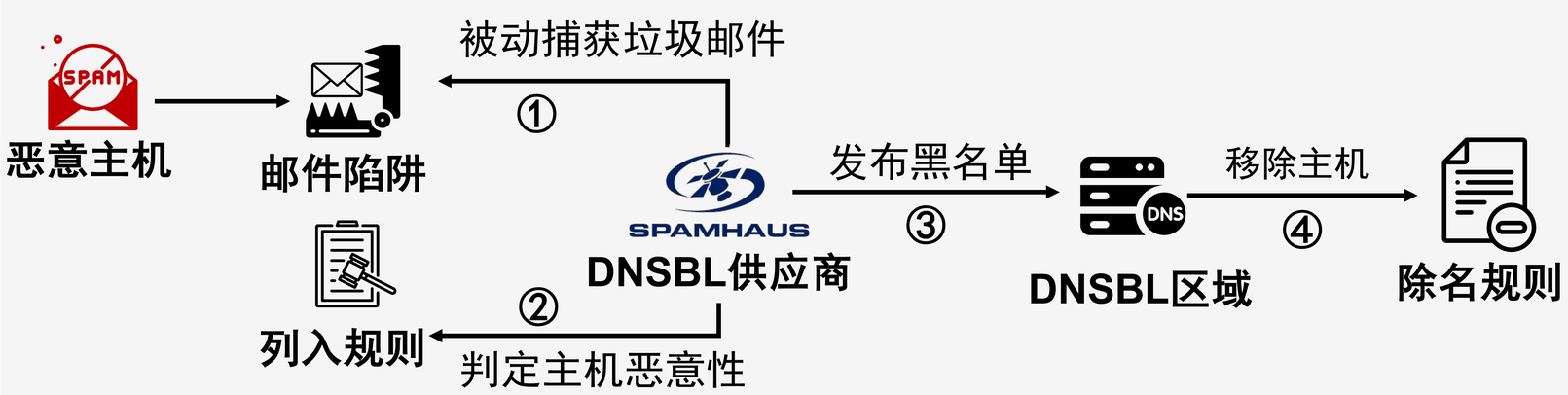
信任滥用危机：电子邮件领域流行黑名单操纵风险的实证研究

李瑞烜，陆超逸，刘保君，张允义，洪赓，段海新，林延中，潘庆峰，杨珉，邵俊

清華大學 Tsinghua University　复旦大學 FUDAN UNIVERSITY　Coremail　浙江工商大學 ZHEJIANG GONGSHANG UNIVERSITY

电子邮件黑名单（DNSBL）通过外表与正常邮件地址无异的邮件陷阱（蜜罐）被动捕获恶意主机

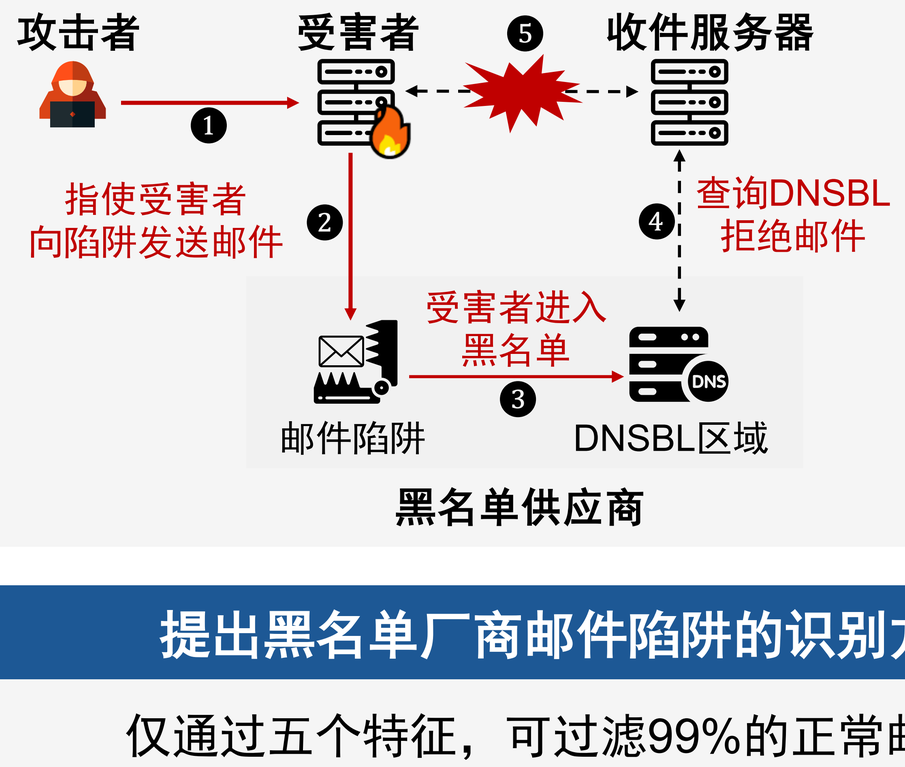


DNSBL被大量知名组织和机构信任

邮件供应商　yahoo!　sina

顶级域名注册局　.xyz　ShortDot THE VALUE IS IN YOUR NAME　RADIX

邮件黑名单操纵攻击：数分钟内将受害者注入黑名单中，隐蔽阻断流行服务器的邮件投递



风险来源：黑名单厂商过分信任单一邮件陷阱；受害者过分信任黑名单

攻击目标：将受害者注入流行DNSBL，使其声誉受损无法投递邮件

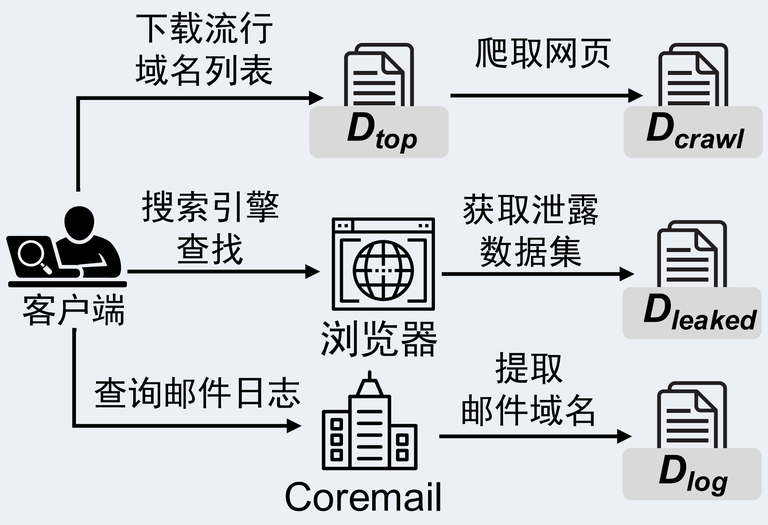
- 攻击者仅需向DNSBL供应商的邮件陷阱发送电子邮件
- 受害者涵盖大型邮件服务供应商、流行网站、重要域名注册局等等
- 整个过程受害者无明显感知，难以溯源

攻击方式：通过合法账号、订阅服务、受控服务器向邮件陷阱发送邮件

提出黑名单厂商邮件陷阱的识别方法，发现14个流行DNSBL供应商的数十万个邮件陷阱域名

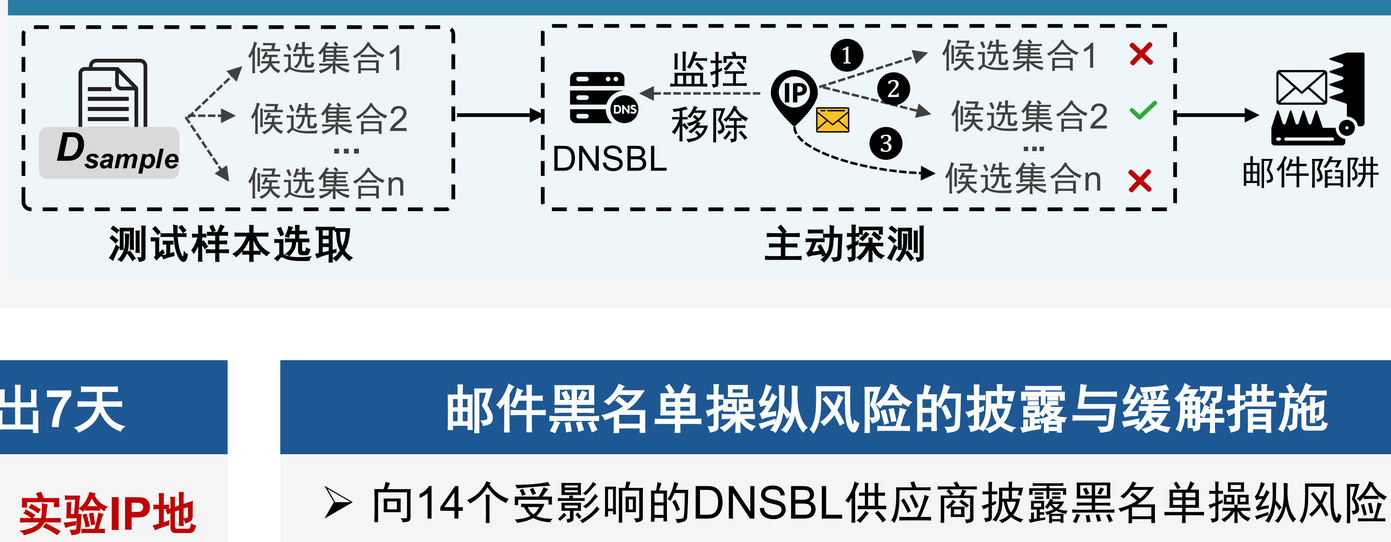
仅通过五个特征，可过滤99%的正常邮件域名，**发现知名威胁情报厂商Spamhaus的14万个邮件陷阱域名**

步骤一：收集邮件地址



步骤二：挑选候选邮件陷阱域名

步骤三：验证邮件陷阱域名



邮件黑名单的操纵危害：注入3分钟，移出7天

- 每分钟向Spamhuas的一个陷阱发送一封邮件，**实验IP地址在3分钟内被注入黑名单**，注入域名通常在6小时之内
- 列入黑名单的主机通常在7天后自动退出
- 四个域名注册局部署DNSBL，**可通过操纵黑名单删除51个顶级域（TLD）下的非受控域名**

邮件黑名单操纵风险的披露与缓解措施

- 向14个受影响的DNSBL供应商披露黑名单操纵风险，并讨论缓解措施，主要是避免暴露和过分信任单一邮件陷阱
- Spfbl采纳意见并承诺修复缺陷，其它供应商承认黑名单的操纵风险，但出于修复成本还在考虑中
- 未来研究：综合现网多方声誉提出抗操纵的邮件黑名单

受影响的主要DNSBL厂商

SPAMHAUS　ESTABLISHED spamcop.net 1998　SURBL　UCEPROTECT-NETWORK　fmb.la　SPFBL.NET
Brukalai.lt　JunkEmailFilter.com　Mailspike.io anubisnetworks　GBUdb.com　Sender Score

HADES Attack: Understanding and Evaluating Manipulation Risks of Email Blocklists.
Network and Distributed System Security Symposium (NDSS) 2025.

李瑞烜, https://ruixuanli.com
lirx25@mails.tsinghua.edu.cn