

Task 2-Email Spoofing & Phishing Email Analysis Report

1. Introduction

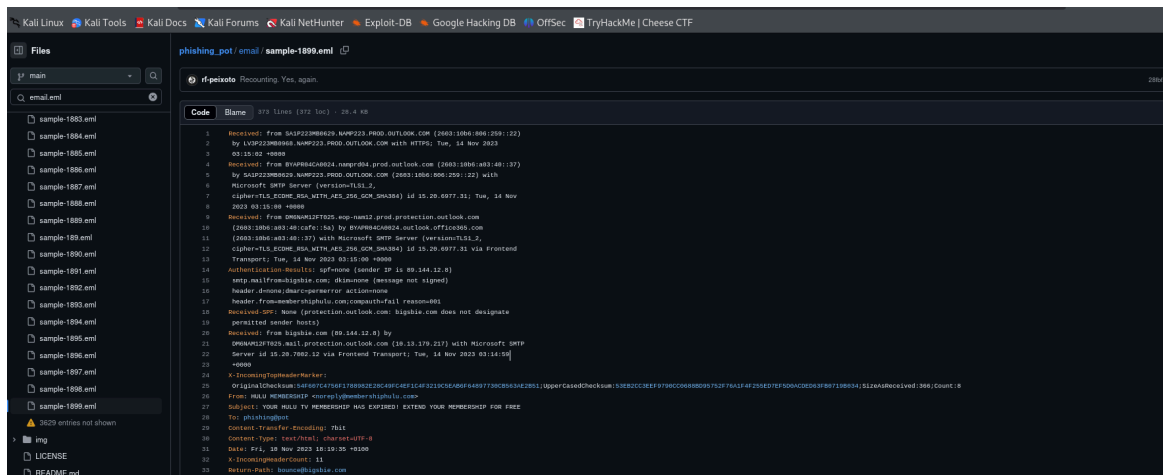
- We might get a phishing email when someone pretends to be a trusted person or company to trick us into giving away passwords, bank details, or clicking on harmful links.
- In email spoofing, the attacker makes the email look like it is coming from someone we know, even though it is not. They fake the sender's address to gain our trust. So, when we see such emails, we should be careful because it is actually a scammer trying to fool us by pretending to be someone we trust.
- Phishing is the trick, and spoofing makes the trick look real.

The objective is to analyze a spoofed email and understand the red flags that will help us identify it and the defensive techniques used to protect against it.

2. Getting a Sample Email

- We can either create a spoof email through a tool called "emkei.cz". This tool is free online fake mailer that lets its user to send spoof mails from any address.
- We can also get spoof mails from publically available sources like :-
 1. [Phish Tank](#)
 2. [GitHub phishing archives](#), etc.

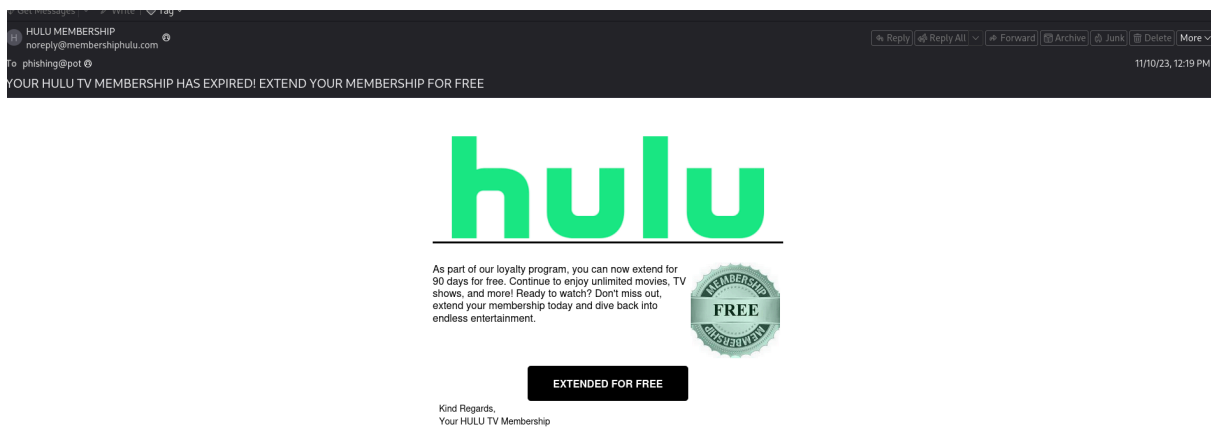
Here, i had picked a Spoof Mail from a publically available git hub repository.



Sample Spoof E-mail

3. Analyzing the Email

- For the header analysis there are several tools used do this task like Mx toolbox, Google Message Header Analyzer, Emailheader.org, etc.
- For this task, I have decided to use MX Player as the preferred tool.



As we can see, this image shows the content of the file, and by looking at it, we can notice some changes and get a rough idea of possible red flags, even without using any tools

Looking at this Hulu email, we can spot several suspicious signs:

1. The sender claims to be "HULU MEMBERSHIP" but uses the email address "noreply@membershipulu.com" instead of an official hulu.com address
2. The subject line uses ALL CAPS and creates fake urgency: "YOUR HULU TV MEMBERSHIP HAS EXPIRED! EXTEND YOUR MEMBERSHIP FOR FREE"
3. The offer seems too good - 90 days completely free just for being a member?
4. There's no personal greeting with your name, which legitimate companies usually include.
5. The "FREE" badge looks cheaply made and unprofessional.
6. The big "EXTENDED FOR FREE" button is trying to make us click without thinking.

4. Summary of the Suspicious Email

Attribute	Details
Sender Name	noreply@membershipulu.com
Sender Email	noreply@membershipulu.com
Date Received	November 10, 2023, 12:19 PM
Recipient	phishing@pot
Subject Line	YOUR HULU TV MEMBERSHIP HAS EXPIRED! EXTEND YOUR MEMBERSHIP FOR FREE
Attachments	None
Main Message Body	The email claims to offer a 90-day free extension as part of a loyalty program. It encourages the user to act quickly and click the link to continue watching shows and movies. It ends with a friendly sign-off and a line about unsubscribing.
Link(s)	https://t.co/8ltGjWbzhy

Site Check

Before we go further, lets check the link with "[Symantec site review](#)", a tool to check a website's reputation and category for security or content classification.

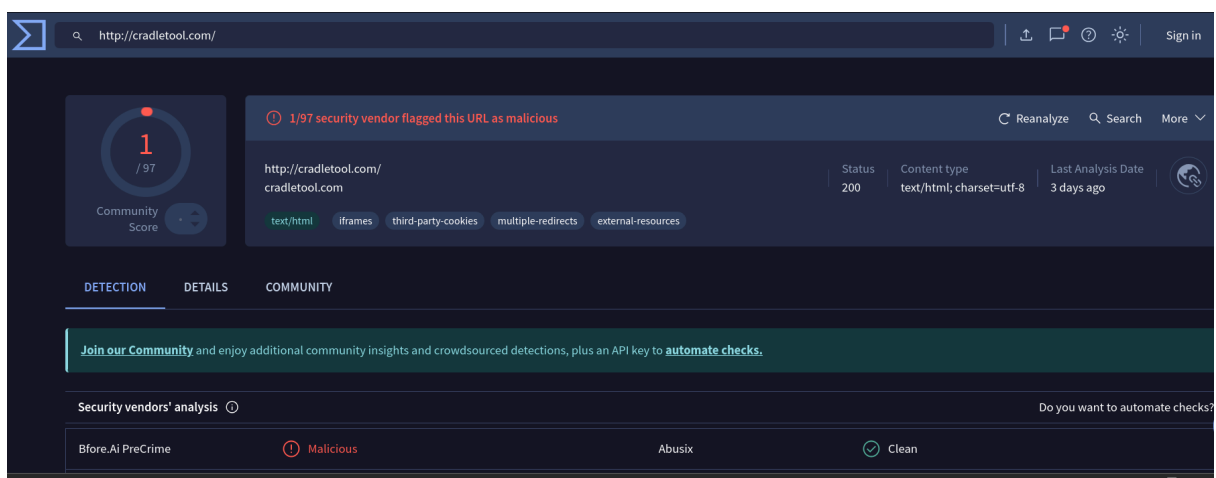
The image displays two screenshots of the Symantec WebPulse Site Review Request form. The top screenshot shows the initial submission of a URL: <http://t.co/8ltGjWbzhy>. The form indicates this is a URL shortening service and shows the redirected URL: <http://cradletool.com/0/0/0/3c8a53cd0573b66bb6f91202a45291d9/>. The bottom screenshot shows the review results for the same URL. A red banner states: "This URL is categorized as a security risk". Below this, the categories are listed as "Suspicious" and "Spam", with a note that the last time it was rated/reviewed was more than 7 days ago. A yellow box provides instructions: "If you feel these categories are CORRECT, click here to learn more about your Internet access policy. If you feel these categories are INCORRECT, please fill out the form below to have the URL reviewed." At the bottom, there is a question: "Do you agree with the current categorization? If not, how would you categorize it?" with two buttons: "Other" and "Risky".

As shown in the image, the URL uses a shortening service that redirects to another webpage, which upon review, is categorized as potentially vulnerable, suspicious, or possibly spam.

Scanning URLs

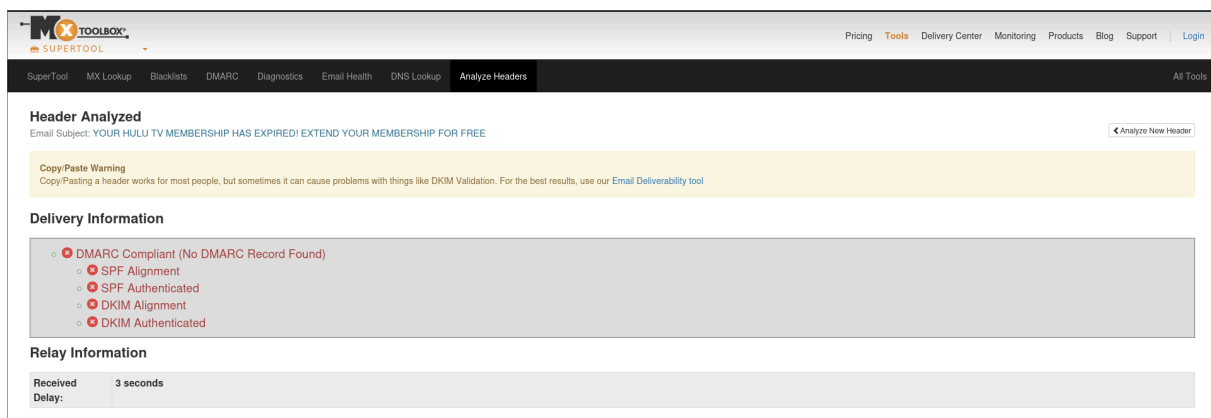
There are several tools available for scanning URLs, such as Virus Total, URLs can, and others. For this analysis, we will proceed using Virus Total.

The scan results show that out of 97 security vendors, only one has flagged the URL as malicious. While this is a potential indicator, it's not enough to confirm anything with certainty. So, let's dig deeper and perform a detailed header analysis and also check for its SPF record.



Header Analysis

Let's move on to the header analysis, which can help us identify some clear red flags under the analysis header tab of MX toolbox.



- DMARC record's are missing
- No SPF alignment
- SPF authentication missing
- DKIM alignment missing
- DKIM authentication missing

Here, we can observe that the email lacks proper authentication measures such as an SPF record. This weakens its credibility. Let's take it a step further and continue our analysis.

Headers Found	
Header Name	Header Value
Authentication-Results	spf=none (sender IP is 89.144.12.8) smtp.mailfrom=bigsbie.com; dkim=none (message not signed) header.d=none; <u>dmARC=permerror action=none</u> header.from=membershiphulu.com; compauth=fail reason=001
Received-SPF	None (protection.outlook.com: bigsbie.com does not designate permitted sender hosts)
X-IncomingTopHeaderMarker	OriginalChecksum:54F607C4756F1788982E28C49FC4EF1C4F3219C5EAB6F64897730CB563AE2B51; UpperCasedChecksum:53EB2CC3EEF9790CC0688BD95752F76A1F4F255ED7EF5D0ACDED63FB07191ved:366;Count:8
From	HULU MEMBERSHIP <noreply@membershiphulu.com>
Subject	YOUR HULU TV MEMBERSHIP HAS EXPIRED! EXTEND YOUR MEMBERSHIP FOR FREE
To	<u>phishing@pot</u>
Content-Transfer-Encoding	7bit
Content-Type	text/html; charset=UTF-8
Date	Fri, 10 Nov 2023 18:19:35 +0100
X-IncomingHeaderCount	11
Return-Path	<u>bounce@bigsbie.com</u>
Message-ID	<aa16a90f-287f-490b-85fc-3313a29864cl@DM6NAM12FT025.eop-nam12.prod.protection.outlook.com>
X-MS-Exchange-Organization	14 Nov 2023 03:15:00.1344 (UTC)

As we scroll down, we can see the detailed email headers, which can help us distinguish between a legitimate message and a suspicious or potentially malicious one.

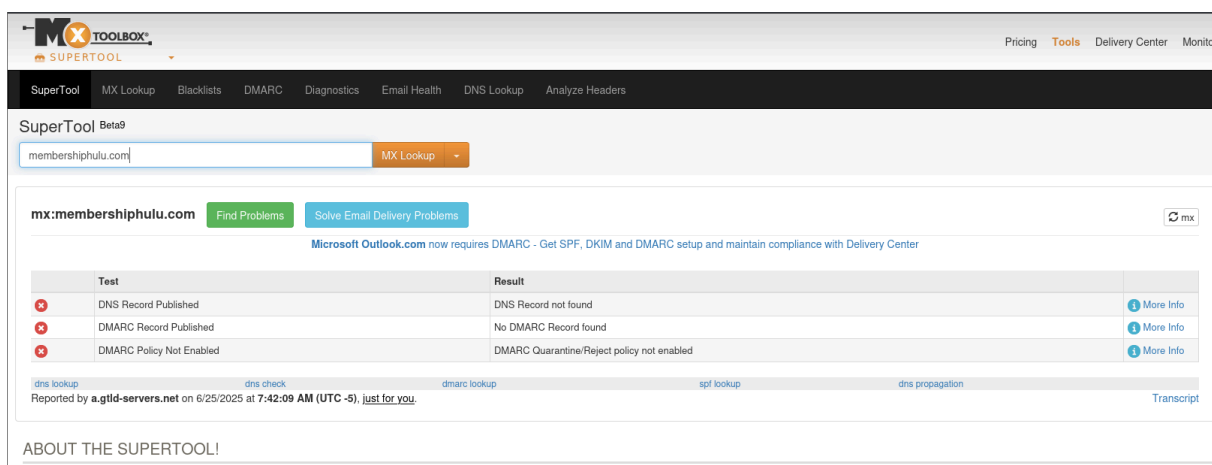
1. First error represents the DMARC perm error, it means that there is a permanent error in the DMARC record of the sender's domain. This usually happens because the DMARC record is written incorrectly or contains invalid values.
2. Second error we noticed is about the sender's email address. When we looked at the email, we saw that it came from a strange and random-looking domain that clearly doesn't belong to Hulu. This makes it quite suspicious because real emails from Hulu should come from their official and familiar domain name.
3. Third error states that the recipient address "phishing@pot" looks odd and possibly fake. This could be used to trick filters or hide the real target, which is a common tactic in email spoofing.

4. The fourth error shows that the return path does not match the sender's domain. This is a red flag, as legitimate companies like Hulu usually have return paths that align with their official domain names.
5. The fifth error shows a DPKIG=none , A DKIM "none" result means that the email did not contain a DKIM signature. In simple terms, the sending domain did not use DKIM to sign the email.

SPF record check

Alright now let us move into a deeper analysis using tools to gain more insights.

- To begin with let us check its SPF record. Sender Policy Framework also known as SPF record helps us verify whether the sender is authentic or not.
- We are using "[MxToolbox.com](https://mxtoolbox.com)" to check if the SPF record exists for the given domain and to confirm whether the sender is authorized to send emails on behalf of that domain.
 - If there are three check marks on Mx Toolbox, it indicates that the domain has a published SPF record. Otherwise, it does not have one.
 - It is also important to verify if the domain is used for email. If yes, there will be a message stating "your email service provider is google apps". If this message is absent, the domain might not be used for email purposes.



The screenshot shows the MxToolbox.com interface. At the top, there's a navigation bar with links like Pricing, Tools, Delivery Center, and Monitor. Below that, a search bar contains 'mx.membershipphulu.com' and a button labeled 'MX Lookup'. The main content area displays the results of the lookup for 'mx.membershipphulu.com'. It includes a table with three tests, all of which failed, indicated by red 'x' icons in the first column.

Test	Result	More Info
DNS Record Published	DNS Record not found	More Info
DMARC Record Published	No DMARC Record found	More Info
DMARC Policy Not Enabled	DMARC Quarantine/Reject policy not enabled	More Info

Below the table, there are links for 'dns lookup', 'dns check', 'dmARC lookup', 'spf lookup', and 'dns propagation'. A note mentions 'Microsoft Outlook.com now requires DMARC - Get SPF, DKIM and DMARC setup and maintain compliance with Delivery Center'. At the bottom, there's a section titled 'ABOUT THE SUPERTOOL!'.

As we can see, there are no DNS or DMARC records or policies available for this domain name.

5. List of Red Flags Identified

Red Flag Category	Observation
DMARC Record	DMARC permerror found, indicating the sender's domain has a misconfigured or invalid DMARC setup.
Sender Email	Came from an unusual, random-looking domain not associated with Hulu, making it highly suspicious.
Recipient Email	The recipient address "phishing@pot" appears fake, likely used to mislead filters or spoof detection.
Return Path	Return path does not match the sender's domain, which is not typical for legitimate companies.
DKIM Signature	DKIM shows as "none," meaning the email wasn't signed by the domain, weakening its authenticity.