

更新其路由以使用该主机作为其下一跳。攻击者可以探测发端者所在的网络，然后通过利用ICMP回波检测发端者的一个活的邻居主机⁵。

5.2 DoS攻击设计

图6展示了我们通过恶意的ICMP重定向进行DoS攻击的步骤。在开始的时候，受害者的发起者和目的地可以正常通信。在我们的攻击中，发起者可能是一个网络服务器，一个开放的DNS解析器，或一个Tor中继节点。相应地，目的地可能是一个网络客户端，一个权威的名称服务器，或一个下一跳的Tor中继节点，分别。路径外攻击者的目的是切断

发端人和目的地之间的通信。该攻击由八个主要步骤组成。

攻击者通过以下方式探测受害发端者的邻近主机
攻击者利用ICMP回波。

通过IP地址欺骗和伪造UDP数据报到受害者发端人的一个监听UDP端口。

受害者发端者被骗建立一个对攻击者来说可预测的UDP套接字，因为套接字的四元组，即源IP地址、目的IP地址、源端口（监听UDP端口）和目的端口（攻击者指定的前一个伪造的UDP数据报的源端口）、

攻击者知道。攻击者假装是通过Traceroute可以观察到的受害者起源地的网关（通过IP地址欺骗），然后伪造一个嵌入已知UDP的ICMP重定向消息。

伪造的ICMP重定向消息。

通过发端人的检查。
发起人更新其路由缓存，并将随后的网络流量（由IP承担的所有类型的网络流量）重定向到邻居家。

顺从地摄取主人。
重定向的流量会被丢弃在转发失效的邻居主机。

这意味着只有一个伪造的ICMP错误信息会导致发端者的DoS。当所有八个步骤都成功时，受害者发端者所在的AS也被认为是脆弱的，即收到§4.2所述的欺骗性ICMP重定向。

5.3 热门网站的案例研究

实验设置。涉及4种主机。1) 目标网络服务器（即我们

通过ICMP回波请求和回复。3) 网络客户端（即目的地），可以访问目标服务器，并接收原始响应。由于道德方面的考虑，所有的客户端都在我们的控制之下。为了全面评估这种攻击在现实世界中的影响，我们在世界各地的不同地点部署了6个controlled客户端（有利位置），即法兰克福、新加坡、加利福尼亚、东京、上海和多伦多。4) 位于俄罗斯的恶意攻击者可以欺骗源IP地址，旨在通过制作ICMP重定向消息来误导焦油服务器的网络流量（发送到我们控制的客户端）进入检测到的邻近主机（即路由黑洞）。如果DoS攻击成功，客户将无法收到来自脆弱服务器的响应。

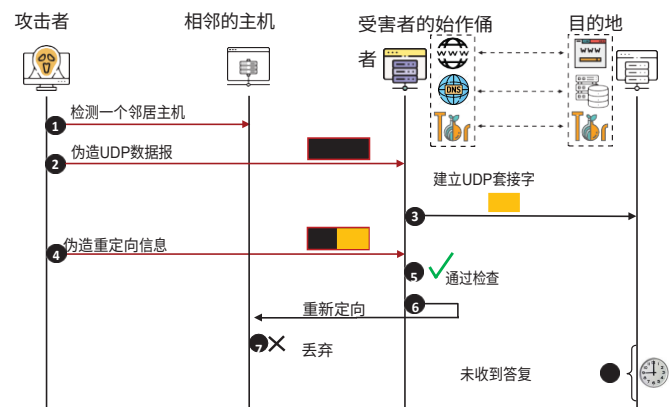


图6：Overview of DoS attacks.

实验结果。图7显示了我们的细节

DoS攻击测量结果。由于不同的网络条件，观察到的易受攻击网站的数量从

不同的视点有很大差异。例如，在弗兰克-此外，我们检测到28,604个脆弱的网站，而在上海、的攻击设计中的受害者发起者，如图6所示），其出站流量可能被伪造的ICMP重定向所操纵。在这个测量研究中，我们使用Alexa前100万网站的服务器作为目标。

2) 目标服务器的邻近主机，它们与服务器居住在同一网络中。这些主机可以被检测到

⁵ 例如，网站 "www.mit.edu" 的一个IP地址是104.76.0.251，我们可以探测到一个IP地址为104.76.0.252的活着的主机是它的邻居，它有相同的TTL和相同的网关（106.187.29.182）从我们的有利位置。

我们只能检测到19,603个脆弱的网站。我们把从六个观测点检测到的易受攻击网站集合在一起（删除在不同观测点检测到的重复网站），然后我们发现位于2872个AS和130个国家的43,081个流行网站对我们的DoS攻击是脆弱的。因此，在Alexa排名前100万的网站中，易受攻击的网站的比例约为4.3%。⁶有趣的是，在统计了我们检测到的最接近的1万个网站中的易受攻击网站的数量后，我们发现，网站的排名越低，它就越有可能被压缩，这也与普通的直觉相一致。

我们阐述了我们的DoS攻击可能失败的原因，如图7所示。平均来说，列表中有17.73%的网站无法从我们的有利位置到达，主要是由于两个原因。首先，我们的客户不能成功地重新

⁶ 2019年，Robert等人[53]测得Alexa前100万名中有1.3%的网站存在TLS padding oracle漏洞[84]。与TLS padding oracle攻击相比，Alexa前100万名中更多的网站容易受到我们的攻击。

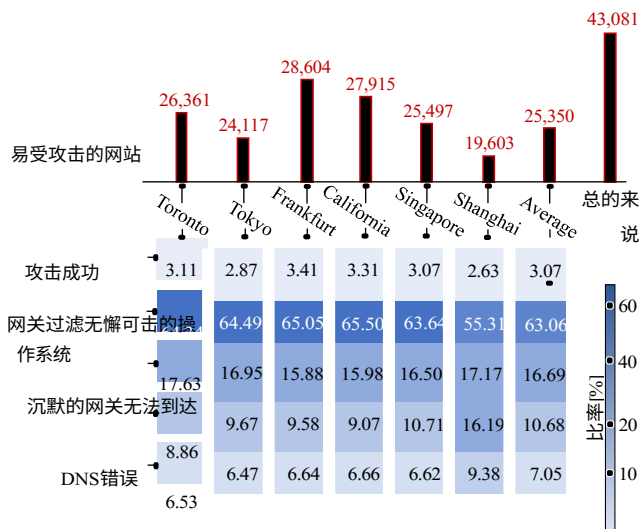


图7：针对流行网站的DoS测量研究。

收到请求网站的DNS回复（在不同的范围内）。阶段，比例在6.47%和9.38%之间变化）。第二，我们的客户无法连接到目标网站（在不同的有利位置，比例在8.86%和16.19%之间）。这两种无法访问的情况主要是由审查制度[71, 82]和ISP过滤规则[66]造成的。在计算我们攻击的成功率时，我们不考虑这些无法访问的网站。沉默的网关造成了16.69%的失败，也就是说，被检测到的网络服务器的网关没有对我们的探测做出反应。这些网关不透露他们的IP地址，因此攻击者不能冒充网关向target服务器发送恶意的ICMP重定向消息。63.06%的失败是由于网关过滤（如入口过滤[28]）或易受攻击的操作系统（如ICMP错误信息节流）。图8展示了我们检测到的脆弱网站的地理分布。

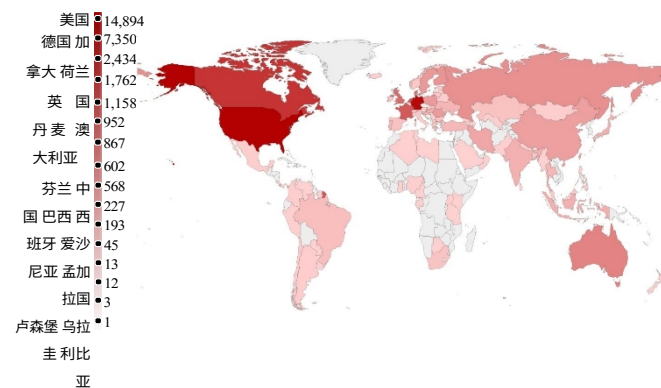


图8：脆弱网站的地理分布。

5.4 额外的攻击场景

ICMP合法性检查中的漏洞，例如，DNS解析器和下游的作者名称服务器之间的通信以及Tor中继节点之间的通信。我们对后端服务器之间的通信的DoS攻击将对现实世界造成更严重的破坏。例如，如果我们能阻止DNS解析器联系其下游权威名称服务器来解析某些域名，那么所有连接到易受攻击的DNS解析器的用户将被阻止访问这些域名。

在我们针对DNS和Tor的DoS攻击测量研究中，公共DNS解析器和Tor中继节点取代了§5.3中的网络服务器（即图-ure 6中的受害者发起者，其出站流量可能被误导到黑洞）。相应地，我们的受控下游授权者命名服务器和Tor中继节点取代了受害者网络客户端（即图6中的目的地）。

表3：DoS攻击测量结果的比较。

目标	数量	无法进入的	无坚不摧的操作系统	数量
		网关	或过滤	Vuls.
DNS解析器	1,951,381	39.69%	15.74%	54,470
				(4.63%)
Tor中继节点	6,518	18.52%	26.22%	186
				(3.50%)
网站	亚历克莎上衣100万	17.73%	16.69%	25,350
				(3.07%)

表3显示了我们在不同网络场景下的DoS攻击测量结果的比较。与热门网站的平均测量结果相比，我们发现互联网上有54,470个开放的DNS解析器（占从Censys[23]获得的1,951,381个目标的4.63%）和186个Tor重铺节点（占从Dan[21]获得的6,518个目标的3.50%）容易受到我们的DoS攻击，这意味着这些公共服务器的网络流量可以被重新操纵。

动的。请注意，在计算易受攻击的比例时，我们不考虑我们在加州部署的权威名称服务器和Tor中继节点的无法访问的目标。不受我们的DoS攻击影响的原因也在表3中列出。

6 网络流量劫持攻击

6.1 威胁模型

图9说明了我们对于网络流量的威胁模型

除了针对个别用户（即阻止一个人访问一个网站），路径外的攻击者甚至可以通过利用以下方式切断后端服务器与服务器之间的通信。

通过恶意的ICMP重定向进行劫持攻击。与DoS攻击的威胁模型不同，在这个模型中，攻击者和网络流量将被恶意操纵的受害者发起者居住在同一个网络中。攻击者和发起者所连接的网关可能是不同的，例如，将客户捆绑在一个公共IP地址后面的NAT设备、企业或家庭网络的路由器、生成和部署流量的SDN控制器。

规则[13]。请注意，尽管攻击者和受害者发端者居住在同一个网络中，但由于发端者和攻击者是通过交换网络（而不是广播链路网络）连接到网关的，所以路径外攻击者无法窃听发端者的流量。攻击者的目的是将发端者的目的地流量重定向到自己身上，并作为发端者的新网关，从而劫持发端者的流量，演变成MITM。

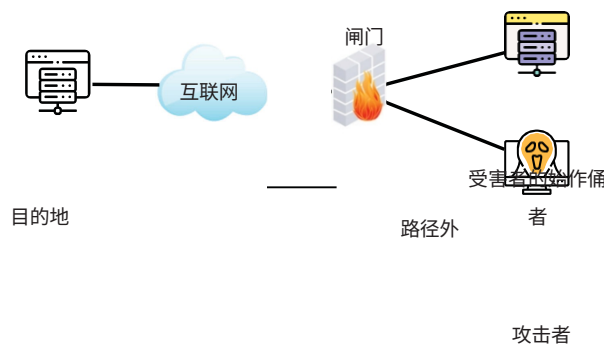


图9：劫持攻击的威胁模型。

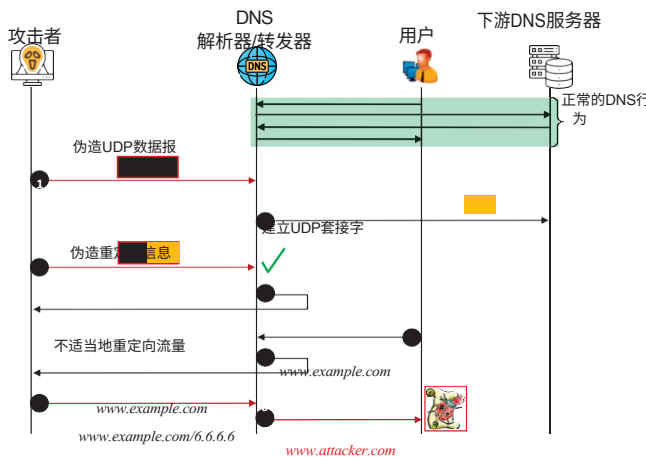
与DoS攻击相比，当攻击者和受害者发起者居住在一个网络中时，IP欺骗是可能的。⁷因为阻止欺骗数据包的安全功能通常部署在网关（较高的侵略层），以过滤流过的网络流量 [28]，ICMP内部欺骗的重定向不通过网关，因此不受阻挡。此外，由于攻击者是受害者发端者的一个活的邻居主机，它在满足最后一个要求并成为新的网关上没有困难（见 §5.1）。

6.2 DNS请求劫持的案例研究

我们的攻击可以在各种情况下进行，以保证网络的安全。我们在一个真实的摄像机网络中进行了一个案例研究，表明我们的攻击可以对NAT网络造成严重的破坏。由于IP地址空间的耗尽，NAT被提议作为一个标准，以允许互联网的扩展继续下去，而不转移到IPv6 [81]。现在，NAT无处不在，特别是在校园网、企业网和住宅网的边缘[47]。在NAT网络中，本地DNS解析器[36, 54]或DNS守护者[36, 72]相当普遍[40, 72, 73]，因为它们可以在本地访问，以减少网络延迟，避免直接暴露于互联网攻击者[35]。在这个问题上，我们表明，路径外攻击者可以劫持来自本地DNS转发器的查询，然后毒害NAT网络的本地DNS缓存。因此，路径外攻击者可以隐蔽地操纵同一网络下所有用户的DNS请求。我们在真实的校园

在一个单一的公共IP地址后面。2) 一个部署在NAT网络中的脆弱的DNS for- warder，它配备了Linux内核5.5版本和BIND 9.16.8。DNS for- warder接收来自NAT网络中用户的DNS请求，然后转发这些查询。3) 一个远程的下游DNS服务器，接收来自转发器的查询，并将答案返回给转发器。在我们的测试中，我们将谷歌的流行DNS服务8.8.8.8设置为下游DNS服务器。4) NAT网络中的受害用户，他们访问本地DNS转发器，获得他们查询的域名的IP地址。5) 位于同一NAT网络中的非路径攻击者-

工作。攻击者没有能力窃听他人的流量，它的目的是通过恶意的ICMP重定向，将DNS转发器的流量重定向到自己身上。因此，攻击者，可以劫持DNS请求，然后毒害整个NAT网络的DNS缓存。



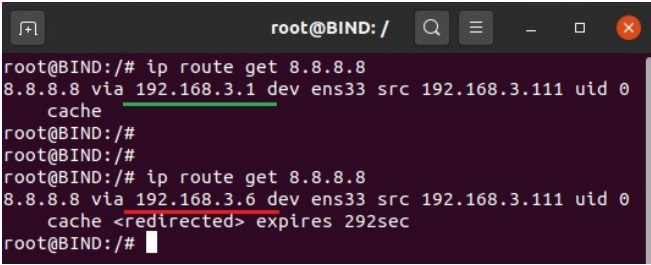
网络中实现了这种攻击，并在道德上显示了其严重性。
实验设置。在这次攻击中涉及5种类型的设备。1) 一个捆绑了120个客户端的HUAWEI NAT网关

⁷ 我们测试了10个真实世界的交换网络，即4个校园以太网LAN，4个企业以太网LAN和2个政府以太网LAN。在所有情况下，我们都能顺利地传递被欺骗的ICMP重定向信息。

图10：NAT网络中的非路径DNS 请求劫持。

实验工作流程。图10展示了如何通过恶意的ICMP重定向在NAT网络中进行非路径DNS请求劫持的工作流程。在正常情况下，DNS的行为是非常直接的。用户向转发器（或解析器）发送DNS查询。转发器和远程服务器完成域名到IP地址的映射，然后将查询结果反馈给用户并缓存在转发器中。在我们的攻击中，攻击者首先冒充服务器向转发器的监听端口5353发送UDP数据报，因为我们观察到多播DNS服务在目标转发器中始终可用。转发器将被欺骗建立一个可预测的UDP套接字，允许攻击者伪造可接受的ICMP重定向消息，并指定攻击机器为转发器的新网关。在转发者对下游DNS服务器的流量被成功重定向后，用户对转发者的DNS查询如果没有被缓存，就会被错误地转发到攻击者那里。然后，路径外的攻击者会丢弃原始的DNS查询，冒充DNS服务器向转发者发送伪造的答案。最后、

转发器用一个假的IP地址回复用户，这个地址也将被缓存在转发器中。因此，由于缓存poisoning，NAT网络中的所有用户都将受到隐蔽的影响。



```
root@BIND: /
root@BIND: /# ip route get 8.8.8.8
8.8.8.8 via 192.168.3.1 dev ens33 src 192.168.3.111 uid 0
cache
root@BIND: /#
root@BIND: /#
root@BIND: /# ip route get 8.8.8.8
8.8.8.8 via 192.168.3.6 dev ens33 src 192.168.3.111 uid 0
cache <redirected> expires 292sec
root@BIND: /#
```

图11：中毒的 DNS解析器的路由缓存。

实验结果。图11显示了易受攻击的本地DNS转发器（其IP地址为192.168.3.111）的中毒路由缓存的结果。该DNS转发器到服务器8.8.8.8的原始网关是192.168.3.1。然而，一旦攻击者执行了我们的劫持攻击，DNS转发器到8.8.8.8的下一跳就会被改写成攻击主线，即192.168.3.6。因此，攻击者可以拦截转发者的查询，然后冒充下游服务器，用假的答案回复转发者。

本地DNS缓存被毒害后，NAT网络中的所有用户都会受到影响，也就是说，路径外攻击者可以任意操纵用户的网络请求。图12显示，由于用户从中毒的DNS转发器收到了假的域名IP地址，用户（出于道德考虑，我们控制下的客户主机）对 "www.yahoo.com "网站的请求被劫持到一个假的网站。由于攻击流量小（实际上只有一个ICMP重定向数据包），劫持攻击是隐蔽的，这意味着成本也可以忽略不计。

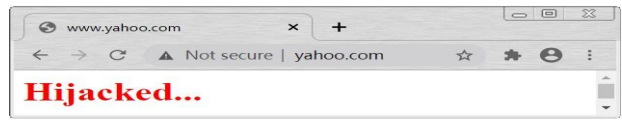


图12：DNS请求被劫持的快照。

7 讨论

负责任的披露。我们向Linux、FreeBSD和AOSP（安卓开源项目）社区报告了该漏洞 和我们的PoC。安卓已经确认了这个漏洞，目前正在与我们讨论对策。我们与

Linux和FreeBSD进行了几轮讨论，但还没有被告知任何决定。此外，我们在互联网上联系了16家受影响的供应商，以披露该漏洞，但还没有收到回复。

7.1 与现有攻击的比较

ICMP重定向攻击以前被认为只是局域网中ARP poisoning的现有操纵攻击的一种替代方法[77, 89]。然而，我们证明本文所开发的攻击是完全不同的。首先，通过利用ICMP合法性检查的漏洞，我们可以远程制作一个可接受的ICMP重定向消息来重写受害者的特定目的地的路由，而不是ARP表。因此，我们的攻击可以在互联网上进行，不受网络拓扑结构的限制。其次，我们的攻击更加隐蔽，因为攻击者只需要向易受攻击的目标发送一个伪造的ICMP重定向信息，而不是广播伪造的数据包（即ARP中毒攻击中的ARP回复数据包，可能导致IDS日志被可疑的流量记录填满）。此外，MAC-IP绑定[59,69]和未经请求的ARP回复丢弃[45,51,78]的对策已经被提出，以防止ARP中毒攻击。相比之下，我们的攻击很难通过这些对抗措施来预防，因为该行为在第二层是正常的。

7.2 来自路由缓存的影响

攻击规模与路由缓存大小有关。一旦攻击者成功地误导了受害者发端者对某一特定目的地的网络流量，受害者将在其路由缓存中用一个新的路由条目替换该目的地的路由条目。因此，多少个目的地的流量可以同时被操纵（即攻击规模）是由受害者发端者的路由缓存大小决定的。在实践中，我们观察到，路由缓存在现代操作系统上是动态分配的，其大小在不同的实现中是不同的。例如，在我们针对装有Linux内核版本3.9.10和5.4.0的脆弱服务器的实验中，我们可以通过向服务器并行发送伪造的ICMP重定向消息（指定不同客户的流量需要被重定向），迫使服务器失去连接，最多可达10240个客户。相比之下，对于装有FreeBSD内核12.2版本的易受攻击的服务器，我们可以迫使服务器同时失去多达55000个客户的连接。在不同的网络场景下，路由缓存大小对我们的DoS攻击的影响是不同的。例如，在我们针对网站和开放的DNS解析器的攻击中，受害者的路由缓存大小对于前者意味着有多少前端网络用户可能同时丢失，而对于后者意味着有多少后端域名可能同时丢失。

由于路由条目的时间限制，攻击失效。在我们的实验

中，我们发现在内核版本为3.9.10及以上的Linux系统中，中毒的路由（即路由缓存中的虚假路由条目是由一个精心制作的ICMP重定向消息导致的）将被缓存300秒。在300秒的时间限制之后，原始路由