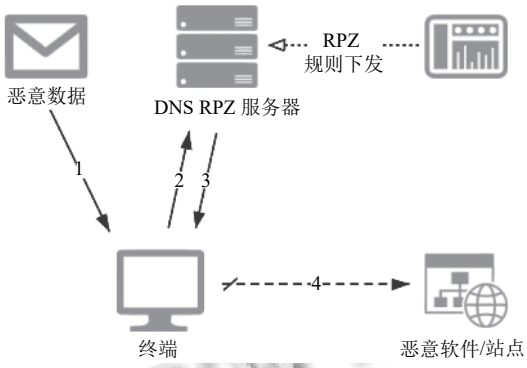

图 1 DNS RPZ 工作原理图

(1) 不法分子通过电子邮件或即时通讯软件, 将包含恶意软件或者域名的链接发送给用户.

(2) 用户点击收到的链接, 终端设备首先要做的就是进行 DNS 解析. 将 DNS 请求发送至 DNS 解析服务器.

(3) 具有 RPZ 功能的 DNS 解析服务器, 向其他系统同步 RPZ 规则, 判断当前请求解析的域名是否为恶意域名, 或者解析到的 IP 是否为恶意 IP, 若是, 则会进行干预, 干预的结果则是由用户下发的规则决定的.

(4) 在 RPZ 的防护下, DNS 请求无法获得正常结果, 或者获得由 ISP 提供的警告页面结果, 从而成功阻止了用户访问恶意站点.

图 1 中 RPZ 规则下发阶段的数据, 一般由 ISP 通过多种方式进行收集, 包括但不限于恶意域名检测系统、被举报的赌博网站、色情网站、钓鱼网站以及其他被监管机构禁止的站点.

4 防护系统构建

整个系统涉及多种类型设备, 核心 DNS 解析功能需要满足负载均衡设计. 系统总体结构如图 2 所示, 系统最基本组成部分共包含 6 个子系统, 以及各子系统所需最小组成模块. 根据实际情况, 可添加其他辅助系统, 如防火墙、入侵检测系统等. 子系统之间数据传递、控制指令下发都是通过局域网完成, 只有缓存系统和递归系统需要接入互联网.

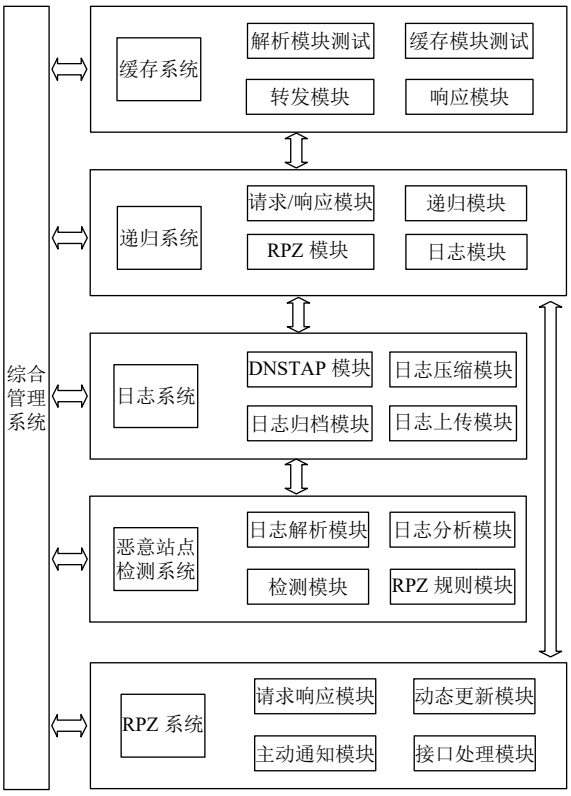

图 2 系统总体架构图

4.1 缓存系统

负责解析用户的 DNS 请求并完成响应, 当接受到请求后, 会首先查找本地系统是否已缓存过相应记录且 TTL 尚未过期, 对于无法利用已有缓存完成响应的情况下, 将请求转发至递归服务器.

4.2 递归系统

一般只接受特定缓存服务器的请求, 不直接对终端用户开放, 可以具备一定的缓存能力, 但是缓存时间不宜过长. 正常情况下, 会从根服务器开始进行递归处理, 直至到达授权服务器, 获取到用户所需数据. RPZ 模块就是工作在该系统中.

4.3 日志系统

负责接收来自递归系统的 DNS 请求响应日志, 进行归档以便后续审计, 同时负责将日志发送至其他系统.

4.4 恶意站点检测系统

该系统接受到 DNS 日志后, 需要进行分析, 当前针对恶意域名的检测有不少相关论文, 也有部分公司有偿提供检测到的恶意域名或者设备的地址, 如 DissectCyber 提供的 RPZone.us 服务.

4.5 RPZ 系统

负责存储所有规则, 提供接口供其他系统动态更

新规则, 更新后, 系统会通知递归系统获取最新的规则数据. 递归系统本身也会定期查询是否有规则数据变更.

4.6 综合管理系统

负责所有系统的运行配置、监控、规则下发, 向其他外部系统提供接口等. 典型的应用就包括, 恶意站点检测系统一旦检测到恶意域名或者 IP, 会向该系统提供的接口上报, 由管理系统向 RPZ 系统下发规则.

5 核心信息交互

RPZ 的规则可以在请求到来之前进行预置, 也可以通过前序的日志进行分析检测得出. 针对第一种预置的情况, 当请求到达时, 在递归系统就会被成功拦截. 第二种场景下, 前序请求会拿到恶意域名结果, 但是后续请求会被拦截.

图 3 为系统工作时, 某特定场景下信息交互的时序图示例. 实际工作时, 因系统分布式部署, 可能存在的网络数据丢失, 导致接口调用超时, 接口需要提供重试、异常处理的能力.

6 配置及实验验证

实验所使用的系统为 Linux 系统 (CentOS Linux release 7.8.2003), 使用 NSD 4.3.6 作为 RPZ 系统的核心软件, 使用 Unbound 1.13.1 作为缓存系统和递归系统的核心软件. 所使用的网络拓扑图, 如图 4.

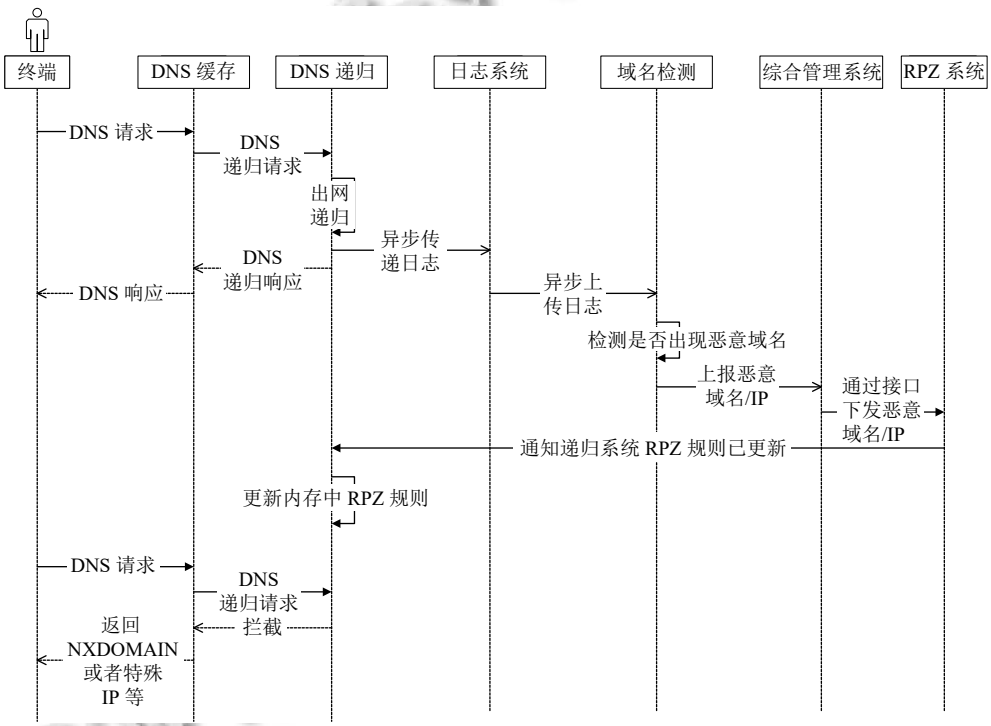

图 3 工作时序图

6.1 系统配置

递归服务器内网地址配置为 172.171.1.16/24. RPZ 服务器内网地址配置 172.171.1.16/24. 硬件 CPU 为 Intel(R) Xeon(R) CPU E3-1225 v3 @ 3.20 GHz. 内存为 16 GB.

6.1.1 递归服务器的配置

Unbound 配置位于/etc/unbound/unbound.conf 中, 部分核心内容如下:

```
01 server:
02     interface: 0.0.0.0@53
03     access-control: 0.0.0.0/0 allow
04     logfile: "/etc/unbound/unbound.log"
05     module-config: "respip validator iterator"
06 rpz:
07     name: rpz.test
08     master: 172.171.1.15
09     allow-notify: 172.171.1.15
10     zonefile: /etc/unbound/rpz.test.zone
```

第 2 行表示在所有地址上监听端口 53. 第 3 行表示不对源地址访问控制. 第 4 行指示日志存储位置. 第 5 行中的配置了 rpz 所需要的 respip 模块. 第 6 行为 rpz 模块配置起始位置. 第 7 行表示 rpz 的 zone 名称为 rpz.test. 第 8 行指示 RPZ 系统的地址. 第 9 行表示允许 RPZ 系统主动通知规则变更. 第 10 行表示同步到的规则文件会存储在 rpz.test.zone 文件中.

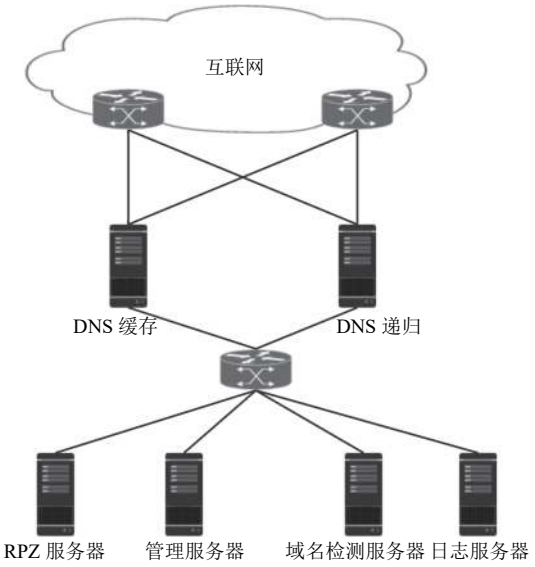

图 4 实验网络拓扑图

6.1.2 RPZ 服务器的配置

NSD 配置位于/etc/nsd/nsd.conf 中, 部分核心内容如下:

```
01 server:
02     logfile: "/var/log/nsd.log"
03     pidfile: "/var/run/nsd.pid"
04     xfrdfile: "/var/db/nsd/xfrd.state"
05 zone:
06     name: rpz.test
07     zonefile: /etc/nsd/rpz.test.zone
08     notify: 172.171.1.16 NOKEY
09     provide-xfr: 172.171.1.16 NOKEY
```

第 2 行表示日志文件位置, 第 3 行表示进程号文件存放位置. 第 4 行指示规则同步过程中, 状态文件的位置, 该文件由软件自动生成和维护. 第 6 行表示 RPZ 的 zone 名称为 rpz.test, 该名称需要与递归系统中一致. 第 7 行指示规则文件存放位置. 第 8 行表示若规则变更时, 会通知 notify 配置的 IP, 可配置多行. 第 9 行用于进行同步控制, 只有允许的递归服务器才能够进行 RPZ 规则同步.

6.2 拦截效果验证

假设 example.com 域名的子域名都为恶意域名. 针对该域名进行多种常见场景的测试验证.

6.2.1 RPZ 规则配置

/etc/nsd/rpz.test.zone 规则文件的配置如下, 其中第 11–13 行通过分号被注释, 修改此文件后, 第 4 行的序列号也需要修改, 否则不会同步至递归系统.

```
01 $ORIGIN rpz.test.
02 $TTL 3600
03 @ IN SOA ns admin (
04         2021042102 ; serial
05                 3600 ; refresh (1 hours)
06                  600 ; retry (10 minutes)
07               604800 ; expire (1 week)
08                  600 ; minimum (1 day)
09                  )
10 *.example.com CNAME .
11 ; *.example.com CNAME *.
12 ; *.example.com A          127.0.0.1
13 ; 32.34.216.184.93.rpz-ip A 127.0.0.2
```

6.2.2 拦截域名, 返回 NXDOMAIN

启用第 6.2.1 节配置文件中的第 10 行, 注释 11–13 行. 使用 dig www.example.com @172.171.1.16 命令测试结果如图 5.

根据 dig 显示的结果表明验证通过, 终端得到的响应为 NXDOMAIN.

6.2.3 拦截域名, 返回 NODATA

启用第 6.2.1 节配置文件中的第 11 行, 注释 10 和 12–13 行. 使用 dig 命令测试结果如图 6.

根据 dig 显示的结果表明验证通过, 终端得到的响应为 NODATA.

6.2.4 重定向域名至特定 IP

启用第 6.2.1 节配置文件中的第 12 行, 注释 10–11 和 13 行. 使用 dig 命令测试结果如图 7.

根据 dig 显示的结果表明验证通过, 终端得到的响应为 127.0.0.1.

6.2.5 重定向恶意 IP 至特定 IP

启用第 6.2.1 节配置文件中的第 13 行, 注释 10–12 行. 配置文件的中 32.34.216.184.93.rpz-ip, 其中, 第 1 个数字 32 表示掩码, 34.216.184.93 是 www.example.com 真实解析 IP 地址反序, 其真实地址为 93.184.216.34.

rpz-ip 为固定字段. 第 14 行的含义就是当递归响应结果中的地址为 93.184.216.34/32 时, 就被替换成 127.0.0.2. 使用 dig 命令测试结果如图 8.

实验结果符合预期, 另外针对 IP 的 NXDOMAIN 和 NODATA 的实验与第 6.2.2 节和第 6.2.3 节相似.

7 结论与展望

本文构建的 DNS 的 RPZ 安全防护系统, 采用 NSD 和 Unbound 等相关核心软件, 进行配置与实践. 验证结果表明, 系统对于防护用户访问到恶意域名或 IP 效果较为明显. 具有良好的实际应用意义与技术参考价值.

```
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 8483
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;www.example.com.               IN      A

;; Query time: 0 msec
;; SERVER: 172.171.1.16#53(172.171.1.16)
;; WHEN: Mon Feb 21 15:26:45 CST 2022
;; MSG SIZE  rcvd: 44
```

图 5 拦截域名, 返回 NXDOMAIN 的测试结果

```
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 57279
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;www.example.com.               IN      A

;; Query time: 0 msec
;; SERVER: 172.171.1.16#53(172.171.1.16)
;; WHEN: Mon Feb 21 15:28:28 CST 2022
;; MSG SIZE  rcvd: 44
```

图 6 拦截域名, 返回 NODATA 的测试结果

```
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 26828
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;www.example.com.               IN      A

;; ANSWER SECTION:
www.example.com.        3600    IN      A       127.0.0.1

;; Query time: 0 msec
;; SERVER: 172.171.1.16#53(172.171.1.16)
;; WHEN: Mon Feb 21 15:29:17 CST 2022
;; MSG SIZE  rcvd: 60
```

图 7 重定向域名至特定 IP 的测试结果

```
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 10690
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;www.example.com.               IN      A

;; ANSWER SECTION:
www.example.com.        3600    IN      A       127.0.0.2

;; Query time: 998 msec
;; SERVER: 172.171.1.16#53(172.171.1.16)
;; WHEN: Mon Feb 21 15:29:57 CST 2022
;; MSG SIZE  rcvd: 60
```

图 8 重定向恶意 IP 至特定 IP 的测试结果

系统所采用的检测子系统是基于较常用的关键字识别. 一个良好的规则库, 对于整个防护系统具有重要意义. 现有不少组织已经开始有偿提供规则库, 如何快速、有效地通过各种手段构建规则库将是下一步的研究重点.

参考文献

1 Mockapetris P. RFC1034: Domain names: Concepts and facilities. Fremont: IETF, 1987.

2 Mockapetris P. RFC1035: Domain names: Implementation and specification. 1987.

3 Romain F, Konstantin R. IDC 2020 global DNS threat report. West Chester, 2020.

4 Borges E. The most popular types of DNS attacks. https://securitytrails.com/blog/most-popular-types-dns-attacks. (2018-11-22) [2021-04-12].

5 Cooney M. Cisco Talos details exceptionally dangerous DNS hijacking attack. Network World (Online). https://www.networkworld.com/article/3389747/cisco-talos-details-exceptionally-dangerous-dns-hijacking-attack.html.(2019-04-17) [2021-04-14].

6 冷春莹, 陆超逸, 张甲, 等. EDU. CN 子域名异常解析现象测量. 通信学报, 2018, 39(S1): 99–103. [doi: 10.11959/j.issn.1000-436x.2018207]

7 Alonso R, Monroy R, Trejo LA. Mining IP to domain name interactions to detect DNS flood attacks on recursive DNS servers. Sensors, 2016, 16(8): 1311. [doi: 10.3390/s16081311]

8 奚玉龙. 基于深度学习的 DDoS 攻击检测模型. 计算机系统应用, 2021, 30(4): 216–221. [doi: 10.15888/j.cnki.csa.007649]

9 Nexusguard. Nexusguard research shows dns amplification attacks grew nearly 4, 800% year-over-year; highlighted by sharp increase in TCP SYN flood. San Francisco: Nexusguard, 2019.

10 李刚, 丁伟, 夏震. CERNET 中的 UDP DRDDoS 攻击. 中国教育网络, 2015, (5): 48–49. [doi: 10.3969/j.issn.1672-9781.2015.05.028]

11 Olzak T. DNS cache poisoning: Definition and prevention. 2006.

12 许成喜, 胡荣贵, 施凡, 等. Kaminsky 域名系统缓存投毒防御策略研究. 计算机工程, 2013, 39(1): 12–17. [doi: 10.3969/j.issn.1000-3428.2013.01.003]

13 Almusawi A, Amintoosi H. DNS tunneling detection method based on multilabel support vector machine. Security and Communication Networks, 2018, 2018: 6137098. [doi: 10.1155/2018/6137098]

14 王琪, 谢坤, 马严, 等. 基于日志统计特征的 DNS 隧道检测. 浙江大学学报 (工学版), 2020, 54(9): 1753–1760.

15 王文通, 胡宁, 刘波, 等. DNS 安全防护技术研究综述. 软件学报, 2020, 31(7): 2205–2220. [doi: 10.13328/j.cnki.jos.006046]

16 郝帅, 白翼铭, 李致成, 等. 反射放大型 DDoS 攻击的预防策略研究. 信息技术与网络安全, 2021, 40(2): 7–13, 23.

17 Cooney M. Worst DNS attacks and how to mitigate them. Network World (Online). https://www.networkworld.com/article/3409719/worst-dns-attacks-and-how-to-mitigate-them.html. (2019-07-18) [2021-04-20].

18 Miller J, Mainor D. WannaCry ransomware campaign: Threat details and risk management. https://www.fireeye.com/blog/products-and-services/2017/05/wannacry-ransomware-campaign.html. (2017-05-15) [2021-04-20].

19 Vixie P. DNS Response Policy Zones (RPZ) draft-vixie-dnsop-dns-rpz-00. https://tools.ietf.org/id/draft-vixie-dnsop-dns-rpz-00.html. (2018-06-23) [2021-04-23].