Email Analysis

Phishing

Phishing is when attackers attempt to trick users into doing 'the wrong thing', such as clicking a bad link that will download malware, or direct them to a dodgy website.

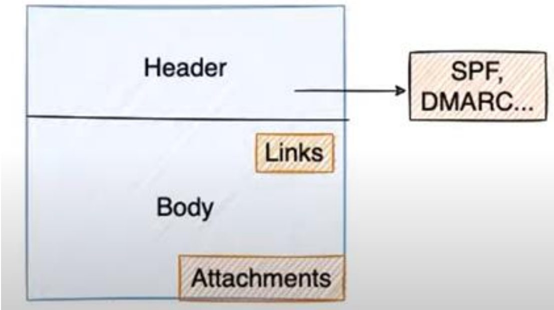
How Email Files Are Used by Threat Actors?

The goal: Make the email look legitimate to increase the chances of the victim to:

- Open links provided in the email
- Enter credentials or sensitive information
- Open malicious attached files

Structure of an email header :

1. **From :** sender's address
2. **To :** receiver's address (including CC and BCC)
3. **Date:** Timestamp, when email was sent
4. **Subject**
5. **Return path :** reply-To
6. **DKIM Signatures**



7. **SPF :** Server that was used to send the email. compare servers with actual domain.
8. **Message-ID :** Unique ID of the email

9. **MIME-Version :** “non-text” contents and attachments

10. **X-received :** mail servers that the mail went through

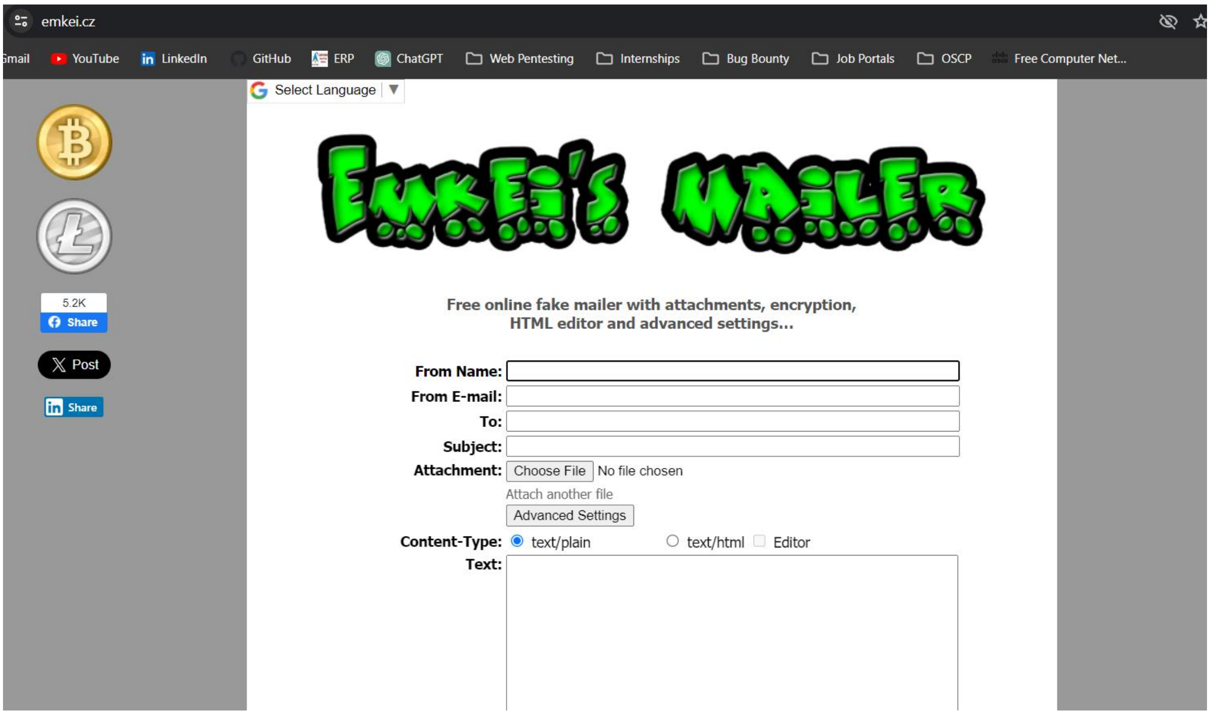
Emails Spoofing - Methods

1. **Spam folder**
   - ➔ Content - flag words, large image with short text
   - ➔ Sender IP and domain reputation

2. **Suspicious sender:**
   - ➔ Email received from outside the org
   - ➔ Suspicious sender
   - ➔ The @<something> part and public domain
   - ➔ Domain name is misspelt
   - ➔ You didn't expect to receive the emails

Tool’s/Source’s for spoofing Email’s

Using “emkei.cz” a person can spoof anyone’s email if they are not using mail server’s that are DMARC Compliance.



Free online fake mailer with attachments, encryption, HTML editor and advanced settings...

From Name:
From E-mail:
To:
Subject:
Attachment: No file chosen
Content-Type: ● text/plain ○ text/html □ Editor
Text:

Information from the header?

- Is the sender authorized?
- Is it malicious email?
- Who it targets?

Tools:

- Whois
- SPF record check

Email Investigation

Scenario 1: Email without any attachment media/link

Let’s send a spoofed mail to a temp mail address using emkei.cz

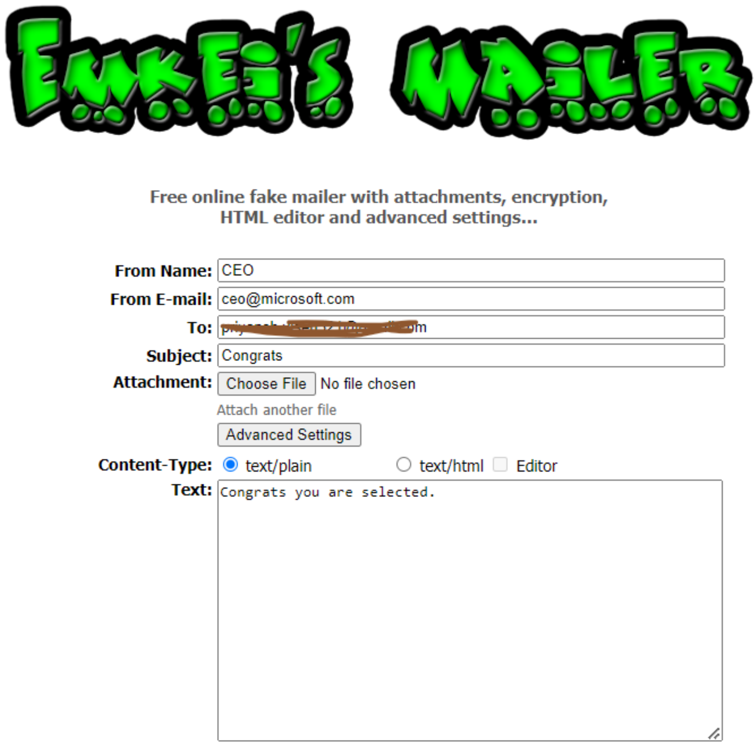
From Name : CEO

From Email : ceo@microsoft.com

To: <temp mail address>

Subject : Congrats

Text: Congrats you are selected.



Free online fake mailer with attachments, encryption, HTML editor and advanced settings...

From Name: CEO

From E-mail: ceo@microsoft.com

To: [redacted]

Subject: Congrats

Attachment: Choose File No file chosen

Attach another file

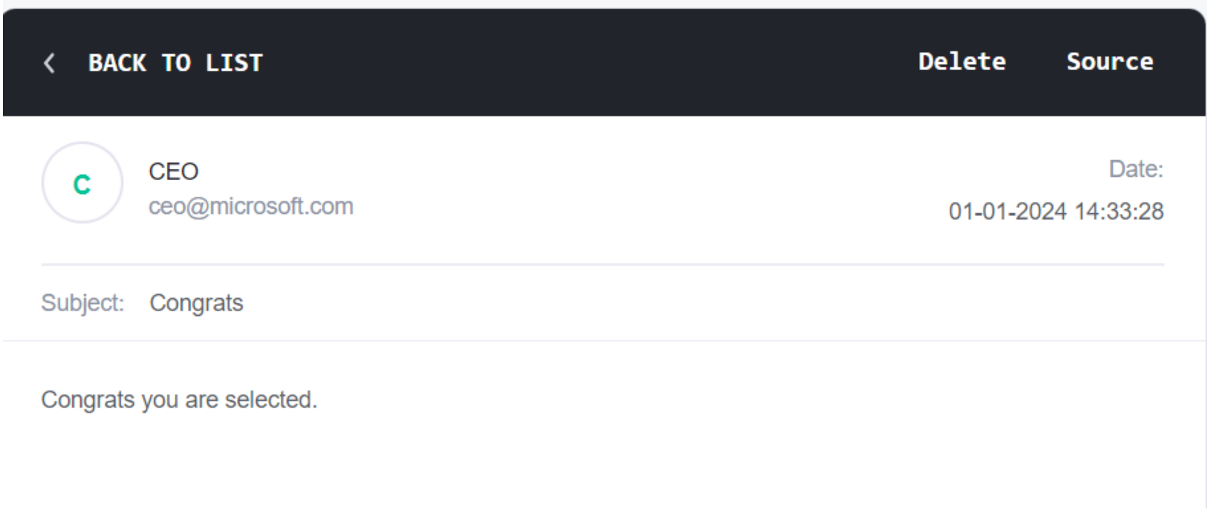
Advanced Settings

Content-Type: ● text/plain ○ text/html □ Editor

Text: Congrats you are selected.

Send The mail and check your inbox

So We have Recevied the mail that says sender address as ceo@microsoft.com



CEO
ceo@microsoft.com

Date:
01-01-2024 14:33:28

Subject: Congrats

Congrats you are selected.

Suppose we are suspecting it that it is a spoofed mail now Let’s analyse the mail and check if the mail is spoofed or not.

1. Download Header Information of the mail and open it with any text editor.

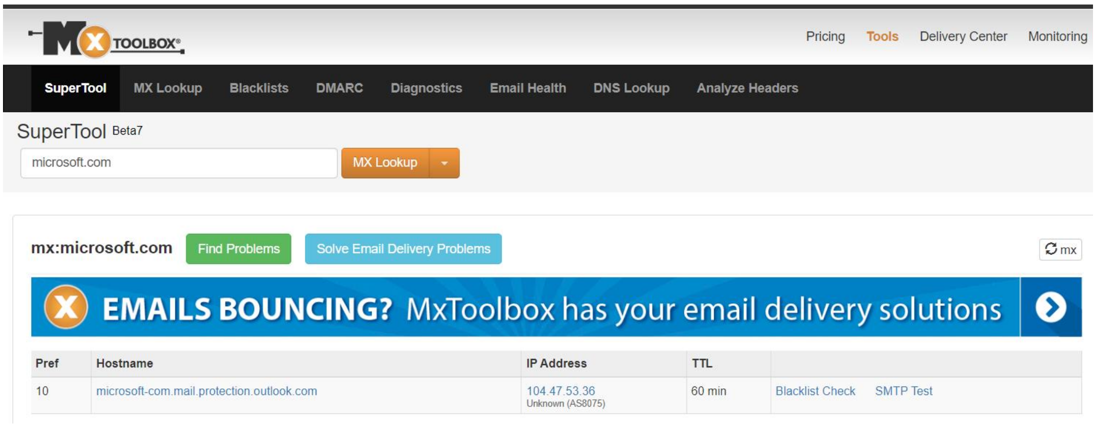
```
Received: from emkei.cz (Unknown [10.244.13.123])
      by c1bf3b2951b1 (Haraka/3.0.2) with ESMTP id 1655179B-4EB5-4FB8-
8A8A-B13E86BE6568.1
      envelope-from <ceo@microsoft.com>;
      Mon, 01 Jan 2024 09:03:28 +0000
Received: by emkei.cz (Postfix, from userid 33)
      id B79AD620545; Mon,  1 Jan 2024 10:03:27 +0100 (CET)
To: xolenah222@vkr1.com
Subject: Congrats
From: "CEO" <ceo@microsoft.com>
X-Priority: 3 (Normal)
Importance: Normal
Errors-To: ceo@microsoft.com
Reply-To: ceo@microsoft.com
Content-Type: text/plain; charset=utf-8
Message-Id: <20240101090327.B79AD620545@emkei.cz>
Date: Mon,  1 Jan 2024 10:03:27 +0100 (CET)

Congrats you are selected.
```

So based on the above email Header we can gather few Important information’s like:

Received: emkei.cz (10.244.13.123)
To: xolaenah222@vkrl.com
From: ceo@microsoft.com

Now Let’s Dive into The Investigation

2. Find The MX Record of the actual domain that is microsoft.com



mx:microsoft.com

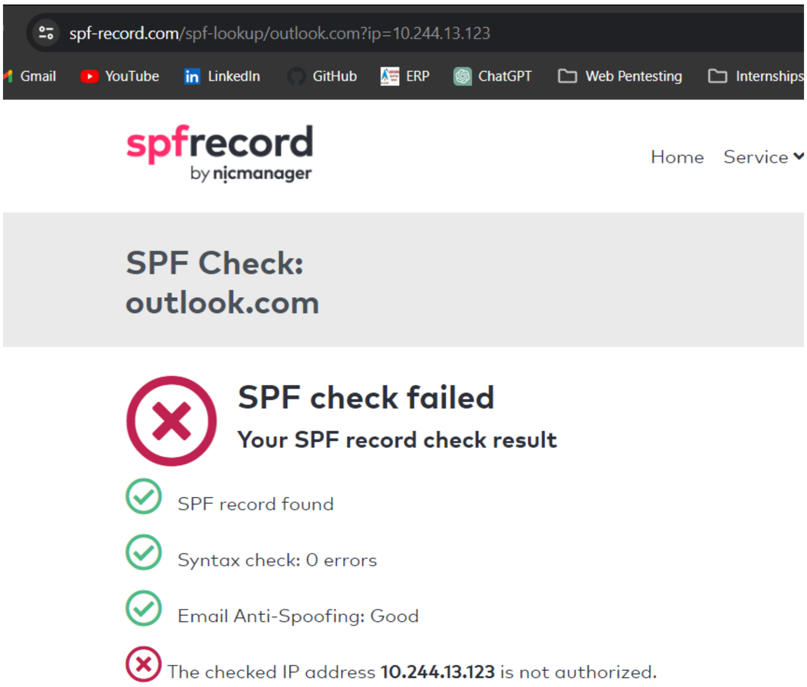
Pref	Hostname	IP Address	TTL	
10	microsoft-com.mail.protection.outlook.com	104.47.53.36 Unknown (AS8075)	60 min	Blacklist Check SMTP Test

Hostname of MX Record of Microsoft: microsoft-com.mail.protection.outlook.com
IP Address from where we received Mail is: 10.244.13.123

3. Let’s Check if Microsoft has SPF Record or not and if yes then if this IP is authorized to send mails on behalf of Microsoft or not.

As we can see that Microsoft has valid SPF Record but This given IP (from which We received mail **is not Authorized** to send mail On behalf of Microsoft).

Source: spf-record.com



SPF Check: outlook.com

SPF check failed

Your SPF record check result

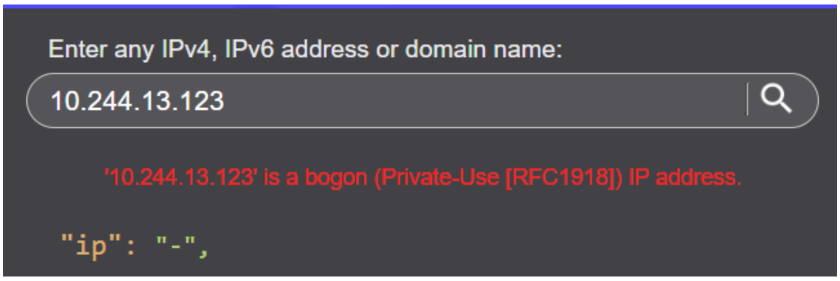
✓ SPF record found

✓ Syntax check: 0 errors

✓ Email Anti-Spoofing: Good

☒ The checked IP address **10.244.13.123** is not authorized.

4. Investigating Further About the source IP We find that it’s a bogon Private IP Address which means that these addresses can be used by anyone without any need to coordinate with IANA or an Internet registry.



Enter any IPv4, IPv6 address or domain name:

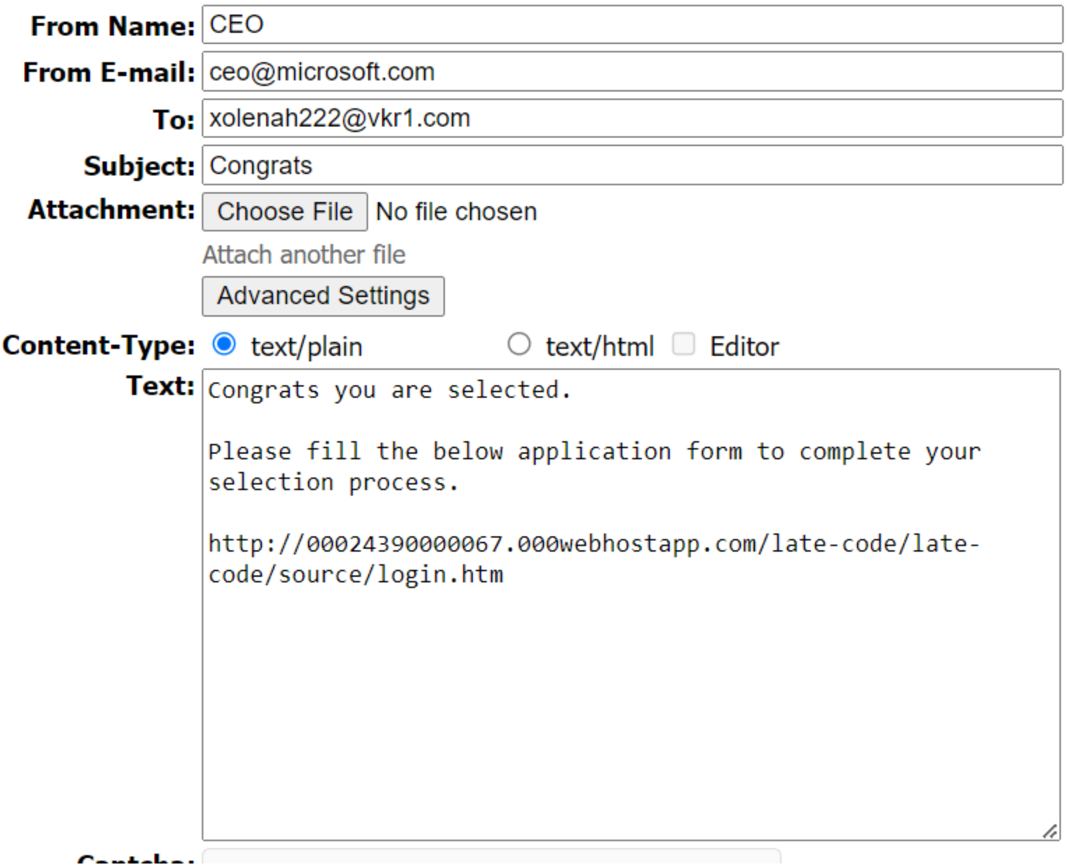
10.244.13.123

'10.244.13.123' is a bogon (Private-Use [RFC1918]) IP address.

```
"ip": "-",
```

Scenario 2: Email With any attached link or media

1. Sending a spoofed mail to victim using fake mailer and this time add a phishing link attachment.



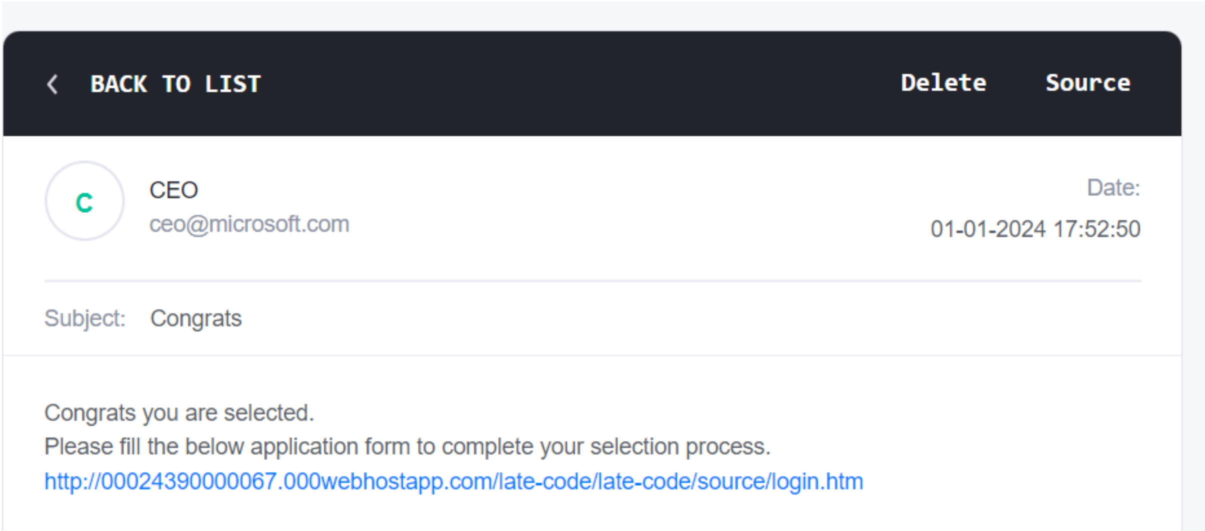
From Name:	CEO
From E-mail:	ceo@microsoft.com
To:	xolenah222@vkr1.com
Subject:	Congrats
Attachment:	Choose File No file chosen

Content-Type: ● text/plain ○ text/html □ Editor

Text:

```
Congrats you are selected.

Please fill the below application form to complete your
selection process.

http://00024390000067.000webhostapp.com/late-code/late-
code/source/login.htm
```

2. Verifying that victim received the mail with attachment.



CEO
ceo@microsoft.com

Date:
01-01-2024 17:52:50

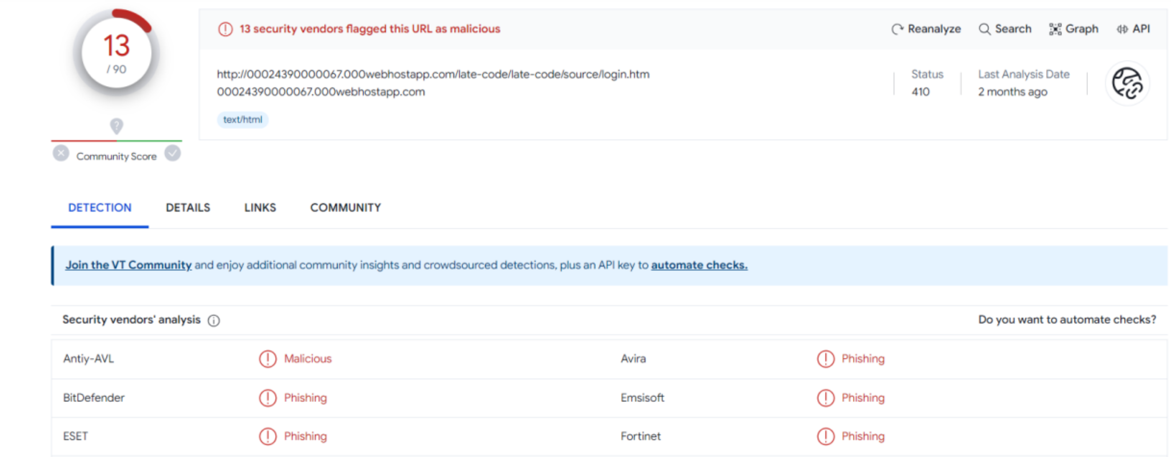
Subject: Congrats

Congrats you are selected.
Please fill the below application form to complete your selection process.
http://00024390000067.000webhostapp.com/late-code/late-code/source/login.htm

3. Perform Email Header Analysis as we performed in scenario 1 to Identify that Mail is spoofed.

4. Copy the URL Attachment and dump it in various platforms to determine whether the URL Attachment is phishing or safe to open.

1. Virustotal



13 / 90

Community Score

13 security vendors flagged this URL as malicious

http://00024390000067.000webhostapp.com/late-code/late-code/source/login.htm
00024390000067.000webhostapp.com

text/html

Status 410

Last Analysis Date 2 months ago

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

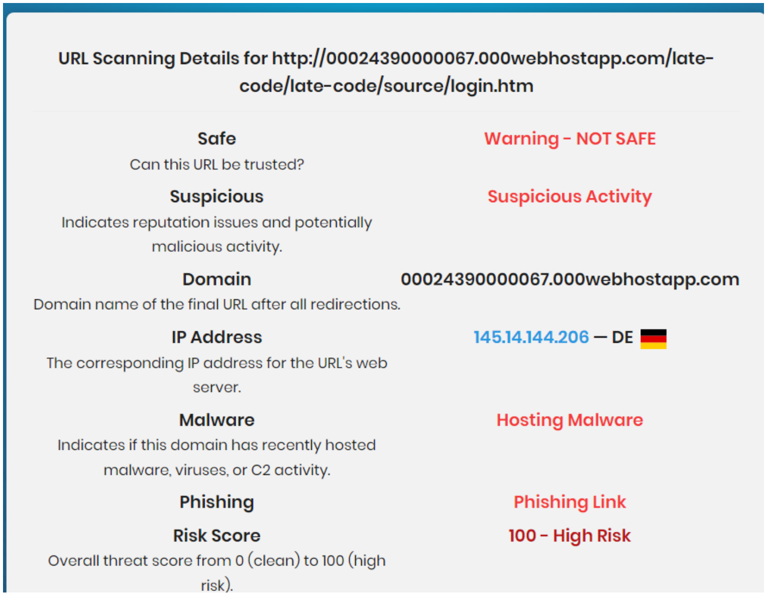
Security vendors' analysis

Do you want to automate checks?

Antiy-AVL	Malicious	Avira	Phishing
BitDefender	Phishing	Emsisoft	Phishing
ESET	Phishing	Fortinet	Phishing

According to Virus Total : **13 Security Vendors** Marked the URL as **Phishing**.

2. ipqualityscore.com

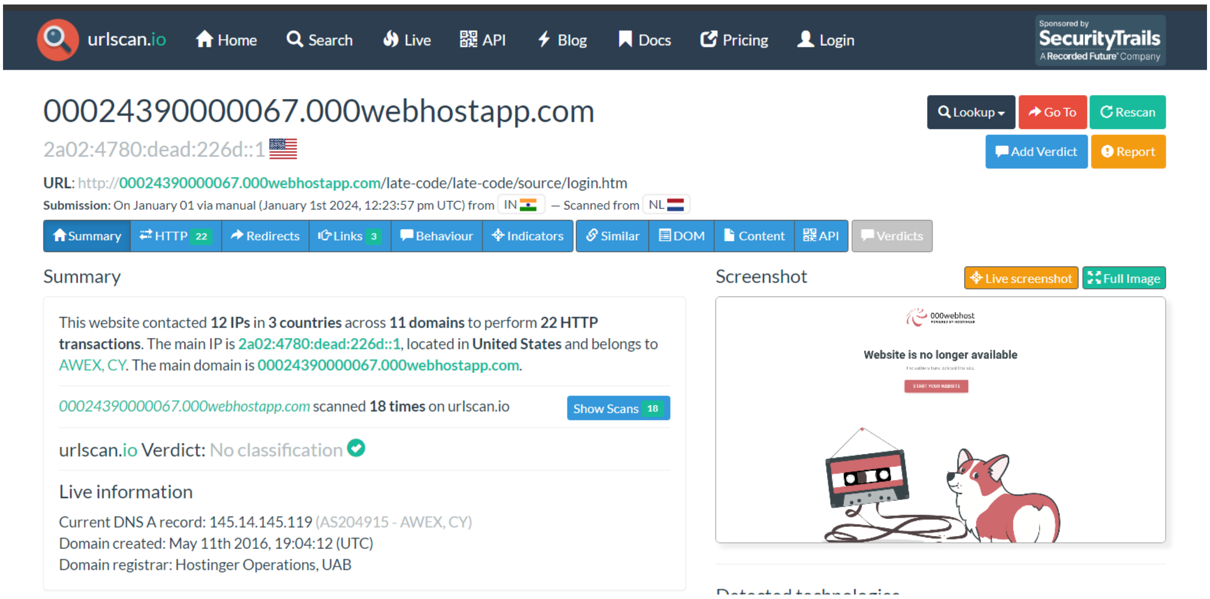


URL Scanning Details for http://00024390000067.000webhostapp.com/late-code/late-code/source/login.htm

Safe Can this URL be trusted?	Warning - NOT SAFE
Suspicious Indicates reputation issues and potentially malicious activity.	Suspicious Activity
Domain Domain name of the final URL after all redirections.	00024390000067.000webhostapp.com
IP Address The corresponding IP address for the URL's web server.	145.14.144.206 — DE
Malware Indicates if this domain has recently hosted malware, viruses, or C2 activity.	Hosting Malware
Phishing	Phishing Link
Risk Score Overall threat score from 0 (clean) to 100 (high risk).	100 - High Risk

- Ipqualityscore report also concludes that this URL is not safe to open and flagged as Phishing link.

3. urlscan.io



000243900000067.000webhostapp.com

2a02:4780:dead:226d::1

URL: http://000243900000067.000webhostapp.com/late-code/late-code/source/login.htm

Submission: On January 01 via manual (January 1st 2024, 12:23:57 pm UTC) from IN — Scanned from NL

Summary

This website contacted **12 IPs** in **3 countries** across **11 domains** to perform **22 HTTP transactions**. The main IP is 2a02:4780:dead:226d::1, located in **United States** and belongs to AWEX, CY. The main domain is 000243900000067.000webhostapp.com.

000243900000067.000webhostapp.com scanned **18 times** on urlscan.io

urlscan.io Verdict: No classification

Live information

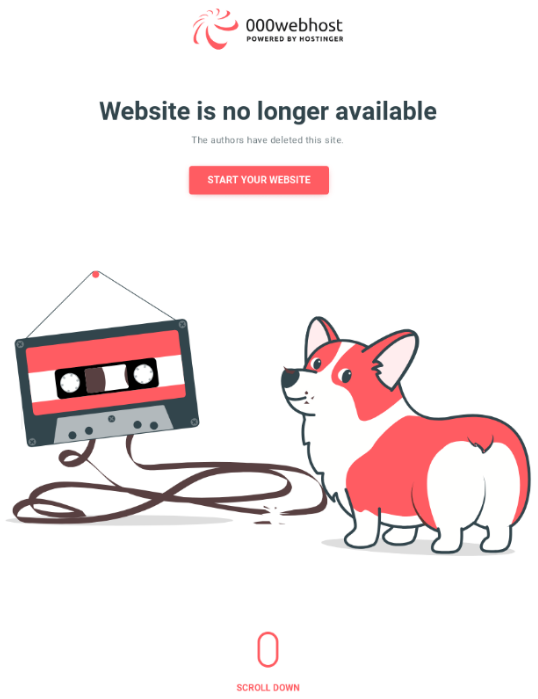
Current DNS A record: 145.14.145.119 (AS204915 - AWEX, CY)
Domain created: May 11th 2016, 19:04:12 (UTC)
Domain registrar: Hostinger Operations, UAB

Screenshot

Website is no longer available

Detected technologies

- urlscan.io doesn’t conclude any verdict whether the link is malicious or not but it shows us summary of what the url is.
- And also visits the link and captures a screenshot of it for us.
- Screenshot Preview Below:

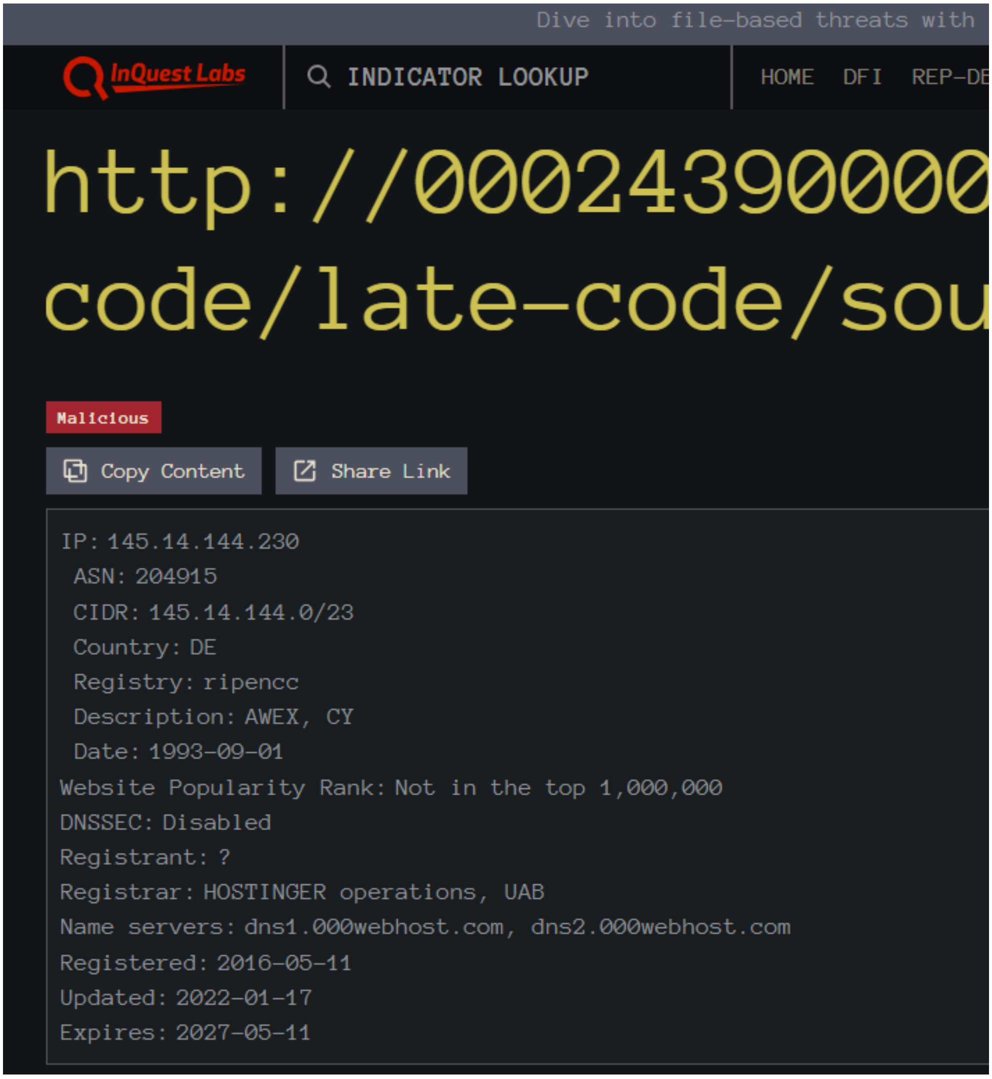


Website is no longer available

The authors have deleted this site.

4. labs.inquest.net

labs.inquest.net has also identified this url as Malicious



http://00024390000
code/late-code/sou

```
IP: 145.14.144.230
 ASN: 204915
 CIDR: 145.14.144.0/23
 Country: DE
 Registry: ripencc
 Description: AWEX, CY
 Date: 1993-09-01
Website Popularity Rank: Not in the top 1,000,000
DNSSEC: Disabled
Registrant: ?
Registrar: HOSTINGER operations, UAB
Name servers: dns1.000webhost.com, dns2.000webhost.com
Registered: 2016-05-11
Updated: 2022-01-17
Expires: 2027-05-11
```

Conclusion

We have used Static analysis on the link. You can perform Dynamic analysis by using a sandbox environment and then visiting the page and manually analyzing it.

Do the same things if the attachment is any kind of file. Just copy the hash value of the file and dump it on various platforms or perform manual dynamic testing on sandbox environment.

Static Analysis:

1. AbuseIPDB

Dynamic analysis:

1. Anyrun
2. Hybrid Analysis
3. Browserling

Additional Techniques

Another technique that attackers use is to perform phishing attacks using normally legal sites. Some of them are as follows.

1. **Using services that offer Cloud Storage services such as Google and Microsoft**

   Attackers try to click on Google / Microsoft drive addresses that seem harmless to the user by uploading harmful files onto the drive.

2. **Using services that allow creating free subdomains such as Microsoft, Wordpress, Blogspot, Wix**

   Attackers try to deceive security products and analysts by creating a free subdomain from these services. Since whois information cannot be searched as a subdomain, it can be seen that these addresses were taken in the past and belongs to institutions such as Microsoft, Wordpress

3. **Form applications**

   Services are available that allow free form creation. Attackers use these services instead of creating a fishing site themselves. Since the domain is harmless under normal conditions, it can pass on to the user without getting stuck on antivirus software. Google Form is an example of these services. When looking at whois information, the domain can be seen to be Google, so the attacker can mislead analysts.