2020 网络威胁初步调研（一）

作者：李玉冰

本文的目的在于通过对 2020 年的网络安全状况（偏 DDoS）分析，找到一种/一类攻击能够和可编程硬件结合。由于时间原因，仅包括 DDoS 的防御企业的威胁报告和部分论文的总结结果，经过初步调研 DDoS 攻击和 IoT 设备组成的僵尸网络密切相关，应将该部分和 Sigcomm 会议的研究内容加入调研内容。

1 Akamai

1.1 主要内容

Akamai2020 年没有根据攻击类别而是针对各个产业进行了报告，包括零售商和酒店、游戏、媒体行业、金融服务。其用于研究的数据来自于 Cloud Security Intelligence（CSI）。疫情期间导致钓鱼事件更加频繁，对认证信息的攻击也更频繁。主要的攻击包括对 Web 应用程序的攻击、认证滥用和 DDoS 攻击。在洗手的同时，管理好个人信息，不要使用重复密码，上网冲浪时谨防钓鱼网站。

Akamai2020 所有报告汇总：https://www.akamai.com/us/en/resources/our-thinking/state-of-the-internet-report/global-state-of-the-internet-security-ddos-attack-reports.jsp

1.2 具体内容

Akamai 2020 报告主要内容，对以下事件进行了总结。

时间	事件	地址
2019.10	cryptomining SSH worm	https://blogs.akamai.com/sitr/2019/10/a-cryptomining-ssh-worm.html
2019.10	Phishing-Baiting the Hook	https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/soti-security-phishing-baiting-the-hook-report-2019.pdf
2019.11	fake Cozy Bear group 的 DDoS 勒索威胁	https://blogs.akamai.com/sitr/2019/11/fake-cozy-bear-group-making-ddos-

		extortion-demands.html
2019.12	感恩节假期的企业应用程序所受威胁	https://blogs.akamai.com/sitr/2019/12/access-and-threat-insights-thanksgiving.html
2019-2020	对金融服务行业的攻击	https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/soti-security-financial-services-hostile-takeover-attempts-report-2020.pdf
2020.04	recycle phishing kits, and simply refreshing them	https://blogs.akamai.com/sitr/2020/04/threat-actors-recycling-phishing-kits-in-new-coronavirus-covid-19-campaigns.html
2020.05	credential stuffing attacks	https://blogs.akamai.com/sitr/2020/05/credential-stuffing-attacks-during-the-covid-19-pandemic.html
2020.06	malware called Stealthworker	https://blogs.akamai.com/sitr/2020/06/stealthworker-golang-based-brute-force-malware-still-an-active-threat.html
2020.08	新的 DDoS 勒索威胁	https://blogs.akamai.com/sitr/2020/08/ransom-demands-return-new-ddos-extortion-threats-from-old-actors-targeting-finance-and-retail.html
2020.09	对游戏产业的威胁报告	https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/soti-security-gaming-you-cant-solo-security-report-2020.pdf
2020.10	IoT 设备被利用到 DDoS 攻击中	https://blogs.akamai.com/sitr/2020/10/exploring-the-iot-afterlife.html

2 NeuStar

2.1 主要内容

受疫情影响，互联网使用率大幅度增加，办公环境从局域网（LAN）转换到了虚拟专用网（VPN）。全球物联网市场正在增长。这让 VPN 和 IoT 都成为更易受攻击的目标。

异常缓慢的网络性能可能表明该站点正在遭受 DDoS 攻击。2020 年上半年发生了更多

更大的 DDoS 攻击。Neustar 检测到的最大攻击为每秒 1.17Tbps，且持续了 5 天 18 小时。攻击趋向于突发和脉冲攻击，当客户意识到被攻击时攻击已结束。攻击载体主要包括服务器内置协议（CLDAP 服务器、Jenkins 服务器的自动发现协议）、DNS 服务器漏（NXNSAttack）、格式错误的数据包（RangeAmp）。Mirai 攻击将不安全的 IoT 设备招募到僵尸网络中，为 DDoS 攻击创造条件，并且存在很多 Mirai 变种。

受疫情影响，一些行业遭受到了严重的打击。人们在疫情期间对游戏的支出大幅增长，并且游戏一直以来都是攻击者的主要目标。媒体流量在疫情期间也大幅增长，但针对媒体的攻击更多的是认证填充攻击。网络购物在疫情期间成为更优的购物选择，电子商务/网络零售商直接依赖于传入流量来获取收入，因此分布式拒绝服务（DDoS）勒索有利可图，也确实出现了 DDoS 勒索事件，复杂的 DDoS 攻击可以在几分钟之内关闭一个站点。疫情更让医疗组织成为被攻击的目标，医院或医疗机构始终具有大量的物联网设备，其中许多都可以被利用，且患者信息是存在于任何地方的最丰富的数据来源之一。

2.2 具体内容

NeuStar 的网站中只找到了 2020 年上半年威胁报告。

世界处于 COVID-19 的浪潮之中，并且这种病毒的影响将持续相当长的一段时间。据《福布斯》报道，**互联网使用率增长了 50%至 70%，流媒体在 2020 年第一季度跃升了 12%以上。**业务人员离开了公司办公室，导致全球网络和安全团队发生了许多变化。IT 部门必须更加重视协作和远程连接工具，同时确保其员工及其业务受到保护。从局域网（LAN）或基于办公室的连接到**虚拟专用网（VPN）**或虚拟化环境的变化引起了无数问题。虽然企业可以通过外部托管某些公共服务（例如网站或电子邮件系统）来获得某种保护，但他们需要仔细考虑自己的 VPN 以及不受外部托管或保护的其他服务。如果企业的公司连接受到攻击（特别是针对其 VPN 的攻击），并且连接中断，则整个员工队伍都将脱机。

使用 VPN 允许全球员工远程登录所面临的挑战是，网络犯罪分子了解到从分布式拒绝服务（DDoS）角度来看，连接不够健壮，这使 **VPN 容易成为这些攻击的目标**。大多数企业使用“vpn”作为 URL 或主机名的一部分这一事实也使攻击者可以轻松识别服务器。通过单个域名系统（DNS）查找，攻击者即可拥有 IP 地址，并且可以通过租用的僵尸网络发起常规的大规模 DDoS 攻击，从而淹没电路，或使用网络协议攻击来瘫痪系统资源。

所有行业都已从新型冠状病毒的浪潮中受到了影响。Internet 流量正在增加，攻击也在

增加。无论是严重的网络犯罪分子还是无聊的青少年，各种类型的攻击者都可能比以往拥有更多的攻击时间。不仅使用 Internet 的人数呈爆炸性增长，而且在线计算机的数量也激增。据《美国商业资讯》预测，“在 COVID-19 危机和迫在眉睫的经济衰退期间，在经修正的复合年增长率（CAGR）的推动下，**全球物联网（IoT）市场**在分析期间将增长 8765 亿美元。）的 31.4%。”

虽然效果不佳的网站可能反映出流量增加，但堵塞网站的流量实际上可能来自 DDoS 攻击。美国联邦调查局（FBI）在 7 月下旬发布了一份通知，**指出识别 DDoS 攻击的一种方法是“异常缓慢的网络性能（打开文件或访问网站）。**”断开连接或质量差的流媒体体验可能足以使客户考虑更改服务或提供商。

网络罪犯很少仅仅为了它而造成破坏。DDoS 入侵的最可能目标之一是为定向攻击铺平道路。**通过检查和过滤流量**，可以阻止许多此类攻击，无论采用哪种机制来防御针对企业基础结构的 DDoS 攻击，都应能够做到这一点。**通过检查流量，查看标题和内容并通过评估信誉来对组合进行评分**，就可以通过所有良好的流量，同时最大程度地减少通过的不良流量。

2020 年 1 月至 6 月与 2019 年同期相比，攻击总数增加了两倍半以上。在此期间观察到的最大攻击规模也是 Neustar 缓解的最大攻击规模，**为每秒 1.17 兆兆位（Tbps），是 Internet 上可见的最大攻击量。一次攻击的最长时间也是 Neustar 见过的最长时间，为 5 天 18 小时**。

从规模上将 2020 年 1 月至 6 月的攻击数量与 2019 年同期的攻击数量进行比较，各种规模的攻击都在增加，但增长最快的类别的最大攻击是每秒 100Gbps 或更高的攻击。

- **攻击大小：**从 2020 年 1 月至 6 月，Neustar 缓解的攻击中有 70%以上为 5 Gbps 或更少。此比较着眼于每个时间段的流量构成，而不是攻击次数。攻击的总数急剧增加。2020 年 1-6 月平均攻击大小为 12Gbps，2019 年同期平均攻击大小为 11Gbps。
- **攻击强度：**将 2020 年 1 月-6 月的攻击强度与 2019 年同期的攻击强度进行比较，Neustar 观察到，2020 年最严重的攻击以每秒 3.5 亿个数据包（Mpps）的速度大大高于该州最严重的攻击在 2019 年同一时期，这种攻击的强度增加了 81%以上，而这些时期的总体平均攻击强度几乎没有变化。
- **威胁载体：**从 2020 年 1 月至 6 月，具有单个载体的攻击数量相当低，具有 4 个以上载体的极其复杂的攻击数量也很少。这些结果可能表明一个事实，即比以往任何时候都更多的攻击者“陷入了 DDoS 游戏”。这样的不良行为者可能会使用多个载体来购买/控制威胁，但是随着复杂性的提高，掌握不断变化的向量的专门技术的攻击者的数量会减少。

DDoS 攻击并不是什么新鲜事物，如 Memcached 放大攻击的 Github 和 Mirai 攻击的 Dyn。但是，从 2020 年 1 月至 6 月，这种前景发生了明显变化。 DDoS 攻击重新成为新闻，并且比以往任何时候都更大，更强烈，并且发生的次数更多。

攻击大小：今年是有记录的最大规模的 DDoS 攻击的来临。Amazon Web Service（AWS）报告说，**其网络上的一个身份不明的客户受到 2.3 Tbps 攻击的攻击，这种攻击持续了几天。尽管攻击者本身未知，但似乎是基于放大的攻击，它使用了劫持的无连接轻量级目录访问协议（CLDAP）服务器。**放大攻击与反射攻击基于相同的前提。一种最著名的放大攻击是使用不受保护的 Memcached 服务器来放大流量。此攻击曾在 2018 年导致 GitHub 瘫痪，并且由于单个请求产生的流量巨大，因此无需使用漫游器即可生成当时创纪录的 1.3 Tbps。这次攻击还突出显示了 Memcached 服务器的数量，这些服务器被设计为在防火墙后面并向 Internet 开放。此后，其中许多服务器已进行了重新配置，但仍有许多可用协议（我们将在后面的部分中考虑），这些协议在设计上是开放的，因此可以用作放大向量。

攻击强度：我们习惯于以 Gbps 或（现在）Tbps 的度量来考虑 DDoS 攻击的数量形式。我们将这些称为攻击的大小，因为大量的流量旨在通过耗尽电路的容量来使其饱和。我们正在听到的另一种攻击类型是高强度攻击，以 Mpps 为单位。这些攻击针对特定的基础结构，传入流量在到达目标的过程中必须经过这些基础结构。之前的最高水位标记为 500 Mpps，今年也突破了 800 Mpps。

攻击成员：尽管上述巨大威胁吸引了人们的关注和头条新闻，但缓解 DDoS 的真正重大新闻是这些攻击的总数。Neustar 以及整个行业的攻击数量急剧增加，尤其是规模较小的攻击。在考虑这种持续发展趋势的原因时，考虑此类攻击的意图是有帮助的，这种攻击可能不足以完全使电路饱和。简而言之，如果攻击者可以不被发现，则可能对站点或资源造成很大的破坏。**保持未被检测到的好方法是将攻击流量保持足够高以造成损害，但又保持足够低以绕过任何会自动表示入侵的流量阈值。**随着 Internet 服务提供商（ISP）对 DDoS 威胁越来越精明，尤其如此。通过保持低音量和高压力，黑客可以实现各种目标。

攻击趋势：在大量攻击中，NeuStar 观察到了几种增长趋势。

- **突发和脉冲：**利用检测到的攻击触发缓解措施并完全重定向到已制定的缓解措施的清理中心之间的较短间隔来进行攻击，这样的攻击被称为突发攻击。流量突然出现并消失得一样快，称为脉冲攻击。在这种攻击中，一连串的流量到达特定的子网然后消失，仅在另一个子网中再次弹出。当客户意识到自己正在受到攻击并转向缓解措施时，攻击已经结束。许多具有关键任务网络的客户已迁移到始终路由

的解决方案，在这种解决方案中，缓解时间约为几秒钟，从而避免了停机时间。

- **载体扩展：**网络参与者越来越有可能**滥用内置网络协议**来对美国网络进行 DDoS 攻击。**CLDAP 协议已经存在了很多年，并且最近已被用于 DDoS 放大**，还有许多其他协议。今年 2 月，在 **Jenkins 服务器**中发现了另一个此类漏洞。Jenkins 服务器是 DevOps 团队通常使用的免费/开源服务器，它们使用它们来构建，测试和部署在云中运行的应用程序。这些服务器具有内置的自动发现协议，该协议默认情况下启用并在面向公众的服务器上公开。2020 年第二季度，发布了一些新威胁。**第一个利用 DNS 服务器漏洞，称为 NXNSAttack。**发现该攻击的研究团队报告说，使用 NXNSAttack 的攻击者可以将简单的 DNS 查询从初始大小的 2 倍扩大到 1,620 倍，从而造成大量流量激增，从而使受害者的 DNS 服务器崩溃。**今年五月还发现了另一种放大方法，称为 RangeAmp。**攻击者可以使用几种不同类型的格式错误的数据包来关闭网站和大量内容分发网络（CDN）。该漏洞利用范围请求（一种 HTTP 标准，旨在允许客户端仅从服务器请求文件的特定部分或范围）这一特点，当发送大型媒体或下载具有暂停和恢复功能的文件时，将使用此类部分请求。虽然任何网站都可能受到此攻击的影响，但它对 CDN 最为危险，据说能够将 CDN 上的流量负载增加 724 到 43,300 倍之间。大多数大型 CDN 供应商已经意识到了这种媒介，并已采取措施防止其使用。

- **机器人：**众所周知，僵尸程序的传播与 IoT 设备的部署成比例地增长，然后可用于 DDoS 攻击。**我们都知道了通过影响 Dyn 的 Mirai 攻击将不安全的 IoT 设备招募到僵尸网络中。**恶意软件如 Gafget（一种 Mirai 变种）的兴起正在不断兴起，僵尸网络正在不断建立。黑客也没有停滞不前。2020 年 2 月，硬件制造商合勤（Zyxel）修复了一个零日漏洞，该漏洞随后被 Mirai 的另一个新变种利用。预计到 2027 年将有超过 410 亿个 IoT 设备在使用，企业实施强大的 DDoS 解决方案的需求不断增长。

购买者已将其大部分支出转移到了网上。“通常 75％的用户会在页面加载时间超过 3 秒后反弹。”在线业务的加载速度较慢网页可能会导致缺乏销售转换和一般的流量损失，并且现代消费者宁愿搜索新页面，也不愿花时间等待页面加载。与今年的互联网流量一样，今年的攻击并未在所有站点上平均分布。一些行业受到了严重的打击。

- **ISP，注册中心和托管站点：**在考虑缓解 DDoS 时，Neustar 具有独特的见解，Neustar 的产品是基于云的，并且与供应商无关，这使得 UltraDDoS Protect 被许多 ISP，注

册机构和网站主机选择为缓解措施的提供商。它们的构建是为了在某种程度上吸收攻击，但是值得注意的是其数量的增加（从 2020 年 1 月到 2020 年 6 月增加了 102％）。

- **游戏，赌博和媒体：**毫不奇怪的是，随着锁定措施的实施，整个 2020 年游戏网站的增长率都很高。据《福布斯》报道，“自 3 月以来，游戏收入每月都在大幅增长。今年 3 月，到 2019 年 3 月，游戏支出增长了 34％。今年四月，游戏比去年同月增长了 73％。而在过去的一个月中，5 月比 2019 年 5 月增长了 53％。”而且，安全行业的人们都知道**游戏网站长期以来一直是攻击者的主要攻击目标**，因此针对这些网站的攻击也就不足为奇了，网站数量也在增长。**4 月中旬，视频游戏公司电子艺界（EA）发生了最大的 DDoS 攻击之一**，当时一系列 DDoS 攻击使服务器脱机。在线赌博行业是可能是而造成的损失最小的潜在行业之一。根据 Grand View Research 的一项研究，在线赌博将大规模的增长，仅在美国，到 2025 年，在线赌博的价值将达到 1029 亿美元。DDoS 攻击可用于持有赎金站点，而其他类型的恶意软件可用于窃取从加密货币到个人身份的所有信息。媒体，尤其是在线视频，满足了这三个目标。“今年视频将占互联网流量的最高 1.9 ZB（相当于 10 亿兆字节），比我们 COVID-19 之前的预测增长 0.2ZB 或 12％。这相当于增加了 2,000 亿小时的 Netflix 观看或缩放视频通话时间。访问量在增加，攻击也是如此，**尽管该行业中观察到的大多数攻击已趋向于凭证填充攻击。**该垂直领域的 Neustar 攻击缓解措施急剧增加，增长了 461％。
- **零售/电子商务：**自大型传染病以来，零售和电子商务受到了广泛的关注，因为从实体店转移到在线商店的紧迫性可能比任何其他行业都要大。《福布斯》（Forbes）4 月底报道，截至 4 月中旬，美国零售商的在线同比收入（YoY）增长了 68％，超过了 1 月初 49％的峰值。截至 4 月 21 日，美国和加拿大的电子商务订单同比增长 129％，所有在线零售订单的增长令人瞩目 146％。这意味着 DDoS 威胁显然是零售商的底线，并且是当前的威胁。根据最近的一份报告，“零售站点和应用程序**直接依赖于传入流量来获取收入**；因此，**分布式拒绝服务（DDoS）勒索**可能有利可图。复杂的 DDoS 攻击可以在几分钟之内关闭一个站点。”同一份报告指出，DDoS 攻击占对在线零售商的所有网络攻击的 21％。
- **医疗：**这一次在 COVID-19 时代显得更加紧迫，这增加了对医疗机构进行 DDoS 攻击的重要性。**医院或医疗机构始终具有大量的物联网设备，其中许多都可以被利用，**

且患者信息是存在于任何地方的最丰富的数据来源之一。所有这些因素共同使医疗保健成为攻击者最理想的目标之一。COVID-19 的大流行一经公布，对医疗服务提供者的攻击就开始了。捷克共和国的布尔诺大学医院（Brno University Hospital）今年 3 月遭到网络攻击，迫使医院关闭了整个网络，并取消了手术。巴黎大学医院信托基金会（AssistancePublique-Hôpitauxde Paris）是一家管理着巴黎地区 39 家公立医院的大学医院信托基金，于 2020 年 3 月 22 日遭到袭击。虽然攻击本身持续时间不长，但确实影响了 Internet 访问，阻止了远程工作人员接收电子邮件、Skype 和其他远程位置。几天后，美国卫生与公众服务部（HHS）成为 DDoS 攻击的受害者。同时，世界卫生组织（WHO）透露，其遭受的网络攻击通常是其系统的两倍，其中包括运行冒充 WHO 内部电子邮件系统的恶意站点的黑客。

3 NetScout

3.1 主要内容

2020 年上半年，DDoS 攻击方法发生了根本性的变化，转变为更短、更快、更困难的复杂多载体攻击。可以在 Cyber Threat Horizon 上了解全球 DDoS 攻击的实时数据。攻击者更倾向于攻击疫情期间人们生存必需的产业，如电子商务、医疗保健、金融服务。

攻击呈现出“持续时间较短+复杂性增加=应对越来越难的攻击的时间更少”的特点。

常出现的攻击策略包括：DNS、TCP SYN、TCP ACK、ICMP、TCP RST、CLDAP、TCP SYN/ACK、NTP、mDNS、SSDP。其中 CLDAP 同 2019 年相比，增长率最高。UDP 反射/放大仍然是攻击者的主要策略，UDP 反射/放大攻击中频繁出现的为 DNS、mDNS、NTP、OpenVPN、SNMP、SSDP。各地区的 DDoS 数据体现了：高通量、短时间的攻击，缩小缓解的响应窗口，并使用多媒介攻击作为烟雾弹增加缓解难度。

在僵尸网络的发展上，Mirai 及其变体仍然统治着不断扩大的基于 IoT 的恶意软件世界。基于 Linux 的恶意软件也呈上升趋势（TrickBot、Drovorub、Lucifer），尤其是针对所有主要设备和操作系统的跨平台恶意软件 Lucifer。并且 NetScout 预计 2020 年及以后会看到 Linux 和跨平台恶意软件的数量增加。

NetScout 认为 2020 年上半年的场景强调了先进的自动化 DDoS 技术的关键作用。

3.2 具体内容

2020 年上半年，DDoS 攻击方法发生了根本性的变化，转变为**更短、更快、更困难的复杂多载体攻击**。攻击者针对在日益数字化的世界中至关重要的在线平台和服务（例如电子商务，教育平台，金融服务和医疗保健服务）的攻击日益增多。有关全球 DDoS 攻击的实时数据，**Cyber Threat Horizon** 是一个非常不错（免费工具）的选择。在疫情期间，NETSCOUT 遭受了前所未有的每月最大数量的攻击，仅 5 月份就有 929,000 次 DDoS 攻击。从 NetScout 的主动威胁级别分析系统（ATLAS®）可以看出，NETSCOUT 威胁情报部门在 2020 年上半年发现了 483 万次 DDoS 攻击，比 2019 年增加了 15％。更明显的是，在大流行封锁期间，DDoS 攻击频率跃升了 25％。从三月到六月攻击者通过复杂的高吞吐量攻击将疫情的必需服务（例如电子商务，医疗保健和教育服务）作为目标，而这些攻击旨在通过短暂的爆发式攻击迅速淹没并击落目标实体。同时学校关闭，导致了游戏在线率的提升。DDoS 攻击会消耗大量带宽和吞吐量，这是我们所有人都需要支付的流量。

复杂的多向量攻击不断增加，复杂的利用 15 种以上媒介的攻击已同比激增 126％，自 2017 年以来猛增了 2851％。同时，平均攻击持续时间比 2019 年上半年下降了 51％。这加起来使防御者头疼不已，持续时间的减少使得他们难以作出反应而得出缓解方案。同时，我们看到 2020 年上半年单媒介 DDoS 攻击减少了 43％。

COVID-19 的广泛传播是全球性的健康危机，但对于网络犯罪分子而言，这是一个难得的商机。它们已经充分利用了优势，发动了许多旨在提高其投资回报率（ROI）的较短，更快，更复杂的攻击。这就给防御者加了一些不好的数学公式：**持续时间较短+复杂性增加=应对越来越难的攻击的时间更少。这样的场景仅强调了先进的自动化 DDoS 技术的关键作用。**

到 2020 年前六个月，全球有 480 万起攻击，但这对全球基础设施有什么影响？服务提供商和企业都需要为此计划，将其视为在数字经济中开展业务的成本。**虽然通常用攻击流量带宽/吞吐量或每秒的数据包数量（pps）来描述容量 DDoS 攻击的影响**，但它们通常具有同等或更大的重要性。面向带宽的攻击可能会淹没网络链接并挤出合法的互联网流量。另一方面，基于吞吐量的攻击会阻碍路由器，交换机和负载平衡器之类的网络基础设施设备转发合法网络流量的能力，并降低服务器处理和响应用户请求的能力。因此，虽然我们在此期间确实观察到了另一种 TB 级攻击，但它并不是过去六个月中最重要的指标。整体而言，DDoS 攻击所消耗的带宽和吞吐量是巨大的问题。

在 2020 年 3 月 11 日至 4 月 11 日的关键时期，我们观察到 DDoS 攻击总流量高达每秒

1.01Pbps 和每秒 208 Gpps 数据包（Gpps）的攻击量，增长了 14%，相对于过去 4 个月观察到的平均值，攻击吞吐量增加了 30%。一方面，**攻击和防御的成本差距太大。**在攻击者方面，引导程序/压力服务便宜且易于使用，以至可以租用 10 分钟的攻击，而费用仅为 35 美分。15 种以上的多媒介攻击显示出稳定的增长。复杂的多媒介攻击也更难以防御，将成功的几率推向了攻击者。此外，DDoS 攻击者拥有大量的免费设备，可用于发起复杂的多矢量 DDoS 攻击。而防御者必须同时支付资源。较小的攻击逐年下降，数字证实了这一点。在过去的一年中，我们看到 15 种以上的媒介攻击显着增长，十种及以下媒介的攻击呈百分比急剧下降。对攻击媒介以及攻击者如何利用它们的研究阐明了 DDoS 威胁格局的不断发展的本质。在评估 DDoS 攻击工具的工具时，NetScout 再次查看了 UDP 反射/放大 DDoS 攻击向量的整体，以确定存在多少可能的设备供攻击者利用和滥用。尽管出现了一些令人惊讶的峰值，但绝大多数仍相对平稳，这表明不幸的是，攻击者不会很快用尽所有选择。图 1 描述了攻击者可用于攻击的反射器/放大器的可用性。

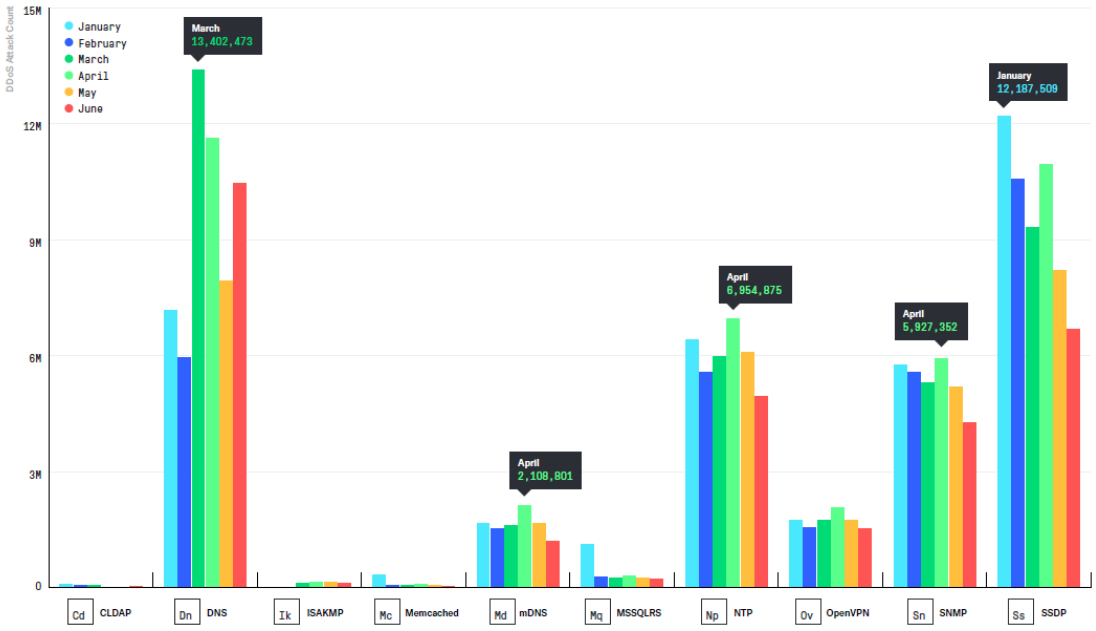

图 1 6 个月 UDP 反射/放大攻击的可用性

尽管 **UDP 反射/放大仍然是攻击者的主要策略**，但基于 TCP 的攻击也显着增长，增加了防御者缓解攻击的难度。值得注意的是，成功破坏服务或系统的 DDoS 攻击通常会导致我们所说的“同情攻击”。换句话说，正常的泛洪型攻击可能会破坏用户尝试连接的服务。因为该服务不可访问，所以它会生成一个同情的 TCP SYN 泛洪。当用户或其他连接的服务查询不可用服务或系统的状态时，通常会看到 ICMP 数据包。

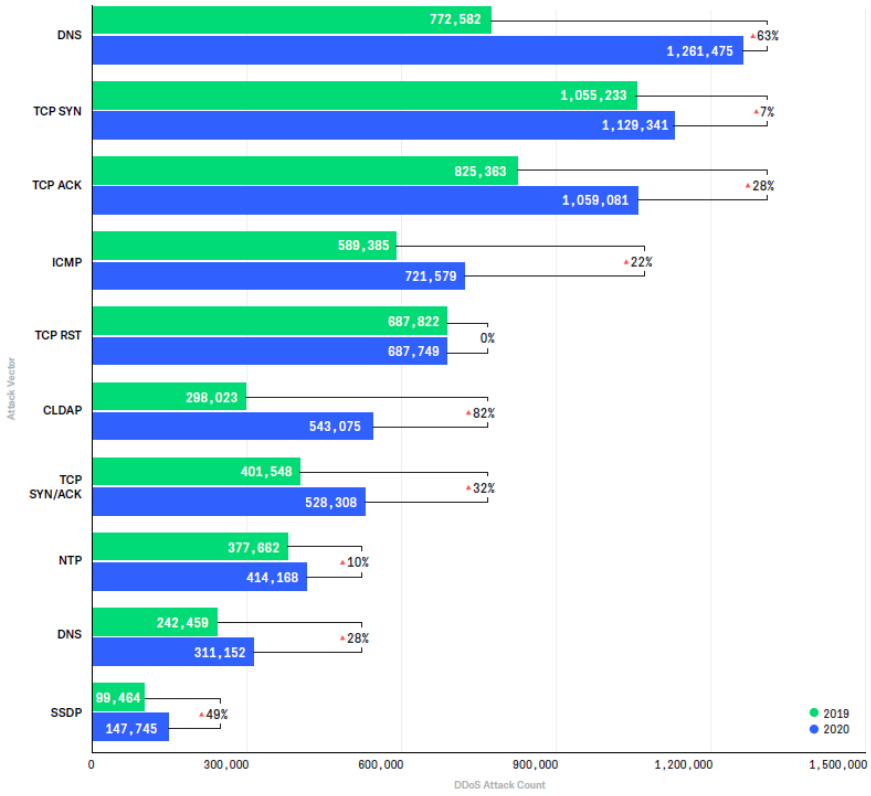

图 2 按攻击计数排名靠前的 DDoS 媒介

总的说来，各地区的 DDoS 数据体现了：高通量、短时间的攻击，缩小缓解的响应窗口，并使用多媒介攻击作为烟雾弹增加缓解难度。在大多数情况下，攻击频率激增，EMEA（欧洲、中东、非洲）地区的增长率为 43%。攻击大小增长不一致。可以承受 1.1 Tbps 攻击的亚太地区增幅最大。每个地区的吞吐量都在增加，这清楚地表明了向**高 pps 攻击**的总体转变旨在**使网络硬件和应用程序**不堪重负。同样，由于攻击者采用了一种有效的“命中即跑”方法，因此**平均攻击持续时间在每个区域都有所下降**，这种方法不仅可以节省资源，而且可以缩短防御者做出响应的时间。最后，我们证明复杂的多媒介攻击的激增并非仅局限于一个地区或国家。回顾过去三年，发现了一种不断增加的攻击复杂性的清晰且不断扩展的模式。

北美地区的攻击频率居高不下，因为该地区的攻击频率，规模和吞吐量都有所增长，但增速与其他地区不同。尽管如此，**持续时间较短的高吞吐量攻击**的总体趋势仍然成立。同时，攻击者针对疫情期间生存至关重要的行业。非商店零售商（包括电子商务购物）的频率增加了 20%，而对教育服务的攻击则增加了 13%。

攻击者将目标对准了 LATAM（拉丁美洲）医院和医生办公室，在医疗系统受到最大压力的情况下攻击了这些至关重要的服务。医院的袭击增加了 80%，而门诊医疗服务（又名医生办公室和诊断实验室）的袭击增加了 30%。更糟糕的是，这些攻击是越来越难以缓解

的高带宽，高吞吐量事务。例如，医院的最大攻击规模猛增了 2788%，而最大吞吐量猛增了 863%。

欧洲、中东和非洲从速度和整体影响两方面，**土耳其经历了与 DDoS 相关的重大动荡。**可能是意识形态冲突的结果，土耳其的最大攻击规模增加了 339%，而最大攻击吞吐量却激增了近 1000%。同时，攻击数量下降了 82%。因此，这意味着该国的公司和 ISP 面临通过其网络的高带宽，高吞吐量 DDoS 流量的显着增长。德国和法国也出现了异常增长，尽管增长幅度并不完全相同。德国的攻击频率增加了 233%，最大攻击规模增加了 226%。同时，在法国，攻击频率跃升了 100%以上，而最大吞吐量却增长了 275%。同时，欧洲，中东和非洲地区也遭受了对大流行生命线行业的攻击。非商店零售商在频率，规模和吞吐量方面都获得了显着的全面增长。包括基于云的服务在内的数据处理，托管和相关服务也受到了越来越多的关注，攻击增加了 30%，攻击增加了 43%，吞吐量提高了 52%。

在总体指标方面，亚太地区的国家有点不寻常。尽管针对日本的攻击增长了 229%，但最大攻击规模和吞吐量均大幅下降，分别为 48%和 84%。同时，中国的攻击频率仅下降了 25%，而最大吞吐量下降了 51%。但是，当涉及到最高的垂直行业目标时（电子商务，教育，云服务和医疗保健），符合疫情的 DDoS 总体攻击趋势。对电子商务的攻击增加了 191%，其中高吞吐量的活动特别受欢迎，增加了 154%。同时，医院的攻击规模和吞吐量分别增长了 98%和 100%。

恶意作者继续做出令人印象深刻的高效努力，以吸取最新的物联网漏洞并推出基于 Mirai 的新变体。**Mirai 仍然统治着不断扩大的基于 IoT 的恶意软件世界**，疫情效应在三月份引发了基于 Mirai 的变体的大规模增长。这些变体包括使用一些旧的和新的漏洞利用方法。最近，一个名为“sora”的 Mirai 变体进行了更新，以包括 F5 BIG-IP 远程代码执行漏洞（CVE-2020-5902）。**大多数物联网僵尸网络往往是短暂的**——一旦**命令和控制（C2）IP 地址被烧毁，僵尸网络就会被烧毁。**建立一个新的 Mirai 僵尸网络的成本和时间很小。

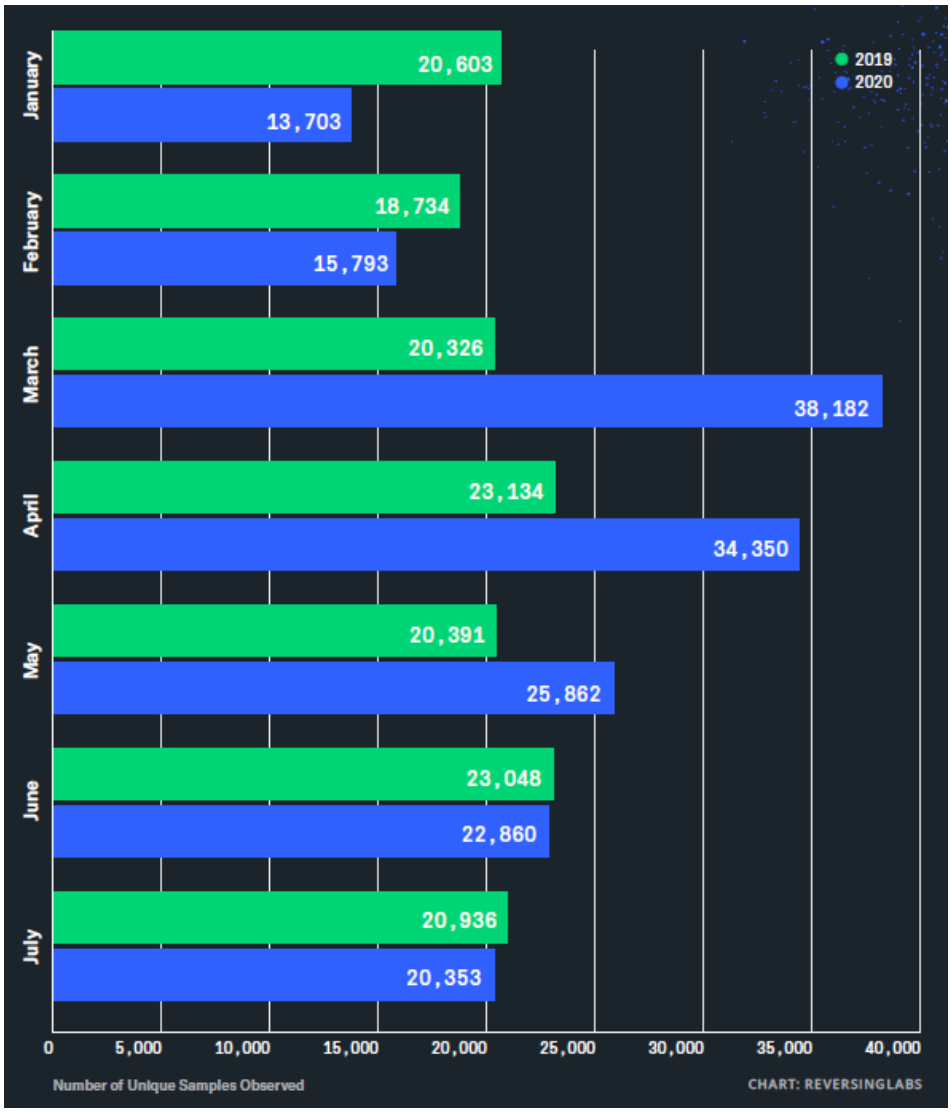

图 3 Mirai2019 和 2020 年对比

物联网威胁前 5 名：Mirai 变体、暴力破解用户名/密码组合、利用尝试

Mirai 变体：与 2019 年相比，我们看到了一组排名前 5 位的 Mirai 变种。对我们的蜜罐深入研究，在 2020 年上半年观察到的前 5 个 Mirai 变种。这些标记是识别所使用变种的好方法。

Mirai Variants	Unique Sources
CORONA	9,160
RETARD	4,030
UNSTABLE	2,625
KYTON	2,201
ARES	1,964

Table 1: Top 5 Mirai Variants

用户名密码组合：与 2019 年相比，我们的蜜罐网络看到用于破坏 IoT 设备的五个密码变化不大。我们的蜜罐观察到的前五个密码都包含在 2016 年的原始 Mirai 僵尸网络中，清晰显示了 Mirai 原始来源在创建变体方面的持续价值。

Username/Password	Unique Sources
root/xc3511	68,140
guest/12345	57,289
admin/admin	57,100
root/vizxv	45,408
guest/guest	44,663

Table 2: Top 5 Username/Password Combinations

漏洞利用：僵尸网络运营商还重用了常见的 IoT 漏洞，以试图将设备破坏并注册到僵尸网络中。虽然新的攻击不断被折叠成新的变种，但蜜罐网络观察到的大多数攻击尝试都是较旧的攻击，与 telnet 密码类似，我们发现前五名的攻击每年没有变化。

Exploit	Unique Sources
Realtek SDK Miniigd UPnP SOAP Command Execution	21,175
Huawei Router HG532 Arbitrary Command Execution	16,633
Hadoop YARN Resource Manager Command Execution	2,348
D-Link DSL OS Command Injection	940
MVPower DVR Shell Command Execution	849

Table 3: Top 5 Exploits

尽管 Mirai 变体是当今互联网上最主要的 IoT 机器人，但一些非 Mirai IoT 恶意软件也引起了骚动。**Gafgyt 是一款多架构 IoT 机器人**，与 Mirai 有许多相似之处。Gafgyt 已使用具

有默认/出厂凭据的 telnet 并利用漏洞传播到易受攻击的 IoT 设备。与 Mirai 一样，Gafgyt 支持多种基于 TCP，UDP 和 HTTP 的 DDoS 攻击。Gafgyt 不断以新的漏洞利用和凭证进行开发，如在 Internet 上疯狂运行的众多变体所示。尽管从 1 月到 2 月与 2019 年相比有所减少，但从 2 月到 6 月，我们发现 Gafgyt 样本出现了大幅增加。样本数量的增加很可能与在此期间远程工作激增所带来的在线消费设备的增加有关。

图 4 Gafgyt 2019 和 2020 年对比

我们还看到基于 Linux 的恶意软件呈上升趋势，如图 11 所示。

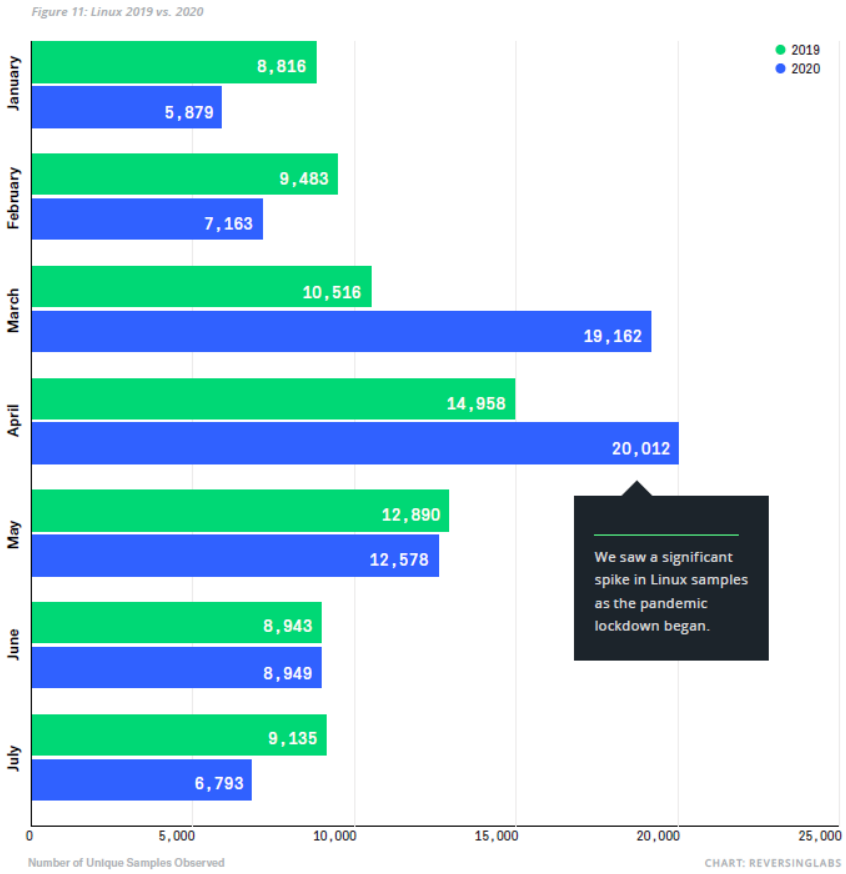

图 4 Linux 2019 和 2020 年对比

Linux 在 Internet 数据中心和通用计算机中的不断增长使这些系统成为恶意软件作者的丰厚目标。随着 Windows Linux 子系统（WLS）5 的发布，您现在可以在 Windows 桌面或服务器上运行完整的 Linux 环境。我们开始看到恶意软件作者利用这些功能不仅针对 Windows，而且针对 Linux。让我们看一些最近基于 Linux 的恶意软件的示例。流行的 **TrickBot 恶意软件将 Anchor 框架移植到 Linux**。所谓的 Anchor_Linux，被用作感染连接到受感染 Linux 服务器的 Windows 系统的枢纽。NSA 和 FBI 发布了有关基于 Linux 的**恶意软件 Drovorub** 的详细信息。Drovorub 支持在受感染的系统上进行数据渗透，端口转发和任意命令执行。

Lucifer，ASERT 研究人员发现了 Lucifer 的 Linux 端口，**Lucifer 是一种混合的加密劫持和 DDoS 恶意软件。**Lucifer 能够进行基于标准 ICMP，TCP 和 UDP 的洪泛攻击，包括欺骗攻击数据包的源 IP。此外，Lucifer 支持 HTTP 应用程序层攻击，包括基本的 HTTP GET 和 POST 泛洪，以及多种版本的 HTTP“ CC” DDoS 攻击。Lucifer 还支持在受感染系统上执行任意命令。与 Trickbot 相似，Lucifer 也可用于感染连接到同一网络的其他 Windows 系统。由于数种 IoT 设备基于 Linux 发行版，因此对于具有创造力的恶意软件作者来说，使用常见的 IoT 漏洞作为一种感染方法，重新编译其恶意软件的 Linux 版本以使其在基于 IoT 的设备

上运行并不是一件容易的事。这将引发针**对所有主要设备和操作系统的跨平台恶意软件新潮流**。Lucifer 机器人肯定是这种情况。它可以在基于 Linux 的系统上运行的事实意味着它可能会危害和利用 Internet 数据中心（IDC）中的高性能，高带宽服务器，并且每个节点在 DDoS 攻击能力方面都承受了更大的压力比大多数在 Windows 或基于 IoT 的 Linux 设备上运行的漫游器的典型情况要好。我们预计 2020 年及以后会看到 Linux 和跨平台恶意软件的数量增加。

4 论文

对 2020 年安全顶会上的 13 篇网络安全方向的论文大致了解一下内容，其研究内容和企业的威胁报告大致相符，对 DNS 缓存投毒的研究较多，并且有一篇论文专门讲述威胁报告中提到的 NXNSAttack。列出其中和可编程网络以及 DDoS 攻击相关的论文摘要。

4.1 EPIC: Every Packet Is Checked in the Data Plane of a Path-Aware Internet

最近的网络研究令人兴奋的发现是，具有路径意识的网络体系结构能够从根本上解决当今 Internet 的许多安全问题，同时提高整体效率并控制对最终主机的路径选择。在本文中，我们考虑了与这一新的网络范式相关的三个重要问题：首先，网络运营商仍然需要能够实施自己的策略，以排除不经济的路径并在数据平面上执行这些决策。其次，终端主机应该能够验证网络实际上遵循了它们的转发决定。最后，中间路由器和接收者都应该能够验证数据包的来源。先前的工作已经考虑了这些属性，但是没有现有的系统能够同时实现强大的安全保证和高效率。我们提出了 EPIC，这是一组数据平面协议，可提供越来越强大的安全性，可以满足上述所有三个要求。与同类系统相比，EPIC 协议的通信开销要低得多：对于实际的路径长度，开销是最先进的系统 OPT 和 ICING 的 3-5 倍。由于在转发过程中仅使用了很少的高效对称密码运算，因此即使在商用硬件上，我们的原型实现也能够使 40 Gbps 链路饱和。因此，通过确保在每个跃点上检查每个数据包，我们朝着高效，安全的未来互联网迈出了重要的一步。

4.2 NXNSAttack: Recursive DNS Inefficiencies and Vulnerabilities

本文揭示了一个新漏洞，并介绍了一种相应的攻击，即无名服务器攻击（NXNSAttack），它会破坏 DNS 系统并使其瘫痪，从而使 Internet 用户难以或无法访问网站，Web 电子邮件，在线视频聊天，或任何其他在线资源。 NXNSAttack 会在 DNS 解析器和 DNS 权威名称服务器之间生成大量数据包。风暴是由解析程序对权威名称服务器的无限制引用响应消息的响应产生的。该攻击比 NXDomain 攻击（例如 Mirai 攻击）更具破坏性：i）递归解析器交换的数据包数量达到超过 1620 倍的放大倍数。 ii）除了负缓存外，攻击还使解析器缓存的“NS”部分饱和。为了减轻攻击的影响，我们建议对递归解析器算法 MaxFetch（k）进行增强，以防止不必要的主动提取。我们在 BIND 解析器上实现了 MaxFetch（1）缓解增强功能，并在真实的 DNS 查询数据集中对其进行了测试。我们的结果表明，MaxFetch（1）既不会降低递归解析器的吞吐量，也不会降低其延迟。发现攻击后，我们执行了负责任的披露程序，一些 DNS 供应商和公共提供商已发布了 CVE 并修补了其系统。

4.3 Programmable In-Network Security forContext-aware BYOD Policies

自带设备（BYOD）已成为企业网络的新规范，但是 BYOD 安全性仍然是首要考虑的问题。上下文感知安全性是一种有前途的方法，该方法基于动态运行时上下文来实施访问控制。最近的工作开发了 SDN 解决方案，以收集设备上下文并在中央控制器上实施访问控制。但是，中央控制器可能成为瓶颈和攻击目标。对于实时决策更改，在遥控器上处理上下文信号也太慢。我们提出了一种新的范例，可编程的网络内安全性（Poise），它通过可编程交换机的出现而得以实现。Poise 的核心是新颖的安全性原语，可以对其进行编程以支持硬件中的多种上下文感知策略。 Poise 的用户指定了简洁的策略，然后 Poise 将它们编译为 P4 中基元的不同配置。与传统的 SDN 防御相比，Poise 能够灵活控制平面饱和攻击，并显着提高了防御敏捷性。

5 结论

仅做为初次调研的结果，对近几年的网络发展和 2020 年的网络安全现状做一个初步的了解。

参考资料

[1]弱密码可猜测密码或硬编码密码：

https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Top_10

[2]全球 DDoS 攻击的实时数据 Cyber Thread Horizon：https://www.netscout.com/horizon

[3]Legner M, Klenze T, Wyss M, et al. {EPIC}: Every Packet Is Checked in the Data Plane of a Path-Aware Internet[C]//29th {USENIX} Security Symposium ({USENIX} Security 20). 2020: 541-558.

[4]Afek Y, Bremler-Barr A, Shafir L. NXNSAttack: Recursive {DNS} Inefficiencies and Vulnerabilities[C]//29th {USENIX} Security Symposium ({USENIX} Security 20). 2020: 631-648.

[5]Kang Q, Xue L, Morrison A, et al. Programmable in-network security for context-aware BYOD policies[C]//Proc. USENIX Security. 2020.