# **Email phishing**

▲ The actual senders are made to look legitimate from the Australian tax office

From: "...mygov messages..." From: ".myGov\_ ATO notice"

From: "Online. myGov. ato."

▲ The return path

<u>send@a1.net</u> and the mail server is <u>smtpout06.a1.net</u> with IP 80.75.33.6 originates from Austria

and is reported for email spam, source AbuselP

<u>send@a1.net</u> and the mail server is <u>smtpout05.a1.net</u> with IP 80.75.33.5 which is used for spam and it's origin is Austria from virustotal

<u>noreply@a1.net</u> and the mail server is <u>smtpout02.a1.net</u> with IP 80.75.33.2 originates from Austria and is flagged as clean by virustotal

phish@cyberlynk.io and the mail server is sonic321-

<u>21.consmr.mail.gq1.yahoo.com</u> with IP 98.137.66.84 originates from America and is flagged as spam and spoofing by AbuseIP

Arr By passing the SPF check, this means the emails were sent from a legitimate server which is authorized. SPF check Arr This is an email authentication whereby the receiving server ensures the sending server was authorized. This ensures that an email was sent from the said domain.

Checking SPF for a1.net domain

# Success!

Everything appears fine with your SPF record. 2 DNS queries

### Found SPF record in DNS:

v=spf1 include:aspf.a1.net include:cspf.a1.net -all

### SPF record resolution:

# Checking SPF for cyberlynk.io

# Success!

Everything appears fine with your SPF record. 2 DNS queries

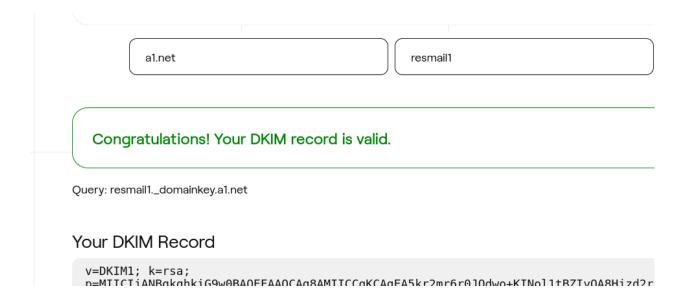
Found SPF record in DNS:

```
v=spf1 include:_spf.mail.hostinger.com ~all
```

SPF record resolution:

```
    cyberlynk.io -
    include:_spf.mail.hostinger.com -
    include:relay.mailchannels.net -
        ip4:23.83.208.0/20
        ip4:35.85.190.185/32
        ~all
```

▲ DKIM stands for domain key identified mail which ensures email has not been tampered with in transit. It uses a digital signature to ensure integrity.



# Checking DKIM more domain <u>yahoo.com</u> selector s2048

yaholo.com	2048 INSPECT DKIM
Congratulations! Your DKIM record is valid.	
Query: s2048domainkey.yahoo.com	
Your DKIM Record	
k=rsa; p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgk HGoQ6dalSMWiLaj8IMcHC1cubJx2gziAPQHVPtFYayyLA4ay ugfBviU8aiPCE4JSFrpxflhMIKV4bt+a1uHw7wLzguCf4YA	JUSNk10/

▲ DMARC stands for domain-based message authentication, reporting and conformance. It builds upon DKIM and SPF, if both are pass, it allows the email.

# Checking mimecast for a1.net domain

V	DMARC1	DMARC protocol version.
р	reject	Apply this policy to email that fails the DMARC check. This policy be set to 'none', 'quarantine', or 'reject'. 'none' is used to collect the DMARC report and gain insight into the current emailflows and their status.
rua	mailto:dmarc-reports@ai.net	A list of URIs for ISPs to send XML feedback to. NOTE: this is not a list of email addresses. DMARC requires a list of URIs of the form 'mailto:test@example.com'.

The policy has been set to reject meaning any unauthenticated email are rejected therefore never making it to the recipient's mailbox. The domain is legit, a telecom company but suspicious sub-domains.

Checking mimecast for cyberlynk.io domain

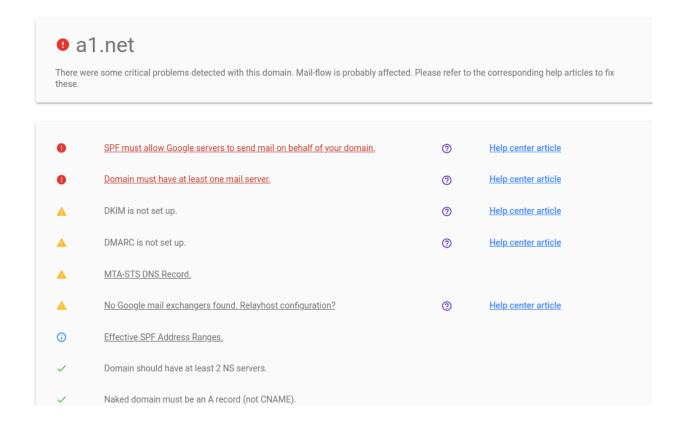
#### neciared tags

Tag	Value	Description
٧	DMARC1	DMARC protocol version.
р	none	Apply this policy to email that fails the DMARC check. This policy be set to 'none', 'quarantine', or 'reject'. 'none' is used to collect the DMARC report and gain insight into the current emailflows and their status.

This is a monitoring way of any emails that simply not being actioned such as quarantine or reject

### Let's check the domains

Upon further analysis using <a href="https://toolbox.googleapps.com/apps/checkmx/">https://toolbox.googleapps.com/apps/checkmx/</a> for the domain a1.net, below is the output. This is a good example of spoofing email headers done well.



# Next domain <u>cyberlynk.io</u>

	Test	Result
8	DMARC Policy Not Enabled	DMARC Quarantine/Reject policy not enabled
<b>②</b>	DNS Record Published	DNS Record found
•	DMARC Record Published	DMARC Record found

## ▲ Using Virus total for the IP 80.75.33.5

# smtpout05.a1.net

There were some critical problems detected with this domain. Mail-flow is probably affected. Please refer to the corresponding help articles to fix these.

0	Domain must have at least one mail server.	<b>⑦</b>	Help center article
<b>A</b>	DKIM is not set up.	<b>⑦</b>	Help center article
<b>A</b>	DMARC is not set up.	<b>?</b>	Help center article
<b>A</b>	MTA-STS DNS Record.		
<b>A</b>	There should be a valid SPF record.	<b>②</b>	Help center article
<b>A</b>	No Google mail exchangers found. Relayhost configuration?	<b>②</b>	Help center article
~	Domain should have at least 2 NS servers.		

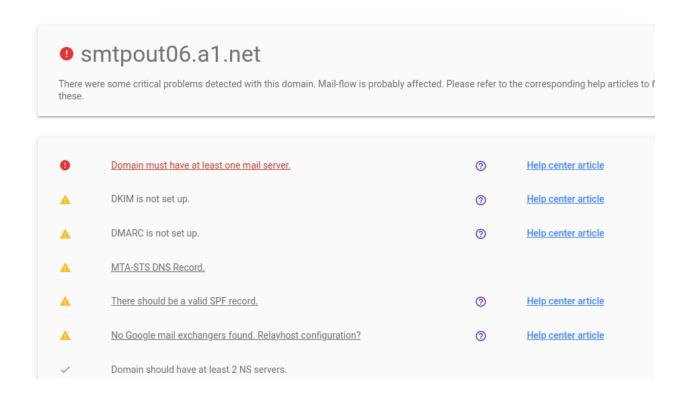
The above red error "Domain must have at least one mail server " means the mail server cannot receive messages, only send them thereby good for spammers.

Using Virus total, the IP has been used to send spam and the tactic is passive DNS replication.



<u>▲ smtpout06.a1.net</u> with the IP 80.75.33.6 which is not blacklisted

Upon further investigation, there are missing records as shown below



There are no Google mail servers, the mail probably came from a third party.

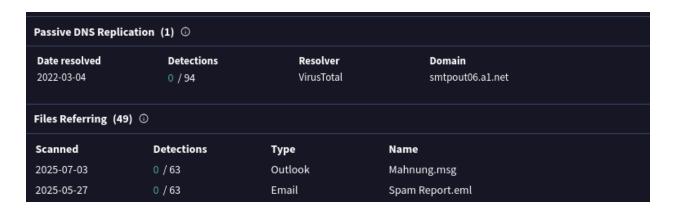
ABuselPDB highlights this mail server has been used for email spam

This IP address has been reported a total of 3 times from 2 distinct sources. 80.75.33.6 was first reported on September 27th 2022, and the most r report was 1 year ago.

Old Reports: The most recent abuse report for this IP address is from 1 year ago. It is possible that this IP is no longer involved in abusive activition

Reporter	IoA Timestamp in UTC	Comment	Categories
✓ <u>Smel</u>	2024-03-01 15:49:32 (1 year ago)	Mail/25/465/587-993/995 Probe, Reject, BadAuth, Hack, SPAM -	Email Spam Hacking Brute-Force
✓ <u>Smel</u>	2023-11-07 13:09:31 (1 year ago)	Mail/25/465/587-993/995 Probe, Reject, BadAuth, Hack, SPAM -	Email Spam Hacking Brute-Force

# It has been flagged as clean



# ▲ Check DKIM by domain <u>a1.net</u> selector resmail1 for IP 80.75.33.2

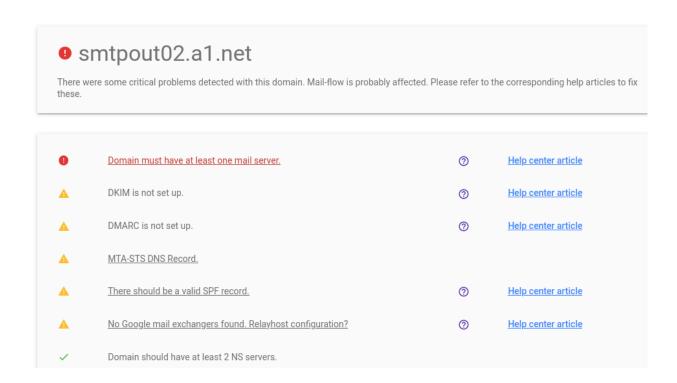
```
— AUTHENTICATION HEADERS —

SPF Check: pass (google.com: domain of noreply@a1.net designates 80.75.33.2 as permitted sender) client-ip=80.75.33.2;

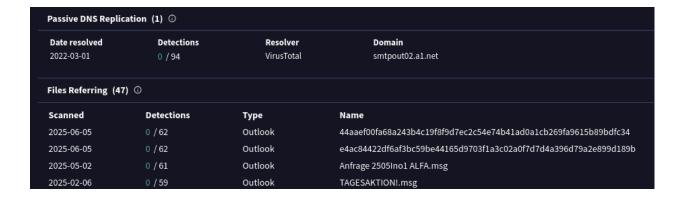
DKIM-Signature: Present
Partial DKIM: v=1; a=rsa-sha256; c=relaxed/relaxed; d=a1.net; s=resmail1; t=1735849398; h=from:from:reply-to:subje...

Authentication-Results: mx.google.com; dkim=pass header.i=@a1.net header.s=resmail1 header.b=k21L98nM; spf=pass (gly@a1.net; dmarc=pass (p=REJECT dis=NONE) header.from=a1.net

Return-Path: <noreply@a1.net>
```



Referencing virustotal, the possible attack is DNS replication attack which is where an attacker can copy previous domains visited by the user and redirect the user to sites they control such as command and control server.



▲ cyberlynk.io domain DMARC from mimecast

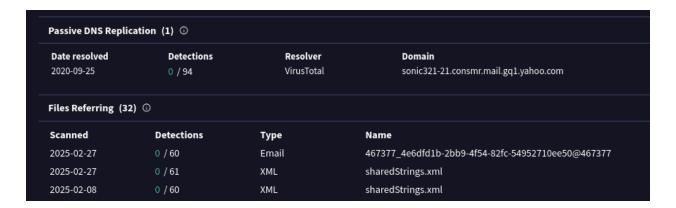
Tag	Value	Description
V	DMARC1	DMARC protocol version.
р	none	Apply this policy to email that fails the DMARC check. This policy be set to 'none', 'quarantine', or 'reject'. 'none' is used to collect the DMARC report and gain insight into the current emailflows and their status.

When the value is p, it means that there are no actions taken such as quarantine and it's monitoring then sending reports.

	lest	nesuit
<b>3</b>	SPF Authentication	SPF Failed for IP - 98.137.66.84
8	DMARC Policy Not Enabled	DMARC Quarantine/Reject policy not enabled
•	SPF Record Published	SPF Record found

### **DKIM** and **DMARC** pass

Passive DNS replication is where a domain name resolves to an IP No security vendor flagged this IP address as malicious



In this scenario, the email has been forwarded therefore the signature is still the same.



#### Base64 decode and it's HTML

:minbmn:ligFzc2vzc2ilbnQbPc9wPg0KDQog1DxwPjxn1gnyzwY91mn0aHBz018vc2nvcnk1cmwu
'XQvM1VRdlYiIGNsYXNzPSJidXR0b24iIHRhcmdldD0iX2JsYW5rIiByZWw9Im5vb3BlbmVyIG5v
:mVmZXJyZXIiPlZpZXcgTXkgUGVyZm9ybWFuY2UgUmV2aWV3PC9hPjwvcD4NCg0KICA8cD5XZSBl
:mNvdXJhZ2UgeW91IHRvIHJldmlldyB5b3VyIHByb2dyZXNzIGFuZCBwbGFuIGZvciB0aGUgbmV4
!CBzdGVwcyBpbiB5b3VyIGNhcmVlci4gWW91ciBjb250aW51ZWQgc3VjY2VzcyBpcyBpbXBvcnRh
:nQgdG8gdXMhPC9wPg0KDQogDQo8L2JvZHk+DQo8L2h0bWw+DQo=



<h3>Hi info.ciactrl@gmail.com,</h3>

We are excited to share with you your personalized performance review for the 2023-2024 per opportunity to reflect on your achievements, identify areas for growth, and set goals for the up

Your feedback is essential in helping us improve our processes and foster a productive, supernorment. Take some time to explore the highlights and key takeaways from your performance re-

<Click the button below to view your detailed performance assessment:</p>

b3J0aXZlIGVudmlyb25tZW50LiBUYWtlIHNvbWUgdGltZSB0byBleHBsb3aHRzIGFuZCBrZXkgdGFrZWF3YXlzIGZyb20geW91ciBwZXJmb3JtYW5jZ5DQogIDxwPkNsaWNrIHRoZSBidXR0b24gYmVsb3cgdG8gdmlldyB5b3VyICcm1hbmNlIGFzc2Vzc21lbnQ6PC9wPg0KDQogIDxwPjxhIGhyZWY9Imh0dbYXQvM1VRdlYiIGNsYXNzPSJidXR0b24iIHRhcmdldD0iX2JsYW5rIiByZVcmVmZXJyZXIiPlZpZXcgTXkgUGVyZm9ybWFuY2UgUmV2aWV3PC9hPjwvcIbmNvdXJhZ2UgeW91IHRvIHJldmlldyB5b3VyIHByb2dyZXNzIGFuZCBwbCdCBzdGVwcyBpbiB5b3VyIGNhcmVlci4gWW91ciBjb250aW51ZWQgc3VjY2bnQgdG8gdXMhPC9wPg0KDQogDQo8L2JvZHk+DQo8L2h0bWw+DQo=



https://shorturl.at/3UQvV is flagged as clean by some vendors and belongs to cloudflarenet

This is base64 encoding in an email. This email also has an attachment which is tied to trick the user to download and open the attachment.

aGVsbG8gaW5mby5jaWFjdHJsQGdtYWlsLmNvbSwgPGJyPiA8YnI+DQpZb3UgaGF2ZSBuZXcgQXNz ZXNzbWVudCBzdGF0ZW1lbnQgUmVhZHkgZm9yIFNjcmVlbmluZy4=

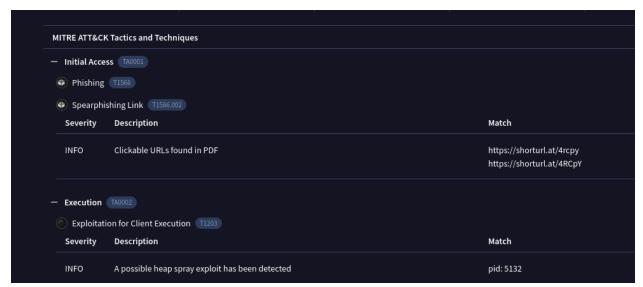
RBC 130 = 3

#### Output

I used a python script to download the attachment, please refer to github for scripts.

The attachment on virus total and was undetected as malicious by some security vendors





The malicious PDF is therefore used as part of initial access and compromise to gain credentials.

🐹 Wireshark Traffic analysis 🔔

No.	Time	Source	Destination	Protocol	Length Info
	7 0.275517071	10.0.0.138	10.0.2.15	DNS	78 Standard query response 0xbd60 No such name A holyflamesnik.site
	8 0.275517344	10.0.0.138	10.0.2.15	DNS	78 Standard query response 0xbe61 No such name AAAA holyflamesnik.site
	9 0.275601547	10.0.2.15	10.0.0.138	DNS	86 Standard query 0x8a6d A holyflamesnik.site.gateway
	10 0.275609396	10.0.2.15	10.0.0.138	DNS	86 Standard query 0x5b6f AAAA holyflamesnik.site.gateway
	11 0.277082529	10.0.0.138	10.0.2.15	DNS	86 Standard query response 0x8a6d No such name A holyflamesnik.site.gateway
	12 0.277082672	10.0.0.138	10.0.2.15	DNS	86 Standard query response 0x5b6f No such name AAAA holyflamesnik.site.gateway
	13 0.278965518	10.0.2.15	10.0.0.138	DNS	78 Standard query 0xcbde A holyflamesnik.site
	14 0.278982585	10.0.2.15	10.0.0.138	DNS	78 Standard query 0xa4d1 AAAA holyflamesnik.site
	15 0.280412586	10.0.0.138	10.0.2.15	DNS	78 Standard query response 0xcbde No such name A holyflamesnik.site
	16 0.280456204	10.0.0.138	10.0.2.15	DNS	78 Standard query response 0xa4d1 No such name AAAA holyflamesnik.site
	17 0.280484266	10.0.2.15	10.0.0.138	DNS	86 Standard query 0xdd7e A holyflamesnik.site.gateway
	18 0.280491318	10.0.2.15	10.0.0.138	DNS	86 Standard query 0xae7f AAAA holyflamesnik.site.gateway
	19 0.281755957	10.0.0.138	10.0.2.15	DNS	86 Standard query response 0xdd7e No such name A holyflamesnik.site.gateway
	20 0.281905825	10.0.0.138	10.0.2.15	DNS	86 Standard query response 0xae7f No such name AAAA holyflamesnik.site.gateway
	21 0.411857018	10.0.2.15	10.0.0.138	DNS	82 Standard query 0x5fc3 A www.holyflamesnik.site
	22 0.411941661	10.0.2.15	10.0.0.138	DNS	82 Standard guerv 0xf8c1 AAAA www.holvflamesnik.site

When the pdf attachement is opened and network traffic capture, there is routing to the suspicious site. The PDF has a link to a domain controlled by the attacker <a href="https://holyflamesnik.site/viewmyprofile/">https://holyflamesnik.site/viewmyprofile/</a> ABuseIPDB reference for 10.0.2.15 used for the DNS protocol compromise.

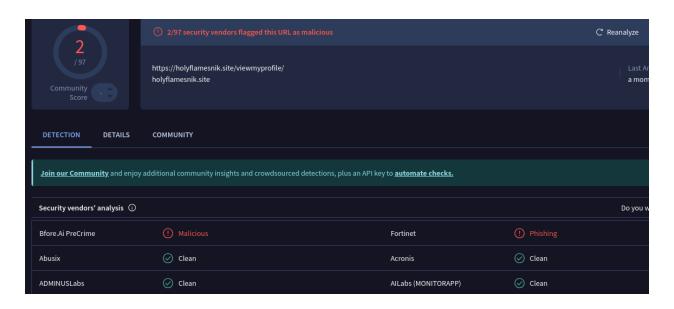




JVBERi0xLjQKJdPr6eEKMSAwIG9iago8PC9DcmVhdG9yIChDaHJvbWl1bSkKL1Byb2R1Y2VyIChT a2lhL1BERiBtMTEwKQovQ3JlYXRpb25EYXRlIChEOjIwMjQxMTIzMDgzMjAwKzAwJzAwJykKL01v ZERhdGUgKEQ6MjAyNDExMjMwODMyMDArMDAnMDAnKT4+CmVuZG9iagozIDAgb2JqCjw8L2NhIDEK L0JNIC90b3JtYWw+PqplbmRvYmoKNiAwIG9iaqo8PC9UeXBlIC9Bbm5vdAovU3VidHlwZSAvTGlu awovRiA0Ci9Cb3JkZXIgWzAgMCAwXQovUmVjdCBbMjI2LjMwNjM0IDcwMC4yMjA10CAzNjguNjkz NiA3NDAuMTE2NTJdCi9BIDw8L1R5cGUgL0FjdGlvbgovUyAvVVJJCi9VUkkgKGh0dHBzOi8vc2hv cnR1cmwuYXQvNFJDcFkpPj4KL1N0cnVjdFBhcmVudCAxMDAwMDA+PgplbmRvYmoKNyAwIG9iago8 PC9GaWx0ZXIgL0ZsYXRlRGVjb2RlCi9MZW5ndGggMTA0Nz4+IHN0cmVhbQp4nH1W24okNwx9r6/w c2A91s0XGAamq7eXPCwkoWE/YJJsWHYC2fw/RJJd7apA9/RUly3L0pF0LHdEav4Xkn4+xN20MsQG rdXw9r78s9g6cmkRcpZAkmpMDSn8+GP58lP4WzUw1pxTrey2jjM18fSJwtd/l9N1efolPD8/fV5/ PuvKy8vpvC5PF1br4frnAh0JqAu0jYoE0AzX9+U5JeSXcP22qESRVCq0al5/D7pCpa9wRMySUeYK Jv3Sf9H9Vd/UZTYfuz5+XpeP1yVyiBXVobolCr99Cv+T/Pi6ELaACcK7j0AofNdRjZazonOMRLnl oKsRMFdSGcTcGjC6kGqS6sJUFSiFN7MUMzGa0EUuVgLXbU1EjXIz91hVSLqemcWFNuJiBlRsGlnF 1XeZKrgpdpmap1RViO4WXehQxPejQ3Spoc6KlchD8f066++3RcjVNGwdxZwpubEgakMzW+reiAkb WOOO/kRtC8oRmxDHlI1bMwiTifIqH+NVUUyJ8ZAbE5JmdJ9Ek2VohMeEm7qWAtqXRyjv6tdnXTl7 RBC 62829 = 819 Output

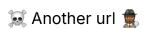
https://shorturl.at/4RCpY resolves to https://holyflamesnik.site/viewmyprofile/on virustotal, confirmed this is a phishing attack

https://shorturl.at/4RCpY)



#curl -i https://shorturl.at/4RCpY shows redirection to the attack owned domain.

```
nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
server: cloudflare
server-timing: cfL4;desc="?proto=TCP&rtt=13246&min_rtt=5679&rtt_var=11967&sent=8&receptore
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>301 Moved Permanently</title>
</head><body>
<h1>Moved Permanently</h1>
The document has moved <a href="https://www.shorturl.at/4RCpY">here</a>.
</body></html>
```



### Input

b21lciBTdXBwb3J0PC9zdHJvbmc+LiBJZiB5b3UgaGF2ZSBhbnkgcXVlc3Rpb25zIG9yIG5lZWQg YXNzaXN0YW5jZSwgcGxlYXNlIGZlZWwgZnJlZSB0byByZWFjaCBvdXQgdG8gdXMgYXQgPGEgaHJl Zj0idGVs0jEzMTMx0CIgc3R5bGU9ImNvbG9y0iAjMzNjY2Zm0yB0ZXh0LWRlY29yYXRpb246bm9u ZTsiPjEzMiAzMDc8L2E+LiANCiAgICAgICAgICAgICAgICAgICAgIDwvcD4gDQogICAgICAg ICAgICAgICAgICAgICAGICA8ZGl2IHN0eWxlPSJ0ZXh0LWFsaWdu0iBjZW50ZXI7IG1hcmdpbi10 b3A6IDIwcHg7Ij4gDQogICAgICAgICAgICAgICAgICAgICAgICAgICAgPGEgaHJlZj0iIyIgc3R5 bGU9ImNvbG9y0iAjNTE1MzRhOyB0ZXh0LWRlY29yYXRpb246IG5vbmU7IG1hcmdpbjogMCAxMHB4 CiAqICAqICAqICAqICAqICAqICAqICAqICAqICASYSBocmVmPSIjIiBzdHlsZT0iY29sb316ICM1 MTUzNGE7IHRleHQtZGVjb3JhdGlvbjogbm9uZTsgbWFyZ2lu0iAwIDEwcHg7Ij5MZWdhbCBJbmZv ICAgICAgICAgICAgICAgICA8YSBocmVmPSIjIiBzdHlsZT0iY29sb3I6ICM1MTUzNGE7IHRleHQt ZGVjb3JhdGlvbjogbm9uZTsgbWFyZ2lu0iAwIDEwcHg7Ij5Qcml2YWN5IFBvbGljeTwvYT4gDQog ICAqICAqICAqICAqICAqICAqICAqICASL2Rpdj4qDQoqICAqICAqICAqICAqICAqICAqICAqIDwvZGl2 PiANCiAgICAgICAgICAgICAGICASL2Rpdj4gDQogICAgICAGICAGICASL3RkPiANCiAgICAGICAG PC90cj4gDQogICAgPC90YWJsZT4gDQo8L2JvZHk+IA0KPC9odG1sPg0K

Output

https://shorturl.at/LqQ15

https://shorturl.at/LqQ15 which is flagged as clean and reports to cloudflarenet #curl -i https://www.shorturl.at/LqQ15

```
recorde-status: DYNAMIC
report-to: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?s=1%2FVuCmRyYQUU%2FbWx0AJaIXS4TdbADd4fOql
group":"cf-nel","max_age":604800}
wel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
werver: cloudflare
werver-timing: cfL4;desc="?proto=TCP&rtt=8671&min_rtt=3782&rtt_var=10562&sent=8&recv=9&lost=0&retrans=0&sent_bytes=30
```

Metflix subscription payment update for subscription legitimacy, email forwarding and use of urgent language.

🖼 A white background color making it obfuscated and %20 is encoding for space

building inext previous all imatch case inegexp in by word
Le%ZUW1GTN=3D%ZZ1UU%Z5%ZZ%ZUDOrGer=3D%ZZU%ZZ%ZUCe.LLpaGG=%UAING=3D%ZZU%ZZU%ZUCe.LLspacing=3D%ZZU%ZZW3E%UA%ZU%
0%20%20%20%20%20%20%20%20%20%20%20%20%20
0%20%20%20%20%20%20%20%20%20%20%20%20%20
0%20%20%20%20%20%20%20%20%20%20%20%20%20
3Ctd%20align=3D%22center%22%20valign=3D%22top%22%20s=%0Atyle=3D%22padding-left:40px;padding-
right:40px;background-color:#ffffff;
.· %22%20bgc=%0Aolor=3D%22#ffffff%22%3E%0A%20%20%20%20%20%20%20%20%20%20%20%20%20%
0%20%20%20%20%20%20%20%20%20%20%20%20%20
pacing=3D%220%22%3E%0A%20%20%20%20%20%20%20%20%20%20%20%20%20%
20%20%20%20%20%20%20%20%20%20%20%20%3Ctbody%3E%0A%20%20%20%20%20%20%20%20%20%20%20%20%20%
20%20%20%20%20%20%20%20%20%20%20%20%20%2
2 <del>0</del> %20%20%20%20%20%20%20%20%20%20%20%20%20%
tyle=3D%22font-size:0;line=%0A-height:0;min-height:40px;%22%20height=3D%2240%22%3E %3C/

The text is also white which adds to more obfuscation, therefore white fonts on white background.

```
font-family:NetflixSans-Bold, Helvetica, Roboto, Segoe UI, sans-serif;font=weight:700;font-size:14px;line-height:17px;letter-spacing:-0.2px;padding:1=ox 20px;color:#fffffff;"><a href=3D"https://qrco.de/bf9xmf?click?s=3DVwtvB1=amp;li=3D{LIST_ID}&amp;e=3DH&amp;unsubcribe=3Dphish@cyberlynk.io&amp;p=3DankthyH9&amp;id=3DY4SR8KTMSIMMBVEV3K047HUSH0LB2FVXACJGAT45CA0AI576U0?dg7=fgbpi6oruegsx0mpaudiwpmxhrutkec4jgbulbeehfwlg38yzjtk9aqn1qpneu6uxiuhpgh5vy=3kme97iykuvhu2jv86pq1&amp;stpe=3Ddefault" style=3D"font-family:NetflixSans=3old, Helvetica, Roboto, Segoe UI, sans-serif;font-weight:700;font-size:14=x;line-height:17px;letter-spacing:-0.2px;text-align:center;text-decoration=none;display:block;color:#fffffff;" target=3D"_blank" rel=3D"noreferrer noo=ener">Update information</a>
```

Using cyberchef, the word is access using the recipe from quoted printable. This is an obfuscation tactic whereby the attacker used letters and numbers that look real.

```
=20
| To ensure uninterrupted <mark>=D0=B0cc=D0=B5ss</mark> to your favorite movies and show=
s, we kindly ask you to update billing information. |
```

🐹 Included valid URLs to make it look legitimate.

```
https://ci3.googl
https://beaconimages.netflix
https://www.netflix.com/browse?g=
https://ci3.go
https://qrco.de/bf9xmf?click?s=3DVwtvB1=
https://help.netflix.com/help?g=3D58ffd66c-8e71-4ed2-af78-6c86=
https://help.netflix.com/contactus?g=3D58ffd66c-8e71-4ed2-af78-6c86a529=
https://ci3.googleusercontent.com/meip=
https://assets.nflxext.com/us/email=
https://www.netflix.co
https://www.netflix.com/TermsOfUse?g=3D58ffd66c-8e71-4ed2-af78-6c86a529dbf7=
https://www.netflix.com/PrivacyPolicy?g=
https://help.netflix.com/help?g=3D58ffd66c-8e71-4ed2-af78-6c86a529dbf7=
https://www.netflix.com/browse?g=3D58ffd66c-8e71-4ed2-af78-6c86a529dbf7=
```

# Conclusion

This phishing campaign used:

- High-quality header spoofing and SPF passing
- Base64 + quoted-printable encoding
- Redirection via short URLs and PDFs
- Abuse of clean infrastructure like cloudflare links

# Recommendations

- Block malicious domains and IPs in gateway firewall
- Submit all IOCs to SIEM/Threat Intel feed
- · Educate users about obfuscated email tactics
- Strengthen email filtering and sandboxing policies

### ▲ Tools and resources

spf checker <a href="https://mxtoolbox.com/spf.aspx">https://mxtoolbox.com/spf.aspx</a>

Cyberchef <a href="https://gchq.github.io/CyberChef/">https://gchq.github.io/CyberChef/</a>

Sandbox <a href="https://app.any.run/#register">https://app.any.run/#register</a>

https://mxtoolbox.com/EmailHeaders.aspx

https://toolbox.googleapps.com/apps/main/

https://dmarcian.com/dkim-inspector/