

Email Header Analysis Report: Suspicious Bitcoin Email Received On 15th of August,2014.

Report by:

ALI CHINASA

Executive Summary

This report looks into a suspicious email that a user (**olaitanoladapo37@gmail.com**) received, which might be a phishing attempt or cyber threat attempt. The email came from an unfamiliar address and had no subject or meaningful content, which are typical signs of phishing or malicious attack.

Overview

The originated email was sent to the user's email account, olaitanoladapo37@gmail.com, from the address resqurobactndes@hotmail.com. Red flags include the sender's domain (hotmail.com) and the absence of a subject line or other important information. The email may have been sent from a reputable mail server because the full email headers show that the message passed DMARC, DKIM, and SPF checks. However, the email still appears suspicious after investigation was carried out using various tools like mailbox validator, Abuseipdb, Mx toolbox , epiesos.com ,virus tool and others due to its content, origin.

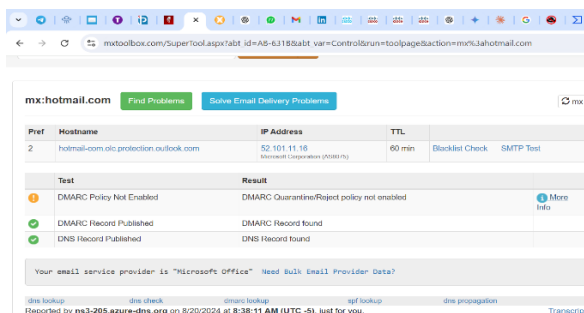
Snapshot of Analysis Tools

This would include a screenshot illustrating the analysis that was done to look for any dangerous payloads utilizing programs like sandbox environments, email header analyzers, and anti-phishing tools. If a sandbox environment was utilized, a screenshot of the email's contents being executed would be displayed.

The artifacts that was analyzed for the purpose of this investigation are listed below:

- Email Address (both returned path and received)
- IP address
- Links attached to the email
- And others

Using the senders email address (resqurobactndes@hotmail.com) ,we discovered that the domain is Hotmail.com and purchasing of the domain is Redmond Washington,USA. And it is reported to be spam and used for malicious purposes.



The screenshot shows the mxtoolbox.com SuperTool interface. At the top, it says 'mx:hotmail.com' with buttons for 'Find Problems' and 'Solve Email Delivery Problems'. Below this is a table with columns: Pref, Hostname, IP Address, TTL, Blacklist Check, and SMTP Test. The table contains one entry for 'hotmail-com.olc.protection.outlook.com' with IP '52.101.11.16' and TTL '60 min'. Below the table, there are sections for 'Test' and 'Result'. The 'Test' section shows 'DMARC Policy Not Enabled' (orange icon), 'DMARC Record Published' (green icon), and 'DNS Record Published' (green icon). The 'Result' section shows 'DMARC Quarantine/Reject policy not enabled', 'DMARC Record found', and 'DNS Record found'. At the bottom, it says 'Your email service provider is "Microsoft Office" Need Bulk Email Provider Data?' and provides links for 'dns lookup', 'mx lookup', 'smtp lookup', and 'dns propagation'.

Pref	Hostname	IP Address	TTL	Blacklist Check	SMTP Test
2	hotmail-com.olc.protection.outlook.com	52.101.11.16 Microsoft Corporation (208817)	60 min		

Test

Test	Result
DMARC Policy Not Enabled	DMARC Quarantine/Reject policy not enabled
DMARC Record Published	DMARC Record found
DNS Record Published	DNS Record found

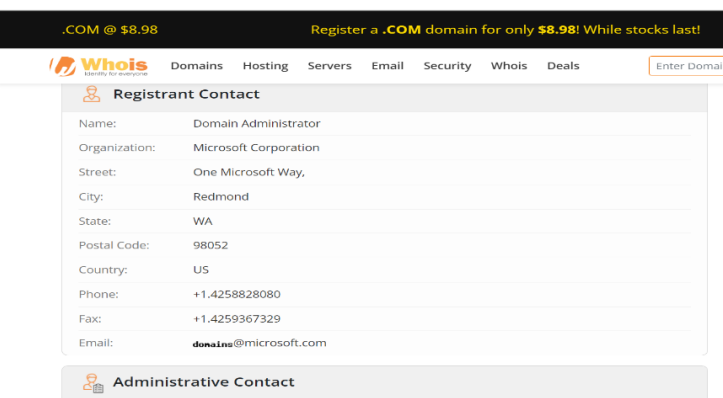
Your email service provider is "Microsoft Office" Need Bulk Email Provider Data?

[dns lookup](#) [mx lookup](#) [smtp lookup](#) [dns propagation](#) [Transcript](#)

Reported by ms3-295.azure-dns on 8/20/2024 at 8:38:11 AM (UTC -5). [Just for you](#)

ABOUT THE SUPERTOOL!

All of your MX record, DNS, blacklist and SMTP diagnostics in one integrated tool. Input a domain name or IP Address or Host Name. Links in the results will guide you either through tools and information. And even have a direct link to the source of the problem.



The screenshot shows the Whois.com website with the 'Registrar Contact' section expanded. It displays contact information for the Domain Administrator, including Name, Organization, Street, City, State, Postal Code, Country, Phone, Fax, and Email. The email address is 'dona1ne@microsoft.com'.

Registrar Contact	
Name:	Domain Administrator
Organization:	Microsoft Corporation
Street:	One Microsoft Way,
City:	Redmond
State:	WA
Postal Code:	98052
Country:	US
Phone:	+1.4258828080
Fax:	+1.4259367329
Email:	dona1ne@microsoft.com

Administrative Contact

The tools used above are mx tool and Whois for the analysis.

Analysis of IP Address

Analysis was carried out using this IP address **2a01:111:f403:2e13::801** and it was flagged 193 times to be malicious and 25% abuse use. The location was of the IP address is found in Austria,Venna. More information can be seen below in the screen shot.IP location was also used to determine the host name and the location.

feedback

2a01:111:f403:2e13::801 was found in our database!

This IP was reported **197** times. Confidence of Abuse is **25%** ?

25%

Important Note: Public IPv6 addresses may implement the SLAAC privacy extension. With this, the interface identifier is randomly generated. The SLAAC privacy extension also implements a time out, which is configurable, so that the IPv6 interface addresses will be discarded and a new interface identifier is generated.

ISP	Microsoft Limited
Usage Type	Data Center/Web Hosting/Transit
Hostname(s)	mail-v1eur05olk20801.outbound.protection.outlook.com
Domain Name	microsoft.com
Country	Austria
City	Vienna, Wien

IP info including ISP, Usage Type, and Location provided by IP2Location

feedback

Raw Whois Results for 2a01:111:f403:2e13::801

```

% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See https://apps.db.ripe.net/docs/HTML-Terms-And-Conditions

ERROR:201: access denied for 2604:a880:400:d0:0:0:40e7:1001
%
% Sorry, access from your host has been permanently
% denied because of a repeated excessive querying.
% For more information, see
% https://apps.db.ripe.net/docs/FAQ/why-did-i-receive-an-error-201-access-denied
% This query was served by the RIPE Database Query Service version 1.113.2 (DEXTER)

```

This page displays the publicly-available WHOIS data for 2a01:111:f403:2e13::801, which belongs to an unknown organization.

Recently Reported IPs:

Intent of the sender

Given the attributes of the email:

- **Lack of a subject:** This is a common tactic used to catch the recipient's curiosity and encourage them to open the email.
- **Suspicious sender email address:** The sender's email address does not match any known contacts, and the username appears randomly generated.
- **Urgency of the email:** The email's design might create a sense of urgency, pushing the recipient to take quick action without careful consideration, which is a common strategy in phishing attempts.

The intent of the sender is malicious. This email was an attempt to perform a phishing attack or deliver malware if the recipient (olaitanoladapo37@gmail.com) interacts with any hidden links or attachments thereby scamming the user.

Conclusion

The suspicious email received by the user on August 15th, 2014, exhibits several classic signs of a phishing attempt or other malicious activity. The absence of a subject, the use of a suspicious and randomly generated email address, and the presence of encoded content all indicate a deliberate attempt to deceive the recipient. Despite passing standard security checks like DMARC, DKIM, and SPF, the email's characteristics and the analysis of the sender's IP address strongly suggest that it is not from a trustworthy source. The intent of the sender appears to be malicious, likely aiming to trick the recipient into interacting with dangerous links or attachments.

Recommendation

Do Not Interact: The recipient should avoid clicking on any links or downloading any attachments from this email.

Report the Email: Forward the email to the IT or security department for further investigation and reporting to relevant authorities.

Block the Sender: Configure email filters to block any future emails from this sender to prevent further attempts.

Increase Awareness: Provide training on recognizing phishing attempts, emphasizing the red flags observed in this case, such as lack of a subject line, suspicious email addresses, and urgency in the message.

Regular Security Audits: Conduct regular security audits and updates to ensure that all anti-phishing tools and email filters are up to date and effective against such threats.