HADES Attack: Understanding and Evaluating Manipulation Risks of Email Blocklists

Ruixuan Li[1], Chaoyi Lu[1], Baojun Liu[1], Yunyi Zhang[1], Geng Hong[2], Haixin Duan[1], Yanzhong Lin[3], Qingfeng Pan[3], Min Yang[2], Jun Shao[4]

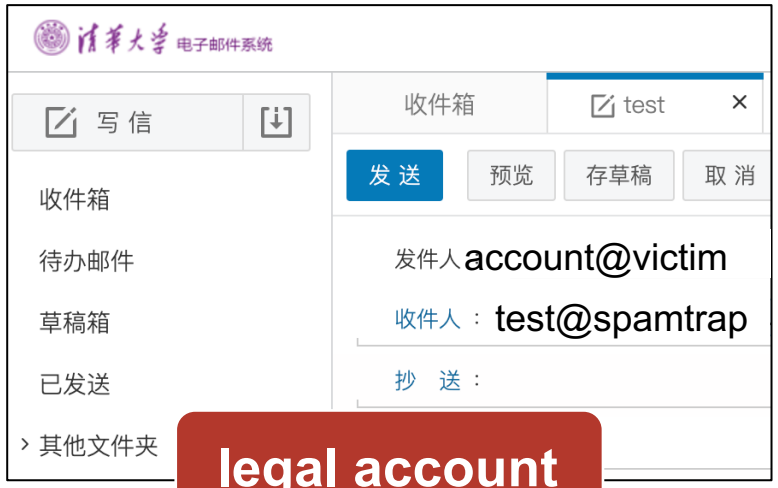
[1]Tsinghua University, [2]Fudan University, [3]Coremail Technology Co. Ltd, [4]Zhejiang Gongshang University

Manipulating DNSBLs: HADES Attack Impact

Inject hosts into popular email blocklists with just a few emails

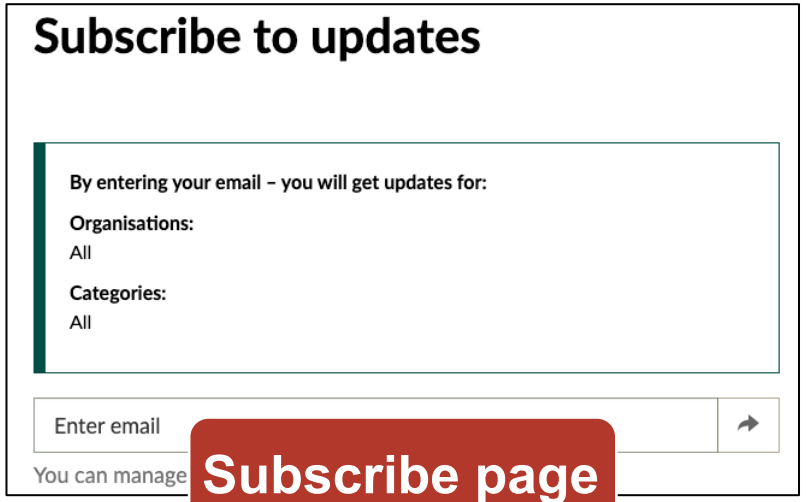
Victims' email deliverability is destroyed, even domain is deleted

Attack Methods



legal account

Hotcrp website



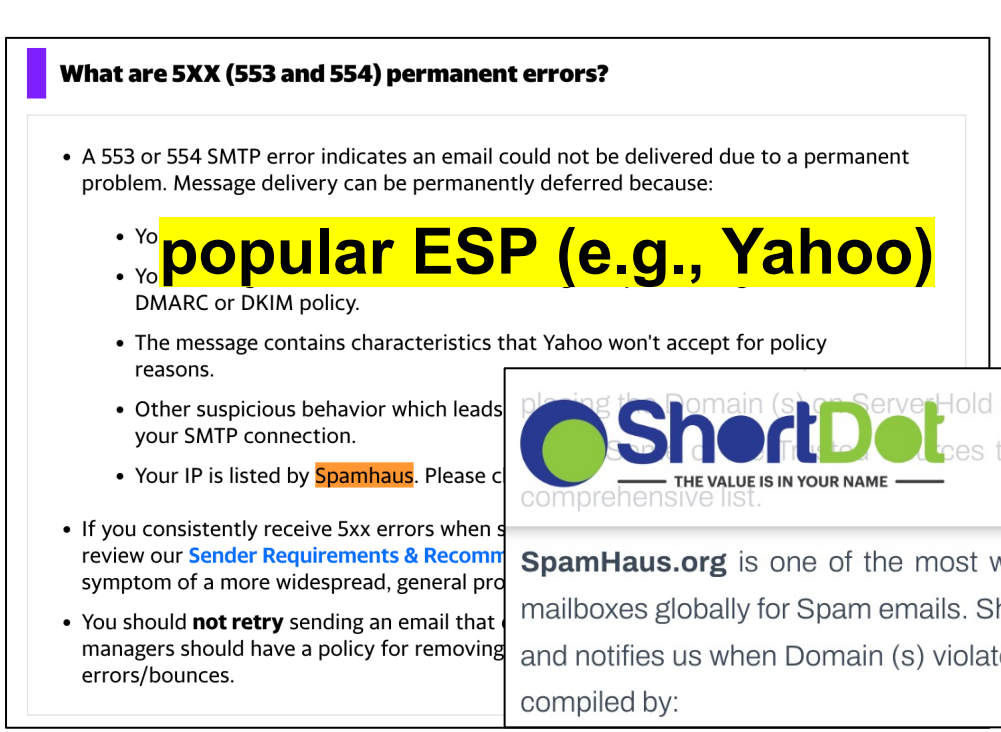
Subscribe page

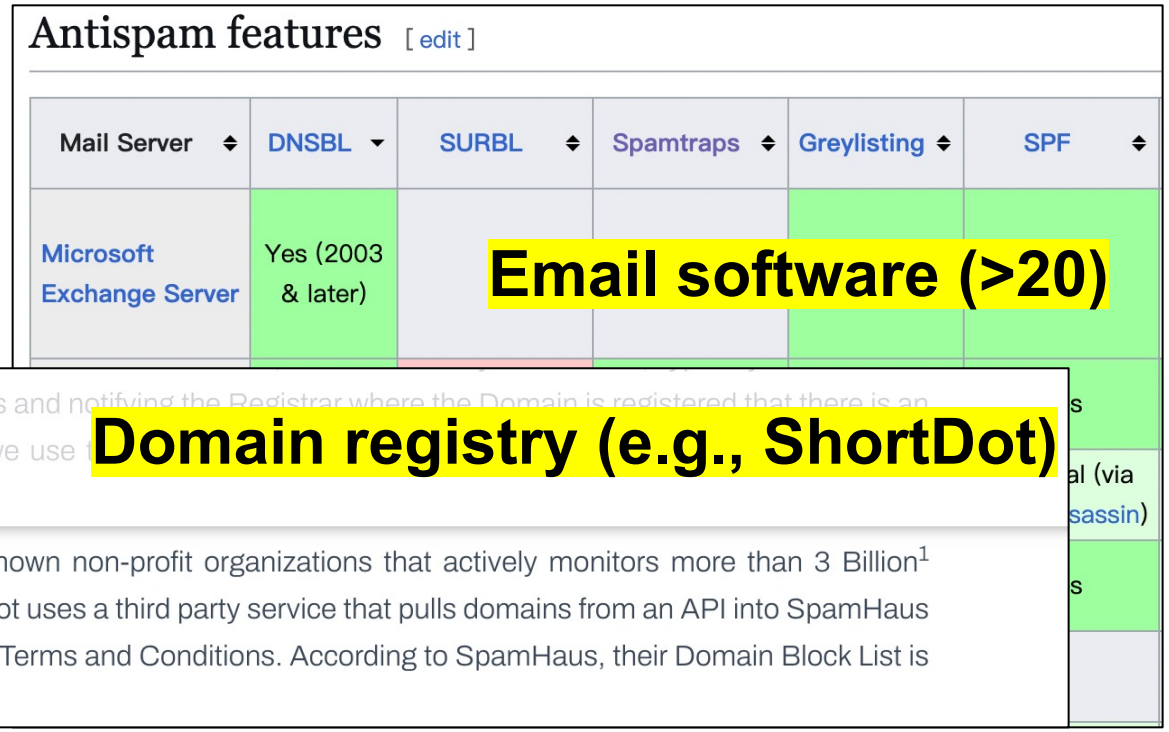
DNS-Based Blocklist (DNSBL)

An important mechanism in the fight against spam

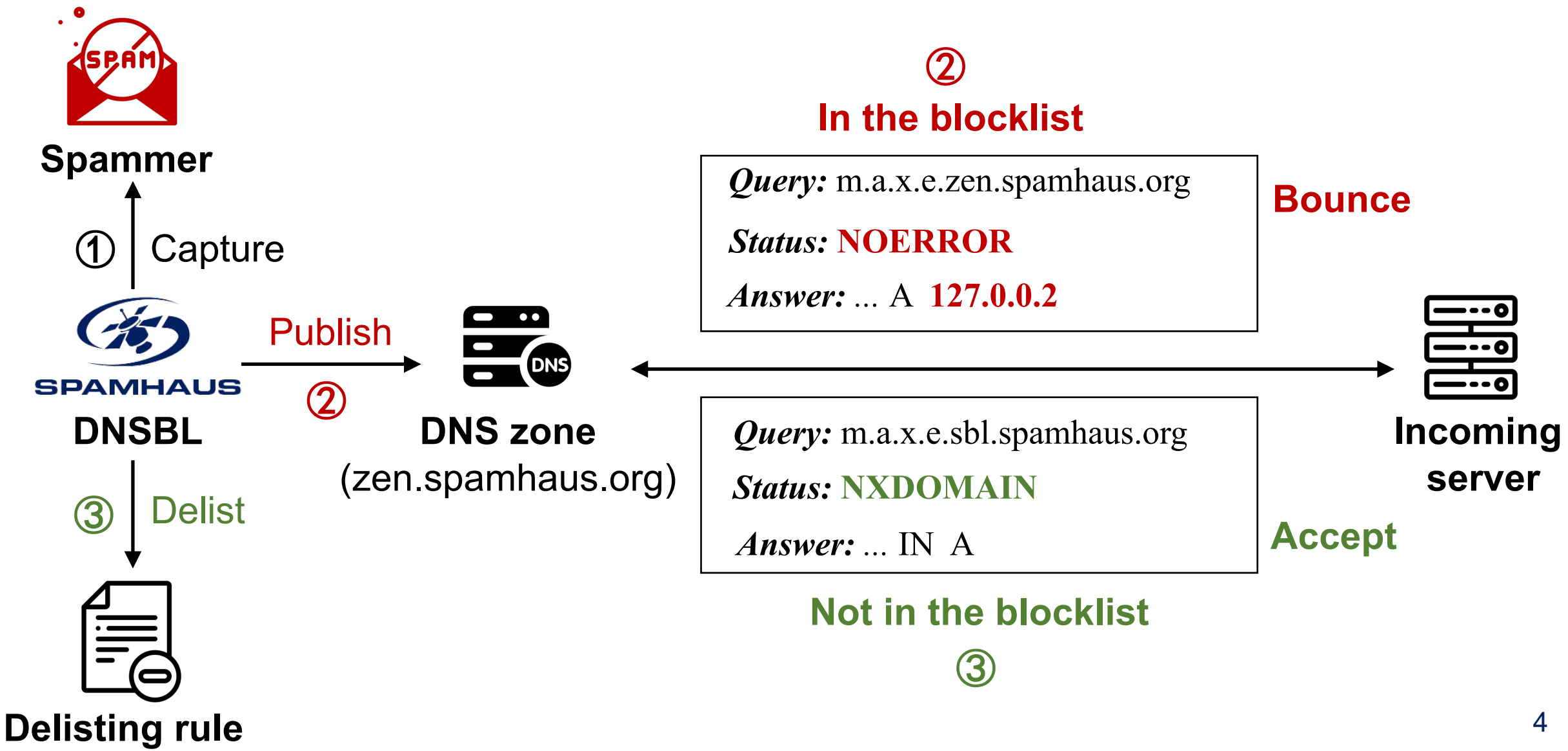
Including IP addresses and domains involved in malicious activities

Adopted by many popular ESPs, email software and domain registries





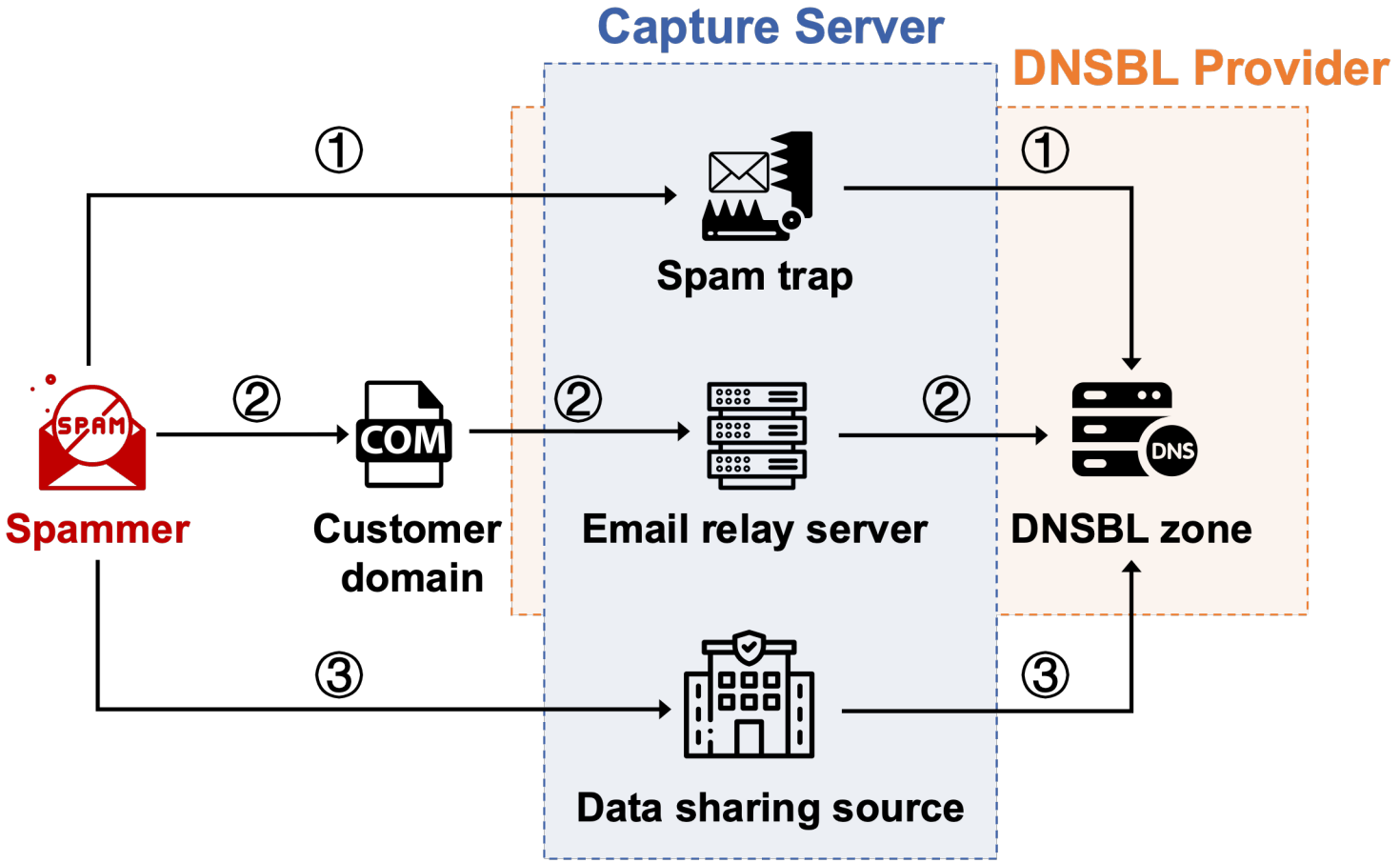
Know the host reputation through a DNS query



Capture server: report abuse to DNSBL providers

From an empirical analysis of 29 DNSBL providers (e.g., spamhaus)

- **Spamtrap** (Main target)
- **Email relay server**
- **Data sharing source**



Takeaway

DNSBL construction heavily rely on capture servers in identifying abusive servers

If the capture servers are identified,

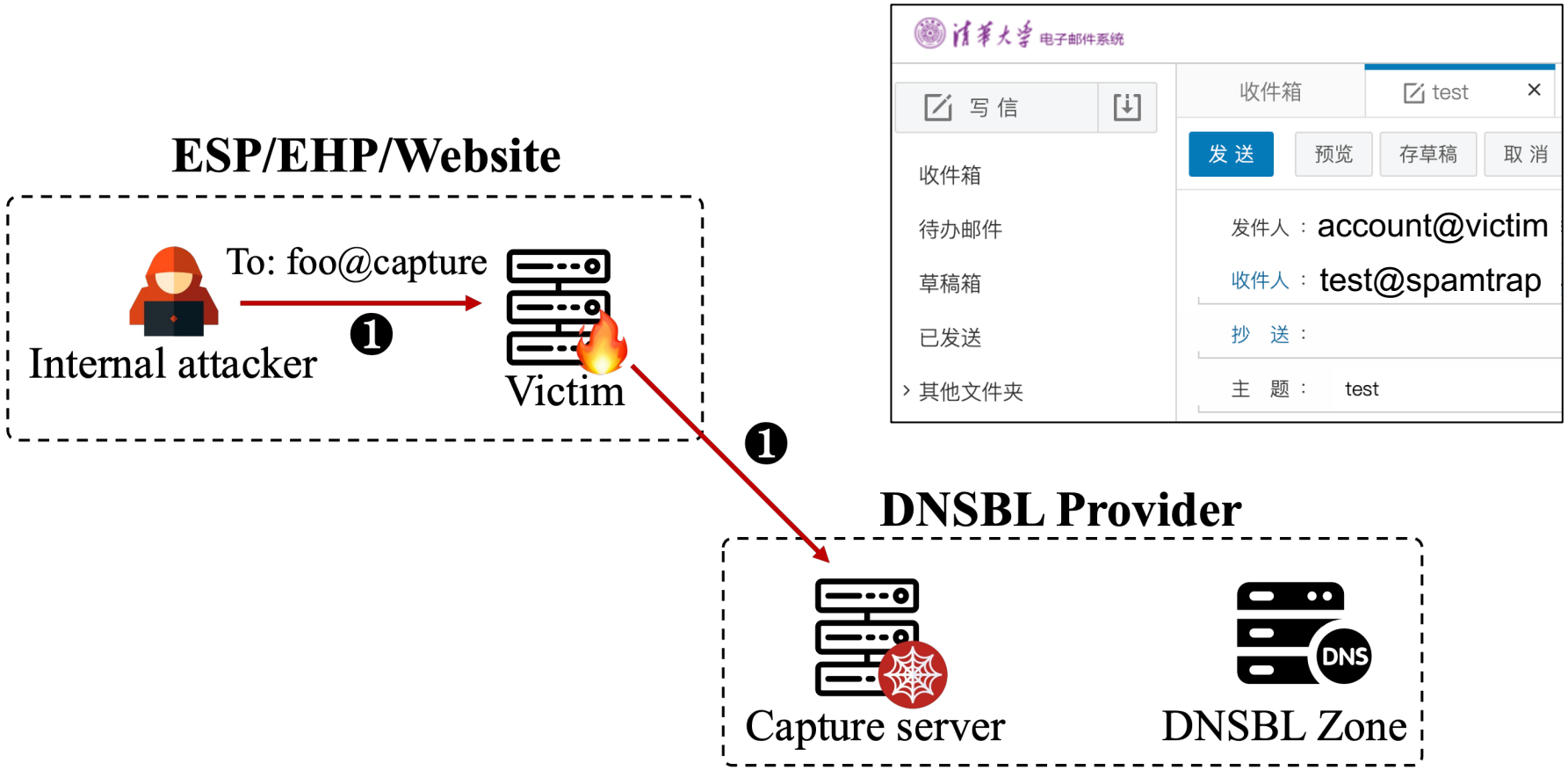
attackers can manipulate DNSBLs by feeding false intelligence

What is the HADES attack

- **Goal:** Compromise email delivery capabilities of outgoing servers, involving ESPs, websites ...
- **Main ability of attacker:** Identify the capture servers
- **Attack method:** Attackers simply instruct victims to send emails to capture servers
- **Attack name:** HADES (greek god of the underworld)

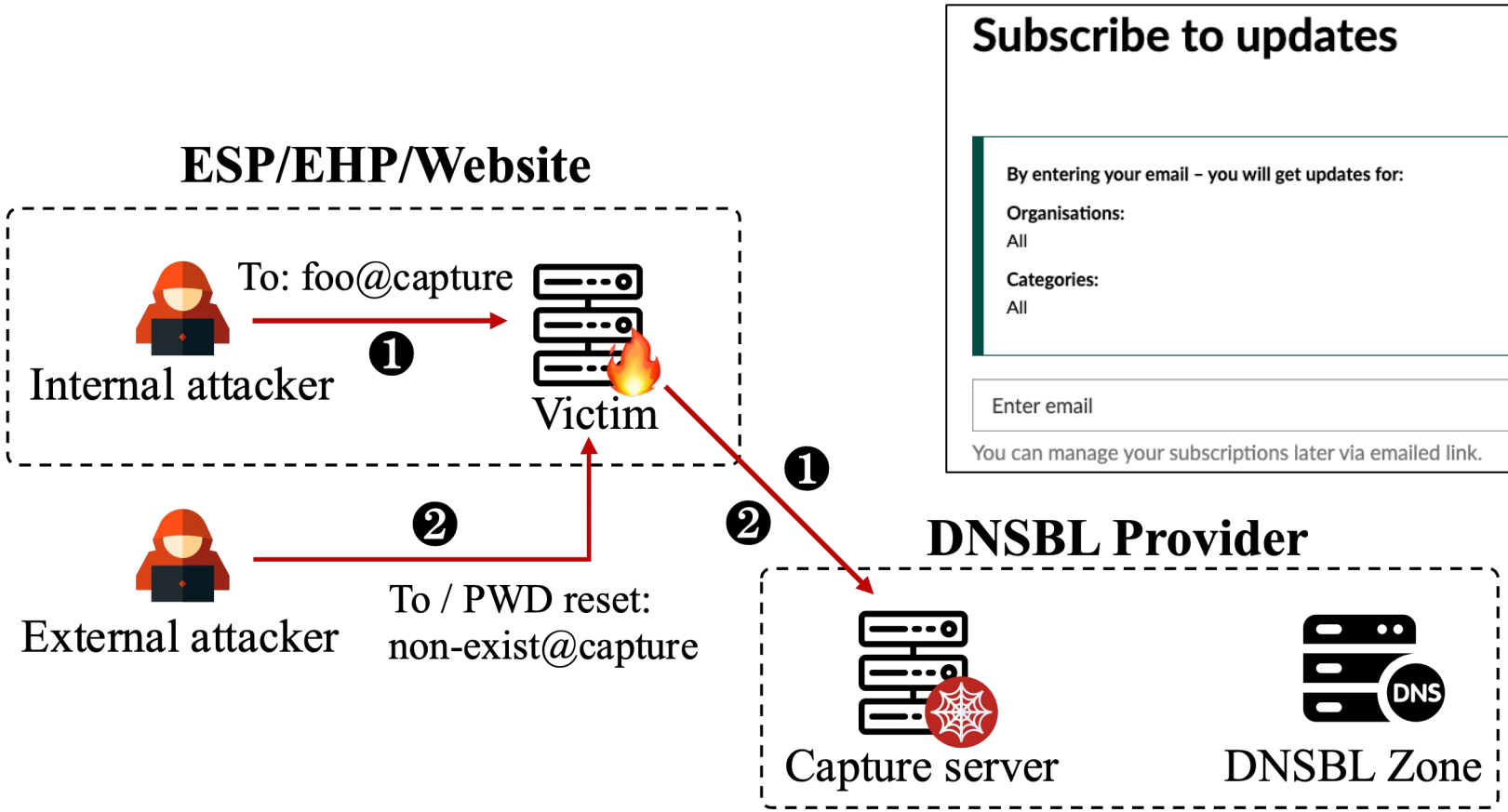
Threat model of HADES - Internal attack

Attackers hold the legitimate accounts of ESPs or enterprises



Threat model of HADES - External attack

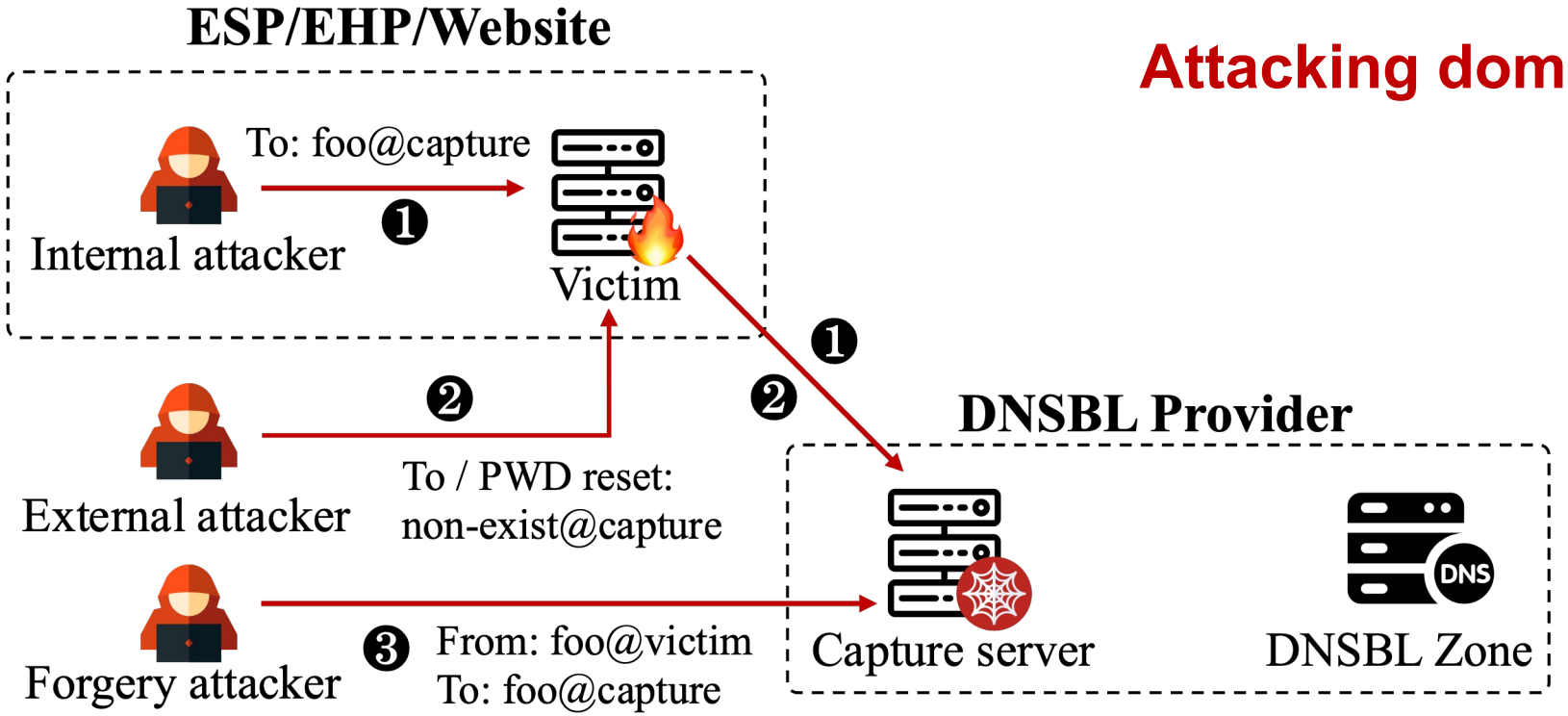
Attackers abuse email subscriptions or password reset services



Threat model of HADES - Forgery attack

Attackers send email from arbitrary IPs to capture servers

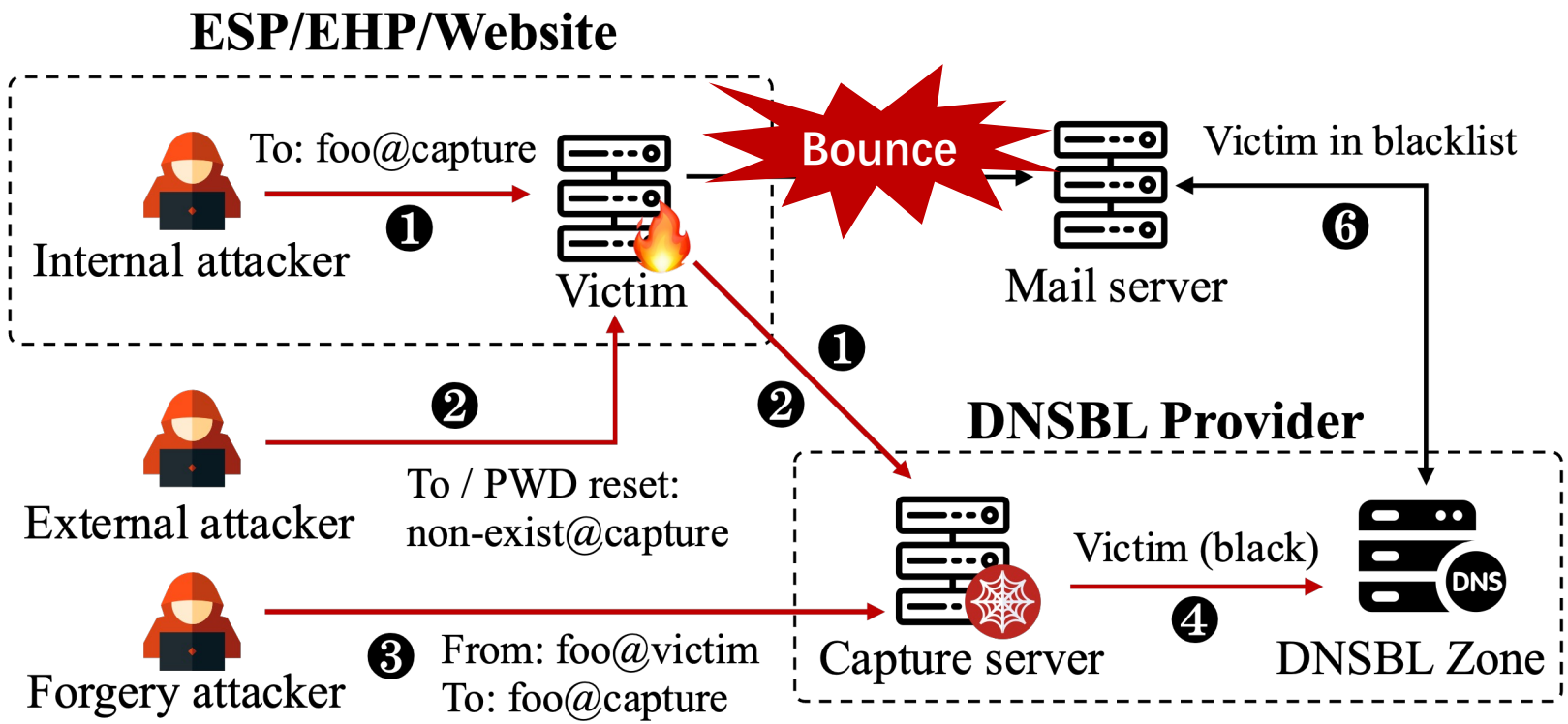
that do not perform sender authenticity checks



Attacking domains only

Threat model of HADES - Consequence

Emails sent by the victim to servers adopting DNSBL failed



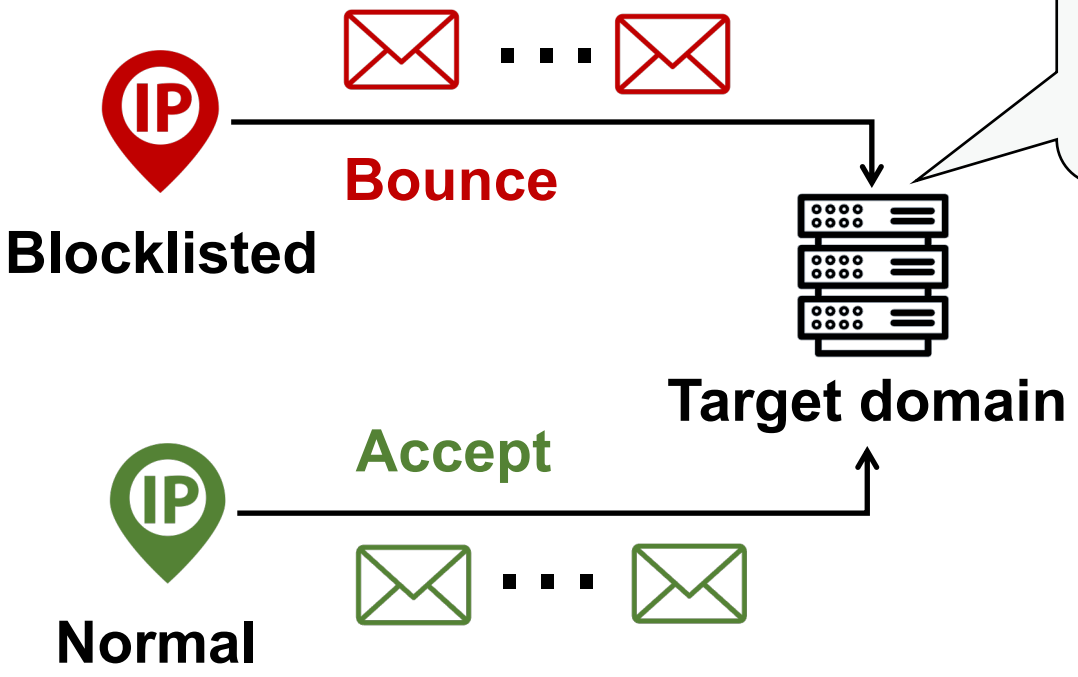
Key questions for implementing HADES

How broadly are DNSBLs adopted by email servers

Are capture servers of DNSBLs easy to discover

Methodology for DNSBL deployment measurement

Active Scan (ethical risks)



Passive Analysis (we used)

Bounce message

550 5.7.1 Service unavailable, Client host blocked using **Spamhaus**

key observations：

Target domain use spamhaus

We cooperated with Coremail, a large email provider, to obtain **190M bounce messages within 15 months** and match DNSBL provider names.

DNSBL is deployed by many email servers

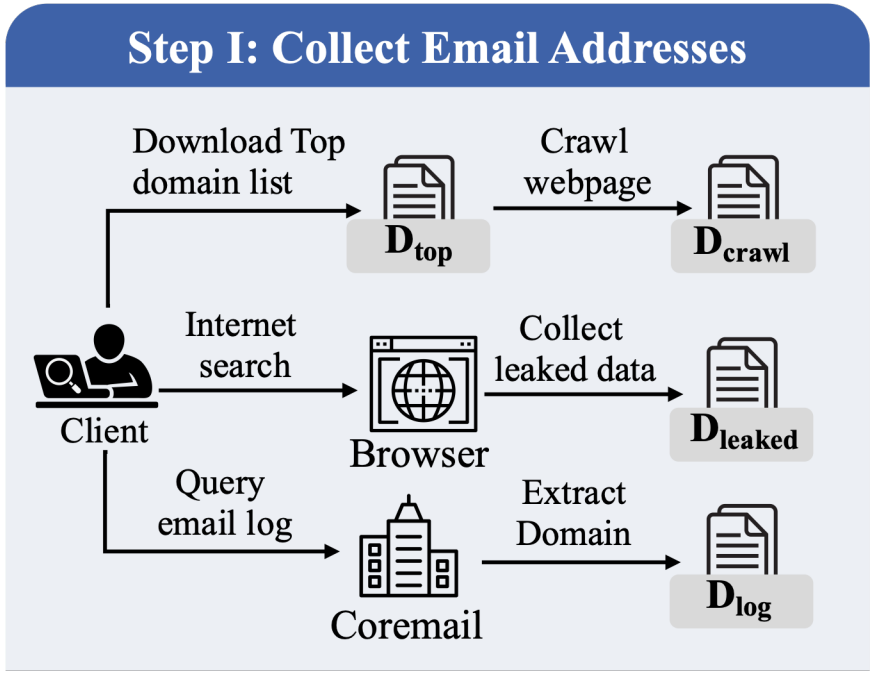
- 307,244 domain names deploy DNSBLs, of which Spamhaus accounts for 90.06%
- 53% of Top 100 domains deploy DNSBLs, 45% of Top 1K domains deploy DNSBLs

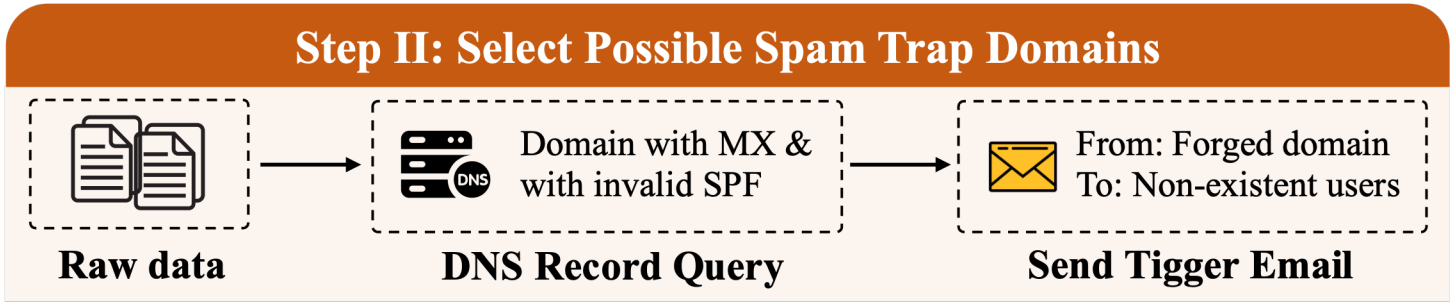
DNSBL	# of domains
spamhaus.org	288,514 (90.05%)
spamcop.net	15,825 (4.94%)
uceprotect.net	3,304 (1.03%)
junkemailfilter.com	3,157 (0.99%)
sorbs.net	2,466 (0.77%)

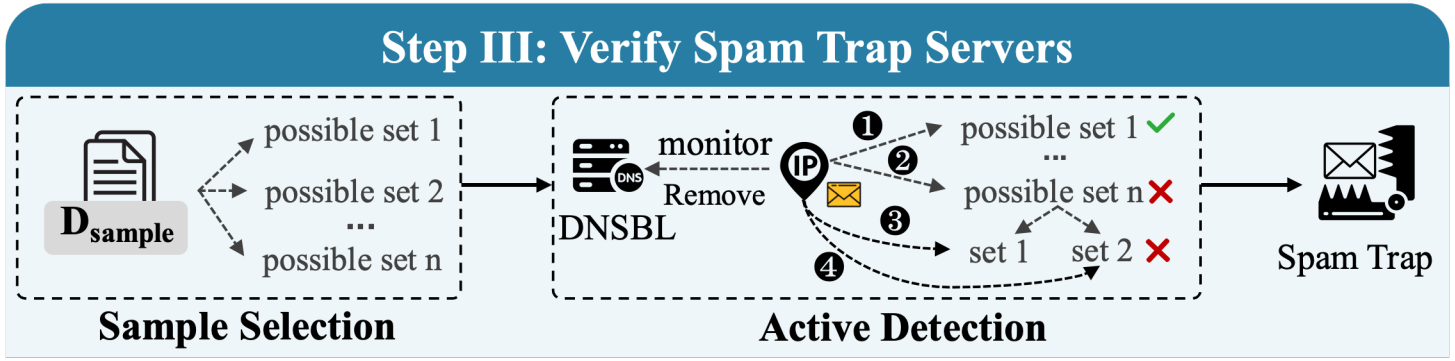
ESP	IP Blocklist	Domain Blocklist
outlook.com	YES	YES
hotmail.com	YES	YES
yahoo.com	YES	NO
icloud.com	YES	YES
tom.com	YES	NO
sina.com	YES	NO
sohu.com	YES	NO

How to discover spamtraps?

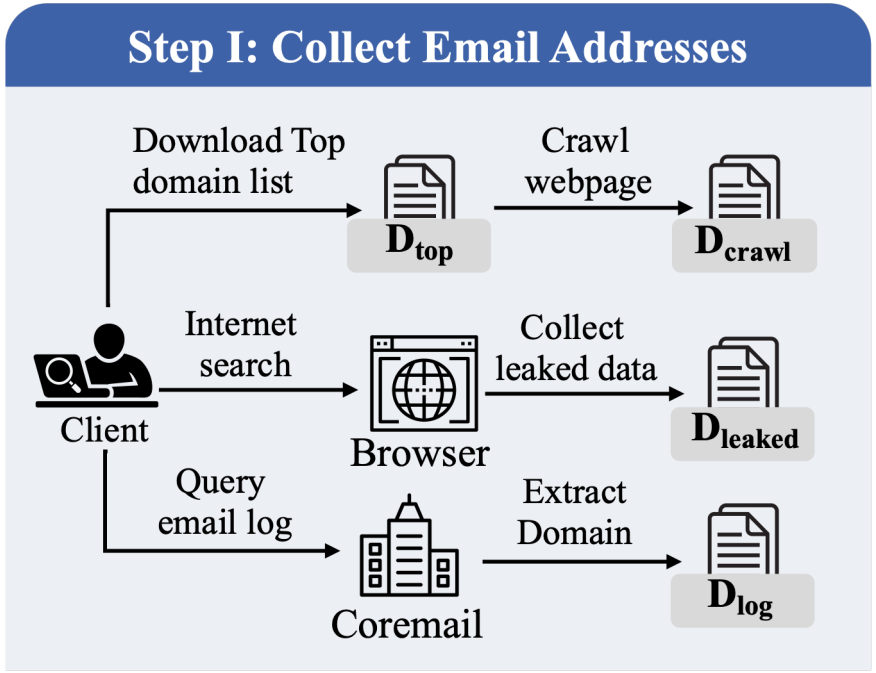
- **Challenge:** Spamtraps are hidden and opaque, and blind detection lead to ethical risks
- **Our Approach:** Shortlist domain datasets through features, and then actively verify spamtraps







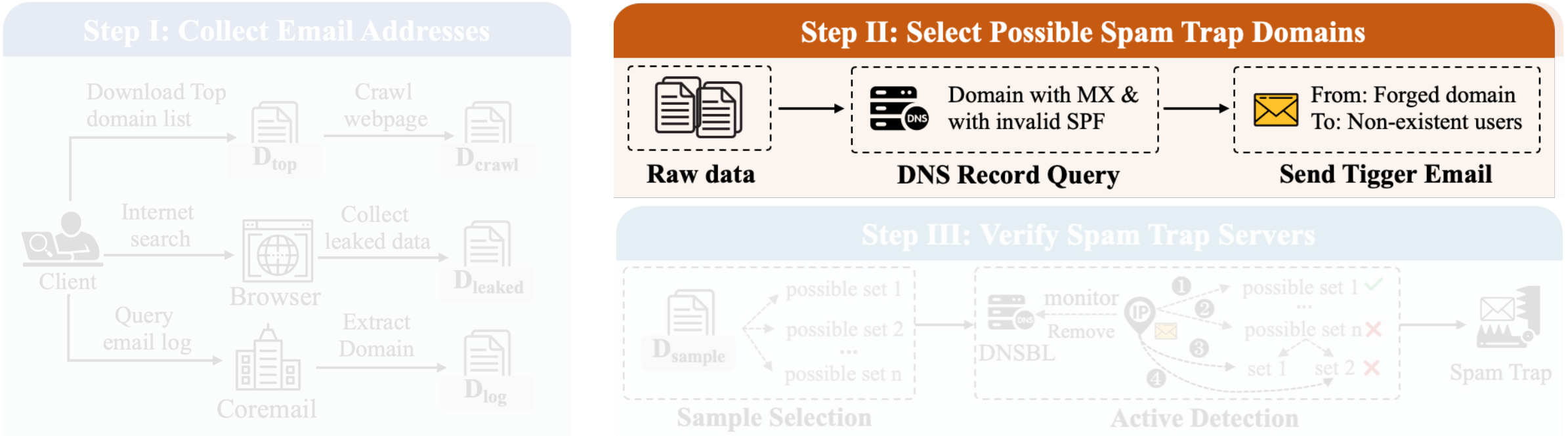
Step I: Collect email addresses



We collected **30M email domains** from four sources to cover as many spamtraps as possible:

- Three Top1M domain lists (D_{top})
- Email address in Top website (D_{crawl})
- Four leaked email datasets (D_{leaked})
- Coremail's email address log (D_{log})

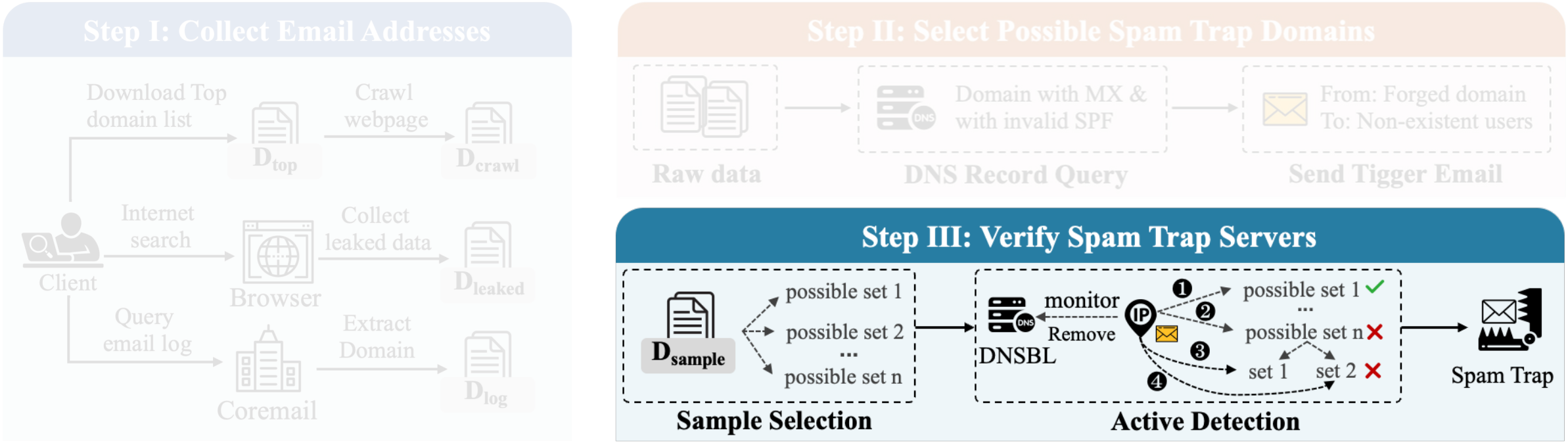
Step II: Select spamtrap domain candidates



We noticed that spamtraps usually do **not send and reject emails**:

- Configure MX record
- Not reject emails with failed authentication
- Not reject emails with non-existent users
- Configure unavailable SPF records
- Not return bounce emails

Step III: Verify spamtrap domains



Actively send emails to different domain candidate sets

If the sender IP hits the DNSBL, the candidate set is narrowed for further detection

To avoid ethical risks, we only carefully selected 21 domains for active verify

(Attackers can easily apply for many IPs for testing)

Spamtraps of 14 DNSBLs can be easily identified

We filter out **99% of email addresses** through our proposed features

In total, we find 140,449 spamtrap domains of Spamhaus

Dataset	# Domains	# with MX	# with unavailable SPF	**# trap candidates**	**# hit DNSBLs**
D_{top}	2,430,940	1,064,761	219,380	**17282 (0.71%)**	**11**
D_{crawl}	208,847	312,532	36,058	**702 (0.33%)**	**3**
D_{leaked}	26,845,147	11,385,214	3,093,727	**233868 (0.87%)**	**12**
D_{log}	3,350,518	2,939,404	500,403	**31102 (0.92%)**	**13**

Vulnerable DNSBLs

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

Manipulation cost: 3 minutes in, 7 days out

The injection cost of the attacker:

- IP addresses are usually within 2 hours, and domains are usually more than 6 hours **(rate: 1/s)**
- It takes only **3 minutes** to inject an ip address into Spamhaus blocklist **(rate：1/m)**
- Spamhaus, junkemailfilter and Sulbl **do not strictly verify email authenticity**, so attackers can inject forged domains

The delist cost of the victim:

- Blocklisted hosts **usually delist automatically after 7 days**
- 5 DNSBL providers do **not support early delist**
- DNSBL providers increase penalties for repeated listings of hosts

Practical considerations

Theoretically, HADES attack could affect all IP addresses with outgoing email capability and arbitrary domains.

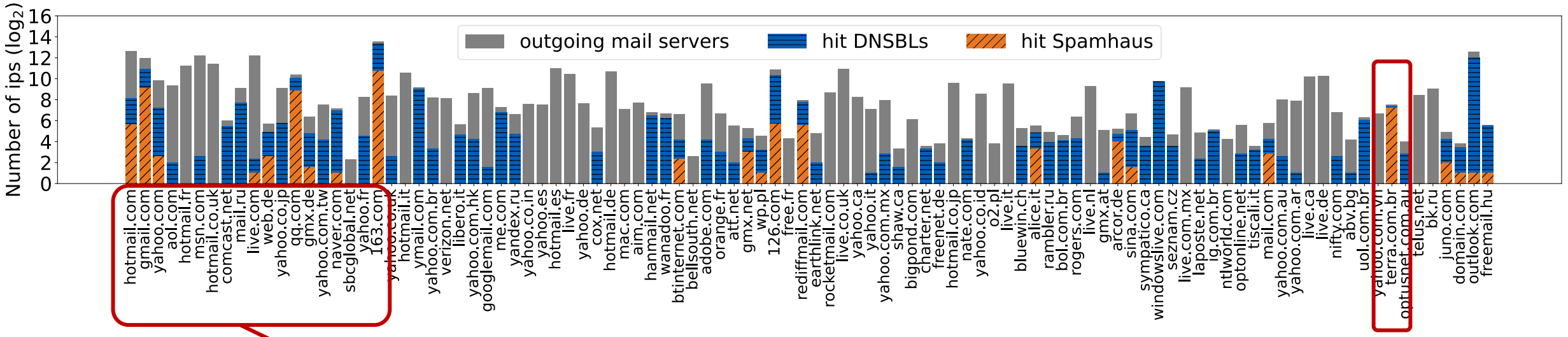
Whether DNSBLs can prevent mis-listing of popular servers

Whether existing security protections are effective against HADES

77% of popular outgoing servers can be listed in DNSBLs

Historically blocklisted servers can be injected into DNSBL again

We monitor reputation of outgoing servers for Adobe Top1K domains within 2 months



Hit Spamhaus

hotmail.com, gmail.com, yahoo.com, live.com, web.de, qq.com, 163.com

Some considerations for attacking high-profile victims

Attacking popular email service providers:

- The number of outgoing servers of popular suppliers is also limited (50% of Adobe Top1K domains are less than 30)

Attacking important websites:

- Email subscription and password reset are the default functions of most popular websites, and 608 government domains support email subscription services

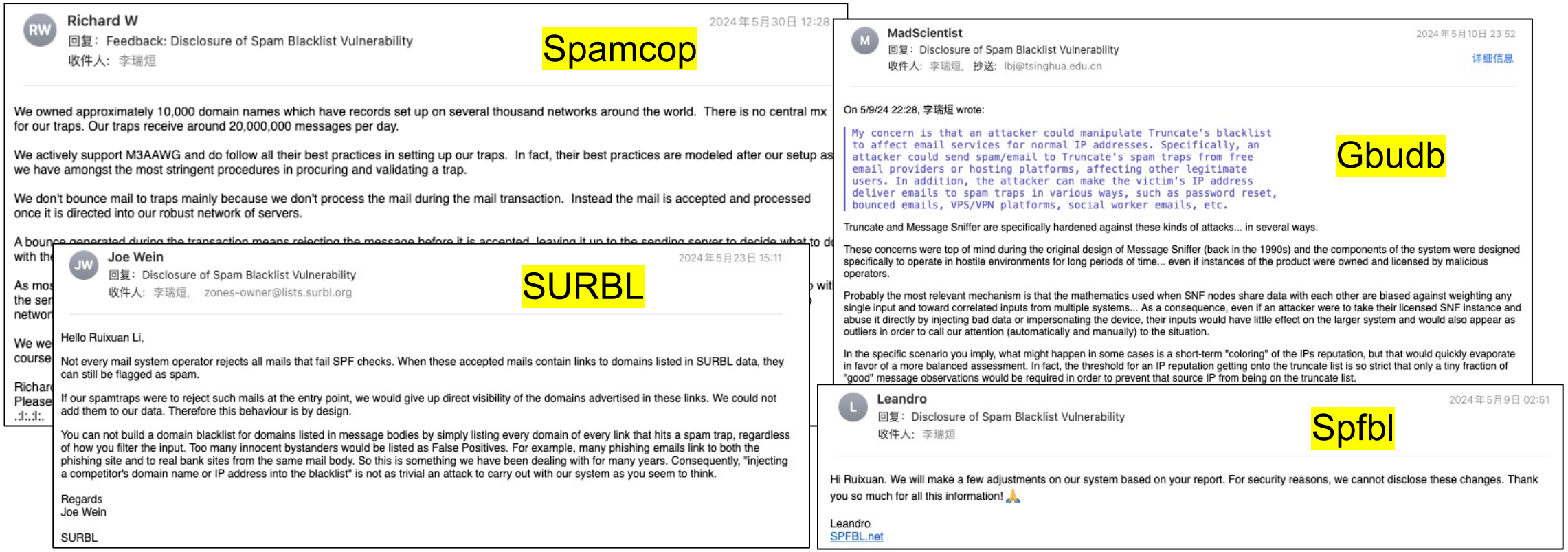
Escalated damage by domain registries:

- 4 registries use DNSBL to delete abusive domains, and domains under 51 TLDs are affected
- A registry (Radix) deletes blocked domains in about one day

Vulnerability Disclosure

Report HADES to all 14 affected DNSBL providers and discuss mitigations:

- Spfbl adopts suggestions and promises to repair
- Other providers recognize the manipulation risk but worry about the cost of fixing it



Thanks for Listening!

Ruixuan Li

Email: *liruixuan@mail.tsinghua.edu.cn*

Website: *https://ruixuanli.com/*