NDSS Symposium 2026

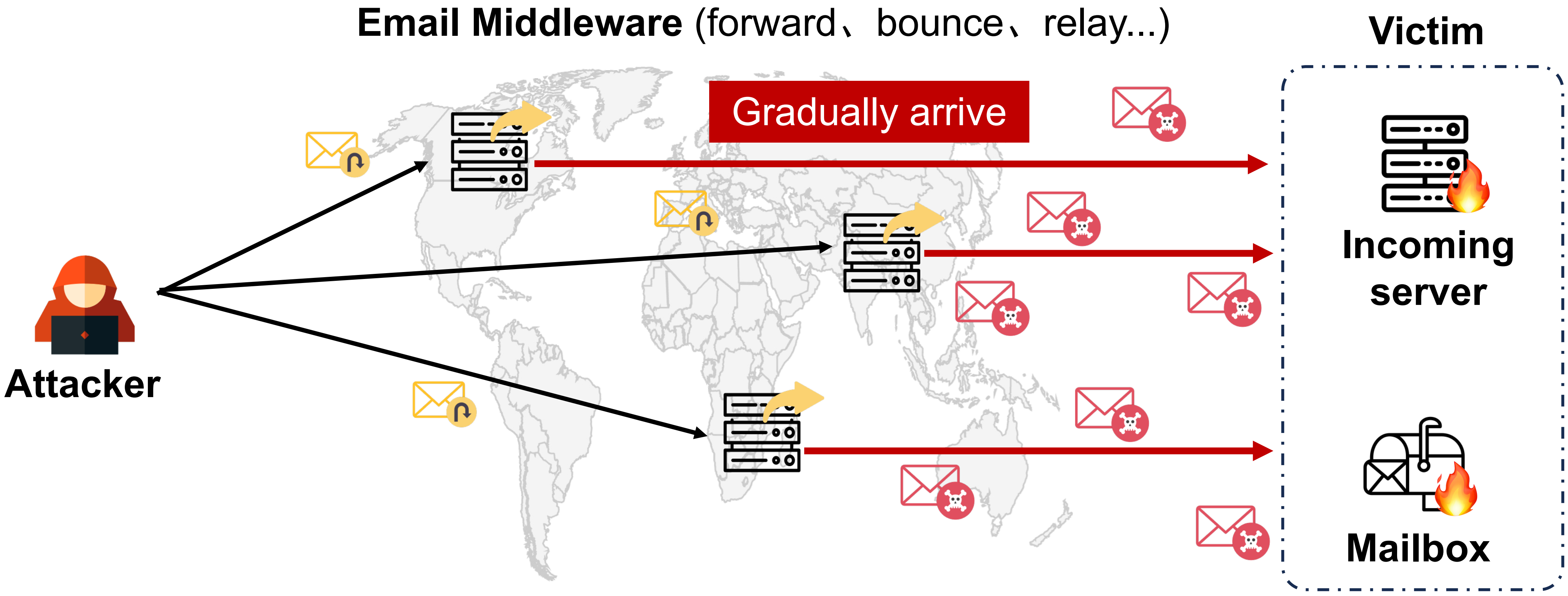
CoordMail: Exploiting SMTP Timeout and Command Interaction to Coordinate Email Middleware for Convergence Amplification Attack

Ruixuan Li[1], Chaoyi Lu[2], Baojun Liu[1], Yanzhong Lin[3], Qingfeng Pan[3], Jun Shao[4]

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

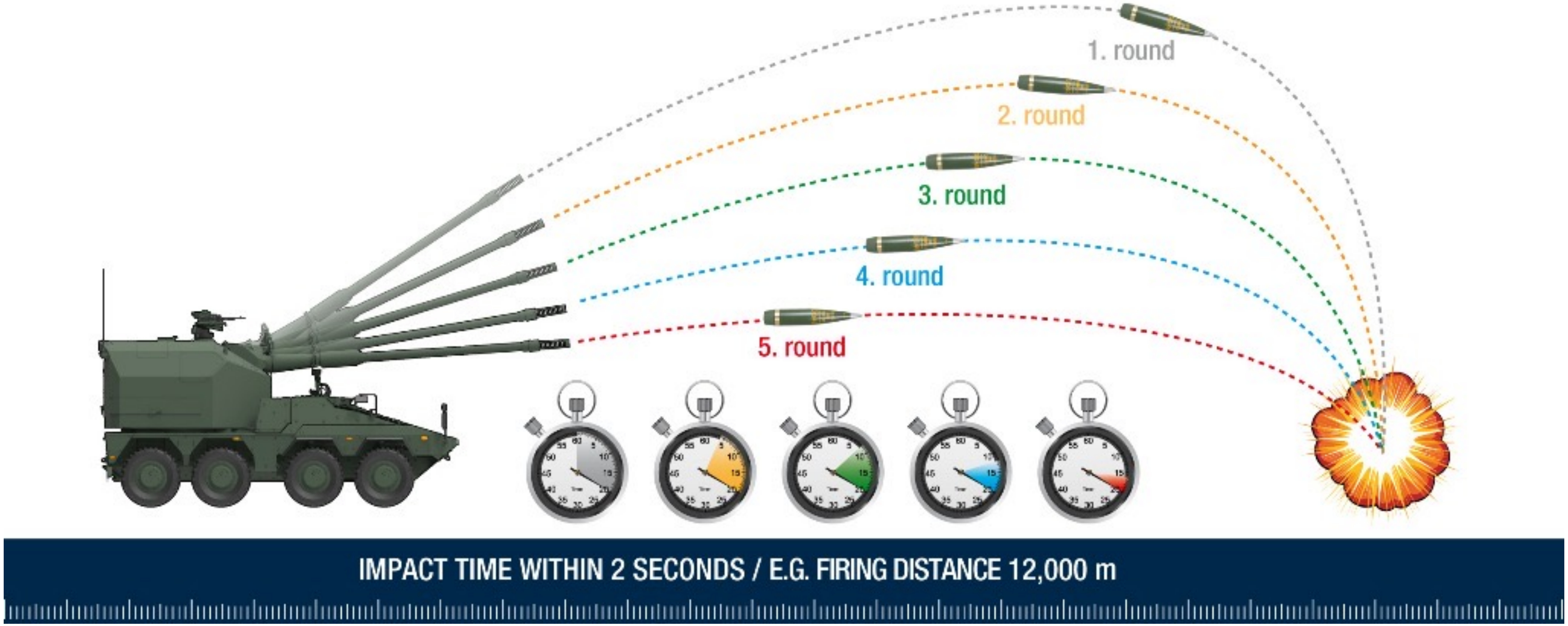
Email traffic amplification attack

- **Traditional:** Reflecting (amplified) emails to victims via email middleware, dependent on the amplification capabilities of a single server (about 100 times).



How to achieve more powerful amplification

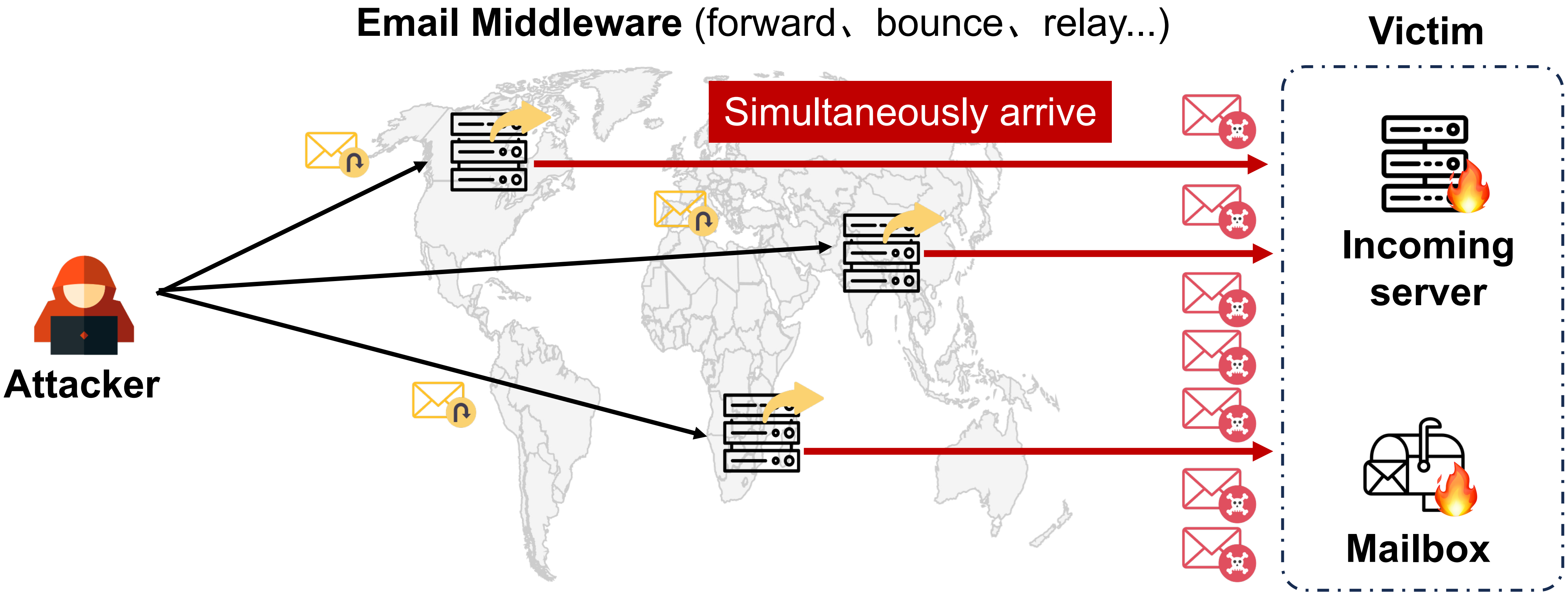
- **Multiple Round Simultaneous Impact:** Several rounds fired in different trajectories reach the target at the same time.


1. round
2. round
3. round
4. round
5. round
IMPACT TIME WITHIN 2 SECONDS / E.G. FIRING DISTANCE 12,000 m

https://en.defence-ua.com/weapon_and_tech/new_2s43_malva_howitzer_arrives_in_the_russian_military_featuring_the_mrsi_capability-8368.html

Threat Model: CoordMail attack

Core idea: CoordMail aggregate reflected emails from different email middleware, causing them to reach the victim simultaneously.



Threat Model: CoordMail attack

Core idea: CoordMail aggregate reflected emails from different email middleware, causing them to reach the victim simultaneously.

Attack impact: CoordMail disrupts the availability of the incoming mail server through explosively amplified traffic.

Attacker requirement: the attacker only needs a low-bandwidth SMTP server to send email.

Victim scope: the victims are IP addresses with email receiving capabilities, such as incoming mail servers of email providers, forwarding platforms, and websites.

Outline

Q1: How to coordinate different email middleware?

Q2: Which email middleware is suitable for constructing attacks?

Q3: What is the effect of the attack?

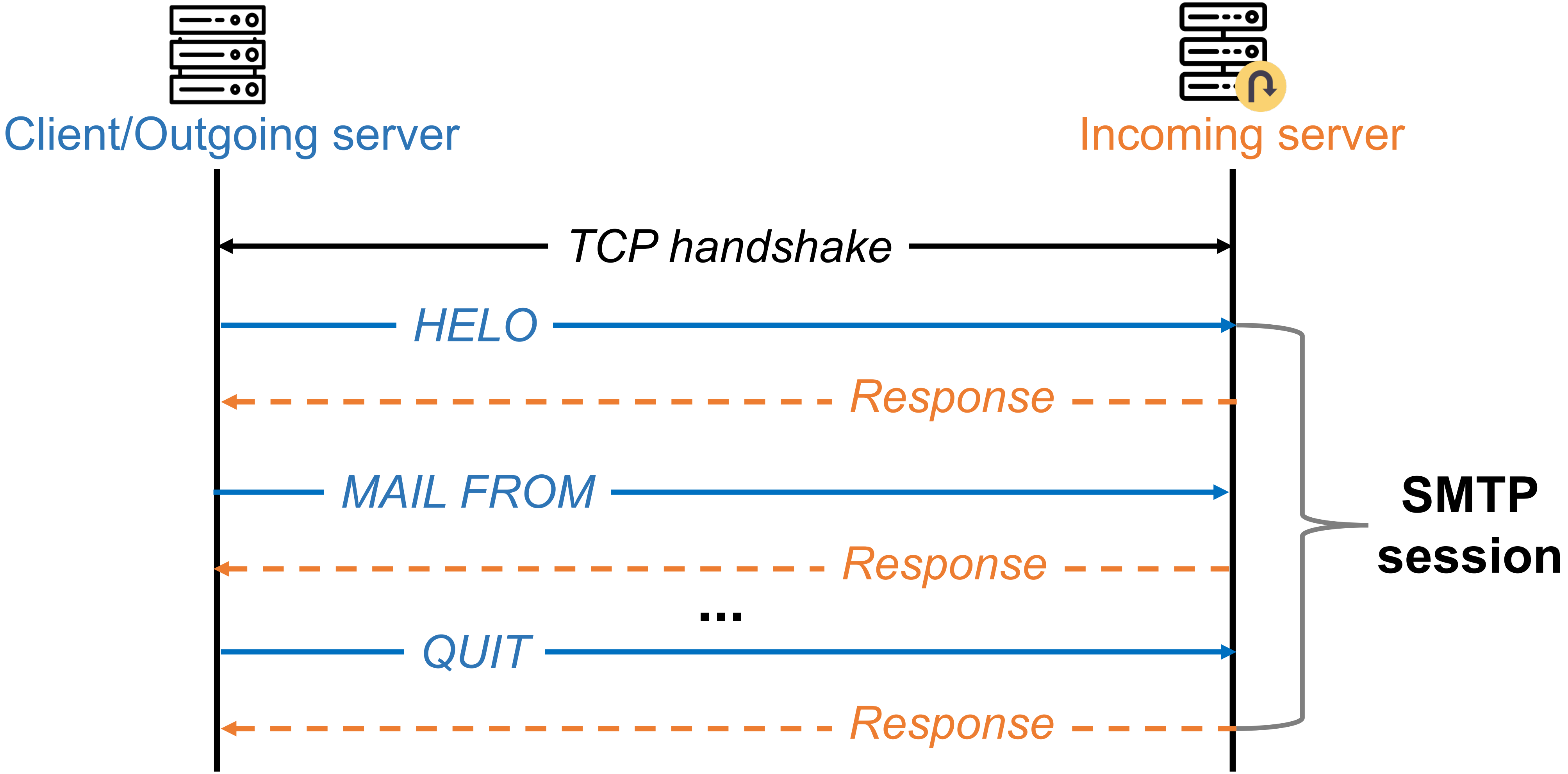
Outline

Q1: How to coordinate different email middleware?

Q2: Which email middleware is suitable for constructing attacks?

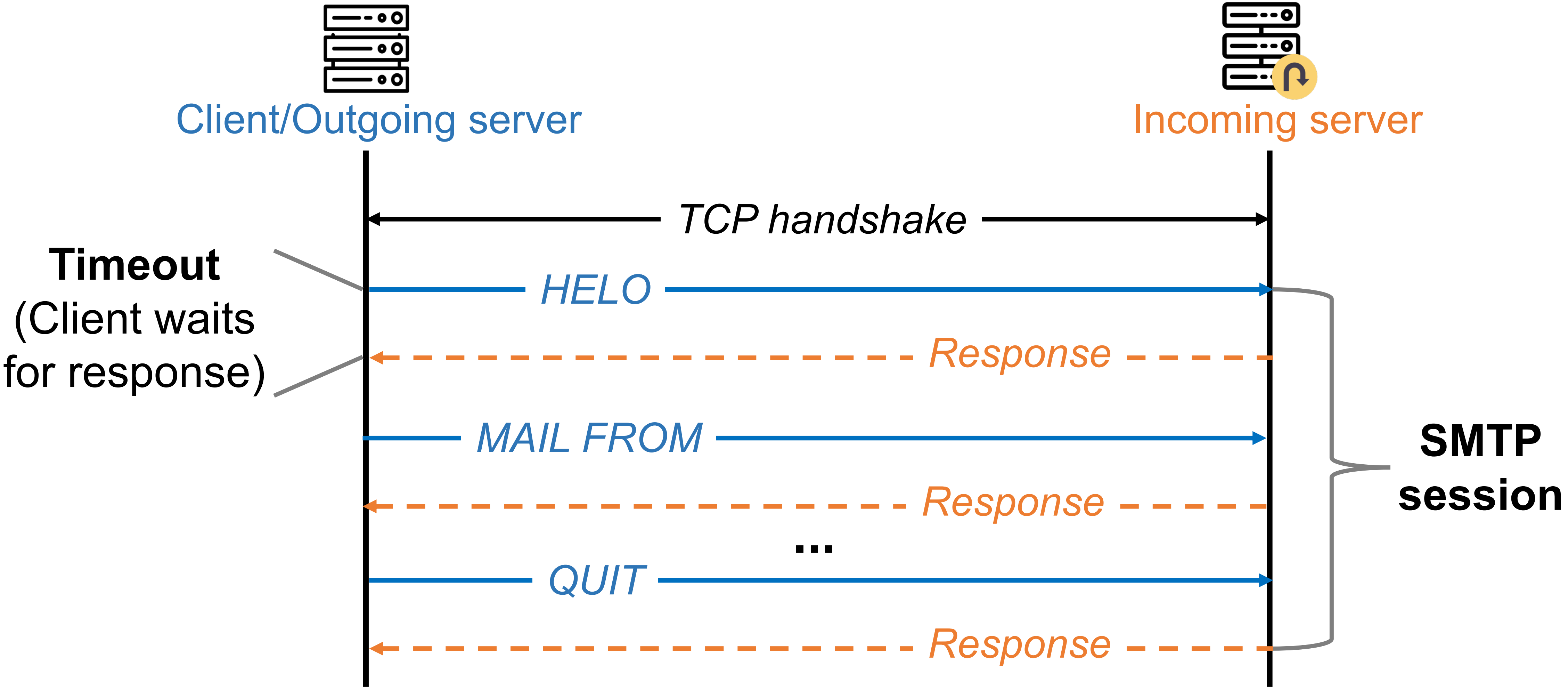
Q3: What is the effect of the attack?

SMTP protocol: Client-controlled interaction



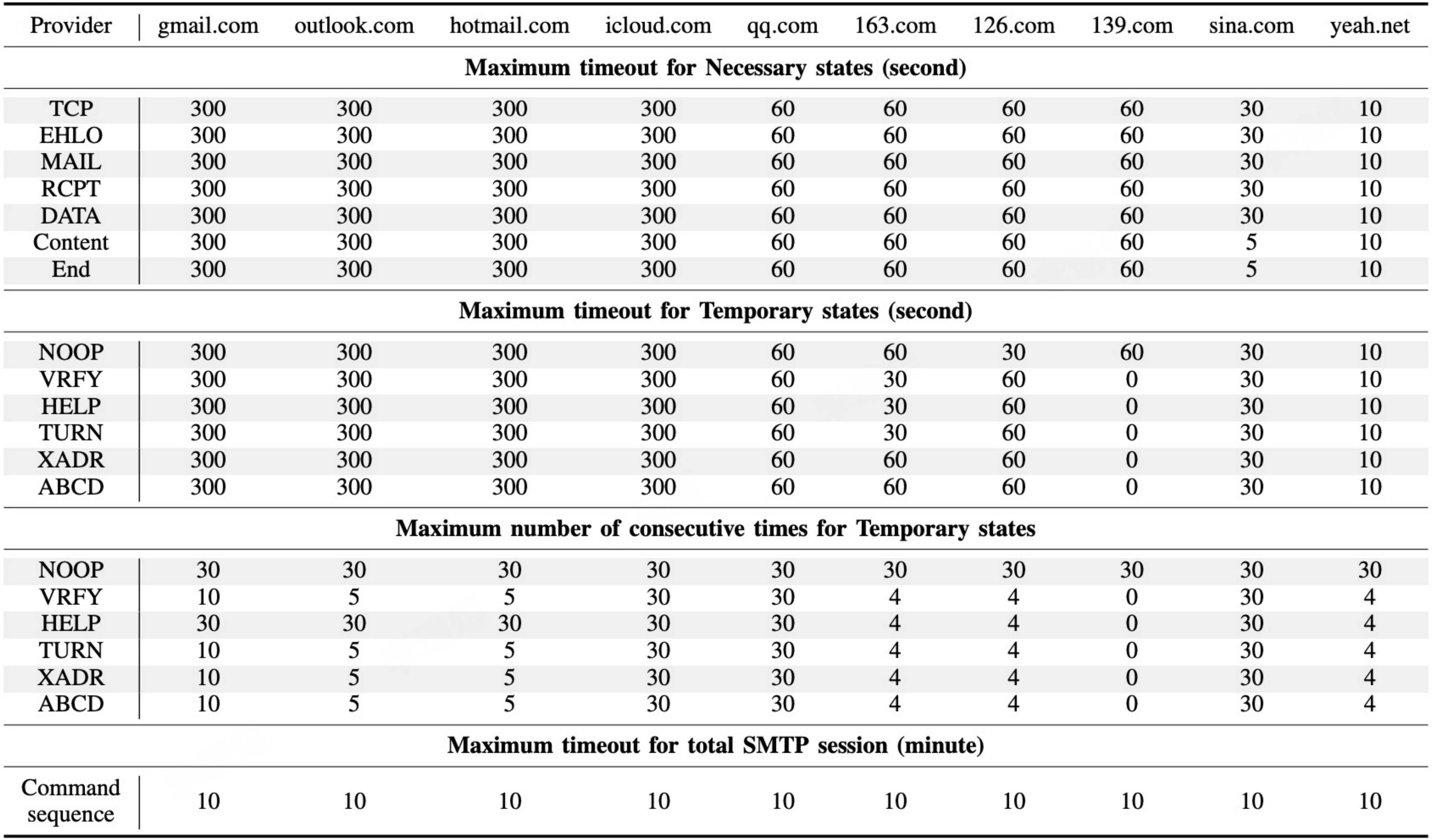
Clients send SMTP commands sequentially to initiate and manage SMTP sessions, while incoming servers respond correspondingly to inform the session status.

SMTP protocol: long session timeout



To ensure reliable delivery of email content, email servers typically support long session timeouts. RFC 821 recommends 5 minutes for each SMTP session state.

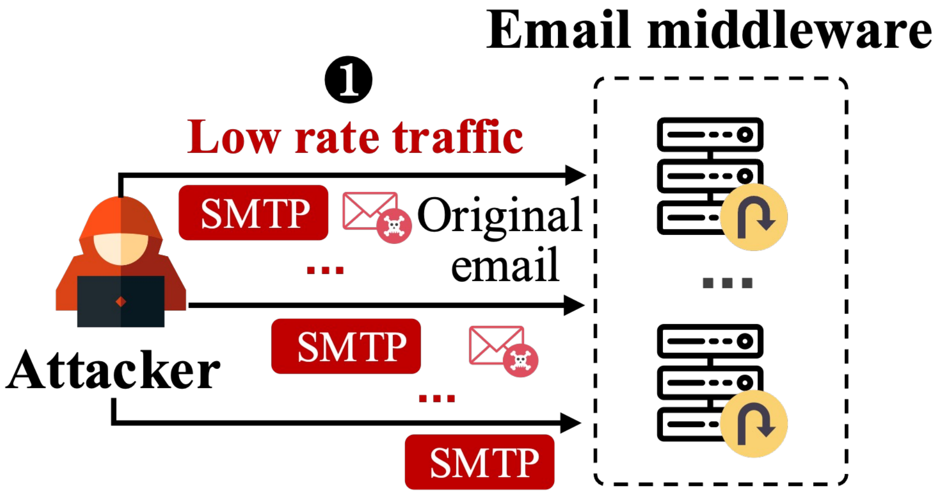
SMTP session timeouts for popular email providers



Provider	gmail.com	outlook.com	hotmail.com	icloud.com	qq.com	163.com	126.com	139.com	sina.com	yeah.net
Maximum timeout for Necessary states (second)										
TCP	300	300	300	300	60	60	60	60	30	10
EHLO	300	300	300	300	60	60	60	60	30	10
MAIL	300	300	300	300	60	60	60	60	30	10
RCPT	300	300	300	300	60	60	60	60	30	10
DATA	300	300	300	300	60	60	60	60	30	10
Content	300	300	300	300	60	60	60	60	5	10
End	300	300	300	300	60	60	60	60	5	10
Maximum timeout for Temporary states (second)										
NOOP	300	300	300	300	60	60	30	60	30	10
VRFY	300	300	300	300	60	30	60	0	30	10
HELP	300	300	300	300	60	30	60	0	30	10
TURN	300	300	300	300	60	30	60	0	30	10
XADR	300	300	300	300	60	60	60	0	30	10
ABCD	300	300	300	300	60	60	60	0	30	10
Maximum number of consecutive times for Temporary states										
NOOP	30	30	30	30	30	30	30	30	30	30
VRFY	10	5	5	30	30	4	4	0	30	4
HELP	30	30	30	30	30	4	4	0	30	4
TURN	10	5	5	30	30	4	4	0	30	4
XADR	10	5	5	30	30	4	4	0	30	4
ABCD	10	5	5	30	30	4	4	0	30	4
Maximum timeout for total SMTP session (minute)										
Command sequence	10	10	10	10	10	10	10	10	10	10

STEP I: Low-speed connection to email middleware

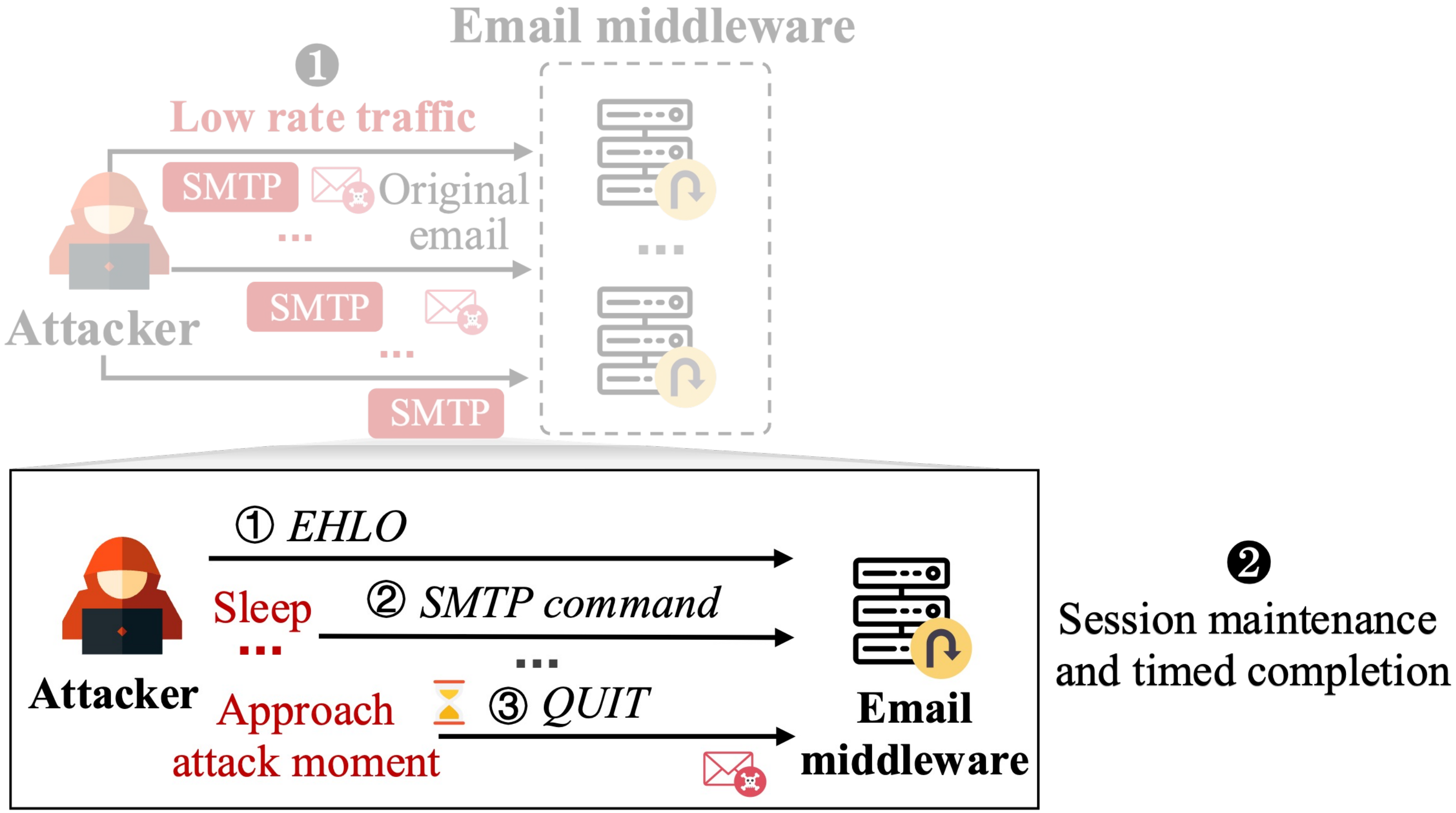
The attacker selects an arbitrary attack moment, and sequentially establishes SMTP connections with email middleware at a low rate.



By establishing only one or a few connections with each email middleware, the attack avoids being blocked for connecting too quickly.

STEP II: Session maintenance and timed completion

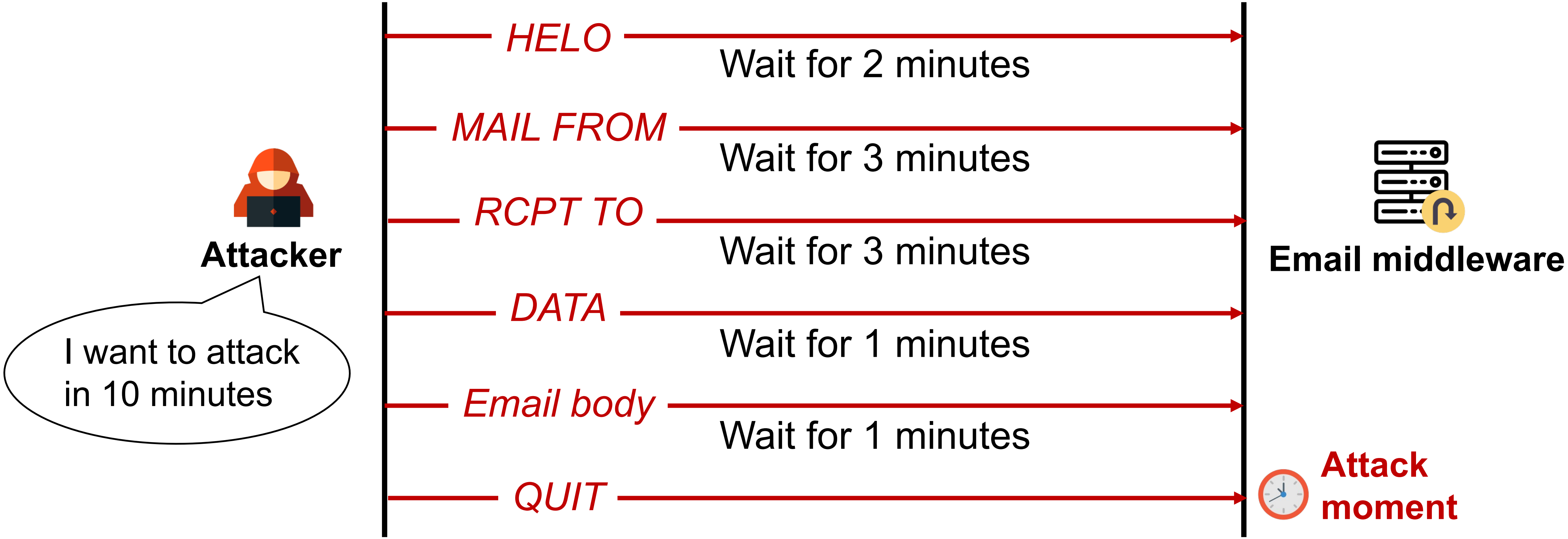
The attacker maintains SMTP connections with each email middleware until close to the attack moment.



STEP II: Session maintenance and timed completion

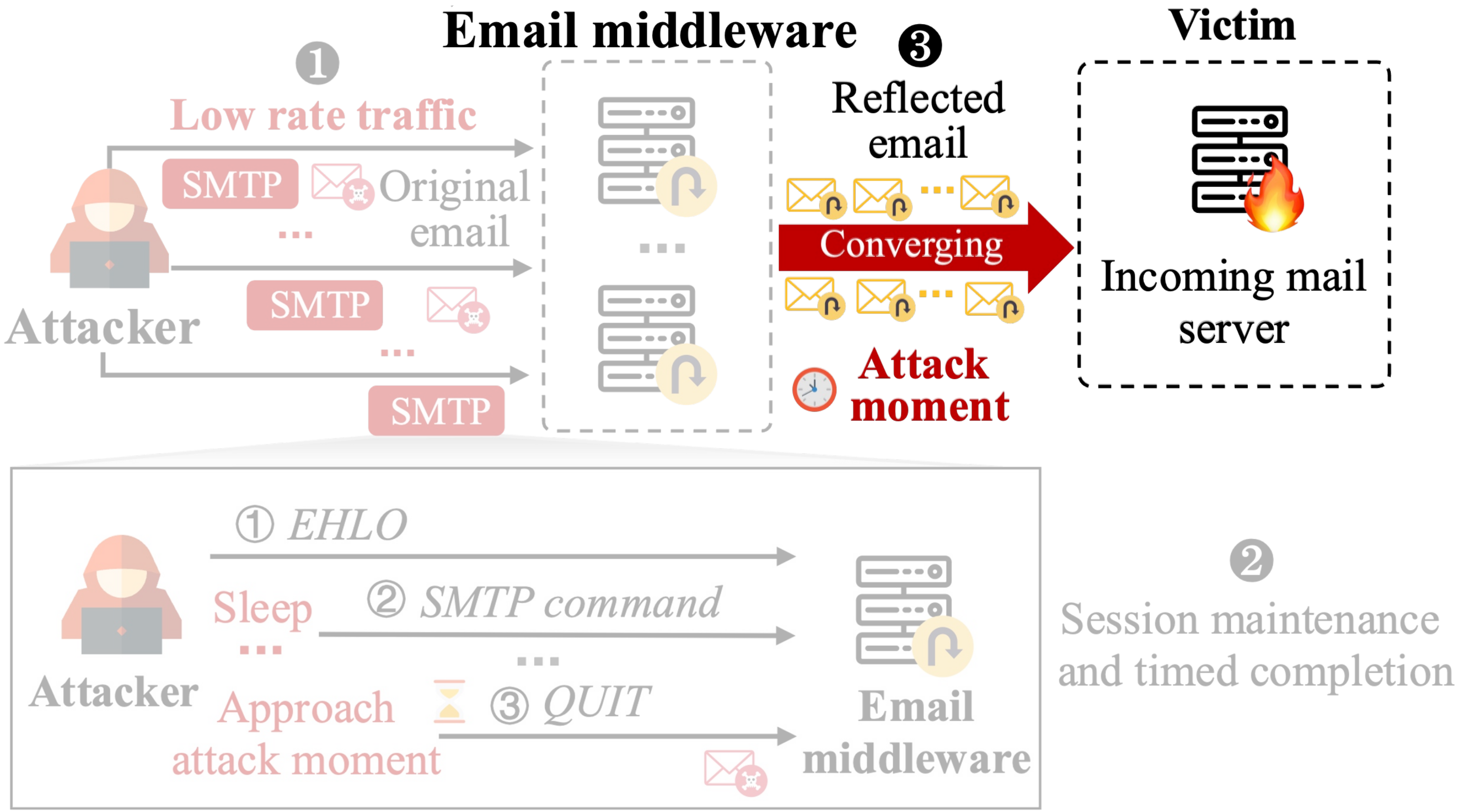
1) The attacker creates SMTP command sequences to specify the sending order of SMTP commands and their corresponding sleep intervals.

2) When the designated moment arrives, the attacker sends the QUIT command to each email middleware.



STEP III: Concentrate reflected emails at victim

After receiving the original emails from the attacker, all email middleware sends reflected emails to the victim within a short period.



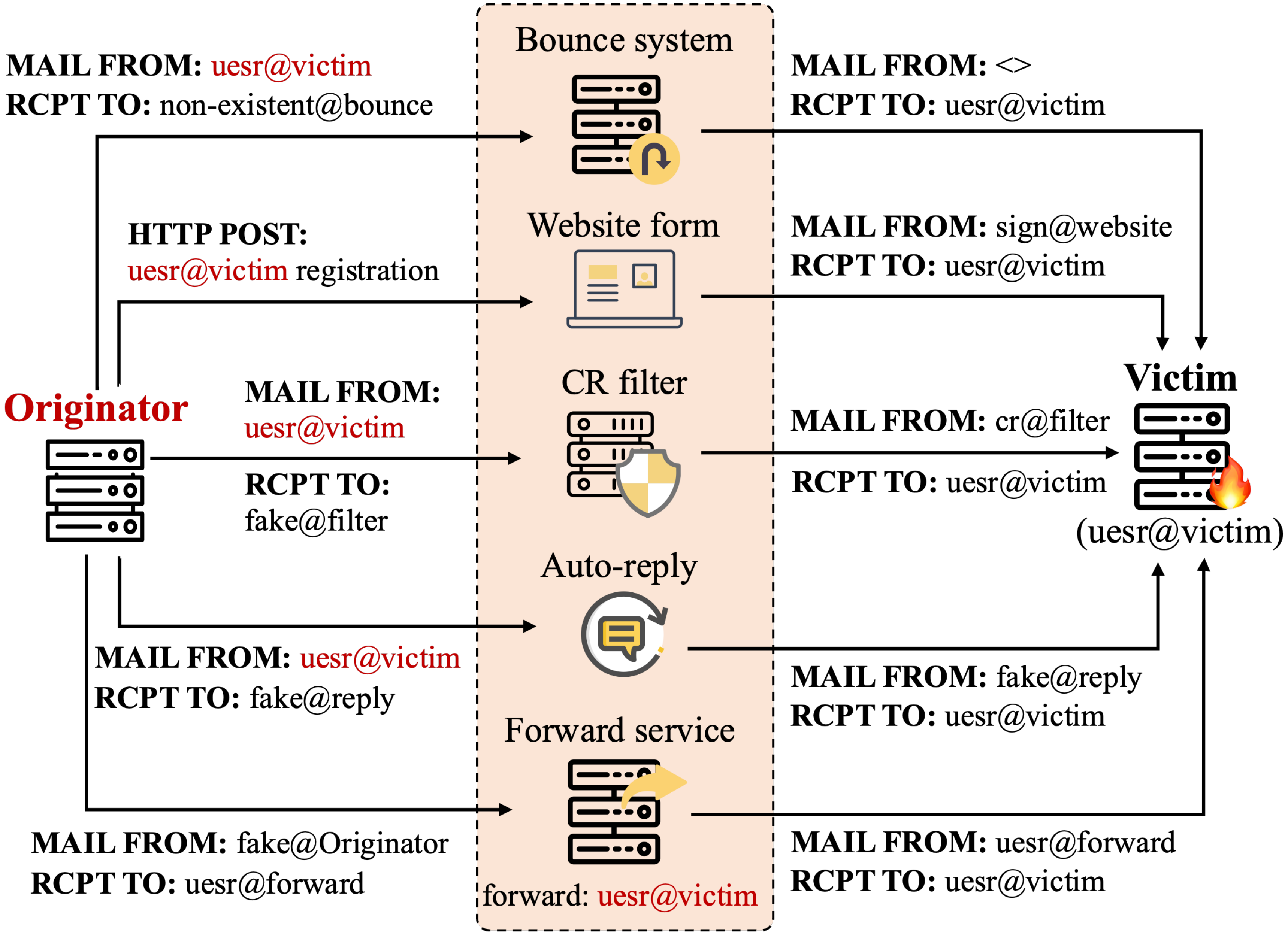
Outline

Q1: How to coordinate different email middleware?

Q2: Which email middleware is suitable for constructing attacks?

Q3: What is the effect of the attack?

Email middleware are numerous and of various types



Bounce system

MAIL FROM: uesr@victim
RCPT TO: non-existent@bounce

MAIL FROM: <>
RCPT TO: uesr@victim

Website form

HTTP POST:
uesr@victim registration

MAIL FROM: sign@website
RCPT TO: uesr@victim

CR filter

Originator

MAIL FROM:
uesr@victim

RCPT TO:
fake@filter

MAIL FROM: cr@filter
RCPT TO: uesr@victim

Victim

(uesr@victim)

Auto-reply

MAIL FROM: uesr@victim
RCPT TO: fake@reply

MAIL FROM: fake@reply
RCPT TO: uesr@victim

Forward service

MAIL FROM: fake@Originator
RCPT TO: uesr@forward

forward: uesr@victim

MAIL FROM: uesr@forward
RCPT TO: uesr@victim

Finding email middleware in the wild

	Original email	Reflected email
Bounce server	***MAIL FROM:*** *exist@victim* ***RCPT TO:*** *non-exist@bounce* ***From:*** *exist@victim* ***To:*** *non-exist@bounce* [Original email body]	***MAIL FROM:*** <> ***RCPT TO:*** *exist@victim* ***From:*** *exist@bounce* ***To:*** *exist@victim* [Bounce body + Original body]
Open email relay	***MAIL FROM:*** *random@attacker* ***RCPT TO:*** *exist@victim* ***From:*** *random@attacker* ***To:*** *exist@victim* [Original email body]	***MAIL FROM:*** *random@attacker* ***RCPT TO:*** *exist@victim* ***From:*** *random@attacker* ***To:*** *exist@victim* [Original email body]
Email forwarder	***MAIL FROM:*** *random@attacker* ***RCPT TO:*** *exist@forward* ***From:*** *random@attacker* ***To:*** *exist@forward* [Original email body]	***MAIL FROM:*** *[code]@forward* ***RCPT TO:*** *exist@victim* ***From:*** *random@attacker* ***To:*** *exist@forward* [Original email body]

We **actively send probe packets** to over 6 million email domains and IP addresses with open TCP/25 ports to identify bounce servers and open email relay servers. Since detecting email forwarders requires manual account registration, we use **passive email logs** to identify forwarding relationships in the real world.

Selecting suitable email middleware for CoordMail

❖ Amplification capability

1) The magnification of the packet size in the reflected email session

2) The number of reflected emails generated by email middleware for one original email

❖ SMTP session timeout

Email middleware support maintaining an SMTP session for more than 10 minutes

❖ Email reflection interval

Email middleware exhibit an average reflection interval of less than 5s with a standard deviation below 500 milliseconds

Email middleware	Total	CoordMail	Suitability
Bounce server	19,184	10,079	●
Open email relay	1,299	584	◉
Forwarding provider	10	6	◉

● means high suitability; ◉ means moderate suitability

Outline

Q1: How to coordinate different email middleware?

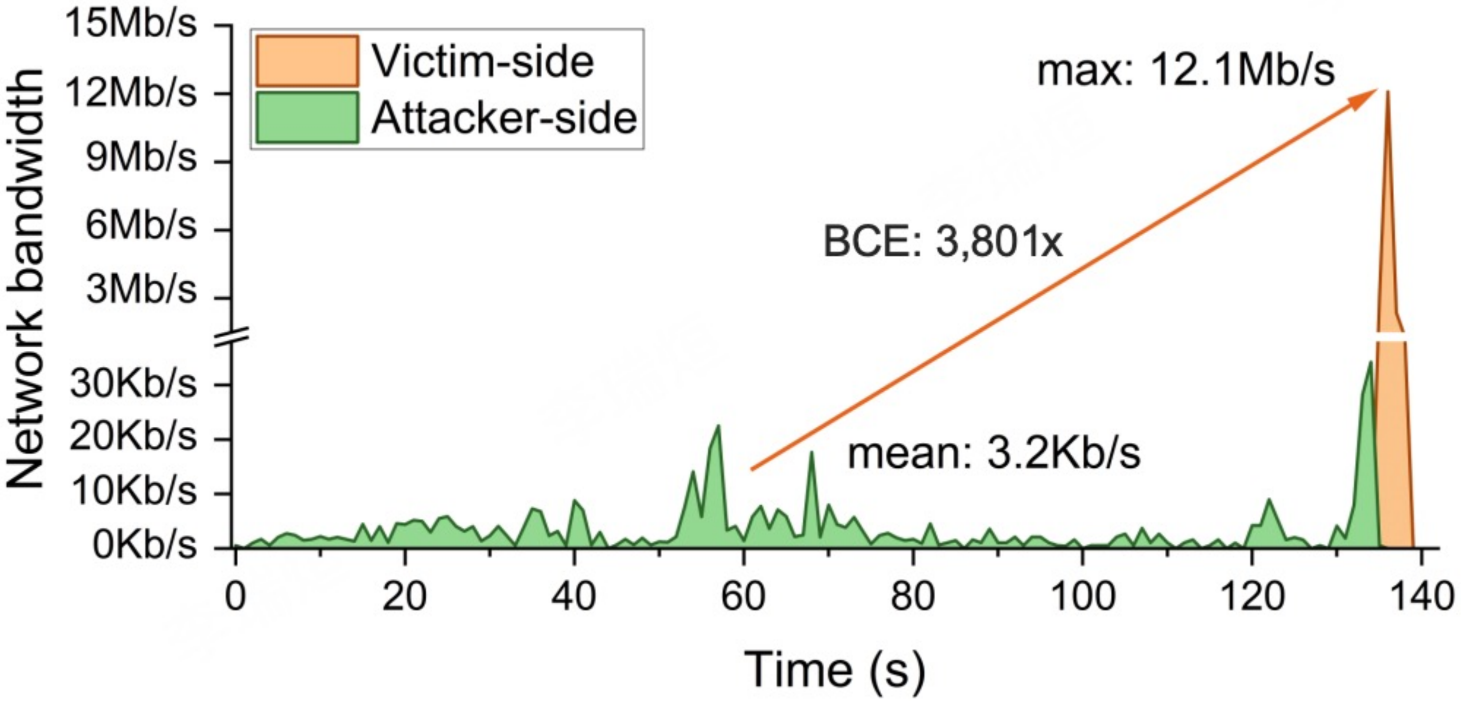
Q2: Which email middleware is suitable for constructing attacks?

Q3: What is the effect of the attack?

Evaluating the traffic amplification effect

Bandwidth concentration efficiency (BCE) indicates the ability of the attack to aggregate traffic on the victim's side, i.e., the multiple of the peak attack traffic bandwidth over the victim's required bandwidth.

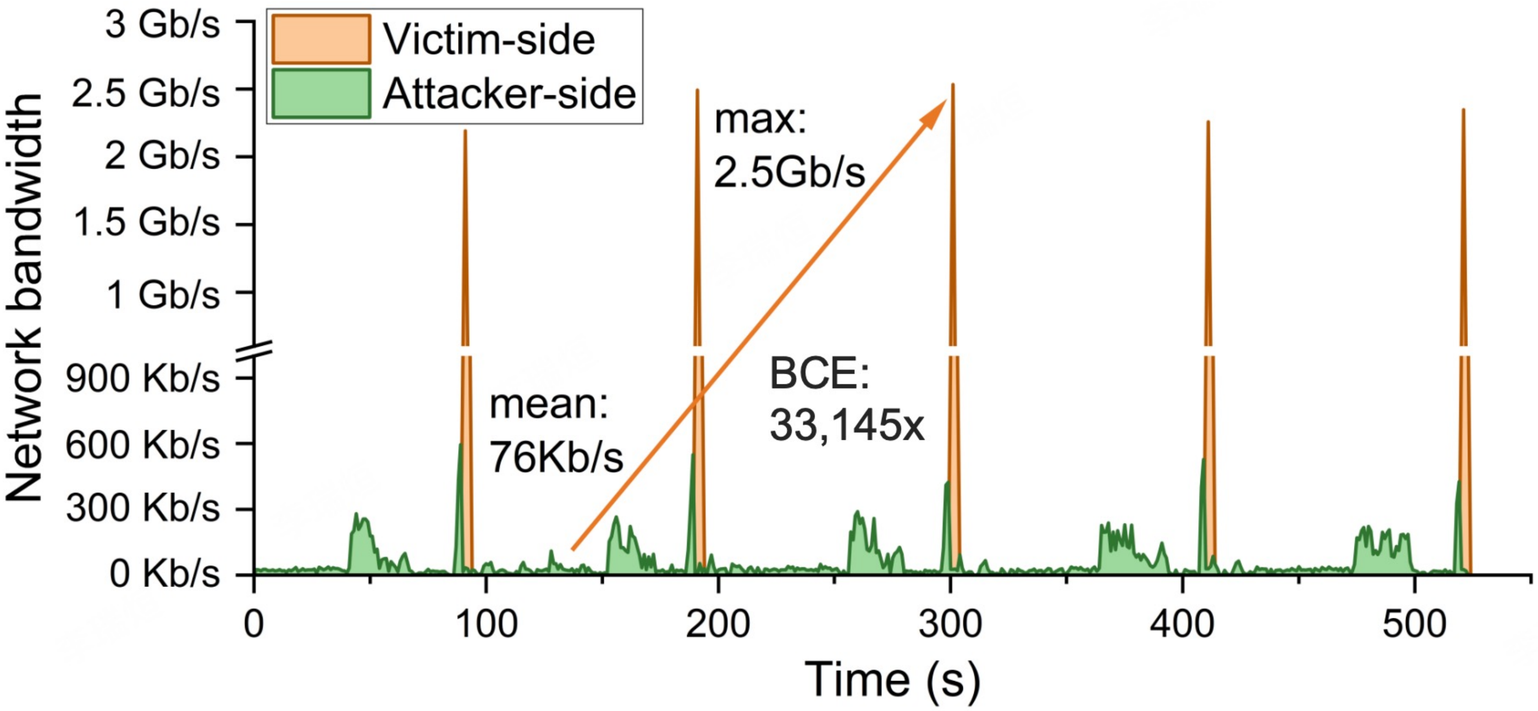
Attacks in the real world (20 email middleware, 5 recipient)



Evaluating the traffic amplification effect

Bandwidth concentration efficiency (BCE) indicates the ability of the attack to aggregate traffic on the victim's side, i.e., the multiple of the peak attack traffic bandwidth over the victim's required bandwidth.

Attacks in the controlled environment (1000 email middleware, 10 recipient)



Analyzing defense effect of security mechanisms

Type	Security mechanism	Defense
Email authenticity	SPF	◉
	DKIM	◉
	DMARC	●
Host reputation	DNSBL	○
	Greylisting	◉
Rate limit	IP sending rate limit	○
	Mailbox receiving rate limit	○

● means effective against CoordMail; ◉ means partially effective; ○ means ineffective

DMARC can effectively block reflected emails generated by CoordMail, while the effectiveness of other security mechanisms is relatively weak.

Mitigation strategies for CoordMail attack

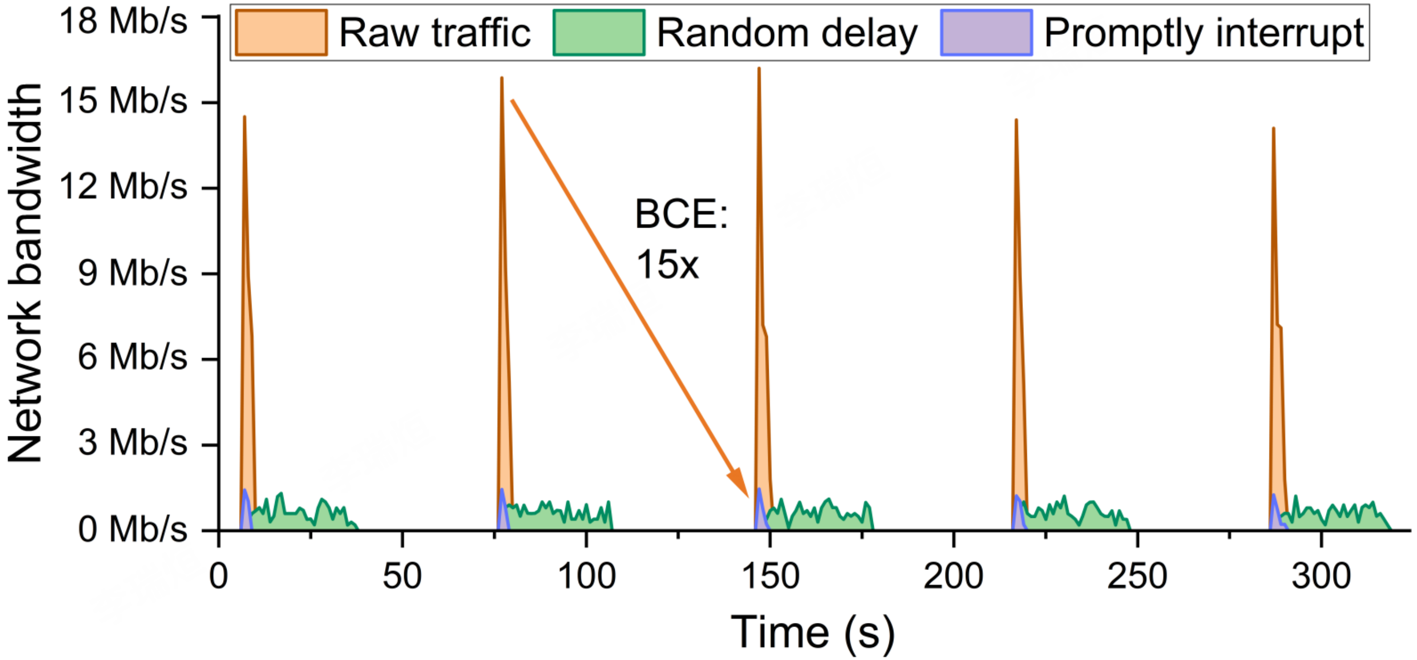
❖ Email middleware

1) Email middleware can add random delay in the process of producing reflected email.

2) Email middleware should limit the number and size of reflected emails.

❖ Email provider

1) Email providers can promptly interrupt reflected emails based on traits (e.g., violation DMARC, empty MAIL FROM field), especially when dealing with large volumes of traffic.



Responsible disclosure

- ## Email middleware

We have received replies from 872 email middleware administrators. Among the valid responses, 49 administrators indicated they were awaiting confirmation, 13 mentioned that their email service was managed by hosting providers, and 22 stated they planned to resolve the issue.

- ## Popular email providers

Among the 14 popular email providers, 8 have acknowledged the threat posed by CoordMail, but most stated that they were not significantly affected. In addition, proton.me plans to improve their mailbox service rate limit.

Thanks for Listening!

Ruixuan Li

Email: *lirx25@mails.tsinghua.edu.cn*

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

清華大學 Tsinghua University

中关村实验室 ZGC LAB

Coremail

浙江工商大學 ZHEJIANG GONGSHANG UNIVERSITY