

# 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

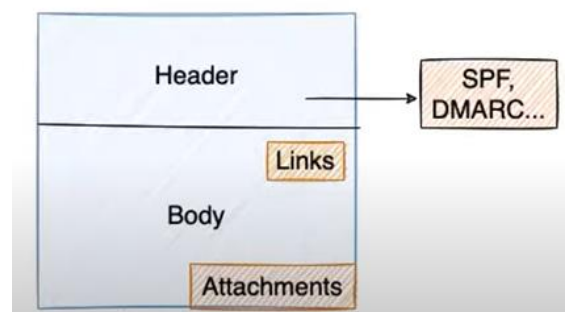
## Structure of an email header :

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

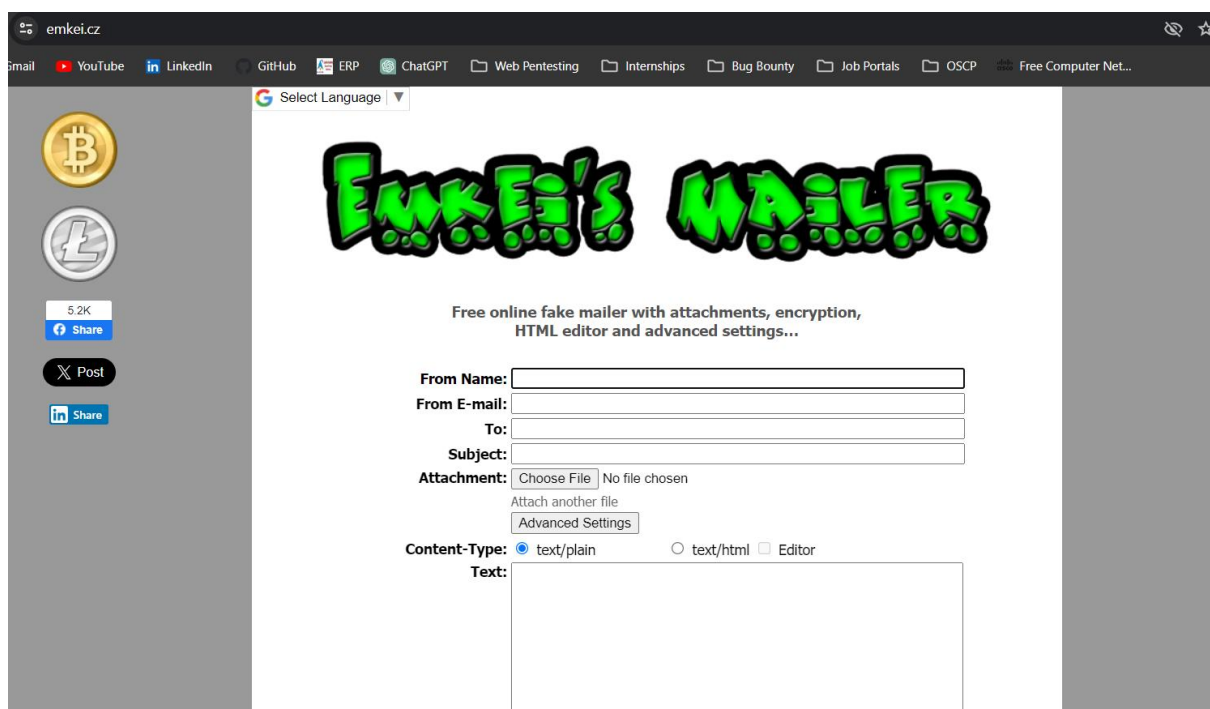
- Content - flag words, large image with short text
- Sender IP and domain reputation

### 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.



The screenshot shows the emkei.cz website interface. The browser's address bar displays 'emkei.cz'. The page features a dark header with navigation links for various services like GitHub, ERP, ChatGPT, Web Pentesting, Internships, Bug Bounty, Job Portals, OSCP, and Free Computer Net... A sidebar on the left contains social media icons for Bitcoin, Litecoin, and buttons for '5.2K', 'Share', 'Post', and 'Share'. The main content area has a large, stylized green logo that reads 'EMKEI'S MAILER'. Below the logo, it states 'Free online fake mailer with attachments, encryption, HTML editor and advanced settings...'. The form includes fields for 'From Name:', 'From E-mail:', 'To:', and 'Subject:'. The 'Attachment:' section has a 'Choose File' button and a 'No file chosen' status. Below this, there are links for 'Attach another file' and 'Advanced Settings'. The 'Content-Type:' section has three radio buttons: 'text/plain' (selected), 'text/html', and 'Editor'. A large text area labeled 'Text:' is at the bottom.

## 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:** temp@mailinator.com

**Subject:** Congrats

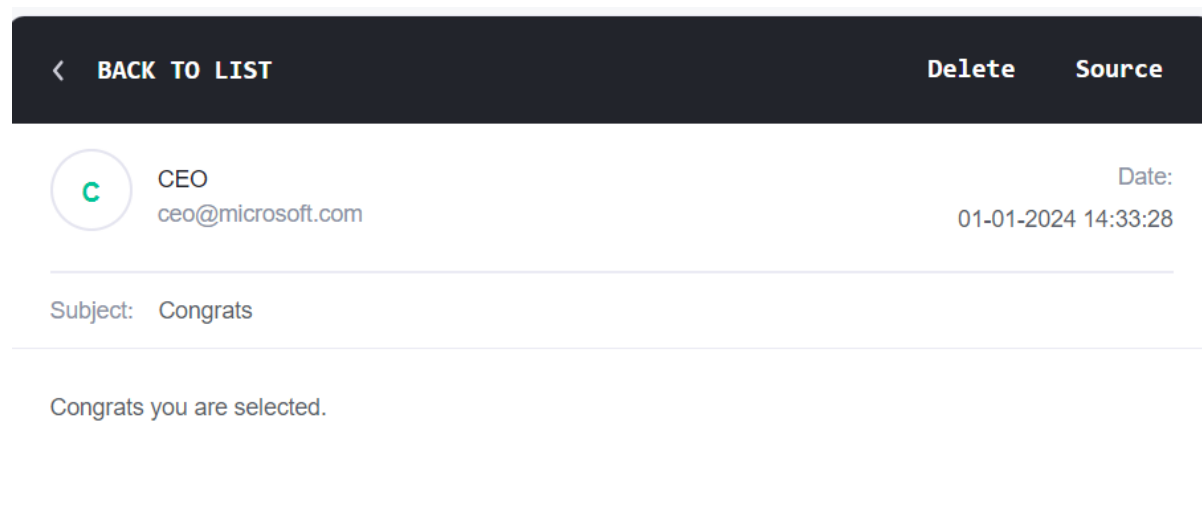
**Attachment:**  No file chosen  
[Attach another file](#)

**Content-Type:** ☒ text/plain ☐ text/html ☐ Editor

**Text:** Congrats you are selected.

Send The mail and check your inbox

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



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@vkrl.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

The screenshot shows the MxToolbox SuperTool interface. The top navigation bar includes links for Pricing, Tools, Delivery Center, and Monitoring. Below this, a secondary navigation bar lists various tools: SuperTool, MX Lookup, Blacklists, DMARC, Diagnostics, Email Health, DNS Lookup, and Analyze Headers. The main input area shows 'microsoft.com' entered in the search field, with an 'MX Lookup' button. Below the input, there are buttons for 'Find Problems' and 'Solve Email Delivery Problems'. A prominent blue banner reads 'EMAILS BOUNCING? MxToolbox has your email delivery solutions'. Below the banner, a table displays the MX record results:

Pref	Hostname	IP Address	TTL	
10	microsoft-com.mail.protection.outlook.com	104.47.53.36 <small>Unknown (AS8075)</small>	60 min	<a href="#">Blacklist Check</a> <a href="#">SMTP Test</a>

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).

The screenshot shows the spf-record.com website. The URL bar indicates the search query: 'spf-record.com/spf-lookup/outlook.com?ip=10.244.13.123'. The page header includes the 'spfrecord by njcmanager' logo and navigation links for Home and Service. The main content area displays 'SPF Check: outlook.com'. Below this, a large red 'X' icon indicates a failed check. The text 'SPF check failed' is followed by 'Your SPF record check result'. A list of check results follows: 'SPF record found' (green check), 'Syntax check: 0 errors' (green check), 'Email Anti-Spoofing: Good' (green check), and 'The checked IP address 10.244.13.123 is not authorized.' (red X).

Source: spf-record.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.

The screenshot shows a search interface with the input '10.244.13.123'. Below the input, a red message states: '10.244.13.123' is a bogon (Private-Use [RFC1918]) IP address. Below this, a JSON snippet is shown: '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:**  No file chosen  
[Attach another file](#)

**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.

[<](#) **BACK TO LIST** **Delete** **Source**



**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

The screenshot shows the VirusTotal analysis page for the URL `http://0002439000067.000webhostapp.com/late-code/late-code/source/login.htm`. The URL is identified as `text/html`. A red circle with the number 13 indicates that 13 security vendors have flagged this URL as malicious. The status is 410, and the last analysis date was 2 months ago. The page includes tabs for DETECTION, DETAILS, LINKS, and COMMUNITY. A blue banner encourages joining the VT Community. Below, a table shows security vendors' analysis:

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

The screenshot shows the ipqualityscore.com report for the URL `http://0002439000067.000webhostapp.com/late-code/late-code/source/login.htm`. The report includes the following details:


- Safe**: Can this URL be trusted? (Warning - NOT SAFE)
- Suspicious**: Indicates reputation issues and potentially malicious activity. (Suspicious Activity)
- Domain**: 0002439000067.000webhostapp.com (Domain name of the final URL after all redirections.)
- IP Address**: 145.14.144.206 — DE (The corresponding IP address for the URL's web server.)
- Malware**: Hosting Malware (Indicates if this domain has recently hosted malware, viruses, or C2 activity.)
- Phishing**: Phishing Link
- Risk Score**: 100 - High Risk (Overall threat score from 0 (clean) to 100 (high risk).)



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


### 3. urlscan.io

 urlscan.io  Home  Search  Live  API  Blog  Docs  Pricing  Login 

00024390000067.000webhostapp.com


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

 Lookup  Go To  Rescan

 Add Verdict  Report


URL: <http://00024390000067.000webhostapp.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  HTTP 22  Redirects  Links 3  Behaviour  Indicators  Similar  DOM  Content  API  Verdicts

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 **00024390000067.000webhostapp.com**.

[00024390000067.000webhostapp.com](#) scanned **18 times** on urlscan.io 

urlscan.io Verdict: **No classification** 

Live information

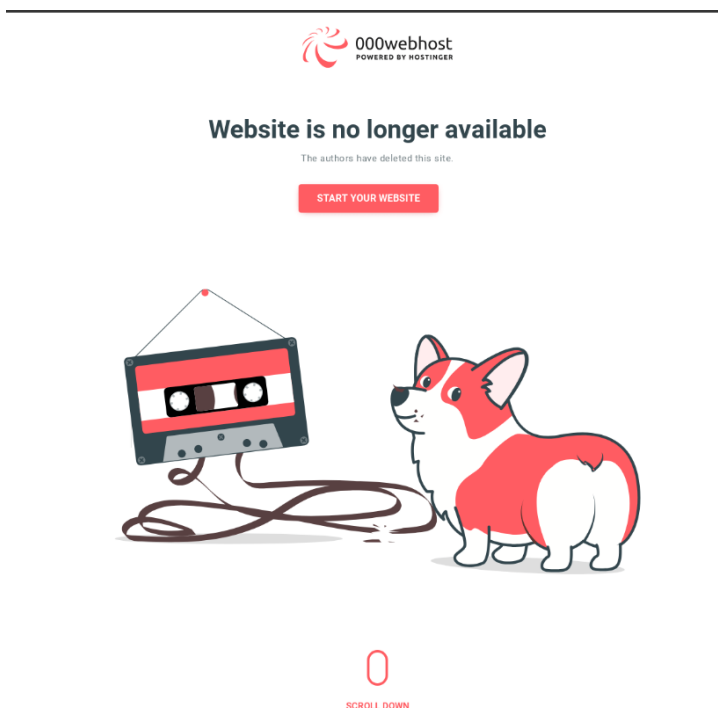
Current DNS A record: **145.14.145.119** (AS204915 - AWEX, CY)  
Domain created: May 11th 2016, 19:04:12 (UTC)  
Domain registrar: Hostinger Operations, UAB

Screenshot  Live screenshot  Full image



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:





## 4. labs.inquest.net

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

Dive into file-based threats with

 [INDICATOR LOOKUP](#) [HOME](#) [DFI](#) [REP-DE](#)

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

Malicious

[Copy Content](#) [Share Link](#)

IP: 145.14.144.230  
ASN: 204915  
CIDR: 145.14.144.0/23  
Country: DE  
Registry: ripenc  
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.