

# COMPARISON REPORT

## GROUP IB VS STYX VIEW SOLUTIONS

GROUP IB VS STYX VIEW SOLUTIONS

GROUP IB VS STYX VIEW SOLUTIONS



GROUP IB  
GROUP CYBERSECURITY



STYX  
STYX VIEW SOLUTIONS



## Table of contents

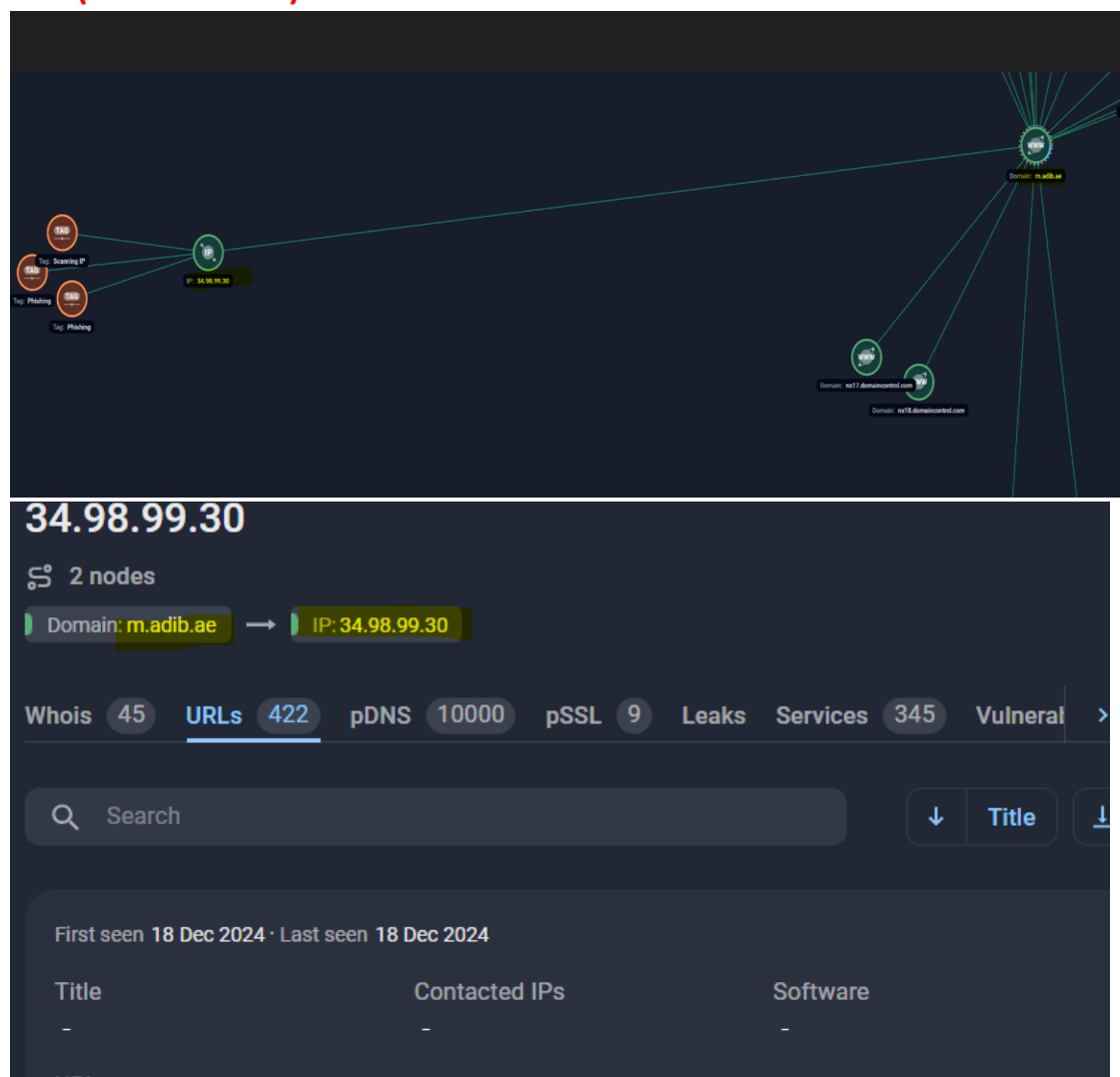
- Summary
- Asset Reputation
- DNS Health
- Network Security
- TLS/SSL Certificate Issues
- Data Leakage Findings
- Brand Risks
- Patching Cadence

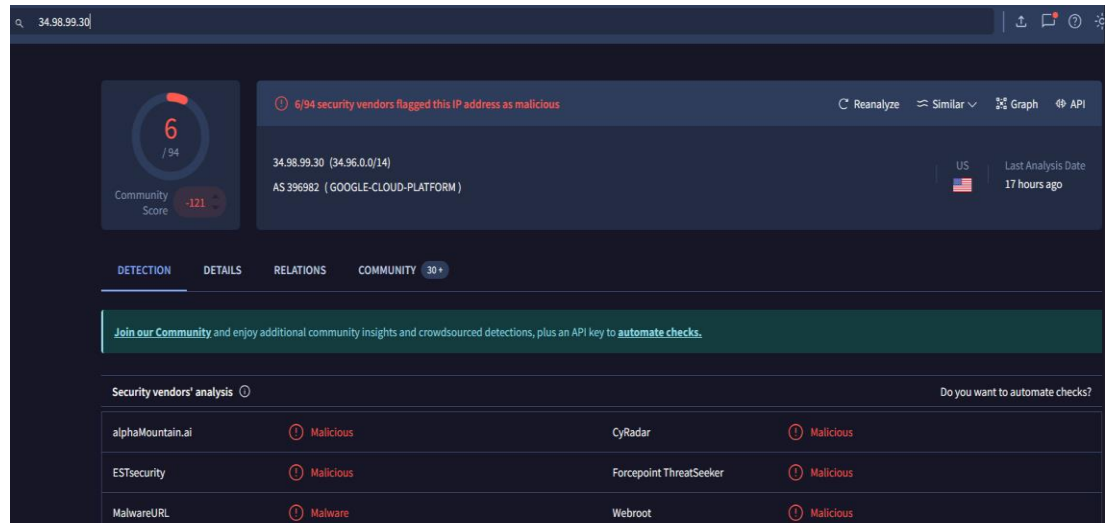
## Summary

Both Group IB and Styx View Solutions are prominent providers of cybersecurity services, catering to businesses and governments to address threats in the digital landscape. While both organizations excel in safeguarding data and systems, they differ in their core competencies, approaches, and market focus, below are comparison between findings on Group IB and styx view

## Asset Reputation

### ➤ m.adib.ae (True Positive)





➤ arodev.adib.ae (False Positive)



➤ promotions.adib.ae (True Positive)



○  
○

632d9707e0cf70d2fe99b1529ad637ab50718664

3 nodes

Domain: promotions.adib.ae → IP: 213.42.26.110 → File: 632...664

Info DNS 821 HTTP 237 TCP 239

First seen 16 Feb 2012 · Last seen 11 Sep 2023

Hash list

md5: f77db63cbcd98391027f2525c14e161f

sha1: 632d9707e0cf70d2fe99b1529ad637ab50718664

sha256: 17deee35f00935d1f2d931dcd0f5b51743ae7505d1f52123f2a3b1f89c8bbc61

sha512: 5ab30f96a0122fdb72dfc744358906840cf7d2afe6d7ad6d058de783cd5d449ff7db35c063466497110031e88d4b189bc71f4b38a86176ee5c98df5d21f27573

File type

PE32 executable for MS Windows (GUI) Intel 80386 32-bit

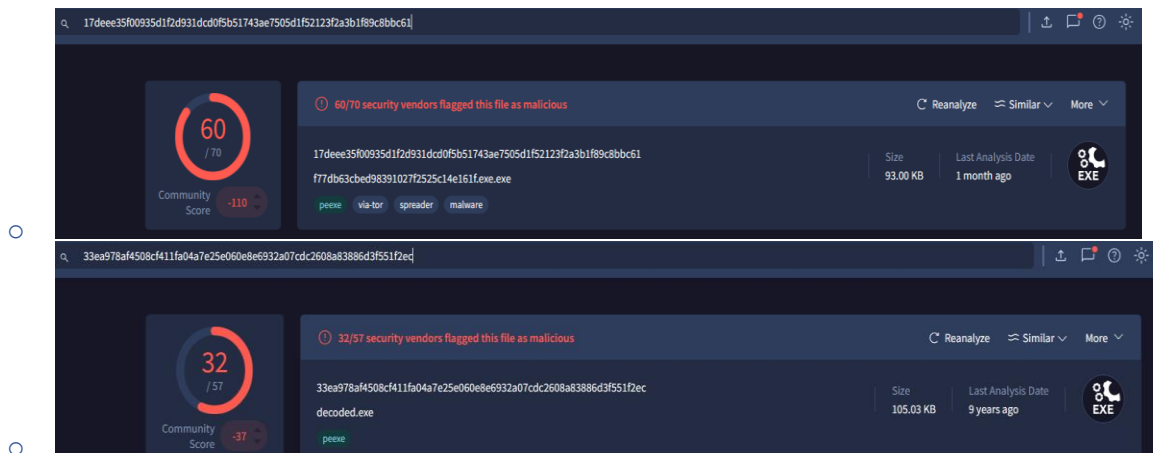
File name

632d9707e0cf70d2fe99b1529ad637ab50718664\_file.ex

Sources

VirusTotal\_SNDBOX VirusTotal\_Jujubox VirusTotal\_Lastline VirusTotal\_Yomi Hunter  
VirusTotal\_Tencent HABO VirusTotal\_Microsoft Sysinternals VirusTotal VirusTotal\_Cuckoofork  
HybridAnalysis VirusTotal\_Dr.Web vxCube VirusTotal\_Rising MOVES Polynom

○



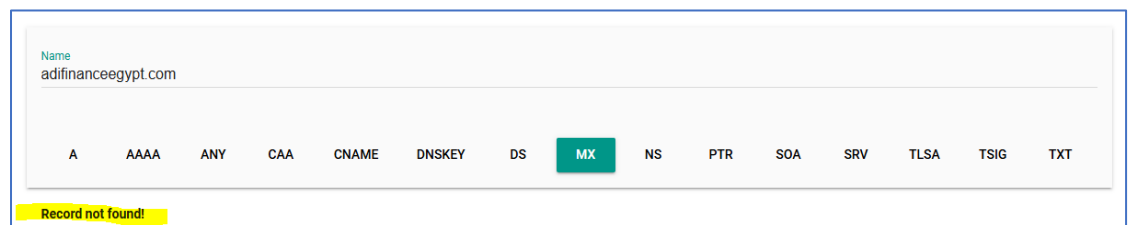
## DNS Health

### Paths:

- ✓ ASM -> Assets -> IP address / Domains
- ✓ ASM -> Management -> Companies

### • No SPF records

- **adifinanceegypt.com (False Positive)**
  - No Mail server for this domain
  - No emails sent or received from them
  -



- 
- Domains below adifinanceegypt.com with No SPF record
  - **adihgroup.com**



Medium severity 46

First seen 09 Jul 2024

Last seen 02 Jan 2025

Total days 176

Detected

Email Security

Reason

Can not get DMARC record!

Company

adifinanceegypt

Website

adifinanceegypt.com

Asset

adihgroup.com

Graph nodes

Domain: adifinanceegypt.com → IP: 52.0.73.32 →

Domain: adihgroup.com

Medium severity 46

First seen 09 Jul 2024

Last seen 02 Jan 2025

Total days 176

Detected

Email Security

Reason

Hostname unable to find a SPF Record!

Value: adihgroup.com

Company

adifinanceegypt

Website

adifinanceegypt.com

Asset

adihgroup.com

Graph nodes

Domain: adifinanceegypt.com → IP: 52.0.73.32 →

Name

adihgroup.com

A

AAAA

ANY

CAA

CNAME

DNSKEY

DS

MX

NS

PTR

SOA

SRV

TLSA

TSIG

TXT

TTL:

1 hour

EXCHANGE:

mailstore1.secureserver.net.

PREFERENCE:

10

MX

TTL:

1 hour

■ qalaa.holdings

Medium severity 46

First seen 09 Jul 2024

Last seen 02 Jan 2025

Total days 176

Detected

Email Security

Reason

Hostname unable to find a SPF Record!

Value: qalaa.holdings

Company

adifinanceegypt

Website

adifinanceegypt.com

Asset

qalaa.holdings

Graph nodes

Domain: adifinanceegypt.com → IP: 52.0.73.32 →

Domain: qalaa.holdings

Name

qalaa.holdings

A

AAAA

ANY

CAA

CNAME

DNSKEY

DS

MX

NS

PTR

SOA

SRV

TLSA

TSIG

TXT

TTL:

59 minutes 59 seconds

EXCHANGE:

smtp.secureserver.net.

PREFERENCE:

0

MX

TTL:

59 minutes 59 seconds

C1 - Internal Information Security

➤ **takka.me (False Positive)**

- No Mail server for this domain
- No emails sent or received from them

Name  
takka.me

A AAAA ANY CAA CNAME DNSKEY DS **MX** NS PTR SOA SRV TLSA TSIG TXT

Record not found!

➤ **burooj.ae (True Positive)**

- Domain with mail server and detected on Group IB with no SPF record

First seen 29 Jul 2024 · Last seen 29 Jul 2024

Severity: **High severity** Asset: **burooj.ae**

Reason: **Hostname unable to find a SPF Record!**

Graph nodes: Domain: **adib.ae** → Email: **dnsadmin@adib.ae** → Domain: **burooj.ae**

First seen 24 Sep 2024 · Last seen 02 Jan 2025

Severity: **Critical severity** Asset: **burooj.ae**

Reason: **DMARC external validation did not pass. Rua/ruf record mailto:rua@dmARC360.com has to stars with `mailto:`**

Graph nodes: Domain: **adib.ae** → Email: **dnsadmin@adib.ae** → Domain: **burooj.ae**



➤ **adibsmartdeals.com (False Positive)**

- No Mail server for this domain
- No emails sent or received from them

Name  
adibsmartdeals.com

A AAAA ANY CAA CNAME DNSKEY DS **MX** NS PTR SOA SRV TLSA TSIG TXT


Record not found!

4 Problems

Category	Host	Result	
✖ http	adibsmartdeals.com	The remote name could not be resolved: 'adibsmartdeals.com' (http://adibsmartdeals.com)	<a href="#">More Info</a>
✖ spf	adibsmartdeals.com	No SPF Record found	<a href="#">More Info</a>
✖ mx	adibsmartdeals.com	DNS Record not found	<a href="#">More Info</a>
⚠ dns	adibsmartdeals.com	SOA Expire Value out of recommended range	<a href="#">More Info</a>

○ **Important note about this domain on Group IB that it is Expired**

First seen 01 Nov 2024 · Last seen 02 Jan 2025

Severity **Critical severity** Asset  **adibsmartdeals.com**

Reason  
**Your domain adibsmartdeals.com expired on 01 Dec 2024!**

Graph nodes  
Domain: **adibsmartdeals.com**

● **DKIM missing**

➤ **adib.eg (False Positive)**

- as shown there is a DKIM for the domain
- but Group IB find that fawryonline.com related to this domain with no DMARC


```
root@leet:~# dig +short s1._domainkey.adib.eg TXT
s1._domainkey.u20087197.wl198.sendgrid.net.
"k=rsa; t=s; p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAXB+hqSzT9tiqZym52+bkbkdTrQTs4FcUFSL65q2UNIQ65tx3+uUQ7hmQR6PET
bRfnBqzwBB70hnvXXN5vi0gtgWHRkgL040zuYXilIITLThdC1WY8qz03zKJpXyoVyum277ZPQHvqNjNdlkfcN5mVzV9tuuAlMl9jBCD7Ed5pwyMPGw7MjMv
y6S6ct+ZK2LkTPDg" "TA/WGMCix/Bkk3WDLkCgZryuxDRWuNXzkmbBBJsT0huhsDGJBQ1Hm3VCLJn9vbW8aKMLFMEU8KiLLJm7Fm9PN+YMFNC88b0fC0Jb
0UmLRL3pqszP9o9WGiskBCWN6g7F0UwC5Iv4ROD1ELVwIDAQAB"
root@leet:~# |
```

First seen 21 Jul 2024 · Last seen 21 Jul 2024

Severity

High severity

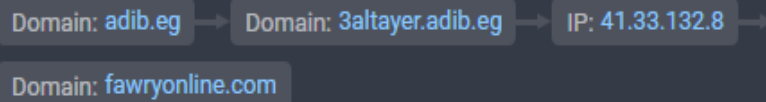
Asset

 fawryonline.com

Reason

Can not get DMARC record!

Graph nodes




First seen 21 Jul 2024 · Last seen 21 Jul 2024

Severity

High severity

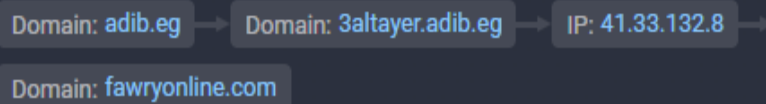
Asset

 fawryonline.com






Reason

Hostname unable to find a SPF Record!

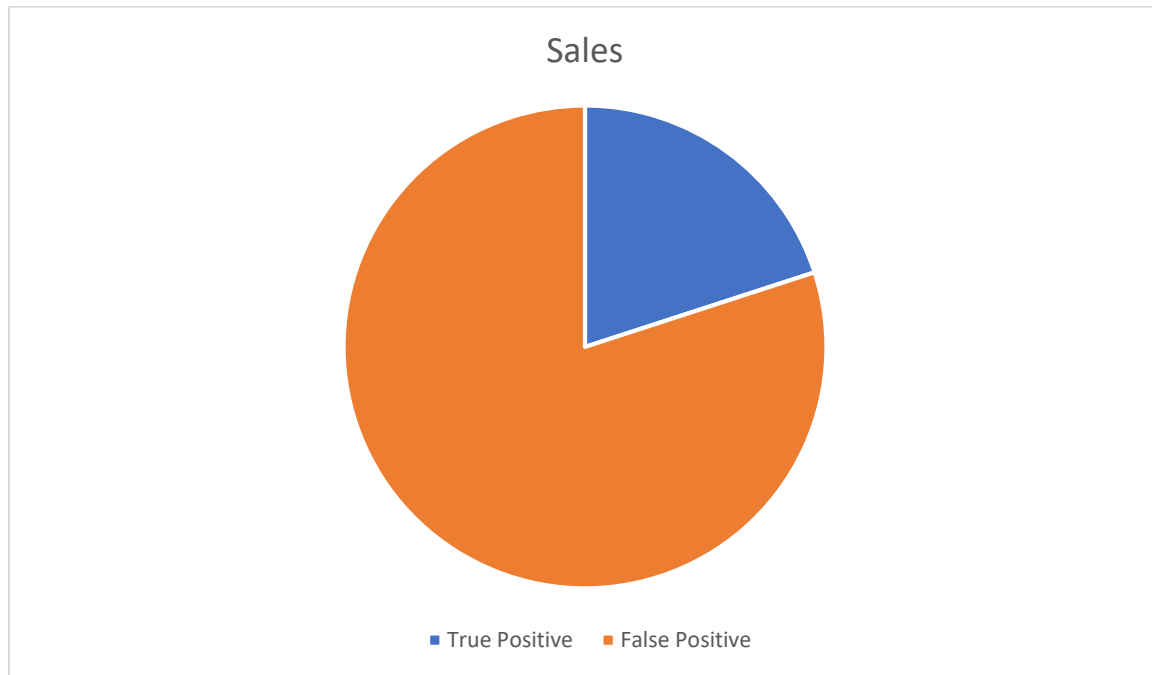
Graph nodes



#### 5 Problems

Category	Host	Result	
 <b>spf</b>	fawryonline.com	No SPF Record found	<a href="#">More Info</a>
 <b>dmarc</b>	fawryonline.com	No DMARC Record found	<a href="#">More Info</a>
 <b>mx</b>	fawryonline.com	No DMARC Record found	<a href="#">More Info</a>
 <b>mx</b>	fawryonline.com	DMARC Quarantine/Reject policy not enabled	<a href="#">More Info</a>
 <b>dns</b>	fawryonline.com	SOA Expire Value out of recommended range	<a href="#">More Info</a>

## DNS Health Statistics



Group IB more accurate than Styx View on DNS Health

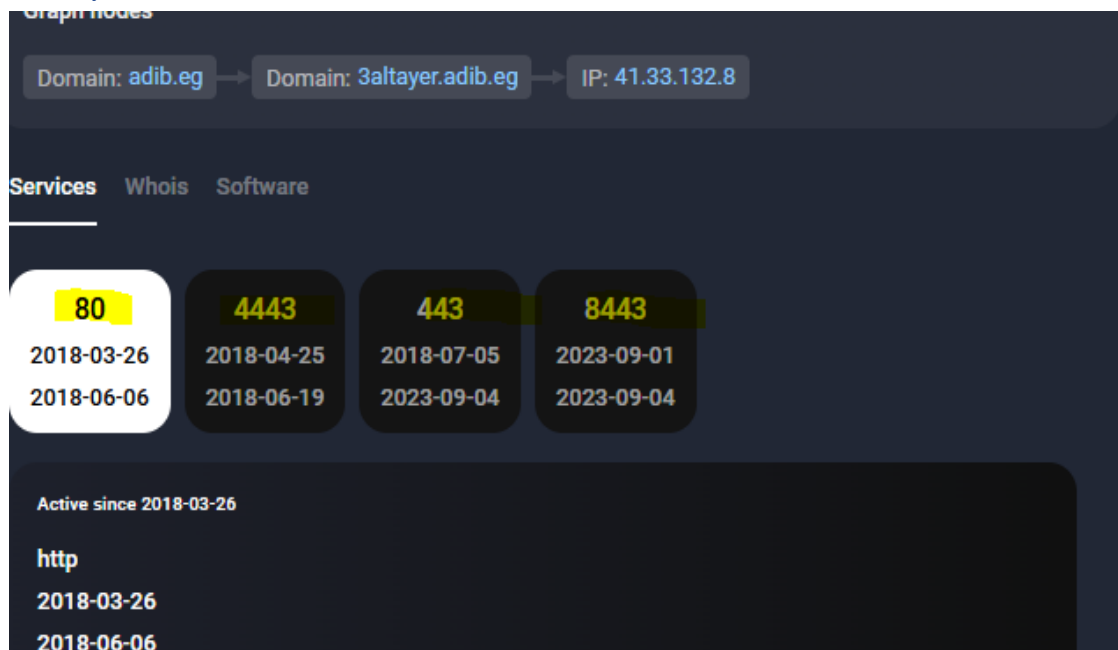
# Network security

## Paths:

✓ ASM -> Assets -> IP address / Domains

### ➤ 3altayer.adib.eg (True Positive)

- Different from the ports found on styx view
- Styx view more accurate



```
(kali㉿kali)-[~]
$ telnet 3altayer.adib.eg 8008
Trying 41.33.132.8...
Connected to 3altayer.adib.eg.
Escape character is '^]'.
Connection closed by foreign host.

(kali㉿kali)-[~]
$ telnet 3altayer.adib.eg 8010
Trying 41.33.132.8...
Connected to 3altayer.adib.eg.
Escape character is '^]'.
Connection closed by foreign host.

(kali㉿kali)-[~]
$ telnet 3altayer.adib.eg 80
Trying 41.33.132.8...
telnet: Unable to connect to remote host: Connection refused

(kali㉿kali)-[~]
$ telnet 3altayer.adib.eg 4443
Trying 41.33.132.8...
telnet: Unable to connect to remote host: Connection refused
```

➤ **adibsharek.adib.ae (True Positive)**

First seen 06 Nov 2024 · Last seen 01 Jan 2025

Severity: **High severity** Asset: **195.229.136.107**

Reason: Found open port 6443 for the remote management. This port is commonly used by Kubernetes.

Graph nodes: Domain: adib.ae → Domain: **adibsharek.adib.ae** → IP: 195.229.136.107

➤ **adib-com-1.fortimailcloud.com (True Positive)**

5443  
2024-11-08  
2024-12-23

9443  
2024-11-06  
2025-01-01

443  
2024-11-06  
2025-01-01

7443  
2024-11-06  
2025-01-01

6443  
2024-11-06  
2025-01-01

8443  
2024-11-06  
2025-01-02

Active since 2024-11-08

ssl

2024-11-08  
2024-12-23

```
{  
  "raw": "ALERT(0x0228)"  
}
```

80  
2019-02-20  
2019-05-27

995  
2024-06-16  
2024-12-28

465  
2024-06-16  
2024-12-30

25  
2023-11-03  
2025-01-02

993  
2024-06-16  
2025-01-02

143  
2023-10-24  
2025-01-02

Active since 2019-02-20

http

2019-05-27  
2019-05-27

```
{  
  "headers": {  
    "Contentlength": "0",  
    "Status": "400 Bad Request",  
    "Content-Type": "text/html; charset=utf-8"  
  },  
  "raw": ""  
}
```

25  
2023-11-03  
2025-01-02

993  
2024-06-16  
2025-01-02

143  
2023-10-24  
2025-01-02

5060  
2023-04-30  
2025-01-01

443  
2023-10-31  
2025-01-02

587  
2024-06-16  
2025-01-02

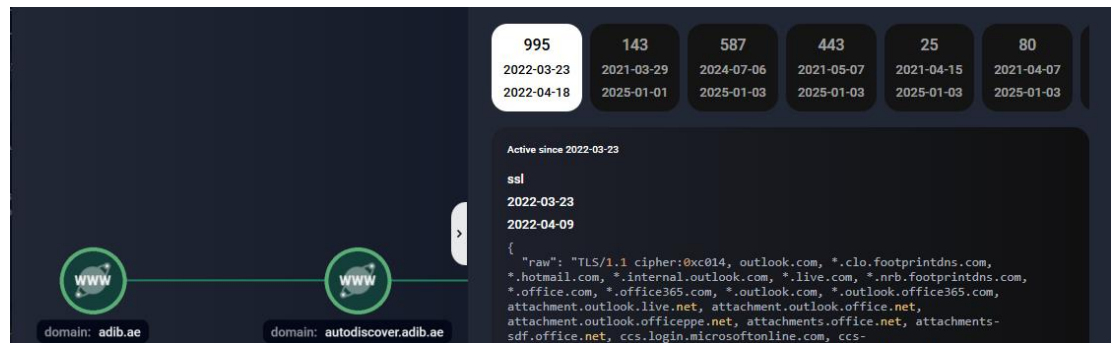
Active since 2023-10-28

pop

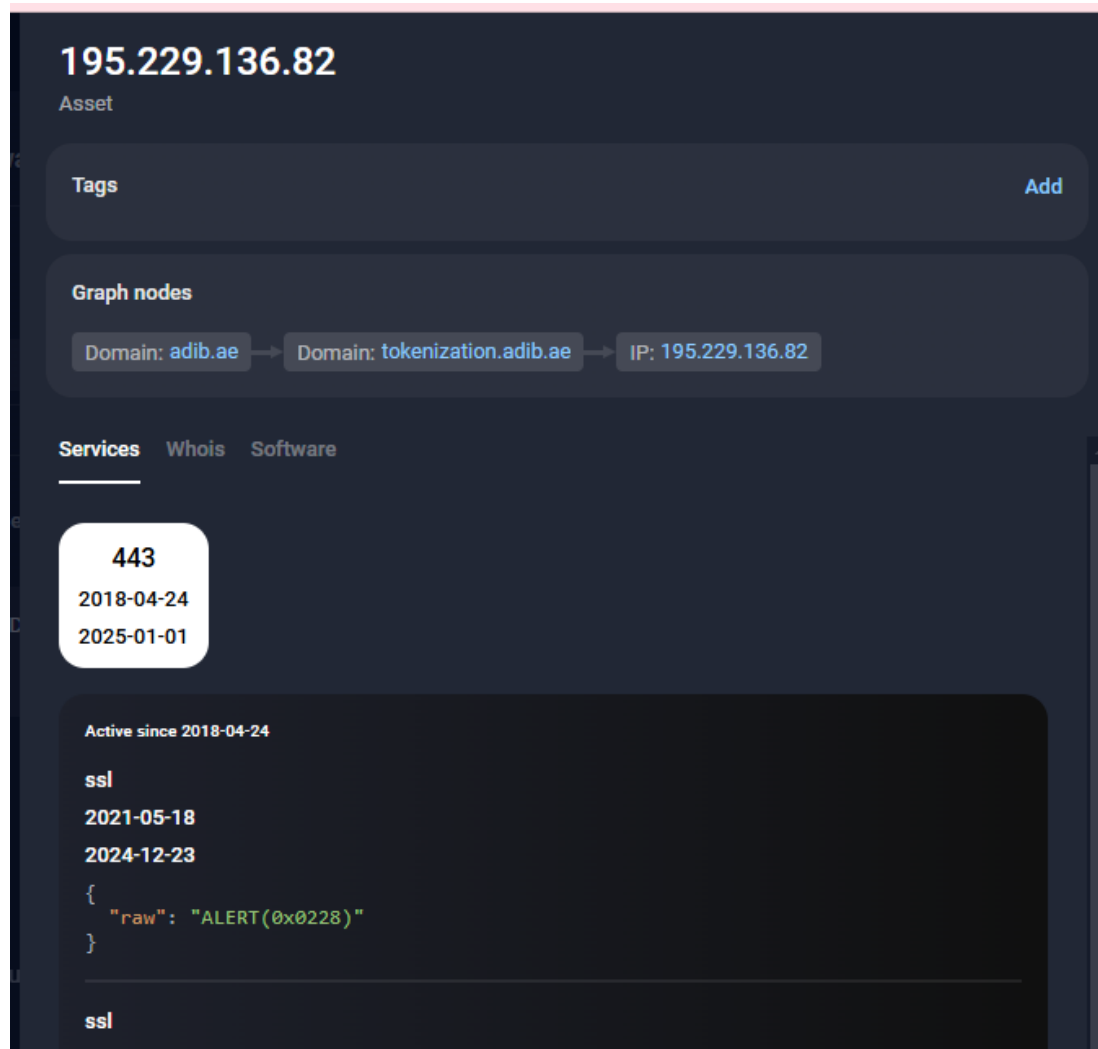
2023-10-28  
2025-01-02

```
{  
  "host": "proxydx39.fortimailcloud.com",  
  "raw": "+OK POP3 ready  
\\x3e251958558.1698510080@proxydx39.fortimailcloud.com\\x3e\\x0a+OK Capability  
list  
follows\\x0aLAST\\x0aTOP\\x0aPIPELINING\\x0aUIDL\\x0aSTLS\\x0a.\\x0a+OK\\x0a"  
}
```

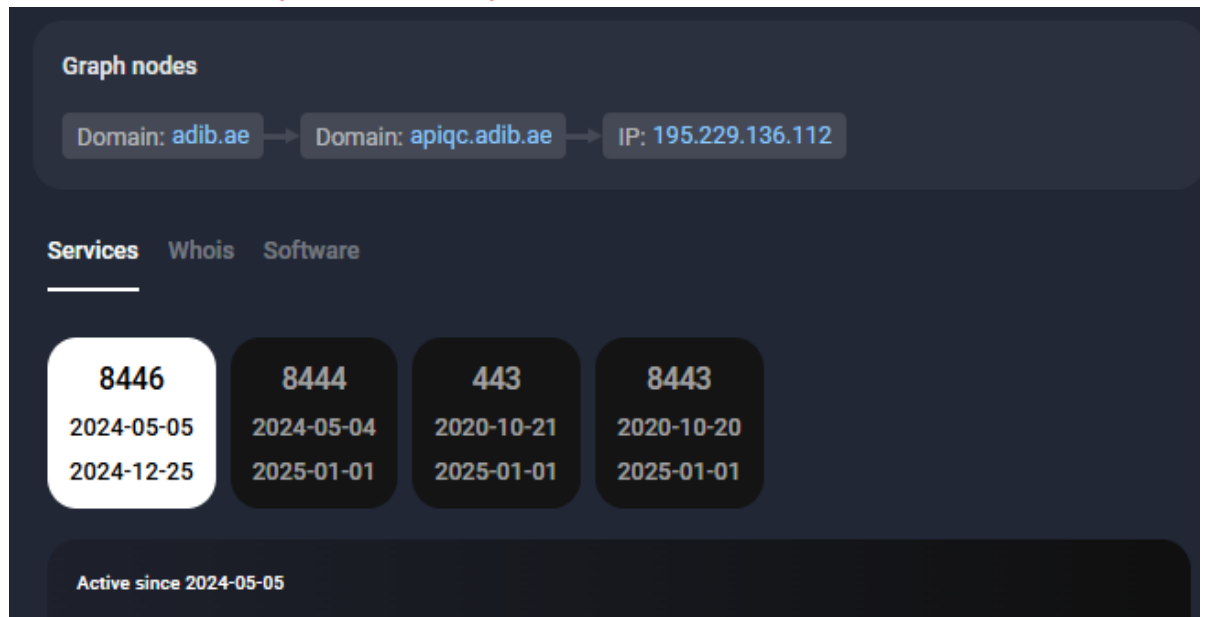
➤ autodiscover.adib.ae (True Positive)



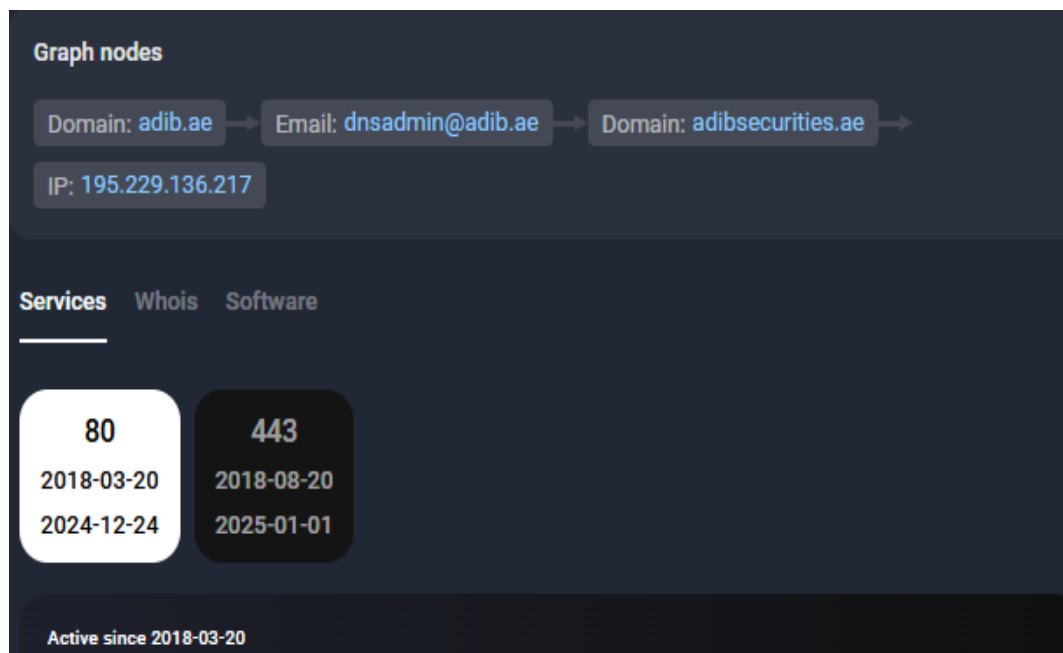
➤ 195.229.136.82 (True Positive)



➤ **195.229.136.112 (True Positive)**



➤ **195.229.136.217 (True Positive)**





➤ **195.229.136.147 (True Positive)**

**Graph nodes**

Domain: [adib.ae](#) → Domain: [zajel1.adib.ae](#) → Domain: [adibdirect.com](#) → IP: 195.229.136.147

**Services** Whois Software

<b>8443</b>	<b>443</b>	<b>1045</b>
2020-10-20	2019-07-15	2024-11-28
2025-01-02	2025-01-01	2025-01-01

Active since 2020-10-20

➤ **195.229.136.128 (True Positive)**

**195.229.136.128**

Asset

Tags [Add](#)

**Graph nodes**

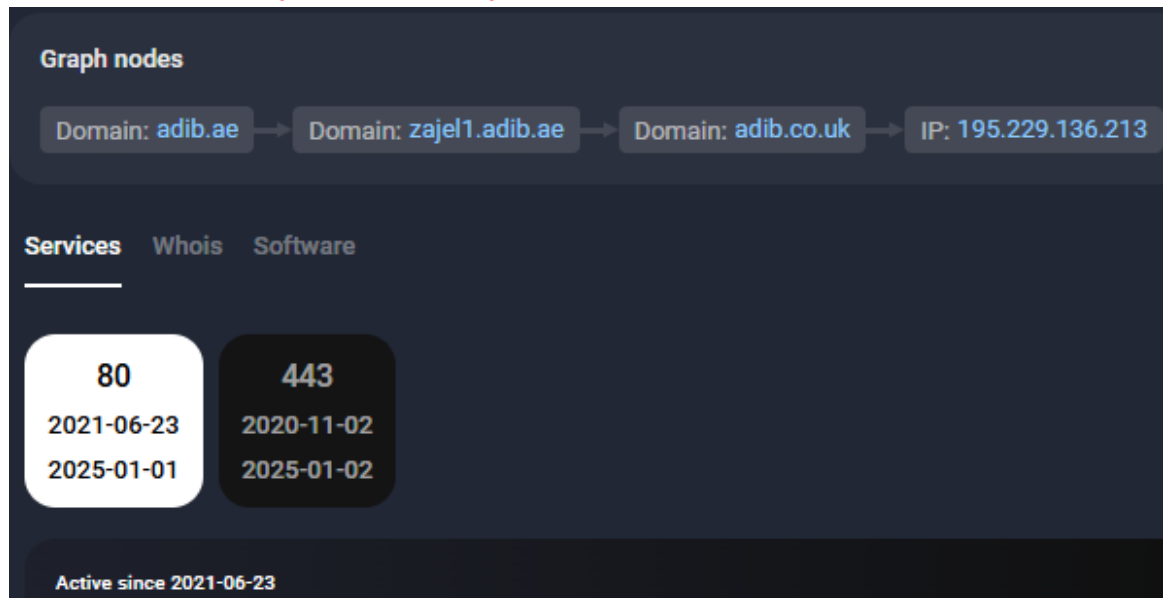
Domain: [adib.ae](#) → SSL: [2db5890638c1f38862c2fc2d9a73efd3472aae6e](#) → IP: 195.229.136.128

**Services** Whois Software

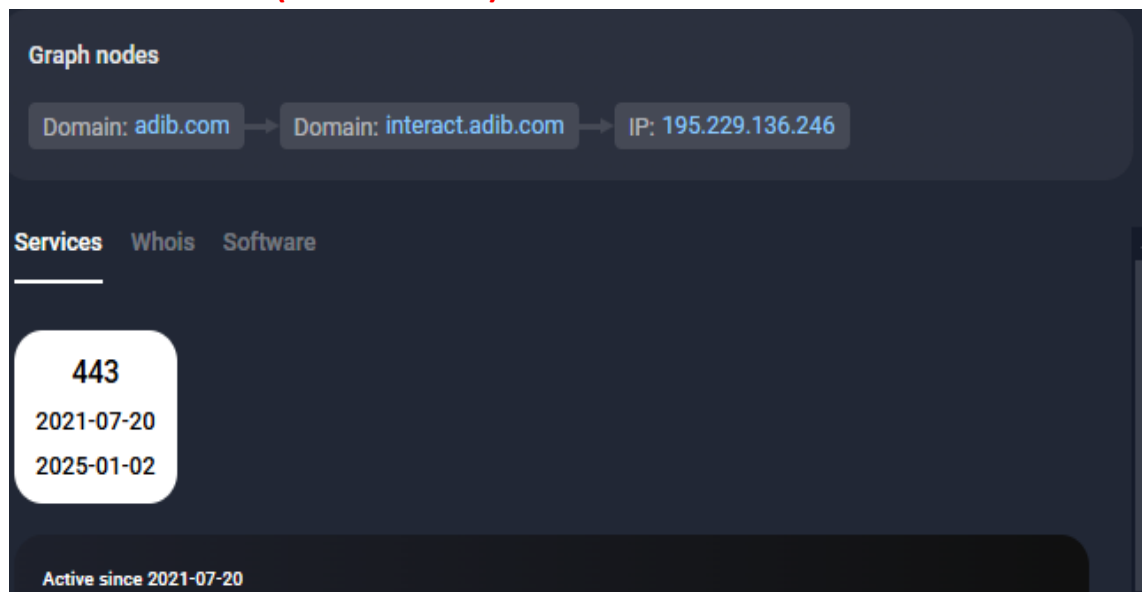
<b>443</b>
2024-05-25
2024-06-02

Active since 2024-05-25

➤ **195.229.136.213 (True Positive)**



➤ **195.229.136.246 (True Positive)**



➤ **195.229.136.176 (True Positive)**

# 195.229.136.176

As of: Jan 04, 2025 3:28pm UTC | Latest

[Summary](#) [History](#) [WHOIS](#) [Explore](#)

## Basic Information

Reverse DNS	mediasrv01.adib.co.ae, <b>adibwealth.ae</b>
Routing	195.229.128.0/18 via EMIRATES-INTERNET Emirates Internet, AE (AS5384)
Services (2)	53/DNS, 443/UNKNOWN

```
(kali㉿kali)-[~]
$ telnet adibwealth.ae 443
Trying 20.203.119.158 ...
Connected to adibwealth.ae.
Escape character is '^]'.
Connection closed by foreign host.
```

➤ **195.229.136.236 (True Positive)**

# 195.229.136.236

As of: Jan 04, 2025 5:23pm UTC | Latest

[Summary](#) [History](#) [WHOIS](#) [Explore](#)

## Basic Information

Reverse DNS	etrade.adibsecurities.ae, etrading.adifs.ae
Forward DNS	etrade.adibsecurities.ae
Routing	195.229.128.0/18 via EMIRATES-INTERNET Emirates Internet, AE (AS5384)
Services (1)	<b>443/HTTP</b>

➤ **195.229.136.71 (True Positive)**

# 195.229.136.71

As of: Jan 05, 2025 4:14am UTC | Latest

[Summary](#) [History](#) [WHOIS](#) [Explore](#)

## Basic Information

**Routing** 195.229.128.0/18 via EMIRATES-INTERNET Emirates Internet, AE (AS5384)

**Services (1)** 443/HTTP

## HTTP 443/TCP

01/05/2025 04:14 UTC

**Details** [VIEW ALL DATA](#) [GO](#)

<https://195.229.136.71/>

**Status** 404 Not Found

```
(kali㉿kali)-[~]
└─$ telnet 195.229.136.71 443
Trying 195.229.136.71...
Connected to 195.229.136.71.
Escape character is '^]'.
Connection closed by foreign host.
```

➤ **195.229.136.72 (True Positive)**

### Graph nodes

Domain: [adib.ae](#) → SSL: [2db5890638c1f38862c2fc2d9a73efd3472aae6e](#) → IP: [195.229.136.72](#)

### Services

443

2024-05-23

2024-06-04

Active since 2024-05-23

➤ **195.229.136.192 (True Positive)**

```
(kali㉿kali)-[~] mple bin olefile-  
$ telnet 195.229.136.192 443 master.zip  
  
Trying 195.229.136.192 ...  
Connected to 195.229.136.192.  
Escape character is '^]'.  
Connection closed by foreign host.
```

➤ **195.229.136.113 (True Positive)**

**Graph nodes**

Domain: adib.com → Domain: jmm.adib.com → IP: 195.229.136.113

**Services** Whois Software

Service	Port	Start Date	End Date
8443	2024-11-06	2025-01-01	
443	2024-05-25	2025-01-01	

Active since 2024-11-06

ssl

➤ **195.229.136.240 (True Positive)**

**Graph nodes**

Domain: adib.com → Domain: jmm.adib.com → IP: 195.229.136.113

**Services** Whois Software

Service	Port	Start Date	End Date
8443	2024-11-06	2025-01-01	
443	2024-05-25	2025-01-01	

Active since 2024-11-06

➤ **195.229.136.160 (True Positive)**

**Graph nodes**

Domain: [adib.ae](#) → Domain: [dtssitibapi.adib.ae](#) → IP: [195.229.136.160](#)

**Services** Whois Software

<b>7444</b>	<b>6444</b>	<b>6443</b>	<b>443</b>	<b>7443</b>	<b>8443</b>
2024-05-04	2024-05-10	2021-05-14	2021-05-20	2021-05-24	2021-06-27
2024-06-01	2024-06-01	2025-01-01	2025-01-01	2025-01-02	2025-01-01

Active since 2024-05-04

**Graph nodes**

Domain: [adib.ae](#) → Domain: [dtssitibapi.adib.ae](#) → IP: [195.229.136.160](#)

**Services** Whois Software

<b>7444</b>	<b>6444</b>	<b>6443</b>	<b>443</b>	<b>7443</b>	<b>8443</b>
2024-05-04	2024-05-10	2021-05-14	2021-05-20	2021-05-24	2021-06-27
2024-06-01	2024-06-01	2025-01-01	2025-01-01	2025-01-02	2025-01-01

Active since 2024-05-04

➤ **195.229.136.238 (True Positive)**

**Graph nodes**

Domain: [adib.ae](#) → SSL: [2db5890638c1f38862c2fc2d9a73efd3472aae6e](#) → IP: [195.229.136.238](#)

**Services** Whois Software

<b>443</b>
2024-05-30
2024-06-04

➤ **195.229.136.140 (True Positive)**

The screenshot shows a network asset profile for IP 195.229.136.140. At the top, under 'Graph nodes', a flow is shown: Domain: adib.ae → Domain: apigateway.adib.ae → IP: 195.229.136.140. Below this, there are tabs for 'Services', 'Whois', and 'Software'. The 'Services' tab is active, displaying a large '443' and two dates: '2020-11-04' and '2025-01-01'.

➤ **195.229.136.143 (True Positive)**

The screenshot shows a network asset profile for IP 195.229.136.143. The IP address is prominently displayed at the top. Below it, the word 'Asset' is visible. There is a 'Tags' section which is currently empty. Under 'Graph nodes', a flow is shown: Domain: adib.ae → Domain: adibdirect-idtb.adib.ae → IP: 195.229.136.143. Below this, there are tabs for 'Services', 'Whois', and 'Software'. The 'Services' tab is active, displaying a large '443' and two dates: '2023-11-07' and '2025-01-01'.



➤ 195.229.136.233 (True Positive)

# 195.229.136.233

Asset

Tags

Graph nodes

Domain: adib.ae → Domain: wfh.adib.ae → IP: 195.229.136.233

Services Whois Software

443

2020-11-04

2025-01-02

➤ 195.229.136.88 (True Positive)

# 195.229.136.88

Asset

Tags

Graph nodes

Domain: adib.ae → Domain: dtsqc.adib.ae → IP: 195.229.136.88

Services Whois Software

8080

2020-10-24

2024-12-18

9443

2024-05-04

2025-01-01

8443

2020-10-22

2025-01-01

7443

2021-05-24

2025-01-01

443

2020-10-21

2025-01-01

8081

2021-06-14

2025-01-02

➤ 195.229.136.212 (True Positive)

# 195.229.136.212

Asset

Tags

Graph nodes

Domain: adib.ae → Email: dnsadmin@adib.ae → Domain: adib.qa → IP: 195.229.136.212

Services Whois Software

80  
2018-03-20  
2025-01-01

443  
2020-11-04  
2025-01-02

➤ 195.229.136.224 (True Positive)

# 195.229.136.224

Asset

Tags

Graph nodes

Domain: adib.ae → SSL: 2db5890638c1f38862c2fc2d9a73efd3472aae6e →  
IP: 195.229.136.224

Services Whois Software

443  
2024-05-29  
2024-06-04

➤ 195.229.136.166 (True Positive)

# 195.229.136.166

Asset

Tags

Graph nodes

Domain: [adib.ae](#) → SSL: [dcc672665aa6b834b343b01829a690b46d218fdb](#) →

IP: [195.229.136.166](#)

Services Whois Software

443

2020-11-02

2024-06-04

➤ 195.229.136.156 (True Positive)

Graph nodes

Domain: [adib.ae](#) → Email: [dnsadmin@adib.ae](#) → Domain: [moneysmart.ae](#) →

IP: [195.229.136.156](#)

Services Whois Software

80

2018-03-20

2025-01-01

443

2020-10-21

2025-01-02

➤ 195.229.136.115 (True Positive)

# 195.229.136.115

Asset

Tags

Add

Graph nodes

Domain: adib.com → Domain: muraselmft.adib.com → IP: 195.229.136.115

Services

Whois

Software

443

2021-05-17

2024-05-04

➤ 195.229.136.215 (True Positive)

Graph nodes

Domain: adib.ae → Email: dnsadmin@adib.ae → Domain: mpmproperties.ae → IP: 195.229.136.215

Services

Whois

Software

80

2018-03-20

2025-01-02

443

2024-05-29

2025-01-02

➤ 195.229.136.158 (True Positive)

# 195.229.136.158

Asset

Tags

Graph nodes

Domain: adib.ae → Domain: murasel.adib.ae → IP: 195.229.136.158

Services Whois Software

443  
2018-08-20  
2025-01-01

➤ 195.229.136.118 (True Positive)

# 195.229.136.118

Asset

Tags

Graph nodes

Domain: adib.ae → SSL: 2db5890638c1f38862c2fc2d9a73efd3472aae6e →  
IP: 195.229.136.118

Services Whois Software

443  
2024-05-25  
2024-06-04

➤ 195.229.136.180 (True Positive)

# 195.229.136.118

Asset

Tags

Graph nodes

Domain: adib.ae → SSL: 2db5890638c1f38862c2fc2d9a73efd3472aae6e →  
IP: 195.229.136.118

Services Whois Software

443  
2024-05-25  
2024-06-04

➤ adibsharek.adib.ae (True Positive)

Issue ID 2766e1935b8af4eda8bbe489be4bbaed

Detected

Issue Info Evidence X

Services Whois Software

5443  
2024-11-08  
2024-12-23

9443  
2024-11-06  
2025-01-01

443  
2024-11-06  
2025-01-01

7443  
2024-11-06  
2025-01-01

6443  
2024-11-06  
2025-01-01

8443  
2024-11-06  
2025-01-02

Active since 2024-11-08

ssl  
2024-11-08  
2024-12-23  
{  
 "raw": "ALERT(0x0228)"  
}

http  
2024-12-23  
2024-12-23  
{  
 "headers": {  
 "LastModified": "Fri, 20 Dec 2024 09:36:13 GMT",  
 "Status": "200 OK",  
 "ContentType": "text/html",  
 "ETag": "67653a8d-1d7",  
 "SetCookie":

domain: adib.ae domain: adibsharek.adib.ae

➤ **simple.adib.ae (True Positive)**

```
(kali㉿kali)-[~]
$ telnet simple.adib.ae 8443

Trying 195.229.136.245 ...
Connected to simple.adib.ae.
Escape character is '^]'.
Connection closed by foreign host.
```

➤ **dtssit.adib.ae (True Positive)**

```
(kali㉿kali)-[~]
$ telnet dtssit.adib.ae 8443

Trying 195.229.136.87 ...
Connected to dtssit.adib.ae.
Escape character is '^]'.
Connection closed by foreign host.
```

➤ **dts.adib.ae (True Positive)**

```
(kali㉿kali)-[~]
$ telnet dts.adib.ae 8443

Trying 195.229.136.87 ...
Connected to dts.adib.ae.
Escape character is '^]'.
Connection closed by foreign host.

(kali㉿kali)-[~]
$ telnet dts.adib.ae 8081

Trying 195.229.136.87 ...
Connected to dts.adib.ae.
Escape character is '^]'.
Connection closed by foreign host.

(kali㉿kali)-[~]
$ telnet dts.adib.ae 8080

Trying 195.229.136.87 ...
Connected to dts.adib.ae.
Escape character is '^]'.
Connection closed by foreign host.
```



➤ **genmob.adib.ae (True Positive)**

```
(kali㉿kali)-[~]  
$ telnet genmob.adib.ae 8443  
Trying 195.229.136.35 ...  
Connected to genmob.adib.ae.  
Escape character is '^]'.  
Connection closed by foreign host.
```

➤ **apigatewaysit.adib.ae (False Positive)**

```
(kali㉿kali)-[~]  
$ telnet apigatewaysit.adib.ae 8443  
telnet: could not resolve apigatewaysit.adib.ae/8443: Name or service not known
```

➤ **195.229.136.219 (True Positive)**

```
(kali㉿kali)-[~]  
$ telnet 195.229.136.219 8443  
Trying 195.229.136.219 ...  
Connected to 195.229.136.219.  
Escape character is '^]'.  
Connection closed by foreign host.
```

➤ **webmail.adib.ae (True Positive)**

```
(kali㉿kali)-[~]  
$ telnet webmail.adib.ae 25  
Trying 20.203.80.193 ...  
telnet: Unable to connect to remote host: Connection refused
```

## Network security Statistics



Styx view better than Group IB on Network security Insecure Ports

# TLS/SSL Certificate Issues

## ➤ 196.204.30.73 (False positive)

### 196.204.30.73

As of: Jan 04, 2025 8:49am UTC | Latest

[Summary](#) [History](#) [WHOIS](#) [Explore](#)

#### Basic Information

**Forward DNS** [egfiddmz01.adib.eg](#)

**Routing** [196.204.0.0/19](#) via [RAYA-AS, EG \(AS24835\)](#)

**Services (1)** [443/HTTP](#)

<b>Criteria</b>	Type: Identity Match: ILIKE Search: 'egfiddmz01.adib.eg'
<b>Certificates</b>	None found

## ➤ support.adib.eg (False positive)

<b>Criteria</b>	Type: Identity Match: ILIKE Search: 'support.adib.eg'
<b>Certificates</b>	None found

## ➤ ftp.adib.eg (False positive)

<b>Criteria</b>	Type: Identity Match: ILIKE Search: 'ftp.adib.eg'
<b>Certificates</b>	None found

➤ **egfiddmz01.adib.eg (False positive)**

Criteria
Type: Identity Match: ILIKE Search: 'egfiddmz01.adib.eg'

Certificates
None found

➤ **3altayer.adib.eg (True Positive)**

Criteria Type: Identity Match: ILIKE Search: '3altayer.adib.eg'							
Certificates	crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities	Issuer Name
	<a href="#">807446931</a>	2018-10-02	2018-10-02	2020-10-01	3altayer.adib.eg	3altayer.adib.eg	C=US, O=DigiCert Inc, CN=DigiCert SHA2 Secure Server CA

➤ **adib.eg (True Positive)**

<a href="#">8819143902</a>	2023-03-06	2023-03-06	2024-04-01	adib.eg	adib.eg www.adib.eg	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert SHA2 Extended Validation Server CA
----------------------------	------------	------------	------------	---------	------------------------	---

➤ **dtssit.adib.ae (True Positive)**

Certificates	crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities	Issuer Name
	<a href="#">8268167551</a>	2022-12-23	2022-12-23	2023-12-22	dtssit.adib.ae	dtssit.adib.ae	C=US, O=DigiCert Inc, CN=DigiCert SHA2 Secure Server CA
	<a href="#">5837368076</a>	2021-12-21	2021-12-21	2022-12-21	dtssit.adib.ae	dtssit.adib.ae	C=US, O=DigiCert Inc, CN=DigiCert TLS RSA SHA256 2020 CA1
	<a href="#">3806528712</a>	2020-12-20	2020-12-20	2022-01-04	dtssit.adib.ae	dtssit.adib.ae	C=US, O=DigiCert Inc, CN=DigiCert TLS RSA SHA256 2020 CA1
	<a href="#">1014014112</a>	2018-12-09	2018-12-09	2020-12-16	dtssit.adib.ae	dtssit.adib.ae	C=US, O=DigiCert Inc, CN=DigiCert SHA2 Secure Server CA

☐ High severity 75 First seen 14 Nov 2024 Last seen 04 Jan 2025 Total days 51 Detected

SSL/TLS Security

Reason

Your SSL certificate expires soon: 2023/12/22!

Common: dtssit.adib.ae Issuer: DigiCert SHA2 Secure Server CA

Valid from: 2022-12-23T00:00:00Z Valid to: 2023-12-22T23:59:59Z

Count of hosts: 10

Company

ADIB

Website

adib.ae

Asset

dtssit.adib.ae

Graph nodes

Domain: adib.ae → Domain: dtssit.adib.ae

☐ High severity 75 First seen 14 Nov 2024 Last seen 04 Jan 2025 Total days 51 Detected

SSL/TLS Security

Reason

Your SSL certificate expires soon: 2023/12/22!

Company

ADIB

Website

Asset

dtssit.adib.ae

Graph nodes

➤ **merchantportal.adib.ae (True Positive)**

Certificates	crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities	Issuer Name
	<a href="#">10891453361</a>	2023-10-25	2023-10-25	2024-10-24	adibacquirer.adib.ae	merchantportal.adib.ae	C=US, O=DigiCert Inc, CN=DigiCert Global G2 TLS RSA SHA256 2020 CA1
	<a href="#">7678294912</a>	2022-10-04	2022-10-04	2023-10-04	adibacquirer.adib.ae	merchantportal.adib.ae	C=US, O=DigiCert Inc, CN=DigiCert SHA2 Secure Server CA

➤ **dtsqc.adib.ae (True Positive)**

☐

High severity 75

First seen 06 Nov 2024

Last seen 04 Jan 2025

Total days 58

Detected

SSL/TLS Security

Reason

Your SSL certificate expires soon: 2023/12/22!

Common: dts.adib.ae

Issuer: DigiCert SHA2 Secure Server CA

Valid from: 2022-12-23T00:00:00Z

Valid to: 2023-12-22T23:59:59Z

Count of hosts: 10

Company

ADIB

Website

adib.com

Asset

dtsqc.adib.ae

Graph nodes

Domain: adib.com

Email: dnsadmin@adib.ae

Domain: adib.ae

Domain: dtsqc.adib.ae

☐

High severity 75

First seen 06 Nov 2024

Last seen 04 Jan 2025

Total days 58

Detected

SSL/TLS Security

Reason

Your SSL certificate expires soon: 2023/12/22!

Common: dts.adib.ae

Issuer: DigiCert SHA2 Secure Server CA

Valid from: 2022-12-23T00:00:00Z

Valid to: 2023-12-22T23:59:59Z

Count of hosts: 10

Company

ADIB

Website

adib.com

Asset

dtsqc.adib.ae

Graph nodes

Domain: adib.com

Email: dnsadmin@adib.ae

Domain: adib.ae

Domain: dtsqc.adib.ae

➤ **dts.adib.ae (True Positive)**

☐

High severity 75

First seen 06 Nov 2024

Last seen 04 Jan 2025

Total days 58

Detected

SSL/TLS Security

Reason

Your SSL certificate expires soon: 2023/12/22!

Common: dts.adib.ae

Issuer: DigiCert SHA2 Secure Server CA

Valid from: 2022-12-23T00:00:00Z

Valid to: 2023-12-22T23:59:59Z

Count of hosts: 10

Company

ADIB

Website

adib.com

Asset

dts.adib.ae

Graph nodes

Domain: adib.com

Email: dnsadmin@adib.ae

Domain: adib.ae

Domain: dts.adib.ae

☐

High severity 75

First seen 06 Nov 2024

Last seen 04 Jan 2025

Total days 58

Detected

SSL/TLS Security

Reason

Your SSL certificate expires soon: 2023/12/22!

Common: dts.adib.ae

Issuer: DigiCert SHA2 Secure Server CA

Valid from: 2022-12-23T00:00:00Z

Valid to: 2023-12-22T23:59:59Z

Count of hosts: 10

Company

ADIB

Website

adib.com

Asset

dts.adib.ae

Graph nodes

Domain: adib.com

Email: dnsadmin@adib.ae

Domain: adib.ae

Domain: dts.adib.ae

➤ **itsm.adib.ae (True Positive)**

☐

High severity 75

First seen 18 Oct 2024

Last seen 04 Jan 2025

Total days 78

Detected

SSL/TLS Security

Reason

Your SSL certificate expires soon: 2022/06/30!

Common: \*.adib.ae

Issuer: DigiCert SHA2 Secure Server CA

Valid from: 2020-06-25T00:00:00Z

Valid to: 2022-06-30T12:00:00Z

Count of hosts: 33

Company

ADIB

Website

adib.ae

Asset

itsm.adib.ae

Graph nodes

Domain: adib.ae

Domain: itsm.adib.ae

☐

High severity 75

First seen 18 Oct 2024

Last seen 04 Jan 2025

Total days 78

Detected

SSL/TLS Security

Reason

Your SSL certificate expires soon: 2022/06/30!

Common: \*.adib.ae

Issuer: DigiCert SHA2 Secure Server CA

Valid from: 2020-06-25T00:00:00Z

Valid to: 2022-06-30T12:00:00Z

Count of hosts: 33

Company

ADIB

Website

adib.ae

Asset

itsm.adib.ae

Graph nodes

Domain: adib.ae

Domain: itsm.adib.ae

➤ **autodiscover.adib.ae (True Positive)**

☐

High severity 75

First seen 18 Oct 2024

Last seen 04 Jan 2025

Total days 78

Detected

SSL/TLS Security

Reason

Can not find autodiscover.adib.ae neither in domains field nor in subject.common field.

Common: outlook.com

Issuer: DigiCert Cloud Services CA-1

Valid from: 2024-06-27T00:00:00Z

Valid to: 2025-06-26T23:59:59Z

Count of hosts: 7008

Company

ADIB

Website

adib.ae

Asset

autodiscover.adib.ae

Graph nodes

Domain: adib.ae

Domain: autodiscover.adib.ae

☐

High severity 75

First seen 18 Oct 2024

Last seen 04 Jan 2025

Total days 78

Detected

SSL/TLS Security

Reason

Can not find autodiscover.adib.ae neither in domains field nor in subject.common field.

Common: outlook.com

Issuer: DigiCert Cloud Services CA-1

Valid from: 2024-06-27T00:00:00Z

Valid to: 2025-06-26T23:59:59Z

Count of hosts: 7008

Company

ADIB

Website

adib.ae

Asset

autodiscover.adib.ae

Graph nodes

Domain: adib.ae

Domain: autodiscover.adib.ae

C1 - Internal Information Security

➤ **m.adib.ae (True Positive)**

☐ **High severity 75** First seen 04 Jan 2025 Last seen 04 Jan 2025 Total days 1 Detected

**SSL/TLS Security**  
Reason  
Can not find m.adib.ae neither in domains field nor in subject.common field.  
Common: ocuz.it Issuer: R10 Valid from: 2025-01-01T00:05:16Z  
Valid to: 2025-04-01T00:05:15Z Count of hosts: 16

Company  
ADIB  
Website  
adib.ae

Asset  
m.adib.ae  
Graph nodes  
Domain: adib.ae → Domain: m.adib.ae

➤ **arodev.adib.ae (True Positive)**

☐ **High severity 75** First seen 12 Dec 2024 Last seen 04 Jan 2025 Total days 22 Detected

**SSL/TLS Security**  
Reason  
Can not find arodev.adib.ae neither in domains field nor in subject.common field.  
Common: developer.adib.com  
Issuer: DigiCert Global G2 TLS RSA SHA256 2020 CA1  
Valid from: 2023-12-21T00:00:00Z Valid to: 2024-12-20T23:59:59Z  
Count of hosts: 3

Company  
ADIB  
Website  
adib.ae

Asset  
arodev.adib.ae  
Graph nodes  
Domain: adib.ae → Domain: arodev.adib.ae

➤ **kip.adib.ae (True Positive)**

☐ **High severity 75** First seen 18 Oct 2024 Last seen 04 Jan 2025 Total days 78 Detected

**SSL/TLS Security**  
Reason  
Can not find kip.adib.ae neither in domains field nor in subject.common field.  
Common: \*.msaproxy.net Issuer: Microsoft Azure RSA TLS Issuing CA 04  
Valid from: 2024-07-14T04:32:17Z Valid to: 2025-07-09T04:32:17Z  
Count of hosts: 1399

Company  
ADIB  
Website  
adib.com

Asset  
kip.adib.ae  
Graph nodes  
Domain: adib.com → Email: dnsadmin@adib.ae →  
Domain: adib.ae → Domain: kip.adib.ae

➤ **wl.mena.adib.ae (True Positive)**

☐ **Medium severity 46** First seen 30 Oct 2024 Last seen 04 Jan 2025 Total days 66 Detected

**SSL/TLS Security**  
Reason  
Can not find csat.verloop.work.gd neither in domains field nor in subject.common field.  
Common: \*.mena.verloop.io  
Issuer: Sectigo RSA Domain Validation Secure Server CA  
Valid from: 2024-10-29T00:00:00Z Valid to: 2025-10-27T23:59:59Z  
Count of hosts: 14

Company  
ADIB  
Website  
adib.ae

Asset  
csat.verloop.work.gd  
Graph nodes  
Domain: adib.ae → Domain: wl.mena.adib.ae →  
IP: 20.46.144.182 → Domain: csat.verloop.work.gd

➤ 20.46.42.80 (True Positive)

# 20.46.42.80

As of: Jan 04, 2025 5:31pm UTC | Latest

[Summary](#)[History](#)[WHOIS](#)[Explore](#)

## Basic Information

Forward DNS

developer.adib.com

Routing

20.40.0.0/13 via MICROSOFT-CORP-MSN-AS-BLOCK, US (AS8075)

Services (1)

443/HTTP

### SSL/TLS Security

Reason

Your SSL certificate expires soon: 2024/12/20!

Common: developer.adib.com

Issuer: DigiCert Global G2 TLS RSA SHA256 2020 CA1

Valid from: 2023-12-21T00:00:00ZValid to: 2024-12-20T23:59:59Z

Count of hosts: 3

### Company

ADIB

Website

adib.ae

### Asset

developer.adib.com

Graph nodes

Domain: adib.ae → Email: dnsadmin@adib.ae → Domain: adib.com → Domain: developer.adib.com

➤ 195.229.136.108 (True Positive)

# 195.229.136.108

As of: Jan 04, 2025 11:53am UTC | Latest

[Summary](#)[History](#)[WHOIS](#)[Explore](#)

## Basic Information

Reverse DNS

adibpayuat.adib.ae

Forward DNS

adibpayuat.adib.ae

Routing

195.229.128.0/18 via EMIRATES-INTERNET Emirates Internet, AE (AS5384)

Services (2)

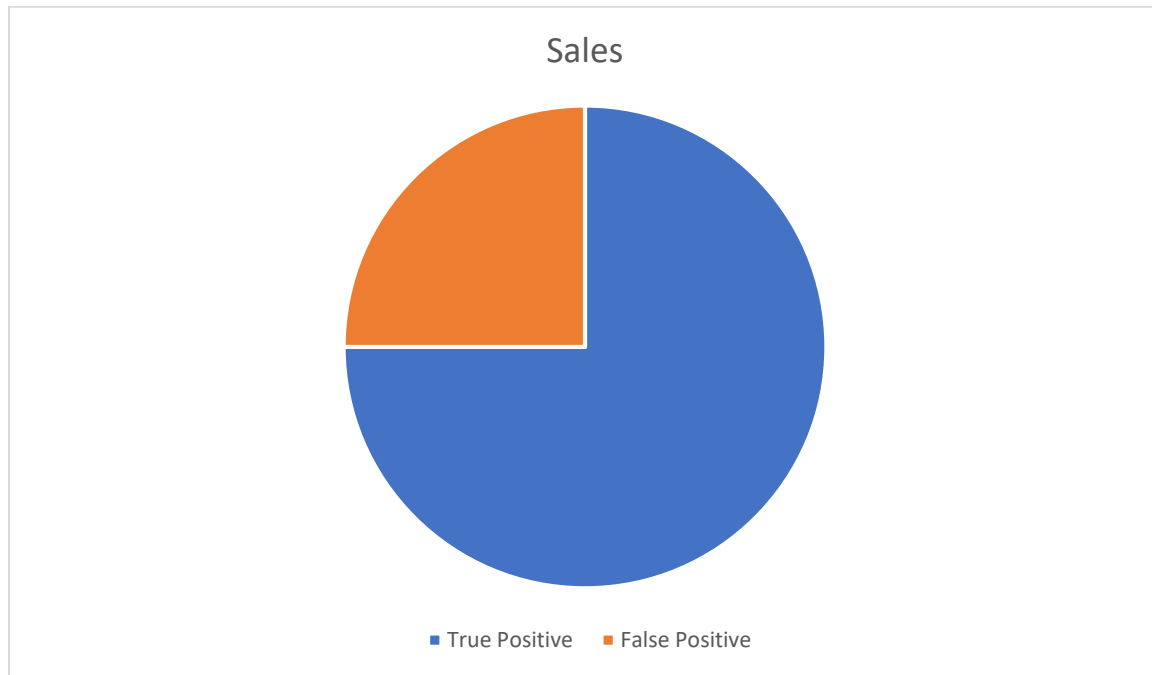
53/DNS, 443/UNKNOWN

CriteriaType: IdentityMatch: ILIKESearch: 'adibpayuat.adib.ae'						
Certificates	crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities
	3417329352	2020-09-23	2020-09-23	2021-09-28	adibpay.adib.ae	adibpayuat.adib.ae
C=US, O=DigiCert Inc, CN=DigiCert SHA2 Secure Server CA						

C1 - Internal Information Security



## TLS/SSL Certificate Issues Statistics



Group IB & Styx View are equal on TLS/SSL certificate Issues

# DATA Leakage Findings

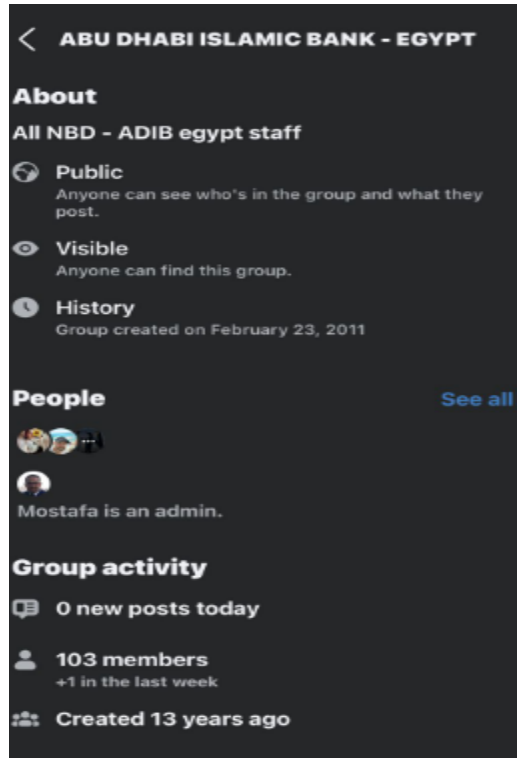
## ➤ 5362 Accounts (True Positive)

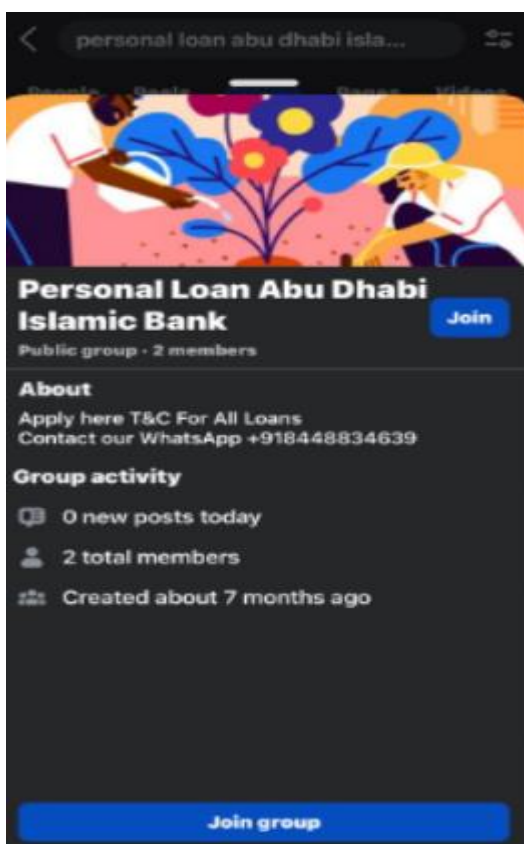
Compromises										
Accounts Bank cards IMEI Mules Public leaks Git leaks Breached DB Shops										
Q Search					Probable corporate access		Source type	Source	Malware	Start - End
First seen	Last seen	Victim's domain	Victim's login	Source type	Source	Malware	Threat actor	Compromised	Events	Found: 1,081
24 Dec 2024	05 Jan 2025	ebanking.a...	mohamedn...	Stealer logs...	https://l... +3	Raccoon +1	Private cha...	05 Jan 2025	4	
30 Dec 2024	30 Dec 2024	adib.eg	MOHAMME...	Stealer logs...	https://l.me...	LummaC2	Private cha...	—	1	
10 Nov 2022	27 Dec 2024	adib.eg	ABDULLAH...	Stealer l... +1	-100176... +5	Vidar +3	free_log... +1	03 Sep 2022	6	
26 Dec 2024	26 Dec 2024	login.micro...	e10209@a...	Stealer logs...	https://l.me...	LummaC2	Private cha...	—	1	
26 Dec 2024	26 Dec 2024	adib.eg	FARESHPP	Stealer logs...	https://l... +1	Raccoon	Private cha...	25 Dec 2024	2	
26 Dec 2024	26 Dec 2024	ebanking.a...	SARAGAB	Stealer logs...	https://l.me...	LummaC2	Private cha...	—	1	
26 Dec 2024	26 Dec 2024	adib.eg	HUSSAEN	Stealer logs...	https://l.me...	LummaC2	Private cha...	—	1	

Group IB better than and collect more data than Styx View

# Potential Social Media Impersonations

## ➤ Social Media (True Positive)





➤ Mobile Apps (True Positive)

○ ff.phoneky.com (not found on Group IB)

ff.phoneky.com/iphone/?q=adib

 NOUVEAU ADIB Direct - Business ★★★★★ 150   Finance PRÉFÉRÉ	 ADIB EGYPT ★★★★★ 30   Finance PRÉFÉRÉ	 ADIB Direct - Business ★★★★★ 150   Finance PRÉFÉRÉ	 NOUVEAU ADIB EGYPT Token ★★★★★ 75   Finance PRÉFÉRÉ	 NOUVEAU ADIB Securities ★★★★★ 75   Finance PRÉFÉRÉ	 ADIB EGYPT ★★★★★ 30   Finance PRÉFÉRÉ	 ADIB ★★★★★ 60   Finance PRÉFÉRÉ
 ADIB Securities ★★★★★ 75   Finance PRÉFÉRÉ	 ADIB ★★★★★ 60   Finance PRÉFÉRÉ	 ADIB EGYPT Token ★★★★★ 75   Finance PRÉFÉRÉ	 NOUVEAU Abu Dhabi Insurance Brokers ★★★★★ 15   Finance PRÉFÉRÉ	 MASJIDKU ★★★★★ 0   Outils PRÉFÉRÉ		

Violations Critical Customer approval required New resolved All Standard view

ff.phoneky.com Status Type Brand Current status date 01 Jan - 04 Jan Quick mode

Web Marketplace Advertising Mobile apps Social networks Instant messengers Presets

○ ko.phoneky.com ((not found on Group IB)

 신규 ADIB Direct - Business ★★★★★ 150   금융 특히 잘하는	 ADIB EGYPT ★★★★★ 30   금융 특히 잘하는	 ADIB Direct - Business ★★★★★ 150   금융 특히 잘하는	 신규 ADIB EGYPT Token ★★★★★ 75   금융 특히 잘하는	 신규 ADIB Securities ★★★★★ 75   금융 특히 잘하는	 ADIB EGYPT ★★★★★ 30   금융 특히 잘하는	 ADIB ★★★★★ 60   금융 특히 잘하는
 ADIB Securities ★★★★★ 75   금융 특히 잘하는	 ADIB ★★★★★ 60   금융 특히 잘하는	 ADIB EGYPT Token ★★★★★ 75   금융 특히 잘하는	 신규 Abu Dhabi Insurance Brokers ★★★★★ 15   금융 특히 잘하는	 MASJIDKU ★★★★★ 0   유틸리티 특히 잘하는		

Violations Critical Customer approval required New resolved All Standard view

ko.phoneky.com Status Type Brand Current status date 01 Jan - 04 Jan Quick mode

Web Marketplace Advertising Mobile apps Social networks Instant messengers Presets

# Patching Cadence

- Nothing Found on Group IB
- But all the CVEs mentioned on StyxView on ADIB as shown below

>	CVE-2022-24785	Red Hat Multiple	Moment.js is a JavaScript date library for parsing, validating, manipulating, and	High	Exploit Available	Apr 4, 2022	Mitigate by IPS (general): activate a corresponding signature (RHSA-2022-5201).
>	CVE-2021-23017	[cpuapr2022-2-	Oracle Blockchain Platform <21.1.2 is prone to multiple vulnerabilities, affecting confidentiality,	High	Exploit Available	Apr 19, 2022	Patch:cpuapr2023:Apply the appropriate patch for Oracle, Bk Oracle has released a patch to address this issue in Oracle B
>	CVE-2021-23017	[cpuapr2022-3-	A security issue in <b>nginx</b> resolver, as used by Oracle Blockchain Platform, was identified,	High	Exploit Available	Apr 19, 2022	Patch:cpuapr2023:Apply the appropriate patch for Oracle, Bk Oracle has released a patch to address this issue in Oracle B
>	CVE-2022-0155, CVE-2022-1365, CVE-2022-	[RHSA-2022:1681]	Red Hat Advanced Cluster Management for Kubernetes 2.4.4 General Availability release	Critical	Exploit Available	May 3, 2022	Patch:RHSA-2022-6156:Apply the appropriate patch for RedH RedHat has released a patch (RHSA-2022-6156) which elimi
>	CVE-2022-0155, CVE-2022-24723, CVE-2022-	[RHSA-2022:1715]	Red Hat Advanced Cluster Management for Kubernetes 2.3.10 General Availability release	Critical	Exploit Available	May 5, 2022	Patch:RHSA-2022-5201:Apply the appropriate patch for RedH RedHat has released a patch (RHSA-2022-5201) which elimi
>	CVE-2022-23913, CVE-2021-42392, CVE-2022-	[RHSA-2022:4922]	A security update is now available for Red Hat JBoss Enterprise Application Platform 7.4. Red	Critical	Exploit Available	Jun 6, 2022	Patch:RHSA-2024-10208:Apply the appropriate patch for Red RedHat has released a patch (RHSA-2024-10208) which elimi

SBV	CVE	Title	Asset Name	Asset OS Name	Asset Importance	Service Ports	Exposure
SBV-133493	CVE-2021-23017	NGINX 0.6.18 - 1.20.0 Remote DoS or Other Vulnerability via Forged UDP Packets - CVE-2021-23017	FidelsGW2.adib.co.eg	Enterprise Linux Server		80/TCP	Protected
SBV-133493	CVE-2021-23017	NGINX 0.6.18 - 1.20.0 Remote DoS or Other Vulnerability via Forged UDP Packets - CVE-2021-23017	EGBNMEDIA01	Unix		443/TCP	Inaccess...
SBV-133493	CVE-2021-23017	NGINX 0.6.18 - 1.20.0 Remote DoS or Other Vulnerability via Forged UDP Packets - CVE-2021-23017	EGBNMEDIA01	Unix		443/TCP	Uncomp...

## Overall

**Group IB** specializes in threat intelligence, strong focus on countering financial and cybercrime, also leaked credentials and DNS Health

**Styx View** better on Attack Surface Management specially network security, and vulnerability management