Email Header Analysis 2

By:

Oladayo Akinyode

Supervisor: Mr. Olaitan

Overview

The email was sent to Olaitan Oladapo on Thu, 15 Aug 2024 with timestamp 06:47:33 -0700 (PDT). The attacker used a personalized email domain. The attacker's technique is phishing and social engineering to request for 1.3426 BTC worth $890707.77 using a shared link to collect the Bitcoin which is linked with the email address of the receiver.

The link is found below:

https://translate.google.com/translate?sl=3Dauto&tl=3Den&hl=3Den&u=3D4a6688=

4dbc.nxcli.io/temp/user/login.php?click=3Dm_news_0057_copy%26googlePIDR=3Do=

laitanoladapo37@gmail.com%26id_list=3DXxuPpTypvrZprzk=20.

The sender's name is Maild Murni with the email address: franklin.polhaupessy@murni.co.id

Method/ Approach

The email analysis started by analyzing the content of the message, The email consist of some phishing indicators:

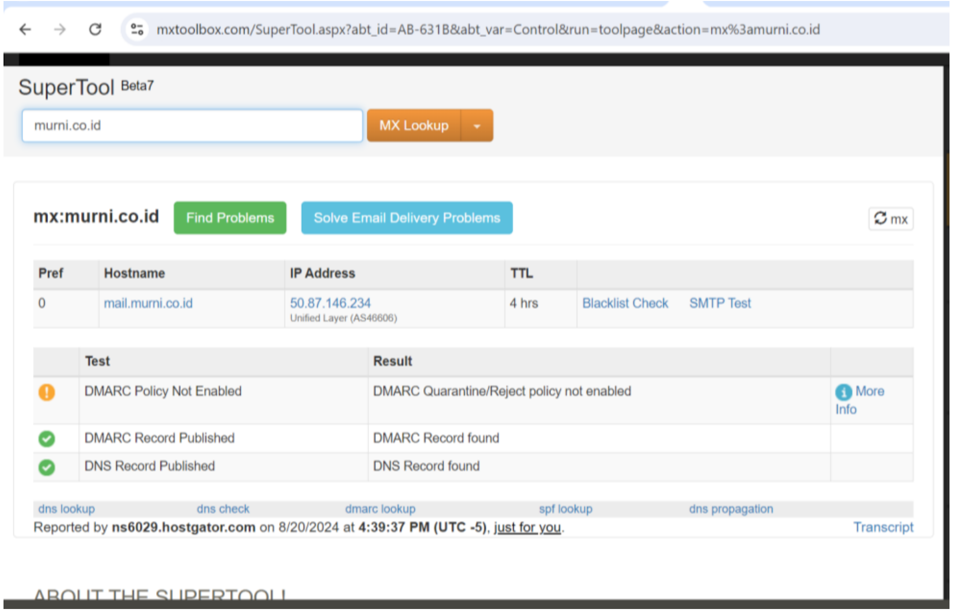
- Social Engineering tactics
- Tone of the message
- Inclusion of phishing link

Analysis

I analyzed the email and the IP address using seven different tools Mx toolbox, Epieos, abuse IPDB, virus total, that's them, browser ling, and Ip location. This is the result generated from the using the email and IP address.

The result from the tools:

Mx toolbox: I looked up the email address and saw that the email has been blacklisted by different users sighting spamming



mxtoolbox.com/SuperTool.aspx?abt_id=AB-631B&abt_var=Control&run=toolpage&action=mx%3amurni.co.id

SuperTool Beta7

murni.co.id

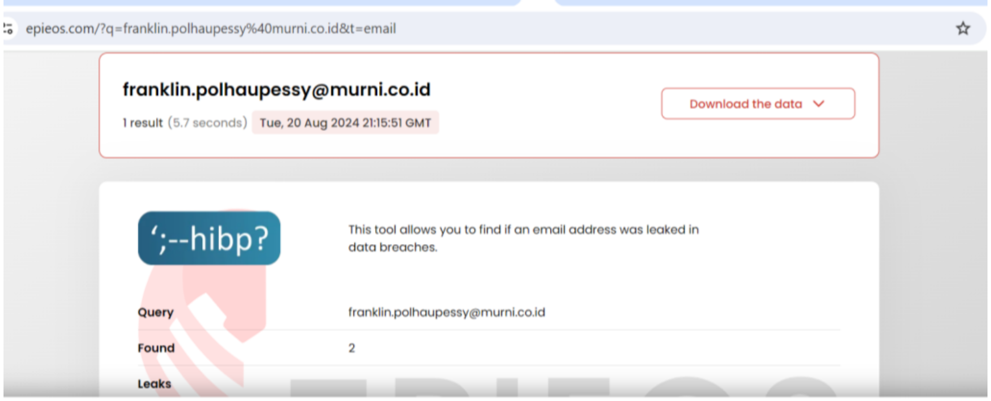
mx:murni.co.id

Pref	Hostname	IP Address	TTL		
0	mail.murni.co.id	50.87.146.234 Unified Layer (AS46606)	4 hrs	Blacklist Check	SMTP Test

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

Reported by **ns6029.hostgator.com** on 8/20/2024 at **4:39:37 PM (UTC -5)**, just for you.

Epieos: The tool has a couple of information regarding the email in their database.



epieos.com/?q=franklin.polhaupessy%40murni.co.id&t=email

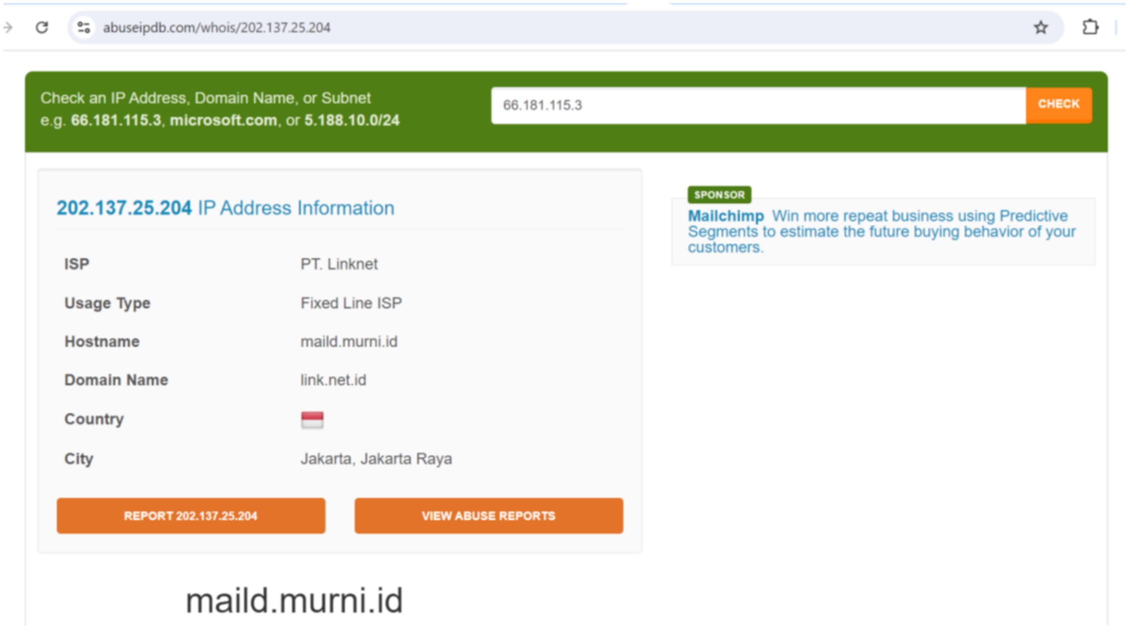
franklin.polhaupessy@murni.co.id

1 result (5.7 seconds) Tue, 20 Aug 2024 21:15:51 GMT

This tool allows you to find if an email address was leaked in data breaches.

Query	franklin.polhaupessy@murni.co.id
Found	2
Leaks	

Abuse Ipdb: This tool has some information about the location of the attacker in their database. I used the IP address. The tool showed us that the attacker is located at Redmond Washington in the U.S.



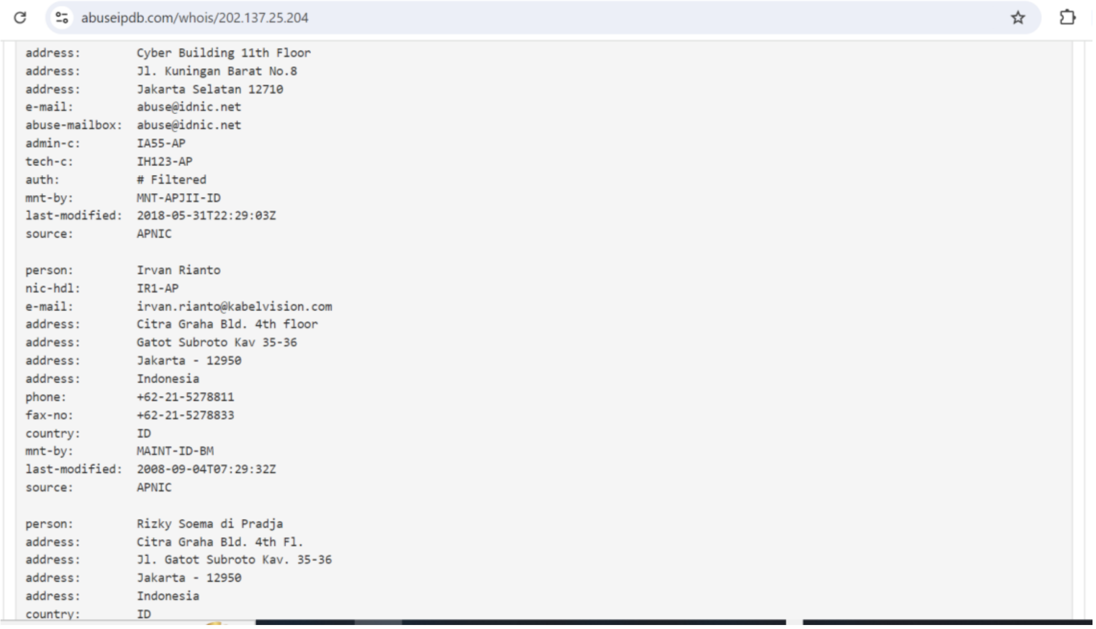
Check an IP Address, Domain Name, or Subnet
e.g. **66.181.115.3**, **microsoft.com**, or **5.188.10.0/24**

202.137.25.204 IP Address Information

ISP	PT. Linknet
Usage Type	Fixed Line ISP
Hostname	maild.murni.id
Domain Name	link.net.id
Country	🇮🇩
City	Jakarta, Jakarta Raya

maild.murni.id

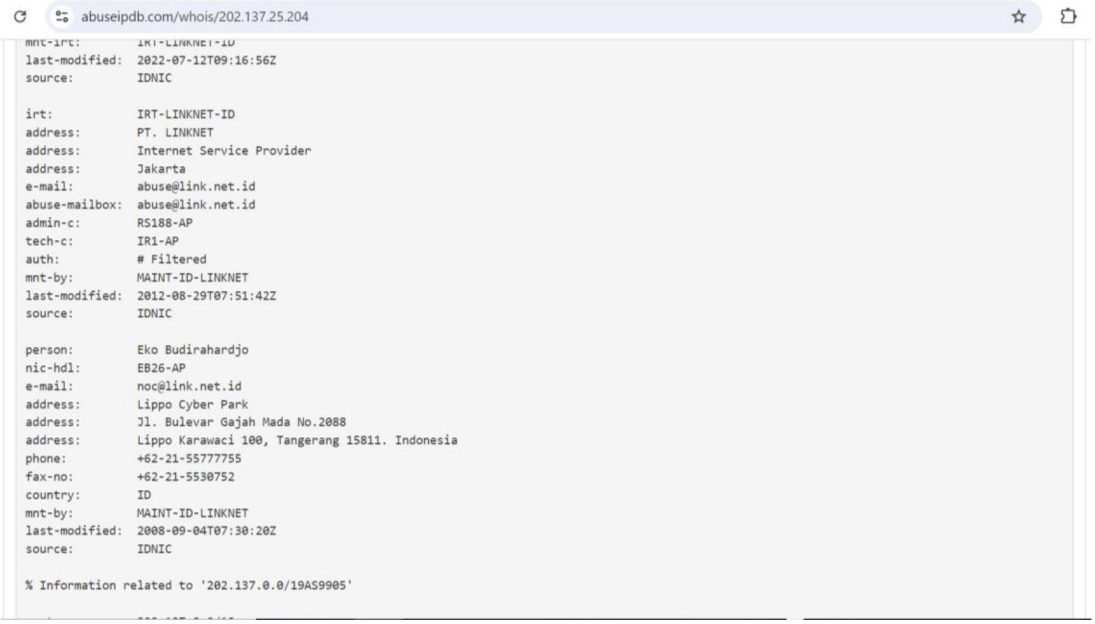
The second image below shows further information about the IP address: **202.137.25.204.** One of the things I observed from this tool is that it gives the name and other information of different users who use the IP address in this location.



```
address:        Cyber Building 11th Floor
address:        Jl. Kuningan Barat No.8
address:        Jakarta Selatan 12710
e-mail:         abuse@idnic.net
abuse-mailbox:  abuse@idnic.net
admin-c:        IA55-AP
tech-c:         IH123-AP
auth:           # Filtered
mnt-by:         MNT-APJII-ID
last-modified:  2018-05-31T22:29:03Z
source:         APNIC

person:         Irvan Rianto
nic-hdl:        IR1-AP
e-mail:         irvan.rianto@kabelvision.com
address:        Citra Graha Bld. 4th floor
address:        Gatot Subroto Kav 35-36
address:        Jakarta - 12950
address:        Indonesia
phone:          +62-21-5278811
fax-no:         +62-21-5278833
country:        ID
mnt-by:         MAINT-ID-BM
last-modified:  2008-09-04T07:29:32Z
source:         APNIC

person:         Rizky Soema di Pradja
address:        Citra Graha Bld. 4th Fl.
address:        Jl. Gatot Subroto Kav. 35-36
address:        Jakarta - 12950
address:        Indonesia
country:        ID
```



abuseipdb.com/whois/202.137.25.204

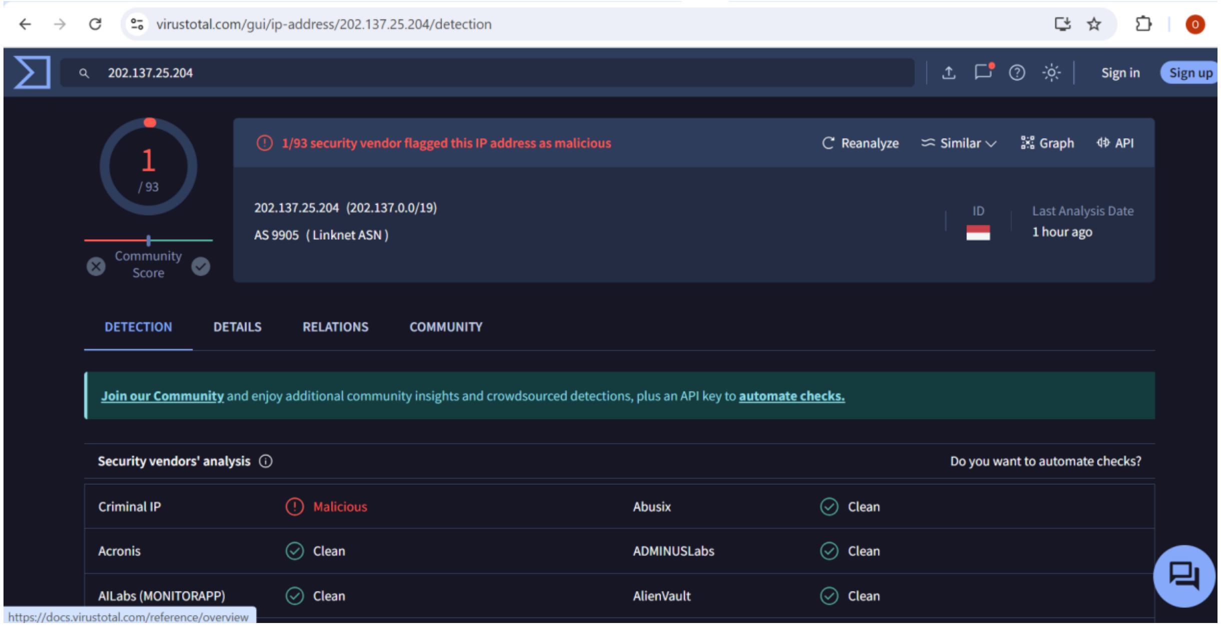
```
mnt-irt:        IRT-LINKNET-ID
last-modified:  2022-07-12T09:16:56Z
source:         IDNIC

irt:            IRT-LINKNET-ID
address:        PT. LINKNET
address:        Internet Service Provider
address:        Jakarta
e-mail:         abuse@link.net.id
abuse-mailbox:  abuse@link.net.id
admin-c:        RS188-AP
tech-c:         IR1-AP
auth:           # Filtered
mnt-by:         MAINT-ID-LINKNET
last-modified:  2012-08-29T07:51:42Z
source:         IDNIC

person:         Eko Budirahardjo
nic-hdl:        EB26-AP
e-mail:         noc@link.net.id
address:        Lippo Cyber Park
address:        Jl. Bulevar Gajah Mada No.2088
address:        Lippo Karawaci 100, Tangerang 15811. Indonesia
phone:          +62-21-55777755
fax-no:         +62-21-5530752
country:        ID
mnt-by:         MAINT-ID-LINKNET
last-modified:  2008-09-04T07:30:20Z
source:         IDNIC

% Information related to '202.137.0.0/19AS9905'
```

Virus Total: This tool flagged the IP address as malicious.



virustotal.com/gui/ip-address/202.137.25.204/detection

202.137.25.204

1 / 93

Community Score

1/93 security vendor flagged this IP address as malicious

202.137.25.204 (202.137.0.0/19)

AS 9905 (Linknet ASN)

ID

Last Analysis Date 1 hour ago

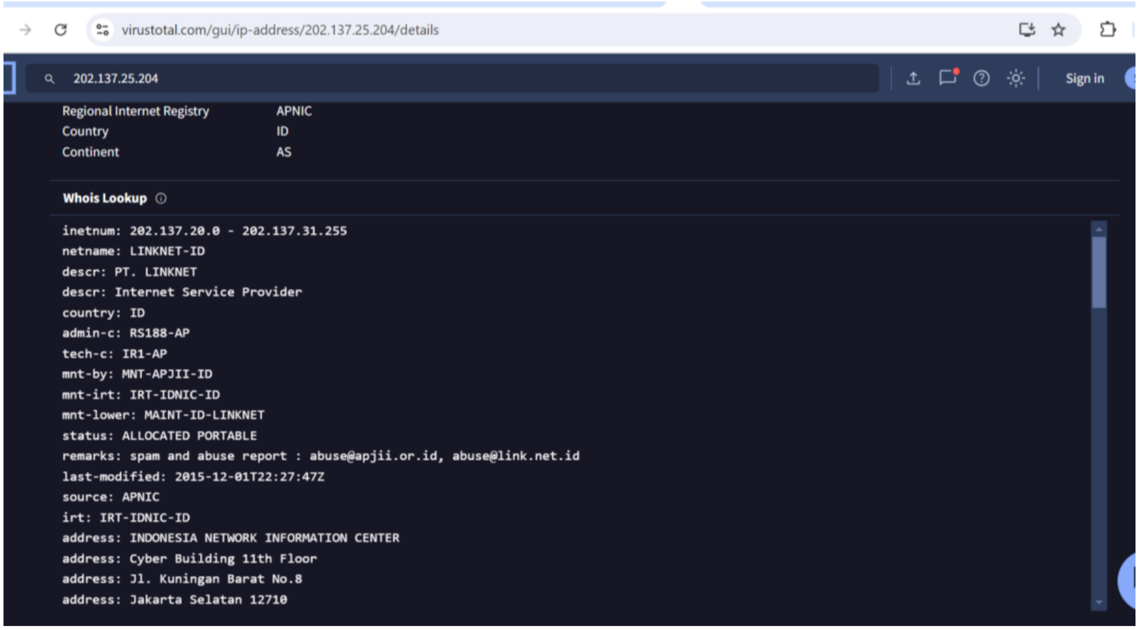
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

Criminal IP	Malicious	Abusix	Clean
Acronis	Clean	ADMINUSLabs	Clean
AILabs (MONITORAPP)	Clean	AlienVault	Clean

https://docs.virustotal.com/reference/overview



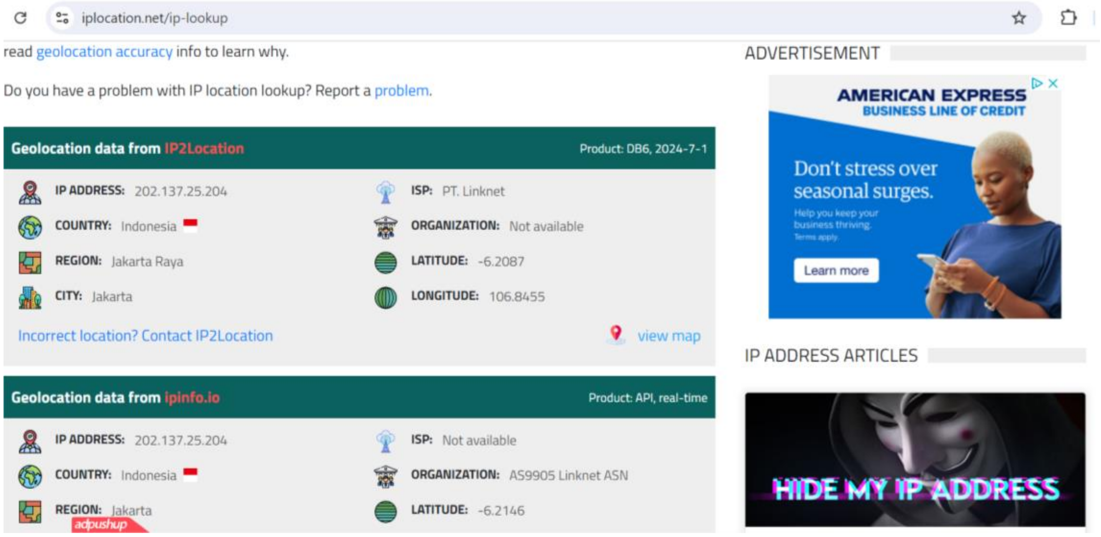
Regional Internet Registry	APNIC
Country	ID
Continent	AS

Whois Lookup

```
inetnum: 202.137.20.0 - 202.137.31.255
netname: LINKNET-ID
descr: PT. LINKNET
descr: Internet Service Provider
country: ID
admin-c: RS188-AP
tech-c: IR1-AP
mnt-by: MNT-APJII-ID
mnt-irt: IRT-IDNIC-ID
mnt-lower: MAINT-ID-LINKNET
status: ALLOCATED PORTABLE
remarks: spam and abuse report : abuse@apjii.or.id, abuse@link.net.id
last-modified: 2015-12-01T22:27:47Z
source: APNIC
irt: IRT-IDNIC-ID
address: INDONESIA NETWORK INFORMATION CENTER
address: Cyber Building 11th Floor
address: Jl. Kuningan Barat No.8
address: Jakarta Selatan 12710
```

Browser ling: This tool could not give us any information

Ip Location: This tool shows the location, longitude, latitude, map and other information of the attacker in Indonesia. The tool gathered information from different Ip websites.



read geolocation accuracy info to learn why.

Do you have a problem with IP location lookup? Report a problem.

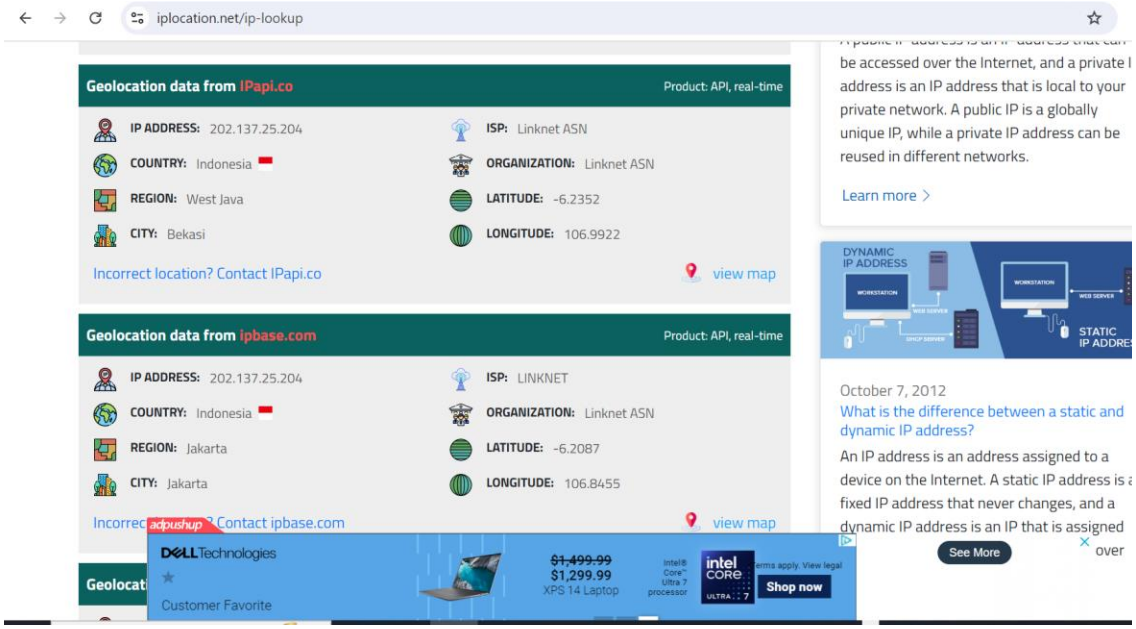
Geolocation data from IP2Location — Product: DB6, 2024-7-1

IP ADDRESS: 202.137.25.204	ISP: PT. Linknet
COUNTRY: Indonesia	ORGANIZATION: Not available
REGION: Jakarta Raya	LATITUDE: -6.2087
CITY: Jakarta	LONGITUDE: 106.8455

Incorrect location? Contact IP2Location — view map

Geolocation data from ipinfo.io — Product: API, real-time

IP ADDRESS: 202.137.25.204	ISP: Not available
COUNTRY: Indonesia	ORGANIZATION: AS9905 Linknet ASN
REGION: Jakarta	LATITUDE: -6.2146



iplocation.net/ip-lookup

Geolocation data from IPapi.co Product: API, real-time

IP ADDRESS:	202.137.25.204	ISP:	Linknet ASN
COUNTRY:	Indonesia	ORGANIZATION:	Linknet ASN
REGION:	West Java	LATITUDE:	-6.2352
CITY:	Bekasi	LONGITUDE:	106.9922

Incorrect location? Contact IPapi.co — view map

Geolocation data from ipbase.com Product: API, real-time

IP ADDRESS:	202.137.25.204	ISP:	LINKNET
COUNTRY:	Indonesia	ORGANIZATION:	Linknet ASN
REGION:	Jakarta	LATITUDE:	-6.2087
CITY:	Jakarta	LONGITUDE:	106.8455

Incorrec... Contact ipbase.com — view map

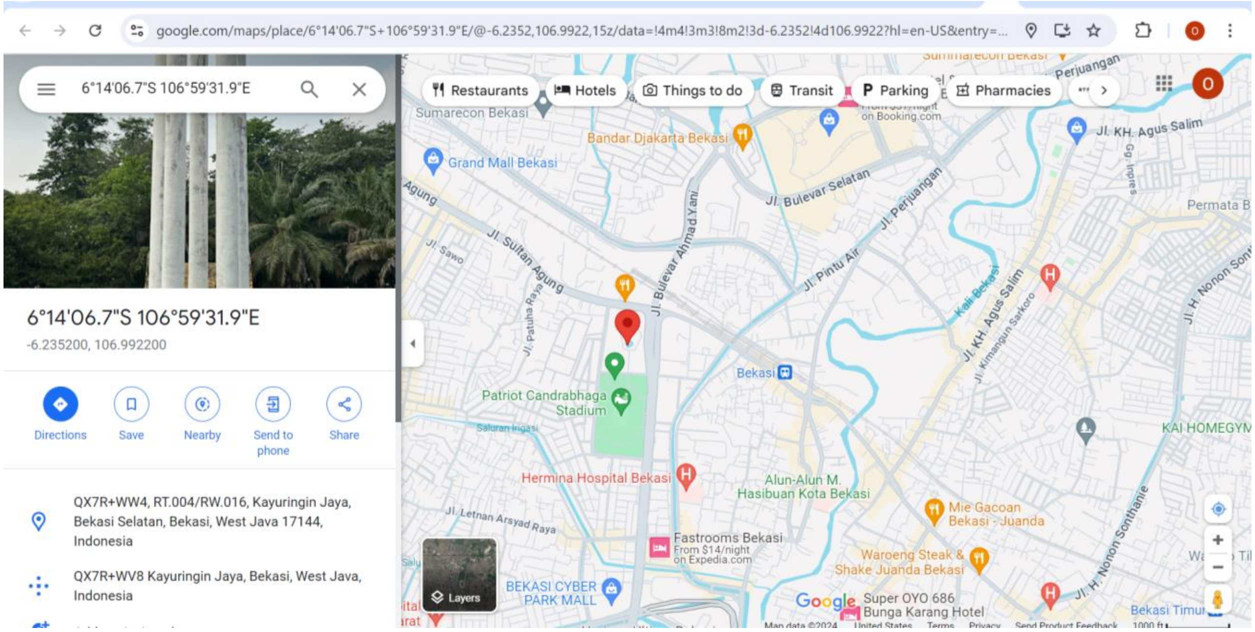
be accessed over the Internet, and a private I address is an IP address that is local to your private network. A public IP is a globally unique IP, while a private IP address can be reused in different networks.

Learn more >

October 7, 2012
What is the difference between a static and dynamic IP address?
An IP address is an address assigned to a device on the Internet. A static IP address is a fixed IP address that never changes, and a dynamic IP address is an IP that is assigned

See More

This tool further provides a map of the attacker's location.



google.com/maps/place/6°14'06.7"S+106°59'31.9"E/@-6.2352,106.9922,15z/data=!4m4!3m3!8m2!3d-6.2352!4d106.9922?hl=en-US&entry=...

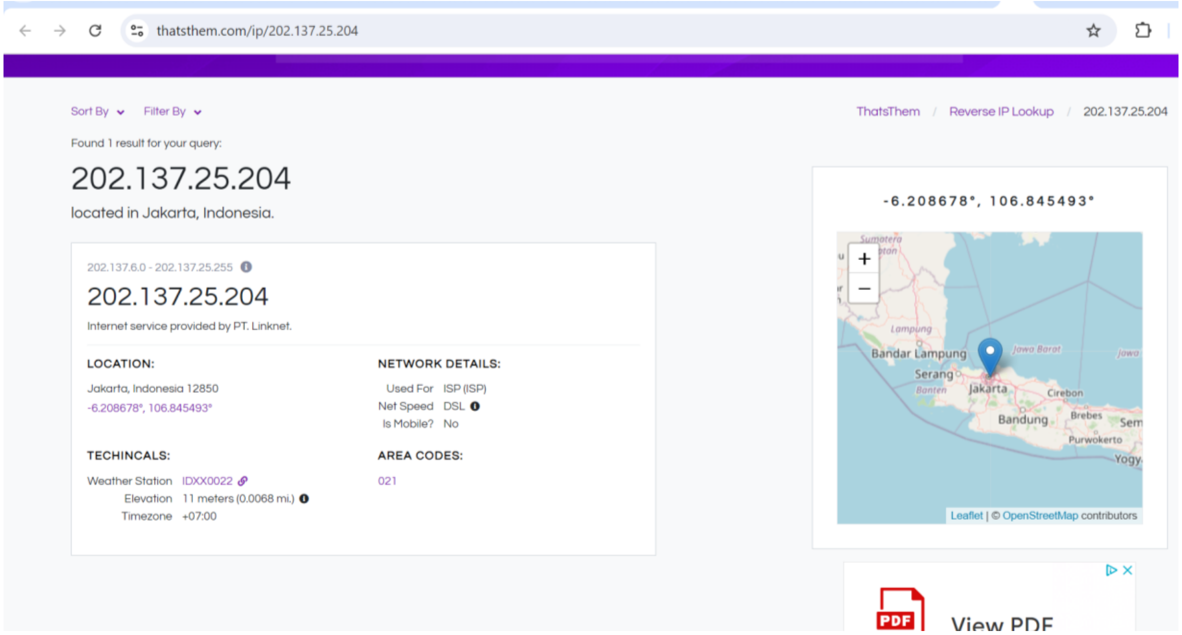
6°14'06.7"S 106°59'31.9"E

-6.235200, 106.992200

QX7R+WW4, RT.004/RW.016, Kayuringin Jaya, Bekasi Selatan, Bekasi, West Java 17144, Indonesia

QX7R+WV8 Kayuringin Jaya, Bekasi, West Java, Indonesia

That’s Them: This tool shows the exact location of the attacker with details and Map of the area where the IP address is located.



thatsthem.com/ip/202.137.25.204

Sort By Filter By

ThatsThem / Reverse IP Lookup / 202.137.25.204

Found 1 result for your query:

202.137.25.204

located in Jakarta, Indonesia.

202.137.6.0 - 202.137.25.255

202.137.25.204

Internet service provided by PT. Linknet.

LOCATION:		NETWORK DETAILS:	
Jakarta, Indonesia 12850		Used For	ISP (ISP)
-6.208678°, 106.845493°		Net Speed	DSL
		Is Mobile?	No

TECHINCALS:		AREA CODES:
Weather Station	IDXX0022	021
Elevation	11 meters (0.0068 mi.)	
Timezone	+07:00	

-6.208678°, 106.845493°

The seven tools we used established that the owner of the email and the IP address has been reported as spam, abuse, malicious, and we were able to pull up the location of the attacker to be Jakarta, Indonesia.

Impression of the sender

The impression of the sender is malicious and the sender's objective is to defraud the owner of 1.3426 BTC the email through the bitcoin address: https://translate.google.com/translate?sl=3Dauto&tl=3Den&hl=3Den&u=3D4a6688=

4dbc.nxcli.io/temp/user/login.php?click=3Dm_news_0057_copy%26googlePIDR=3Do=

laitanoladapo37@gmail.com%26id_list=3DXxuPpTypvrZprzk=20.

Conclusion

The IP address and email address belong to a malicious user in Jakarta, Indonesia. The attacker is using social engineering and phishing tactics to make the user fall for the trap of stealing 1.3426 BTC worth $890707.77 from the user by clicking the phishing link. My analysis using seven different tools shows that the user is malicious and the intention is to defraud the email user. They are group of attackers using the same IP address to perform their malicious operations but the name used is in the email is Maild Murni.

Recommendations

This is my recommendation:

- The receiver should report the email for phishing and social engineering

- The user should not make payment to the address and should always report this kind of email to the SOC team or government agencies.
- If this email is received by a couple of our staff, our team should organize end-user training to sensitize the staff more about this kind of malicious email.