

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

Report by:

ALI CHINASA

Executive summary

This email appears to be a phishing attempt, posing as a trustworthy cloud mining service in an attempt to trick the recipient into clicking on a malicious link. The email asks the recipient to click on a link to view their balance and states that they have amassed a sizeable quantity of Bitcoin through cloud mining. The email appears to be a part of a larger effort to spread malware or obtain sensitive data, based on the examination of both its headers and content.

OVERVIEW

The email claims to be from Support **franklin.polhaupepsy@murni.co.id** and informs the recipient, **olaitanoladapo37@gmail.com**, that they have a balance of 1.3426 BTC, worth approximately \$890,707.77, supposedly earned through cloud mining. The email encourages the recipient to click on a provided link to access their balance. Several red flags are present, including a suspicious reply-to address, the use of random characters in the headers, and a message that plays on the recipient's potential financial greed.

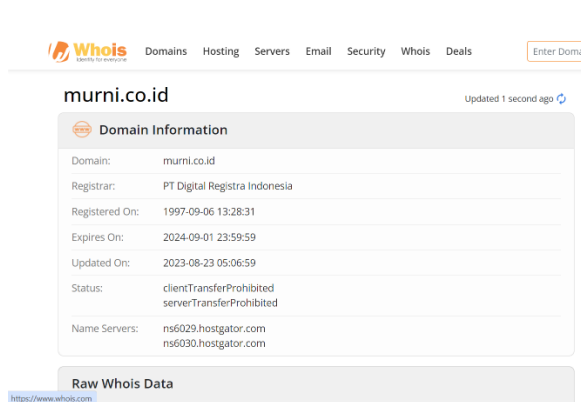
Snapshot of Analysis Tools

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:

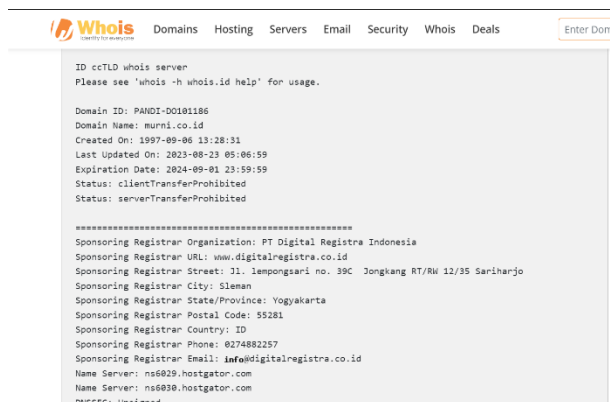
- Email Address (both returned path and received)
- IP address
- Links attached to the email
- And others

Using the senders email address (franklin.polhaupessy@murni.co.id) ,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 Whois website interface. The domain 'murni.co.id' is entered in the search bar. The results show domain information including the registrar (PT Digital Registra Indonesia), creation date (1997-09-06), and expiration date (2024-09-01). The status is 'clientTransferProhibited' and 'serverTransferProhibited'. The name servers are ns6029.hostgator.com and ns6030.hostgator.com.

Domain Information	
Domain:	murni.co.id
Registrar:	PT Digital Registra Indonesia
Registered On:	1997-09-06 13:28:31
Expires On:	2024-09-01 23:59:59
Updated On:	2023-08-23 05:06:59
Status:	clientTransferProhibited serverTransferProhibited
Name Servers:	ns6029.hostgator.com ns6030.hostgator.com



The screenshot shows the raw whois data for the domain 'murni.co.id'. It includes details such as the domain ID (PAWDI-DOI01186), creation date (1997-09-06), last updated date (2023-08-23), expiration date (2024-09-01), and status (clientTransferProhibited, serverTransferProhibited). It also lists the sponsoring registrar organization (PT Digital Registra Indonesia) and their contact information.

```
ID ccTLD whois server
Please see 'whois -h whois.id help' for usage.

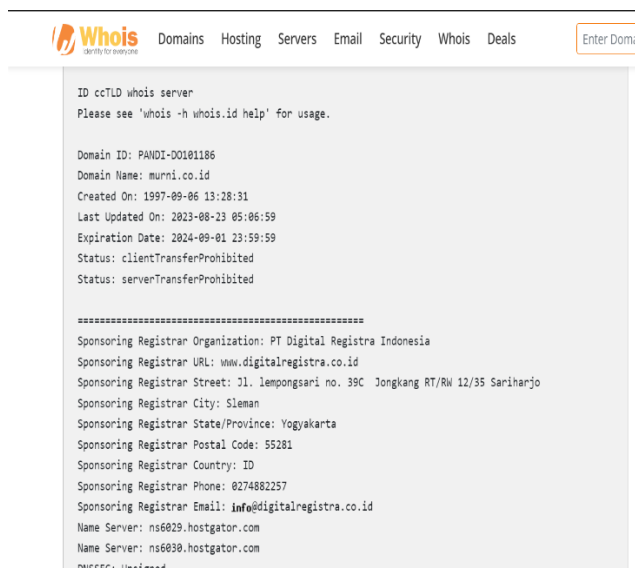
Domain ID: PAWDI-DOI01186
Domain Name: murni.co.id
Created On: 1997-09-06 13:28:31
Last Updated On: 2023-08-23 05:06:59
Expiration Date: 2024-09-01 23:59:59
Status: clientTransferProhibited
Status: serverTransferProhibited

*****
Sponsoring Registrar Organization: PT Digital Registra Indonesia
Sponsoring Registrar URL: www.digitalregistra.co.id
Sponsoring Registrar Street: Jl. Iemponsari no. 39C Jongkang RT/RW 12/35 Sariharjo
Sponsoring Registrar City: Sleman
Sponsoring Registrar State/Province: Yogyakarta
Sponsoring Registrar Postal Code: 55281
Sponsoring Registrar Country: ID
Sponsoring Registrar Phone: 0274882257
Sponsoring Registrar Email: info@digitalregistra.co.id
Name Server: ns6029.hostgator.com
Name Server: ns6030.hostgator.com
DNSSEC: Unsigned
```

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

Analysis of IP Address

Analysis was carried out using this IP address **202.137.25.204** and it was flagged. The location was of the IP address is found in Jarkata,Indonesia.More information can be seen below in the screen shot.IP location was also used to determine the host name and the location.

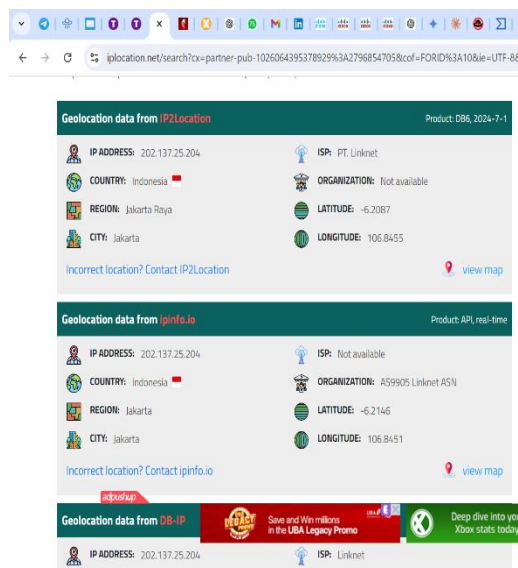


The screenshot shows the raw whois data for the domain 'murni.co.id'. It includes details such as the domain ID (PAWDI-DOI01186), creation date (1997-09-06), last updated date (2023-08-23), expiration date (2024-09-01), and status (clientTransferProhibited, serverTransferProhibited). It also lists the sponsoring registrar organization (PT Digital Registra Indonesia) and their contact information.

```
ID ccTLD whois server
Please see 'whois -h whois.id help' for usage.

Domain ID: PAWDI-DOI01186
Domain Name: murni.co.id
Created On: 1997-09-06 13:28:31
Last Updated On: 2023-08-23 05:06:59
Expiration Date: 2024-09-01 23:59:59
Status: clientTransferProhibited
Status: serverTransferProhibited

*****
Sponsoring Registrar Organization: PT Digital Registra Indonesia
Sponsoring Registrar URL: www.digitalregistra.co.id
Sponsoring Registrar Street: Jl. Iemponsari no. 39C Jongkang RT/RW 12/35 Sariharjo
Sponsoring Registrar City: Sleman
Sponsoring Registrar State/Province: Yogyakarta
Sponsoring Registrar Postal Code: 55281
Sponsoring Registrar Country: ID
Sponsoring Registrar Phone: 0274882257
Sponsoring Registrar Email: info@digitalregistra.co.id
Name Server: ns6029.hostgator.com
Name Server: ns6030.hostgator.com
DNSSEC: Unsigned
```



The screenshot shows the results of an IP location analysis for the IP address 202.137.25.204. The results are displayed in a table format, showing the IP address, country (Indonesia), region (Jakarta Raya), city (Jakarta), latitude (-6.2087), and longitude (106.8455). The ISP is identified as PT Linknet. The analysis is performed using IP2Location and IPinfo.io services.

Geolocation data from IP2Location	
IP ADDRESS:	202.137.25.204
COUNTRY:	Indonesia
REGION:	Jakarta Raya
CITY:	Jakarta
LATITUDE:	-6.2087
LONGITUDE:	106.8455
ISP:	PT Linknet

Geolocation data from ipinfo.io	
IP ADDRESS:	202.137.25.204
COUNTRY:	Indonesia
REGION:	Jakarta
CITY:	Jakarta
LATITUDE:	-6.2146
LONGITUDE:	106.8451
ISP:	Not available

Intent of the sender

The sender's intent is malicious. The purpose of the email is to trick the recipient into clicking on the provided link. Upon clicking, the recipient may be directed to a website that could steal personal information (such as login credentials) or download malicious software onto the recipient's device. The use of a reputable-looking email address and references to Bitcoin and cloud mining are designed to add legitimacy to the message, increasing the likelihood of success in the phishing attempt.

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.

Email content

The email's body, which includes a call-to-action link, balance details, and a greeting, is formatted like a cloud mining notification. The email offers a link to continue and access the money, claiming that the recipient's devices have been automatically collecting cryptocurrency. The goal of this email is to trick the recipient into clicking on the link, which is a malware distribution site or phishing website. Using a search engine's change url to disguise the link is a frequent way to get around email security checks. The reference to an important amount of money is meant to grab the recipient's attention and force them to take action without thinking things through.

Conclusion

This email is a clear example of a phishing attempt. It uses social engineering techniques, such as financial incentives and a sense of urgency, to manipulate the recipient into engaging with a fraudulent link. SOC analysts and cybersecurity professionals should be aware of such tactics and advise users to avoid clicking on links in unsolicited emails, especially when they contain offers that seem too good to be true. Proper email filtering and user awareness training are essential to defend against such threats.

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.