

HADES Attack: Understanding and Evaluating Manipulation Risks of Email Blocklists

Ruixuan Li¹, Chaoyi Lu¹, Baojun Liu¹, Yunyi Zhang¹, Geng Hong², Haixin Duan¹,
Yanzhong Lin³, Qingfeng Pan³, Min Yang², Jun Shao⁴



Coremail



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



Authors (anonymous) *
List the authors, including email addresses and author information.

- 1. random1@spamtrap
- 2. random2@spamtrap
- 3. random3@spamtrap
- 4. Hotcrp website

Subscribe to updates

By entering your email – you will get updates for:
Organisations:
All
Categories:
All

Enter email
You can manage

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

What are 5XX (553 and 554) permanent errors?

- A 553 or 554 SMTP error indicates an email could not be delivered due to a permanent problem. Message delivery can be permanently deferred because:
 - You are using a **popular ESP (e.g., Yahoo)**
 - You are using a DMARC or DKIM policy.
 - The message contains characteristics that Yahoo won't accept for policy reasons.
 - Other suspicious behavior which leads to rejecting your SMTP connection.
 - Your IP is listed by **Spamhaus**. Please consider removing it from your network.
- If you consistently receive 5xx errors when sending emails, please review our **Sender Requirements & Recommendations** page. This is a symptom of a more widespread, general problem.
- You should **not retry** sending an email that has failed. Instead, email administrators should have a policy for removing failed emails and bounces.

Antispam features [edit]

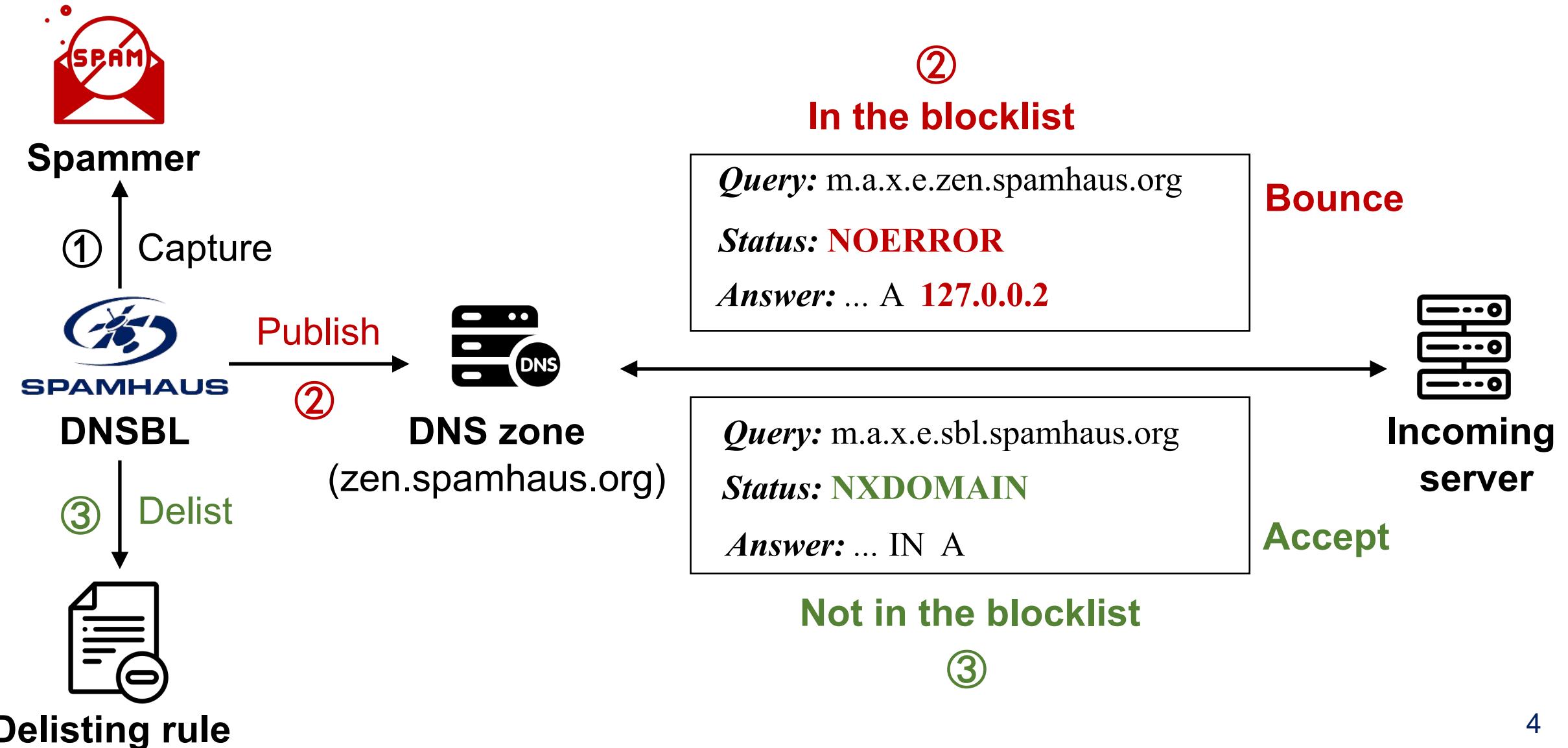
Mail Server	DNSBL	SURBL	Spamtraps	Greylisting	SPF
Microsoft Exchange Server	Yes (2003 & later)				

Email software (>20)

Domain registry (e.g., ShortDot)

SpamHaus.org is one of the most well known non-profit organizations that actively monitors more than 3 Billion¹ mailboxes globally for Spam emails. ShortDot uses a third party service that pulls domains from an API into SpamHaus and notifies us when Domain (s) violate our Terms and Conditions. According to SpamHaus, their Domain Block List is compiled by:

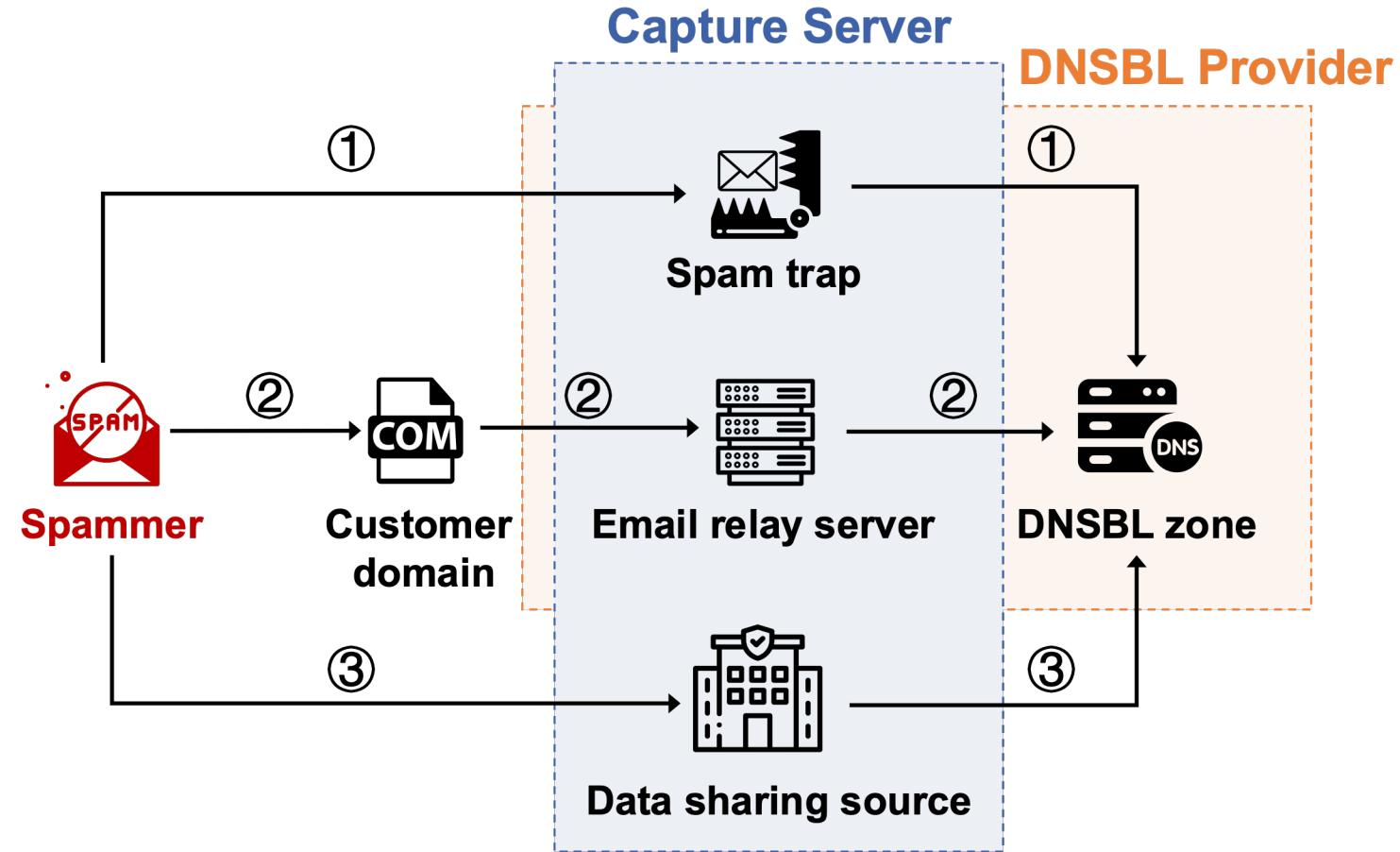
Know the host reputation through a DNS query



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**

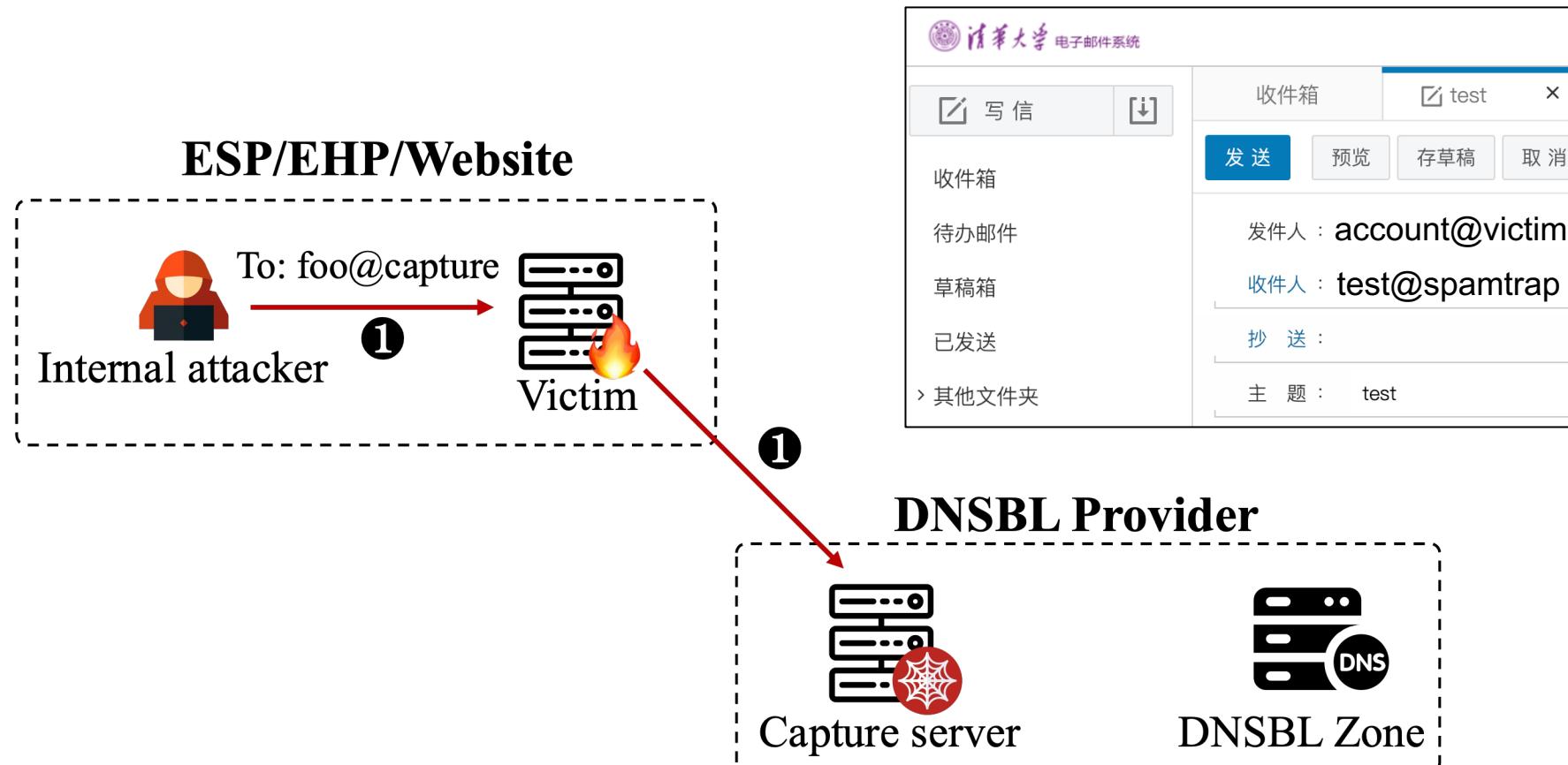
If the capture servers are identified,
attackers can manipulate DNSBLs by feeding false intelligence

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)

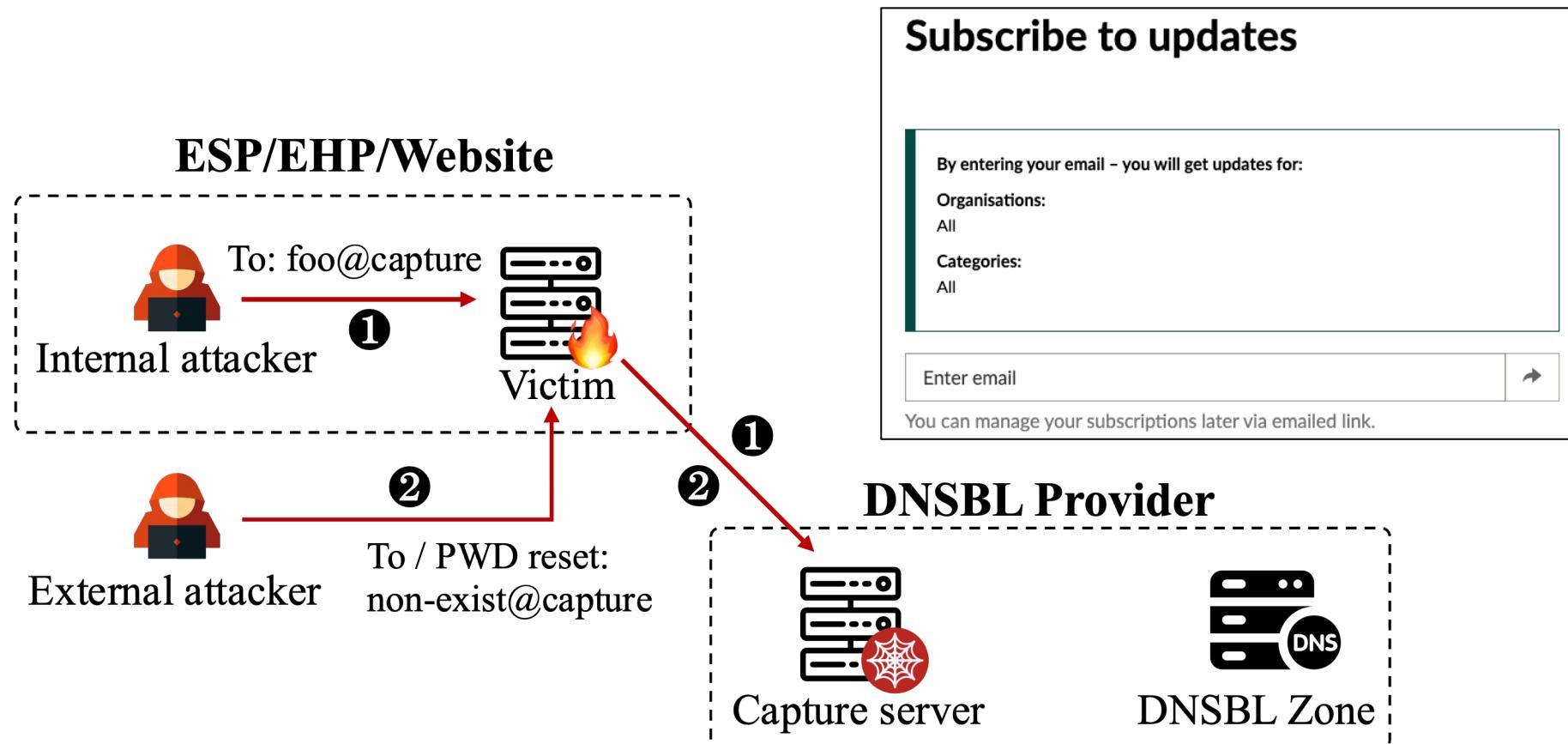
Threat model of HADES - Internal attack

Attackers hold the legitimate accounts of ESPs or enterprises



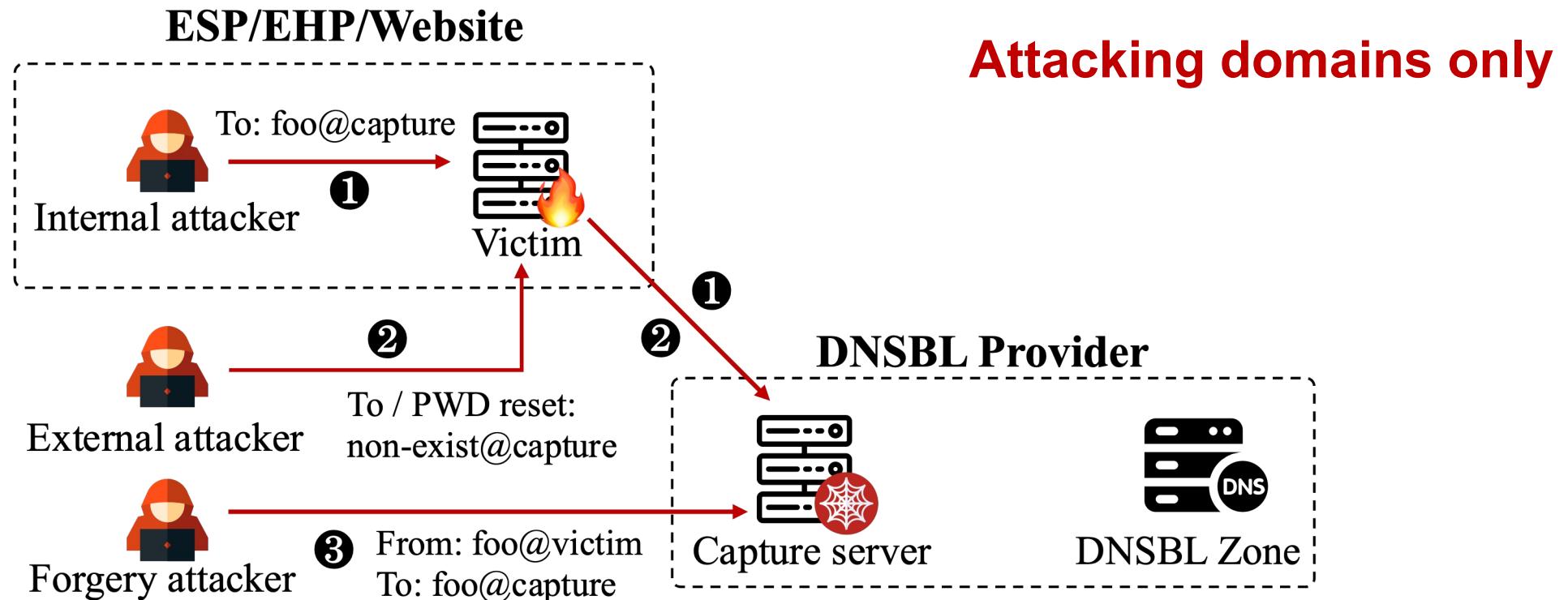
Threat model of HADES - External attack

Attackers abuse email subscriptions or password reset services



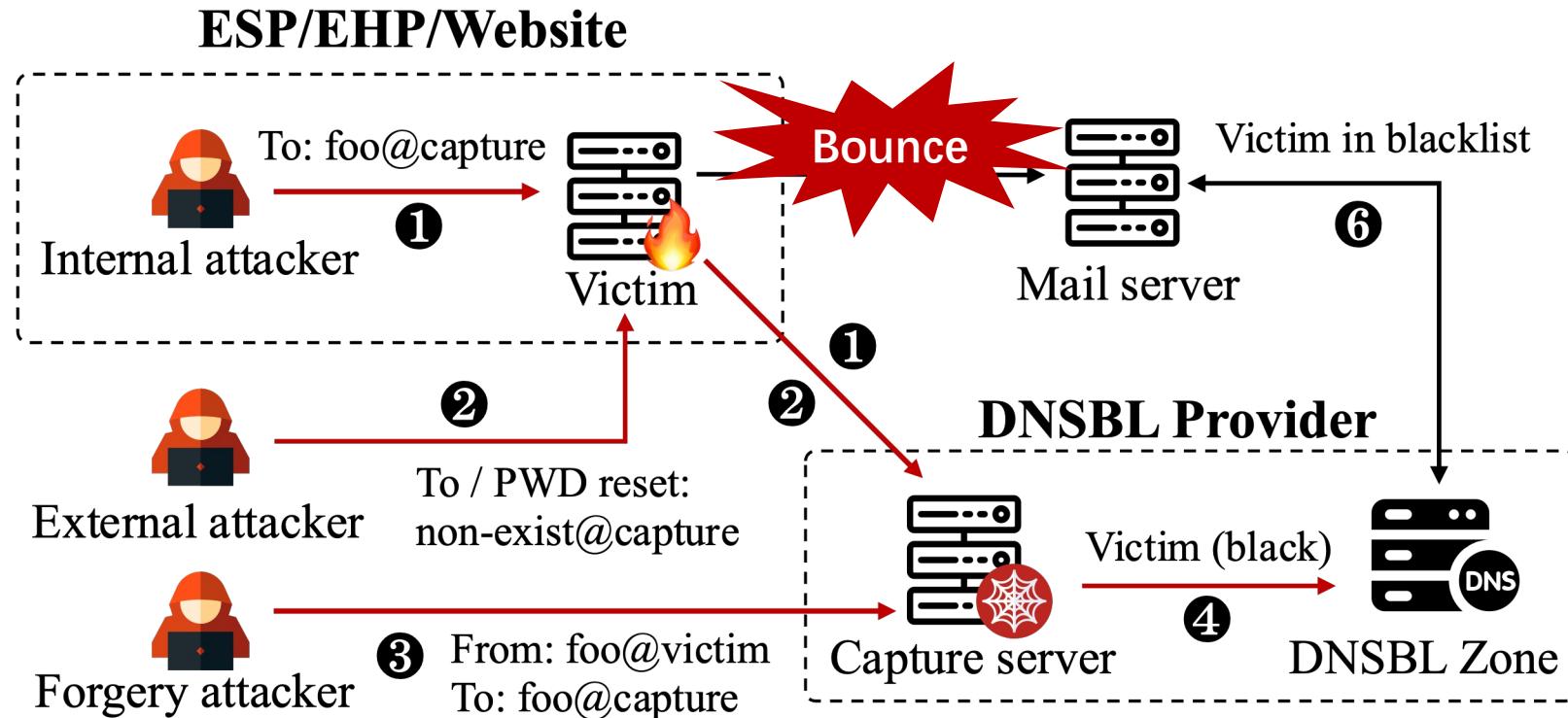
Threat model of HADES - Forgery attack

Attackers send email from arbitrary IPs to capture servers
that do not perform sender authenticity checks



Threat model of HADES - Consequence

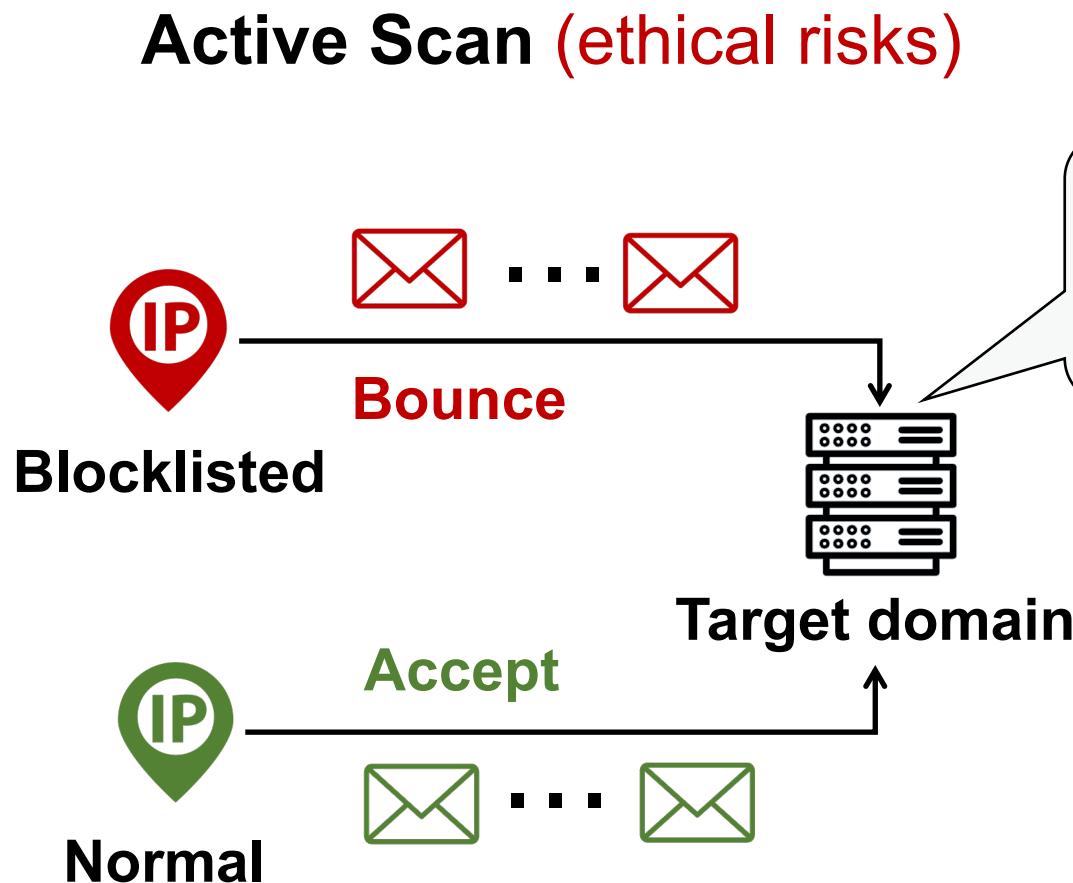
Emails sent by the victim to servers adopting DNSBL failed



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



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

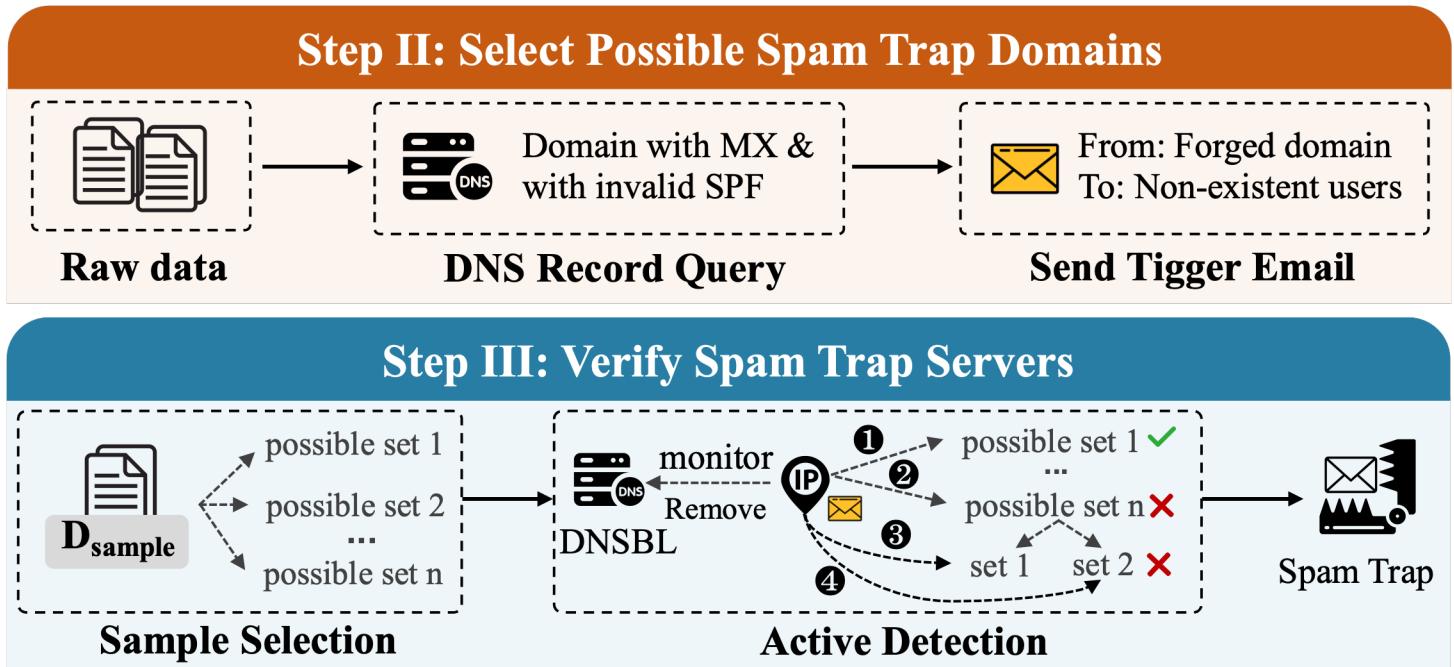
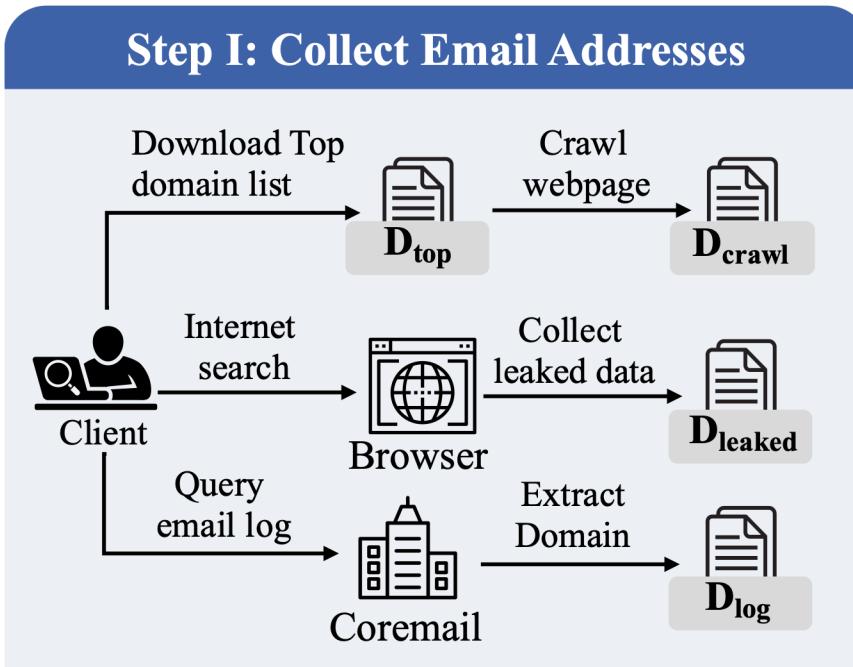
- 307,244 domain names deploy DNSBLs, of which Spamhaus accounts for 90.06%
- 53% of Top 100 domains deploy DNSBLs, 45% of Top 1K domains deploy DNSBLs

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%)

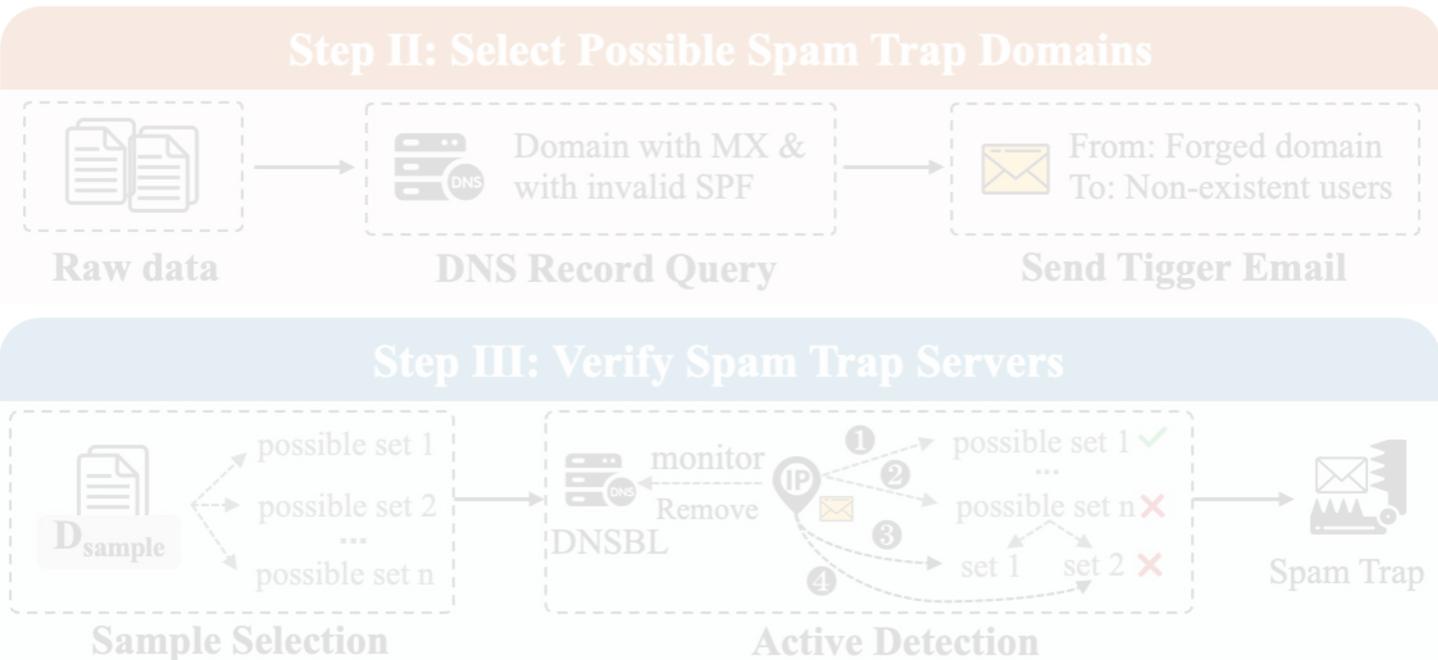
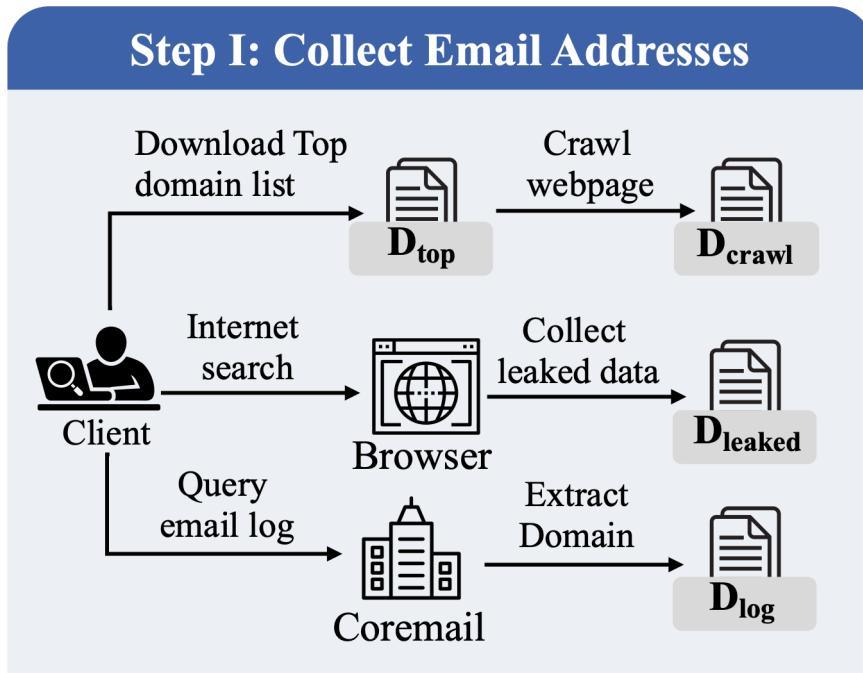
ESP	IP Blocklist	Domain Blocklist
outlook.com	YES	YES
hotmail.com	YES	YES
yahoo.com	YES	NO
icloud.com	YES	YES
tom.com	YES	NO
sina.com	YES	NO
sohu.com	YES	NO

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



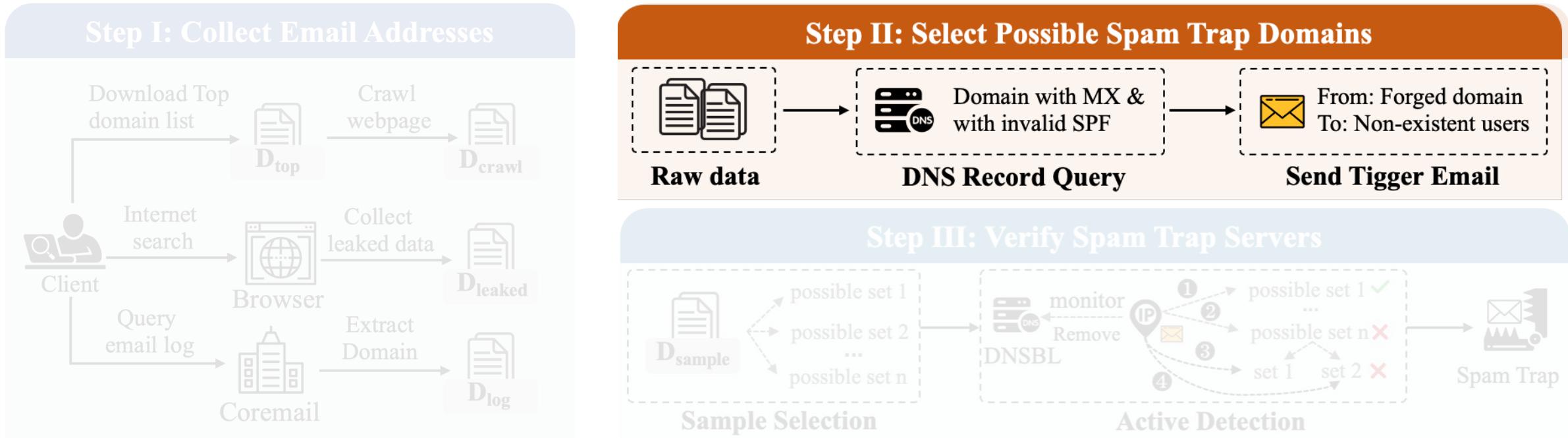
Step I: Collect email addresses



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

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

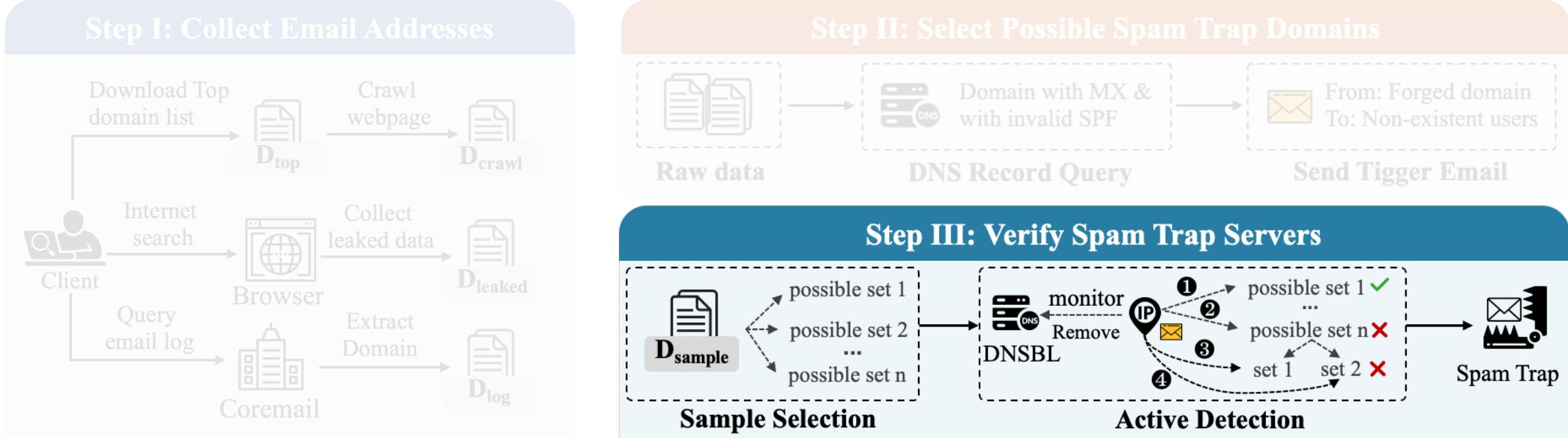
Step II: Select spamtrap domain candidates



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**



Brukalai.lt



JunkEmailFilter.com



Mailspike.io
anubisnetworks

GBUdb.com



Sender Score
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

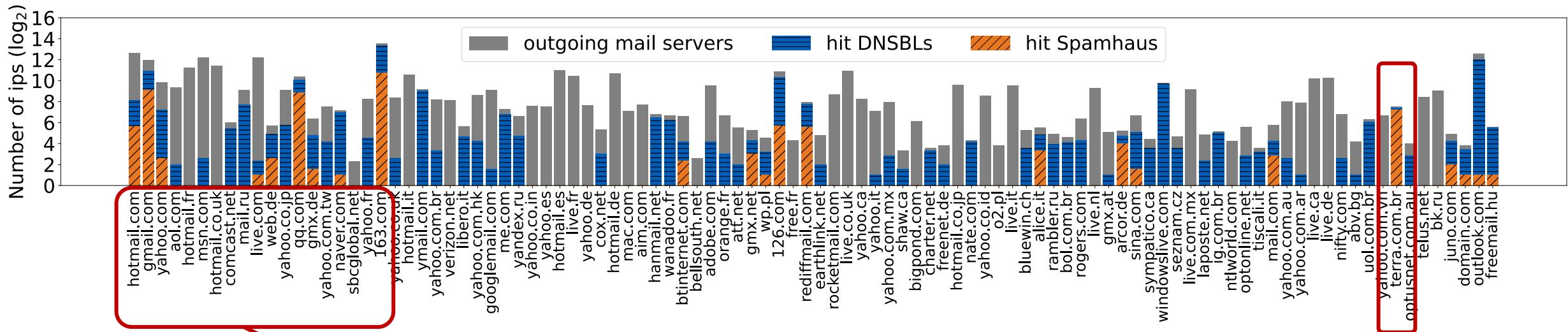
**Theoretically, HADES attack could affect all IP addresses
with outgoing email capability and arbitrary domains.**

- ? 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

Richard W
回复: Disclosure of Spam Blacklist Vulnerability
收件人: 李瑞烜

2024年5月30日 12:28

Spamcop

We owned approximately 10,000 domain names which have records set up on several thousand networks around the world. There is no central mx for our traps. Our traps receive around 20,000,000 messages per day.

We actively support M3AAWG and do follow all their best practices in setting up our traps. In fact, their best practices are modeled after our setup as we have amongst the most stringent procedures in procuring and validating a trap.

We don't bounce mail to traps mainly because we don't process the mail during the mail transaction. Instead the mail is accepted and processed once it is directed into our robust network of servers.

A bounce generated during the transaction means rejecting the message before it is accepted, leaving it up to the sending server to decide what to do with the message.

JW Joe Wein
回复: Disclosure of Spam Blacklist Vulnerability
收件人: 李瑞烜, zones-owner@lists.surbl.org

2024年5月23日 15:11

SURBL

Hello Ruixuan Li,

Not every mail system operator rejects all mails that fail SPF checks. When these accepted mails contain links to domains listed in SURBL data, they can still be flagged as spam.

If our spamtraps were to reject such mails at the entry point, we would give up direct visibility of the domains advertised in these links. We could not add them to our data. Therefore this behaviour is by design.

You can not build a domain blacklist for domains listed in message bodies by simply listing every domain of every link that hits a spam trap, regardless of how you filter the input. Too many innocent bystanders would be listed as False Positives. For example, many phishing emails link to both the phishing site and to real bank sites from the same mail body. So this is something we have been dealing with for many years. Consequently, "injecting a competitor's domain name or IP address into the blacklist" is not as trivial an attack to carry out with our system as you seem to think.

Regards
Joe Wein
SURBL

MadScientist
回复: Disclosure of Spam Blacklist Vulnerability
收件人: 李瑞烜, 抄送: lbj@tsinghua.edu.cn

2024年5月10日 23:52

Gbudb

On 5/9/24 22:28, 李瑞烜 wrote:

My concern is that an attacker could manipulate Truncate's blacklist to affect email services for normal IP addresses. Specifically, an attacker could send spam/email to Truncate's spam traps from free email providers or hosting platforms, affecting other legitimate users. In addition, the attacker can make the victim's IP address deliver emails to spam traps in various ways, such as password reset, bounced emails, VPS/VPN platforms, social worker emails, etc.

Truncate and Message Sniffer are specifically hardened against these kinds of attacks... in several ways.

These concerns were top of mind during the original design of Message Sniffer (back in the 1990s) and the components of the system were designed specifically to operate in hostile environments for long periods of time... even if instances of the product were owned and licensed by malicious operators.

Probably the most relevant mechanism is that the mathematics used when SNF nodes share data with each other are biased against weighting any single input and toward correlated inputs from multiple systems... As a consequence, even if an attacker were to take their licensed SNF instance and abuse it directly by injecting bad data or impersonating the device, their inputs would have little effect on the larger system and would also appear as outliers in order to call our attention (automatically and manually) to the situation.

In the specific scenario you imply, what might happen in some cases is a short-term "coloring" of the IPs reputation, but that would quickly evaporate in favor of a more balanced assessment. In fact, the threshold for an IP reputation getting onto the truncate list is so strict that only a tiny fraction of "good" message observations would be required in order to prevent that source IP from being on the truncate list.

L Leandro
回复: Disclosure of Spam Blacklist Vulnerability
收件人: 李瑞烜

2024年5月9日 02:51

Spfbl

Hi Ruixuan. We will make a few adjustments on our system based on your report. For security reasons, we cannot disclose these changes. Thank you so much for all this information! 🙏

Leandro
SPFBL.net

Thanks for Listening!

Ruixuan Li

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

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



Coremail

