DNS 安全白皮书

摘　　要

DNS 是域名解析系统的英文缩写，是 Internet 的一项核心基础服务，它对我们和所有的联网设备使用网络服务都非常关键，是网络的基础设施。其重要性主要体现在两方面：一是为整个互联网应用提供基石。从目前来说不管是传统的 PC 和手机端，还是新基建中着力发展的 5G、物联网、工业互联网和卫星互联网，都需要通过 DNS 协议访问服务器；二是随着新经济的发展，网络空间内的经济活动逐渐增加且愈发重要，域名和 IP 作为整个互联网的基础要素，逐渐成为一国在网络空间内的战略资源。

正是由于 DNS 在整个网络中发挥的关键作用，近年来针对和利用 DNS 的攻击形势也愈加严峻。据来自 360 网络安全研究院（360Netlab）的研究数据表明，在城域网级别的 DNS 流量中，大约有万分之一到万分之五的 DNS 请求是恶意的。而现代企业中每个员工平均每天发出的 DNS 请求大约是两千次。这意味着如果一个企业拥有一千名员工，那么企业的网络出口处每天可以录得两百到一千次 DNS 恶意请求。发现并阻断这些恶意请求，甚至通过 DNS 恶意请求回溯被黑客攻陷的设备并清除恶意代码，应该成为政府企业网络纵深防御的重要组成部分。因此如何通过有效手段对 DNS 数据进行分析，实现准确识别以达到减少网络恶意行为的发生已变得非常重要。

作为 360 安全大脑的一环，360 安全 DNS 从 2013 年提供服务开始，到今年已迈进了第八个年头；每日提供 DNS 服务超过千亿次，历史累计提供 DNS 访问次数超过千万亿次，总可靠性超过 4 个 9。同时，自 2018 年开始提供增强的安全 DNS 服务后，每日拦截恶意域名更是超过四百余万次，累计拦截超过 36 亿次，总可靠性超过 4 个 9。

目　　录

1 背景介绍

今天，互联网已成为我们生活中不可或缺的一部分。从社交到金融、购物再到旅游，我们生活的方方面面都离不开互联网的支持。但是随着互联网的广泛使用，相关的问题也开始一一浮现，在这其中网络安全更是成为大多数网络用户首要关注的问题。同时伴随着网络的飞速发展，网络攻击的常态化也让越来越多的政府机构、企业和个人用户感到头疼，众多国内外一线企业以及知名人士都曾成为网络攻击的受害者。

而在形式众多的网络攻击中，DNS 攻击可以说是最为常见的一种，但是它的存在感却一直较低，那么接下来就让我们来了解下什么是 DNS 攻击，以及看看它是如何展开工作的。

1.1 DNS 定义

DNS，全称 Domain Name System，即域名解析系统，是 Internet 的一项核心基础服务。它通过使用分层的分布式数据库来处理 Internet 上的域名和 IP 地址之间的映射，主要用于 Internet 等 TCP/IP 网络中。当用户在应用程序中输入域名时，DNS 服务可以将此域名解析为对应的 IP，也就是说当我们访问一个网站时，其实访问的是网站的 web 服务器，而每台服务器在互联网上都有唯一的数字格式的 IP 地址标识。

DNS 对我们和所有的联网设备使用网络服务非常关键，是网络的基础设施。其重要性主要体现在两方面：一是为整个互联网应用提供基石。从目前来说不管是传统的 PC 和手机端，还是新基建中着力发展的 5G、物联网、工业互联网和卫

星互联网，都需要通过 DNS 协议访问服务器；二是随着新经济的发展，网络空间内的经济活动逐渐增加且愈发重要，域名和 IP 作为整个互联网的基础要素，逐渐成为一国在网络空间内的战略资源。

1.2 DNS 工作原理

DNS 的出现让用户在进行域名访问时更加简单便捷。以 360 官网为例，其唯一的数字格式 IP 地址为：36.110.213.10，如果每次打开网站都需要记忆和输入这样的点分十进制数字串是很不方便的。但如果我们输入域名，类似 www.360.cn 这样的形式，相对来说就更便于记忆。DNS 的作用就是将域名翻译成 IP 地址供客户端使用，简单来说就相当于手机里的电话簿，通过相关手段将电话号码与姓名互相映射。

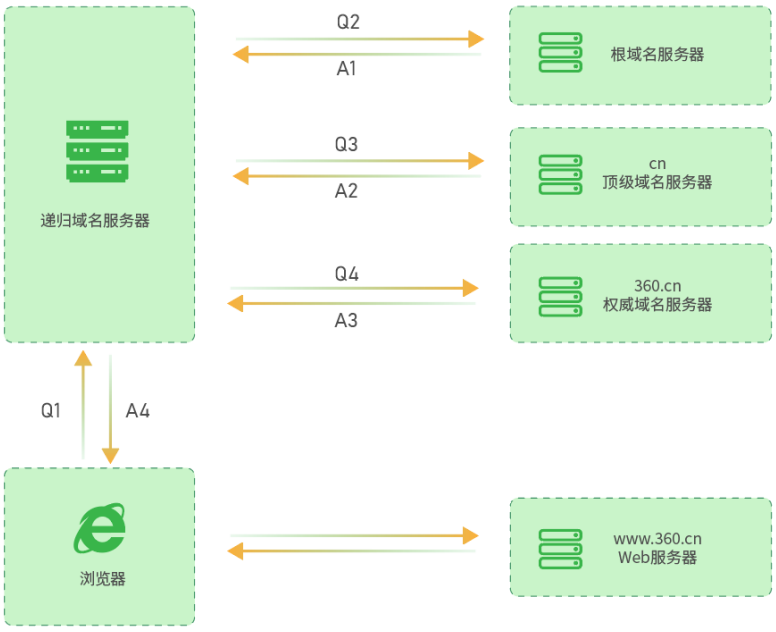

图 1 DNS 工作流程

DNS 的工作流程主要分为客户端和服务器两个部分，客户端作为提问者向服务器询问某个域名，服务器则根据域名回答对应的 IP 地址。在实际的使用中，当用户在浏览器中键入域名 www.360.cn 时，主要的流程为：

（1）浏览器客户端向所配置的递归域名服务器发出解析 www.360.cn 域名的 DNS 请求报文（图中的 Q1）。相当于对递归域名服务器说“请给我 www.360.cn 所对应的 IP 地址”。

（2）递归域名服务器收到请求后，先查询本地缓存。假设没有查到该域名对应记录，则递归域名服务器向所配置的根域名服务器发出请求解析.cn 域名的 DNS 请求报文（图中的 Q2）。

（3）根域名服务器收到查询请求后，通过查询得到.cn 顶级域名所对应的顶级域名服务器，然后向递归域名服务器返回一条应答报文（图中的 A1）。相当说“我现在告诉.cn 域名所对应的顶级域名服务器地址”。

（4）递归域名服务器在收到根域名服务器的 DNS 应答报文，得到.cn 顶级域名所对应的顶级域名服务器地址后，再次向对应的顶级域名服务器发送一条请求解析 360.cn 域名的 DNS 请求报文（图中的 Q3）。

（5）.cn 顶级域名服务器在收到 DNS 请求报文后，先查询自己的缓存，假设也没有该域名的记录项，则查询 360.cn 所对应的权威域名服务器，然后也向本地名称服务返回一条 DNS 应答报文（图中的 A2）。相当于说“我现在告诉你 360.cn 域名所对应的权威域名服务器地址”。

（6）递归域名服务器在收到.cn 顶级域名服务器的 DNS 应答报文，得到 360.cn 二级域名所对应的权威域名服务器地址后，再次向对应的权威域名服务器发送一条请求解析 www.360.cn 域名的 DNS 请求报文（图中的 Q4）。

（7）360.cn 权威域名服务器在收到 DNS 请求报文后，在它的 DNS 区域数据库中查找，最终得出了 www.360.cn 域名所对应的 IP 地址。然后向递归域名服务器返回到条 DNS 应答报文（图中的 A3）。相当于说“www.360.cn 域名的 IP 地址为 36.110.213.10”。

（8）递归域名服务器在收到权威域名服务器后，向 DNS 客户端返回一条 DNS 应答报文（图中的 A4），告诉浏览器所得到的 www.360.cn 域名的 IP 地址，这样浏览器就可以正常访问这个网站了。

1.3 DNS 相关安全问题

总体来说，DNS 相关的安全问题可以分为两类：针对 DNS 的攻击和利用 DNS 进行的攻击。其中：

- 针对 DNS 的攻击。又分为针对 DNS 协议的攻击和针对 DNS 服务器的攻击。其主要思路是利用 DNS 协议或服务器的弱点，通过攻击 DNS 服务或服务器的方式来达到攻击使用 DNS 服务的其他网络业务的目的；
- 利用 DNS 进行的攻击。其主要思路是恶意代码利用 DNS 通道，实现与远程控制中心的通信，从而执行报活、传输窃取到的数据、获取攻击指令和执行攻击指令等恶意操作。

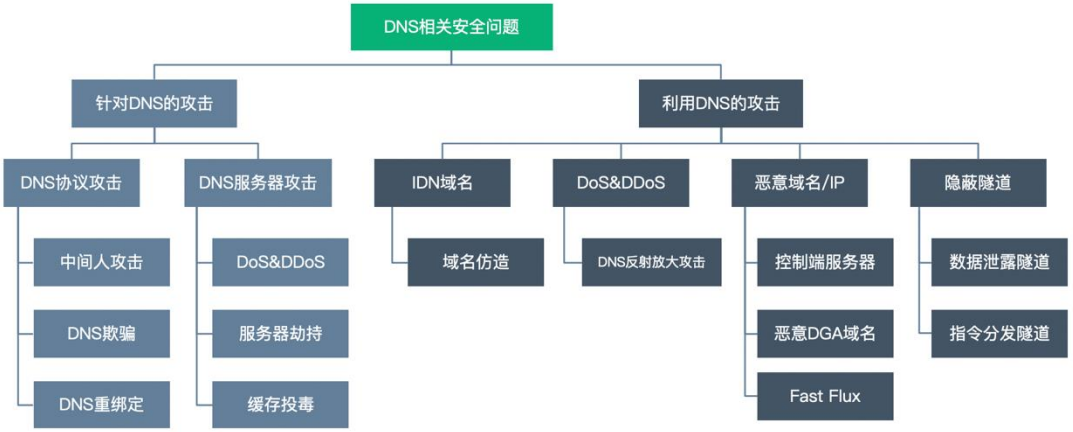

图 2 DNS 相关安全问题

下面我们分别看一下这两种不同类别的典型攻击方式:

1.3.1 针对 DNS 的典型攻击

- DDoS 攻击

DDoS 攻击（Distributed Denial of Service)也叫做分布式拒绝服务攻击，攻击者所针对的目标是服务可用性。他们通过操纵大量傀儡机，利用目标系统网络的服务功能缺陷或者消耗其系统资源，使得该目标系统无法提供正常的服务。

虽然随着互联网技术的发展，计算机的处理能力逐年增长，让该攻击方式的困难程度加大了，但是相比基本的 DoS 攻击，DDoS 可以通过利用更多的傀儡机（肉鸡）来发起进攻，只要攻击者控制了足够多的肉鸡持续进行攻击，就能够使被攻击者的网络服务被拖垮至发生中断。而且由于 DDoS 的攻击方式可以在攻击时对源 IP 地址进行伪造，隐蔽性极强，因此对于该种攻击的检测也相对困难，难以防范。

针对 DNS 服务的 DDoS 攻击会导致 DNS 服务不可用，从而使得一切需要使用到该 DNS 的网络服务都无法正常运行，导致大面积网络故障，带来经济损失，甚至其他更严重的后果。

- DNS 缓存投毒

DNS 缓存投毒，是一种十分普遍的攻击。它是利用虚假 Internet 地址替换掉域名系统表中的地址，进而制造破坏。攻击者通过查找并利用 DNS 或域名系统中存在的漏洞，以便将有机流量从合法服务器吸引到虚假服务器上。当网络用户在带有该虚假地址的页面中进行搜寻并访问某链接时，网页浏览器由于受到该虚假条目的影响而打开了不同的网页链接，在这种情况下蠕虫、木马、浏览器劫持等恶意软件就可能会被下载到本地用户的电脑上，导致很多严重的安全问题出现。

之前在对 DNS 工作原理进行介绍时本文曾提到，实际使用中当用户在浏览器中键入域名时，会首先在本地缓存服务器中寻找结果，并且所有的应答信息都将被缓存在本地缓存服务器中，因此攻击者利用这一特性，先是将假的地址植入到 DNS，然后让服务器对假地址进行缓存记录，最终在用户键入网址时把流量牵引到攻击者服务器，完成缓存投毒的整个攻击流程。

DNS 缓存投毒的主要风险是窃取用户数据，因此该攻击的主要目标为医院、金融机构和在线零售商。一旦目标被攻击成功，就意味着任何密码，信用卡或其他个人信息都可能受到损害。另外如果互联网安全提供商的网站被欺骗，那么用户的计算机还可能会受到如病毒或特洛伊木马等的影响。

- DNS 流量劫持

所谓的 DNS 流量劫持是指用户在进行网页浏览时，被强制访问某些网页，或者在 App 使用中出现弹窗等现象。目前在移动互联网环境下，流量劫持主要分为两类：

- 域名劫持。表现为在用户正常联网状态下(如 3G、4G 和 WiFi 等状态)，目标域名会被恶意地错误解析到其他 IP 地址上，造成用户无法正常使用服务。
- 数据劫持。对于返回的内容，会在其中强行插入弹窗或嵌入式广告等其他内容，干扰用户的正常使用，对用户体验构成极大伤害。

流量劫持不仅会给用户造成损害，也会让相关互联网公司的商誉和利益被严重伤害。同时由于劫持流量者提供的信息服务完全脱离监管，也可能存在着传播诈骗、色情等低俗甚至严重违法信息的现象。

1.3.2 利用 DNS 的典型攻击

不管是钓鱼网站、垃圾邮件，还是僵尸网络、勒索软件，甚至 APT，绝大多数网络恶意行为都避不开对 DNS 的使用。其中典型的攻击方式有：

- DNS 隐蔽隧道

DNS 隐蔽隧道(DNS Tunneling)是将其他协议的内容封装在 DNS 协议中，然后通过 DNS 通信完成传输数据的技术。由于 DNS 是网络的基础设施，所以网络出入口处的防火墙等安全设备几乎不会过滤掉 DNS 流量，于是这就给了攻击者机会来利用 DNS 实现下发远程控制指令、进行文件传输等操作。

DNS 隐蔽隧道又分为直连隧道和中继隧道。其中，直连隧道是指：客户端直接和指定的 DNS 服务器建立连接，然后将需要传输的数据通过 DNS 协议进行通信。这种方式的优点是具有较高速度，但蔽性弱、易被探测追踪的缺点也很明显。而中继隧道是指：客户端通过 DNS 迭代查询而实现的 DNS 隧道，这种方式非常隐秘，而且可在绝大部分场景下部署成功。但由于数据包到达目标

DNS 服务器前需要经过多个节点的跳转，数据传输速度和传输能力比直连方式慢很多。

在实际攻击行为中用到 DNS 隐蔽隧道的场景，对隐蔽性要求很高，而速度相对来说没那么重要，因此中继隧道被使用的更多。

- DNS 反射放大攻击

DNS反射放大攻击主要是利用DNS回复包比请求包大的特点，放大流量，伪造请求包的源IP地址为受害者IP，将应答包的流量引入受害的服务器。

正常DNS查询方式

DNS攻击方式

攻击者通过不断向DNS服务器发送伪造了源IP地址的解析请求，从而放大攻击流量。发送的 DNS 查询请求数据包大小一般为 60 字节左右，而查询返回结果的数据包大小通常为 3000 字节以上，因此，使用该方式进行放大攻击能够达到 50 倍以上的放大效果。只要能够控制足够多的终端向DNS服务器发送伪造了源IP的DNS解析请求，就能够实现对该IP对应服务的DDoS攻击。

1.4 DNS 攻击（给客户）带来的危害

作为互联网世界的道路交通导航系统，如果 DNS 服务被黑客攻击，就会造成互联网导航系统的全面中断或混乱。其中最为明显的结果就是无法正常上网，或者网络访问被错误的导航到其他的服务器上，比如本来要访问电商网站，却被

错误的 DNS 服务导航到钓鱼网站，那么网民在钓鱼网站输入的帐号密码信息就会被盗，给用户带来信息泄露以及金钱上的损失。

而大规模的 DNS 劫持，则往往会造成断网，因为大型网站的访问量较大，一般的钓鱼网站服务器无法承受大流量的访问而瞬间瘫痪，网民也就无法访问相关网页。

虽然如今已有很多企业开始全力以赴地应对网络安全威胁，以期能检测和规避网络攻击，但依然还有大部分企业并没有对 DNS 安全起到足够重视，因此仍有大量相关企业的数据、资产和信誉长期处于风险之中。

思科曾在 2016 的年度安全报告中提出，近 91.3%的已知恶意软件被发现使用 DNS 作为主要手段，但 68%的企业却忽略了这个问题，并没有对 DNS 解析进行监测，思科将这种现象称之为“DNS 盲点”。同时 Coleman Parkes 公司发布的《2017 全球 DNS 威胁调查》报告也表明，DNS 攻击造成的年度平均损失是 220 万美元，76%的公司企业在过去 12 个月中成为了 DNS 攻击的受害者（比去年上涨 2%）。2019 年 IDC 全球 DNS 威胁报告更是指出，全球有 82%的企业遭受过 DNS 攻击，63%的企业因为 DNS 攻击导致业务中断，平均损失超过 100 万美金。

以上的种种数据均表明，DNS 的攻击形势愈加严峻，有越来越多的企业因为 DNS 攻击而受到影响，因此如何通过有效手段对 DNS 数据进行分析，实现识别和检测以达到减少网络恶意行为的发生正变得非常重要。

2 DNS 攻击案例介绍

近年来，利用 DNS 进行攻击事件不在少数，下面本文将从大量案例中选取一些热点事件进行介绍。

2.1 DNS 大规模攻击事件

2009 年 5 月，DNSPod 主站及多个 DNS 服务器遭受超过 10G 流量的恶意攻击，DNSPod 电信主力 DNS 服务器被迫离线。对此 DNSPod 声称在遭遇恶意攻击后便被电信骨干网封掉 IP，虽然 DNSPod 及时更换 IP，但由于 DNS 协议限制，DNS 更改 IP 最多需要 72 小时才能生效，因此依然造成很多用户域名一直无法解析。

就在 DNSPod 发布致歉信的近似时间里，另一轮高强度恶意攻击向 DNSPod 涌来，导致 DNSPod 服务完全中断，其下所有域名均无法访问，包括暴风影音网站。由于大量暴风影音用户打开暴风影音网页或者使用其提供的在线视频服务，导致用户提交的访问申请无法找到正确的服务器，积累不断的访问申请让各地电信网络负担成倍增加，网络出现堵塞。

因此从 2009 年 5 月 19 日晚 21 时左右开始，江苏、安徽、广西、海南、甘肃、浙江六省陆续出现大规模网络故障，很多互联网用户出现访问互联网速度变慢或者无法访问网站等情况。

后续工信部对事件发布公告称，事件原因为暴风网站域名解析系统受到网络攻击出现故障，导致电信运营企业的递归域名解析服务器收到大量异常请求而引发拥塞。今后将进一步做好网络监控工作，发现异常情况及时处理，尽量减少对

用户的影响，保障用户享受到通畅的网络服务。而互联网人士则认为此次攻击表现出互联网、尤其是 DNS 服务器的脆弱性。未来如果不在此方面进行加强，后果将不堪设想。

2.2 2016 DYN Cyber Attack

2016 年 10 月，北美地区大量用户反馈若干重要的互联网网站无法正常访问。包括 Twitter、Spotify、Netflix、Airbnb、Github、Reddit 以及纽约时报等主要网站都受到黑客攻击。据悉造成本次大规模网络瘫痪的原因是 Dyn Inc.的服务器遭到了 DDoS 攻击。

相比其他 DNS 攻击事件，有几个特别之处值得我们关注：

首先，这次攻击发生在美国，并导致了美国全国范围内大面积的网络访问不畅，大量的美国网民对这次攻击有亲身体会。因为美国在整个互联网领域内的先进性，这种事件特别值得引起注意；

其次，因为有了大量网民的抱怨，当天白宫例行记者会议、稍后美国大选电子委员会都对这一事件发表了评论，这标志着攻击事件从单纯的网络安全事件上升到国计民生问题；

再次，这次攻击事件中，产生攻击的受控端，俗称肉鸡的设备，由大量家用路由器、网络摄像头组成。这些所谓的物联网设备，首次在 DDoS 攻击领域内正式亮相，并且一登台就引发了轰动整个网络世界的攻击；

最后，在整个安全社区和执法机构的联合努力之下，背后的 Mirai 僵尸网络三名原作者在次年落网并随后被美国司法部起诉，这代表了在网络空间里，依然是邪不胜正，天网恢恢疏而不漏。

因此有部门专家认为此次事件是迄今为止影响最大的攻击事件，意味着承载着互联网基础设施核心的 Dyn 以及其它公司开始成为越来越多 DDoS 的攻击目标，不仅遭受攻击的数量和种类大增，而且攻击时长以及遭受攻击的复杂性也都在增加。

2.3 WannaCry（永恒之蓝）蠕虫病毒

2017 年 5 月 12 日，WannaCry 在全球大爆发，影响范围超过 150 个国家 200,000 终端。WannaCry 蠕虫病毒有一个开关域名，即 www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com。在蠕虫感染过程中，有效载荷通过 445 端口上的 MS17-010 漏洞投递并成功启动后，会尝试访问特定域名的网页。如果成功访问网页，则随即退出，蠕虫会被压制，不会进一步发作；如果访问网页失败，蠕虫会开始破坏动作，并随后弹框勒索赎金。

在 WannaCry 的传播和破坏路径中，DNS 起到了重要的作用，这是由于开关域名的解析和访问完全依赖 DNS 协议。在早期该域名没被注册时，WannaCry 呈现了爆炸式传播和发作的态势，但在安全研究人员注册了该域名后的几个小时后，该病毒的传播就得到了有效压制。研究人员因此自嘲说“意外地拯救了世界”。

3 DNS 攻击应对方法

通过对 DNS 攻击事件的案例梳理可以发现，如何有效进行 DNS 的安全防护非常重要，保护 DNS 的安全从某种角度来说就是保护企业和个人的财产和信息安全，对于相关的防护策略，相关专家建议可以从以下几个方面着手[1]：

- **采用 DNSSEC 技术**

DNSSEC 技术是指利用数字签名和公钥来实现 DNS 数据的完整性与可靠性，利用 DNSSEC 技术通过权威域名服务器用自己的私钥签署资源记录，然后解析服务器用权威的公钥认证来自权威域名服务器的数据，如果秘钥验证成功，则意味着接 DNS 获得的数据信息来自可以信任的权威域名服务器，再进行解析服务器接收数据，有效的提高了连接的安全性。如果身份秘钥验证失败，则意味着 DNS 接收到的数据信息可能是不被信任的有风险信息，DNS 可以拒绝接入。

- **采用 DOT/DOH 技术**

DOT/DOH 是通过将原本在链路上传输的明文 DNS 数据进行加密来达到防止 DNS 数据在链路上被窃听，篡改和劫持的目的。用一个不是很贴切但近似的类比来说，我们可以将其理解为是 HTTP VS HTTPS。尽管在 DNS 社区对此类技术尤其是 DOH 技术的使用还存在一些争议，但是随着 Chrome 和 Firefox 等客户端浏览器的支持，以及 Cloudflare，Google 等大型 DNS 解析器厂家在服务器端的支持。加密 DNS 传输整个趋势应该很快就会普及开来。目前作为国内的 DNS 安全的重要推进者，360 浏览器和 360DNS 已展开密切合作，360 浏览器已经完

[1] 胡芳芳.DNS 安全风险与应对策略研究[J].科技传播，2019，11(23):119-120.

全支持了 DOH。未来网民上网时面临的 DNS 劫持问题也将会在不久后得到极大的缓解。

- **部署 Anycast**

部署 Anycast 是利用网络路由的技术方案来增强 DNS 的安全性能。通过对 Anycast 的部署，可以实现 DNS 中提供相同服务的服务器组公用统一的 IP。客户端向 DNS 发送的数据连接请求可以利用 Anycast 接入最近的一台服务器主机上，采用此技术方案能够有效阻止 DDoS 攻击，这是由于当网络攻击者利用僵尸网络对 DNS 攻击时，采用的僵尸网络上的主机具有不同的地理位置，并且各自有独立的 IP 地址，这些巨量的网络信息会通过 Anycast 分布到不同的 DNS 服务器上，进而缓解了单一服务器的运行压力，利用大量的分散式服务器能够一定程度上减少 DDoS 攻击对 DNS 的破坏性。

- **区块链技术**

目前 DNS 系统是基于根域名服务器的集中式管理系统，一旦根域名服务器出现故障，整个互联网将受到严重影响。随着块链技术的快速发展，相关机构利用分块链分散的特点，推动了块链技术和 DNS 系统的集成，基于集中式块链技术的网络安全比传统的集中式域名服务器安全，它可以支持域名管理，防止域名服务器缓存和中毒，区块链通过其网络节点构建 DNS 信息，能够有效提升 DNS 的安全性能。

- **DNS 数据检测**

正如前文指出的“近 91.3%的已知恶意软件被发现使用 DNS 作为主要手段”，因此通过对 DNS 数据检测来发现网络中的恶意威胁是一个非常有效的网络威胁检测手段。

通过分光或镜像的方式从 DNS 服务器获取 DNS 解析流量，进行协议还原后配合专业的域名威胁情报库和 PassiveDNS 数据库，能够从中发现利用 DNS 的恶意行为。

在整个威胁生命周期中，DNS 数据检测的方式主要在恶意程序发起远程通信时发挥作用，能够抓恶意程序于现行，并能实时阻断其恶意行为，是非常有效的网络安全方案。

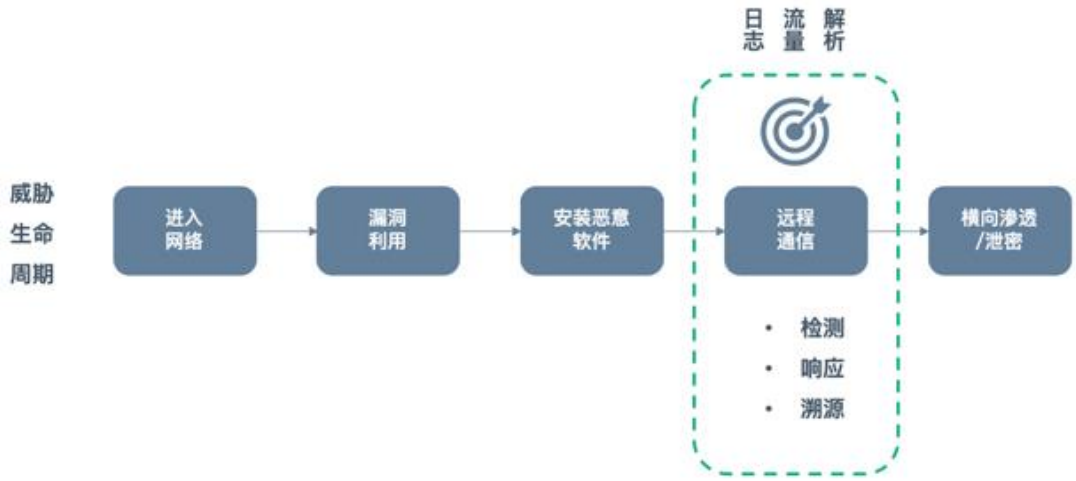

图 3 DNS 用于威胁检测的思路

另外对于 DNS 的安全最佳实践，美国国土安全部的网络安全和基础设施安全局（CISA）也提供了一些具体建议，其中包括：

- 更新 DNS 账户密码。这将终止未经授权的犯罪分子对当前可能拥有的账户的访问权限。
- 验证 DNS 记录，以确保它们按预期进行解析，而不是重定向到其他地方。这将有助于发现任何活动的 DNS 劫持。
- 审核公共 DNS 记录，以验证它们是否被解析到了预期的地方。
- 搜索与域相关的加密证书，吊销任何欺诈性请求的证书。

对于代理未请求的已颁发证书，监视证书透明日志。这将帮助防御者注意到是否有人试图模仿他们或者监视他们的用户。

4 DNS 攻击研究趋势

DNS 域名系统作为大规模分布式网络，可以抽象为一个有向图。NS 名字服务器和解析器构成图的节点，而 NS 名字服务器和解析器之间的路由则构成了有向图的边。因此加强 DNS 的安全性就是要加强这些节点和边的安全性。节点的安全主要通过安全评估来保证，包括安全漏洞扫描和权威名字服务器可用性测量；边的安全性则体现在关键路由发现和保护上。此外，DNSSEC 有效配置与平滑过渡、DNS 配置错误检测以及对 DNS 攻击的检测和防御等问题也是未来研究的热点问题。

- **基于 DNS 系统安全评估**

DNS 域名系统安全评估主要是依据“木桶原理”对 DNS 域名系统安全方面进行测评，发现 DNS 域名系统中存在的薄弱环节。另外要对特定 DNS 域名系统请求进行监测，统计其中无效 DNS 请求，分析其对 DNS 系统的影响。具体评估方法包括安全漏洞扫描和权威名字服务器分布探测。

- **基于 DNS 域名系统关键路由点防护**

DNS 域名系统防护关键路由的第一要点为如何定位。DNS 关键路由发现需要对目标 NS 服务器进行分布式路由探测，然后将探测结果进行分析和综合，最终找到大部分路由的汇接点。探测结果的准确性依赖于测试机的分布情况，测试机分布越广泛，探测结果就越准确。通过对 DNS 系统的关键路由进行防护，能够有效分析造成网络时延的成因并定位故障点，极大改善整个互联网的性能和 QoS 服务质量，并对互联网关键基础设施的规划建设和安全防护起到很好的指导作用。

- **DNS 异常检测和安全防护**

现实网络中存在两种异常行为，一种是由恶意攻击引起的，一种是系统在软件设计、编码和系统配置过程中的脆弱性所导致的。可以通过基于流量(volume)和报文载荷(payload)特征的方法进行检测。DNS 安全防护是保证网络信息系统保密性、完整性、可用性、可控性和不可否认性的综合技术。

- **DNS 攻击反向追踪**

网络犯罪之所以如此猖獗，在很大程度上是由于网络的开放性使得对攻击者的追踪和惩罚难以实施，无法形成强大的网络威慑力，致使攻击者肆无忌惮地进行破坏。反向追踪技术可以从源头上消除攻击并最终形成网络威慑力。

- **DNS 基于大数据的深度对比分析**

DNS 大数据分析可对出网内用户流量的流向、DNS 请求数据、出网数据，网内数据，流向其他运营商数据，网内相关信息。可详细统计本地数据、外域数据、缓存数据、CDN 数据等。分析统计网内移动终端业务、固网业务等，并以可视化方式综合分析结果。

- **DNS 安全在 AI 领域内的应用**

基于 AI 智能学习和数据挖掘的 DNS 关键技术，包含基于监督式学习网络的 DNS 服务器入侵检测方法、基于用户查询序列模式学习的 DNS 性能提升策略、DNS 使用挖掘框架以及基于潜在语义学习的 DNS 扩展应用。针对 DNS 服务器的入侵检测过程转换为机器学习中的监督学习过程或者分类问题，可以按照 AI 智能学习基本原理将入侵检测过程分为三个子过程：特征提取过程、模型学习过程及线上检测过程。

5 360DNS 威胁检测防御系统

未来随着越来越多的政府服务上线，DNS 的攻击面也将进一步扩大。并且相比之下政府受到的 DNS 攻击风险也要更大。据 360 网络安全研究院（360Netlab）收集到的信息也表明，在城域网级别的 DNS 流量中，大约有万分之一到万分之五的 DNS 访问是恶意的。而现代企业中每个员工平均每天发出的 DNS 请求大约是两千次。这意味着如果一个企业拥有一千名员工，那么企业的网络出口处每天可以录得两百到一千次 DNS 恶意请求。阻断这些恶意请求，应该成为政府企业网络纵深防御的一部分。

因此 360 团队认为：目前受到 DNS 攻击最为严重的主要还是政府和企业，我们需要对此作出积极地应对。从网络安全的角度来说，提供安全稳定的 DNS 服务和部署专业的 DNS 威胁检测和防御设备就是一个提升 DNS 安全的有效手段。

360 企业安全集团利用 360 在网络安全行业十余年累计的经验以及海量的安全数据，推出了 360DNS 威胁检测防御系统——一个集 DNS 解析、威胁检测和防御等功能于一体，提供有效检测和阻断方案的防御系统。在较低部署难度和较低成本前提下，360DNS 威胁检测防御系统能够有效提升企业内部网络安全威胁发现和处置能力，为企业网络安全纵深防御领域的重要一环。

图 4 360DNS 威胁检测防御系统架构

方案通过提供 DNS 解析服务或分光的方式，获取网络内 DNS 流量，通过重组和还原后在此基础上进行 DNS 请求/响应的分析和检测。

图 5 360DNS 威胁检测防御系统测试环境数据

作为 360 安全大脑的一环，360 安全 DNS 从 2013 年提供服务开始，到今年已经迈进了第八个年头；每日提供 DNS 服务超过千亿次，历史累计提供 DNS 访问次数超过千万亿次，总可靠性超过 4 个 9。同时，自 2018 年开始提供增强的安全 DNS 服务后，每日拦截恶意域名更是超过四百余万次，累计拦截超过 36 亿

次，总可靠性超过 4 个 9。未来，360DNS 威胁检测防御系统将继续致力于防护利用 DNS 进行的网络攻击，为企业及个人用户的网络安全建设保驾护航。

附：

360 企业安全集团官网：https://b.360.cn/

360 安全 DNS 官网：https://dns.360.cn/

360 网络安全研究院（360Netlab）官网：http://netlab.360.com/