

1. Top 10 Entities

Total number of entities	53
Total number of links	61

Ranked by Incoming Links

Rank	Type	Value	Incoming links
1	DNS Name	45.63.92.252.vultrusercontent.com	4
2	IPv4 Address	45.63.92.252	3
3	Location	Santa Clara, US	2
4	Company	Vultr Holdings, LLC	2
5	AS	20473	2
6	Netblock	45.63.92.0-45.63.93.255	2
7	Censys Software	Linux	2
8	GreyNoise Noise	No Noise Detected	1
9	alphaMountain Category	Malicious	1
10	Location	Santa Clara, California (United States)	1

Ranked by Outgoing Links

Rank	Type	Value	Outgoing links
1	IPv4 Address	45.63.92.252	58
2	DNS Name	45.63.92.252.vultrusercontent.com	1
3	Domain	www.quickvol.work.g	1
4	Domain	quickvol.work.g	1
5	Location	Santa Clara, US	0
6	Company	Vultr Holdings, LLC	0
7	AS	20473	0
8	Netblock	45.63.92.0-45.63.93.255	0
9	Censys Software	Linux	0
10	GreyNoise Noise	No Noise Detected	0

Ranked by Total Links

Rank	Type	Value	Total links
1	IPv4 Address	45.63.92.252	61
2	DNS Name	45.63.92.252.vultrusercontent.com	5
3	Location	Santa Clara, US	2
4	Company	Vultr Holdings, LLC	2
5	AS	20473	2
6	Netblock	45.63.92.0-45.63.93.255	2
7	Censys Software	Linux	2
8	Domain	www.quickvol.work.g	1
9	Domain	quickvol.work.g	1
10	GreyNoise Noise	No Noise Detected	1

2. Entities by Type

ASs (1)

20473

Censys Service Details (3)

3128/HTTP	4106/SSH
8888/HTTPS	

Censys Softwares (4)

Linux	OpenSSH
Squid	openssh

Companies (3)

American Registry for Internet Numbers, Ltd.	Constant Company, LLC
Vultr Holdings, LLC	

DNS Names (14)

109278637.coridas.ru	166247104.coridas.ru
188727861.coridas.ru	198455199.coridas.ru
222447903.coridas.ru	229381994.coridas.ru
2378984.coridas.ru	45-63-92-252.ipv4.nknlabs.io
45.63.92.252.vultrusercontent.com	57546881.coridas.ru
80738215.coridas.ru	api.bestrdp.me
quickvol.work.gd	usw3.theepicbrowser.com

Domains (2)

quickvol.work.g	www.quickvol.work.g
-----------------	---------------------

GreyNoise Noises (1)

No Noise Detected

IPQS Tags (7)

Abuse velocity: high	Active Vpn
Bot Status	Proxy
Recent Abuse	Tor
Vpn	

IPv4 Addresses (5)

45.63.0.0	45.63.127.255
45.63.92.0	45.63.92.252
45.63.93.255	

Ipv4 Addr (1)

45.63.92.252

Locations (5)

Santa Clara	Santa Clara, California (United States)
Santa Clara, US	Santa Clara, United States
United States	

Netblocks (2)

45.63.92.0-45.63.92.255	45.63.92.0-45.63.93.255
-------------------------	-------------------------

Organizations (1)

Choopa, LLC

PolySwarm Scans (1)

45.63.92.252

SSL Certificates (1)

40e313630ea5fe1fde5ce98dc4cf0240be58ea10

WHOIS Records (1)

45.63.92.252

alphaMountain Categories (1)

Malicious

3. Entity Details



IPv4 Address
maltego.IPv4Address
45.63.92.252

Weight	6
IP Address	45.63.92.252
Internal	false
Proxy (IPQS)	true
Fraud Score	100
Recent Abuse (IPQS)	true
Active Vpn (IPQS)	true
Bot Status (IPQS)	true
Tor (IPQS)	true
US	
IP whois	<pre># # ARIN WHOIS data and services are subject to the Terms of Use # available at: https://www.arin.net/resources/registry/whois/tou/ # # If you see inaccuracies in the results, please report at # https://www.arin.net/resources/registry/whois/inaccuracy_reporting/ # # Copyright 1997-2023, American Registry for Internet Numbers, Ltd. # # # Query terms are ambiguous. The query is assumed to be: # "n 45.63.92.252" # # Use "?" to get help. # The Constant Company, LLC CONSTANT (NET-45-63-0-0-1) 45.63.0.0 - 45.63.127.255 Vultr Holdings, LLC NET-45-63-92-0-23 (NET-45-63-92-0-1) 45.63.92.0 - 45.63.93.255 # # ARIN WHOIS data and services are subject to the Terms of Use # available at: https://www.arin.net/resources/registry/whois/tou/ # # If you see inaccuracies in the results, please report at # https://www.arin.net/resources/registry/whois/inaccuracy_reporting/ # # Copyright 1997-2023, American Registry for Internet Numbers, Ltd. #</pre>
Vpn (IPQS)	true
Context	45.63.92.25
Abuse Velocity (IPQS)	high

Google Maps
' 37.3924,-121.9623 '

IPQS Fraud Score

Fraud score: 100

This is an overall fraud score in the context of online user or customer screening (e.g. automated webshop checkout validation).

According to IPQS: 'Fraud Scores ≥ 75 are suspicious, but not necessarily fraudulent.' IPQS recommends 'flagging or blocking traffic with Fraud Scores ≥ 85 .'

IPQS Tag: Proxy

Indicates this IP address is suspected to be a proxy (SOCKS, Elite, Anonymous, VPN, Tor, etc.).

IPQS Tag: Recent Abuse

This value will indicate if there has been any recently verified abuse across IPQS' network for this IP address. Abuse could be a confirmed chargeback, compromised device, fake app install, or similar malicious behavior within the past few days.

IPQS Tag: Bot Status

Indicates if bots or non-human traffic has recently used this IP address to engage in automated fraudulent behavior. Provides stronger confidence that the IP address is suspicious.

IPQS Tag: Vpn

Indicates this IP is suspected of being part of a VPN. This can include data center ranges which can become active VPNs at any time. The "proxy" status will always be true when this value is true.

IPQS Tag: Tor

Indicates this IP suspected is of being part of TOR. This can include previously active TOR nodes and exits which can become active TOR exits at any time. The "proxy" status will always be true when this value is true.

IPQS Tag: Active Vpn

Identifies active VPN connections used by popular VPN services and private VPN servers.

IPQS Tag: Abuse Velocity

Abuse velocity: high

Display Information



















































[READ FULL REPORT FOR 45.63.92.252](#)














alphaMountain Threat Report


Categories	Malicious
Categorization Confidence	0.71
Threat Score	9.06
Possible Typo Of	

Threat Report at alphaMountain

[Details at threatYeti.com](#)

Incoming (3)		
	DNS Name	45.63.92.252.vultrusercontent.com
	Domain	quickvol.work.g
	Domain	www.quickvol.work.g
Outgoing (58)		
	AS	20473
	AS	20473
	Censys Service Details	3128/HTTP
	Censys Service Details	4106/SSH
	Censys Service Details	8888/HTTPS
	Censys Software	Linux
	Censys Software	Linux
	Censys Software	OpenSSH
	Censys Software	Squid
	Censys Software	openssh
	Company	American Registry for Internet Numbers, Ltd.
	Company	Constant Company, LLC
	Company	Vultr Holdings, LLC
	Company	Vultr Holdings, LLC
	DNS Name	109278637.coridas.ru
	DNS Name	166247104.coridas.ru
	DNS Name	188727861.coridas.ru
	DNS Name	198455199.coridas.ru
	DNS Name	222447903.coridas.ru
	DNS Name	229381994.coridas.ru
	DNS Name	2378984.coridas.ru
	DNS Name	45-63-92-252.ipv4.nknlabs.io
	DNS Name	45.63.92.252.vultrusercontent.com
	DNS Name	45.63.92.252.vultrusercontent.com
	DNS Name	45.63.92.252.vultrusercontent.com
	DNS Name	45.63.92.252.vultrusercontent.com
	DNS Name	57546881.coridas.ru
	DNS Name	80738215.coridas.ru
	DNS Name	api.bestrdp.me
	DNS Name	quickvol.work.gd
	DNS Name	usw3.theepicbrowser.com
	GreyNoise Noise	No Noise Detected
	IPQS Tag	Abuse velocity: high
	IPQS Tag	Active Vpn
	IPQS Tag	Bot Status
	IPQS Tag	Proxy
	IPQS Tag	Recent Abuse
	IPQS Tag	Tor
	IPQS Tag	Vpn
	IPv4 Address	45.63.0.0
	IPv4 Address	45.63.127.255
	IPv4 Address	45.63.92.0
	IPv4 Address	45.63.93.255
	Location	Santa Clara
	Location	Santa Clara, California (United States)

	Location	Santa Clara, US
	Location	Santa Clara, US
	Location	Santa Clara, United States
	Location	United States
	Netblock	45.63.92.0-45.63.92.255
	Netblock	45.63.92.0-45.63.93.255
	Netblock	45.63.92.0-45.63.93.255
	Organization	Choopa, LLC
	PolySwarm Scan	45.63.92.252
	SSL Certificate	40e313630ea5fe1fde5ce98dc4cf0240be58ea10
	STIX2 Ipv4 Addr	45.63.92.252
	WHOIS Record	45.63.92.252
	alphaMountain Category	Malicious



DNS Name
maltego.DNSName
45.63.92.252.vultrusercontent.com

Weight	75
DNS Name	45.63.92.252.vultrusercontent.com
Image	https://storage.googleapis.com/ipinfo_maltego/icon_ipinfo.png





Google Maps

' 37.3924,-121.9623 '


Censys DNS Information


[Open Reverse DNS name on Censys dashboard](#)
Resolved at: 2023-10-06T10:58:41.054943216Z

Incoming (4)

	IPv4 Address	45.63.92.252
	IPv4 Address	45.63.92.252
	IPv4 Address	45.63.92.252
	IPv4 Address	45.63.92.252

Outgoing (1)

	IPv4 Address	45.63.92.252
---	--------------	--------------





Location
maltego.Location
Santa Clara, US

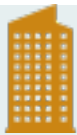
Weight	100
Name	Santa Clara, US
Country	US
City	Santa Clara
Street Address	
Area	
Area Code	
Country Code	US
Longitude	-121.9623
Latitude	37.3924
Image	https://storage.googleapis.com/ipinfo_maltego/icon_ipinfo.png

Google Maps

' [37.3924,-121.9623](#) '

Incoming (2)

 IPv4 Address	45.63.92.252
 IPv4 Address	45.63.92.252



Company

maltego.Company

Vultr Holdings, LLC

Weight	72
Name	Vultr Holdings, LLC

Display Information



ThreatMiner

Data Mining for Threat Intelligence

[READ FULL REPORT FOR 45.63.92.252](#)

Info

Relevance:	0.44057
Count:	1

Incoming (2)

 IPv4 Address	45.63.92.252
 IPv4 Address	45.63.92.252



AS

maltego.AS

20473



Weight	50
AS Number	20473

Censys Autonomous System Number Information

AS-CHOOPA

AS Number	20473
Name	AS-CHOOPA
BGP Prefix	45.63.80.0/20
Country Code	US
Organization	

Incoming (2)

 IPv4 Address	45.63.92.252
 IPv4 Address	45.63.92.252





Netblock

maltego.Netblock

45.63.92.0-45.63.93.255

Weight	50
IP Range	45.63.92.0-45.63.93.255
Country	US
AS	20473
First IP	45.63.92.0
Route	45.63.80.0/20
Last IP	45.63.93.255
Net Name	NET-45-63-92-0-23
Domain	http://www.constant.com/
Name	AS-CHOOPA
Source	ARIN

Incoming (2)

 IPv4 Address	45.63.92.252
 IPv4 Address	45.63.92.252



Censys Software

maltego.censys.Software

Linux


Weight	0
Component Uniform Resource Identifiers	
Edition	
Language	
Other Key	
Other Value	
Other Family	Linux
Part	o
Product	Linux
Source	OSI_APPLICATION_LAYER
SW Edition	
Target HW	
Target SW	
Uniform Resource Identifier	cpe:2.3:o:canonical:ubuntu_linux:20.04:*****:
Update	
Vendor	Ubuntu
Version	20.04

Censys Software Information

[Open product on Censys dashboard](#)

[Open CPE on nvd.nist.gov](#)

Incoming (2)

 IPv4 Address	45.63.92.252
 IPv4 Address	45.63.92.252



Domain

maltego.Domain

[www.quickvol.work.g](#)

Weight	0
Domain Name	www.quickvol.work.g
WHOIS Info	

Censys Domain Information

[Open domain on Censys dashboard](#)

Outgoing (1)

 IPv4 Address	45.63.92.252
--	--------------



Domain

maltego.Domain

[quickvol.work.g](#)

Weight	0
Domain Name	quickvol.work.g
WHOIS Info	

Censys Domain Information

[Open domain on Censys dashboard](#)

Outgoing (1)

 IPv4 Address	45.63.92.252
--	--------------



GreyNoise Noise

greynoise.noise

No Noise Detected

Weight	100
GreyNoise Noise	No Noise Detected

Incoming (1)

 IPv4 Address	45.63.92.252
--	--------------



alphaMountain Category

maltego.alphamountain.Category

Malicious

Weight	0
alphaMountain Category	Malicious
Text	

Incoming (1)

 IPv4 Address	45.63.92.252
--	--------------



Location

maltego.Location

Santa Clara, California (United States)

Weight	100
Name	Santa Clara, California (United States)
Country	
City	
Street Address	
Area	California
Area Code	CA
Country Code	US
Longitude	-121.962
Latitude	37.3931
Continent	North America
Postal code	95054
Timezone	America/Los_Angeles

Info

Information retrieved from the Maxmind GeoLite2 DB.
[Available Here.](#)

Incoming (1)

 IPv4 Address	45.63.92.252
--	--------------



Netblock

maltego.Netblock

45.63.92.0-45.63.92.255

Weight	100
IP Range	45.63.92.0-45.63.92.255

Incoming (1)

 IPv4 Address	45.63.92.252
--	--------------



Censys Service Details

maltego.censys.ServiceDetails

3128/HTTP

Weight	0
IP Address	45.63.92.252
Banner Hex	485454502f312e31203430302042616420526571756573740d0a5365727665723a2073717569642f342e31300d0a4d696d652d56657273696f6e3a20312e300d0a446174653a20203c524544411435445443e0d0a436f6e74656e742d547970653a20746578742f68746d6c3b636861727365743d7574662d380d0a436f6e74656e742d4c656e6774683a20333531340d0a582d53717569642d4572726f723a204552525f494e56414c49445f55524c20300d0a566172793a204163636570742d4c616e67756167650d0a436f6e74656e742d4c616e67756167653a20656e0d0a582d43616368653a204d4953532066726f6d205553572d53462d3167622d32340d0a582d43616368652d4c6f6f6b75703a204e4f4e452066726f6d205553572d53462d3167622d32343a333132380d0a5669613a20312e31205553572d53462d3167622d3234202873717569642f342e3130290d0a436f6e6e656374696f6e3a20636c6f73650d0a
Perspective ID	PERSPECTIVE_TELIA
Transport Protocol	TCP
Description	3128/HTTP
Port	3128
Service banner	HTTP/1.1 400 Bad Request Server: squid/4.10 Mime-Version: 1.0 Date: <REDACTED> Content-Type: text/html; charset=utf-8 Content-Length: 3514 X-Squid-Error: ERR_INVALID_URL 0 Vary: Accept-Language Content-Language: en X-Cache: MISS from USW-SF-1gb-24 X-Cache-Lookup: NONE from USW-SF-1gb-24:3128 Via: 1.1 USW-SF-1gb-24 (squid/4.10) Connection: close
Service	3128:HTTP

Censys Host Information

[Open service on Censys dashboard](#)

Extended Service Name	HTTP
Source IP	167.94.146.55
Port	3128
Transport Protocol	TCP
Observed At	2023-10-05T08:40:39.342210112Z

Incoming (1)

 IPv4 Address	45.63.92.252
--	--------------



Censys Service Details

maltego.censys.ServiceDetails

4106/SSH

Weight	0
IP Address	45.63.92.252
Banner Hex	5353482d322e302d4f70656e5353485f382e327031205562756e74752d347562756e7475302e39
Perspective ID	PERSPECTIVE_NTT
Transport Protocol	TCP
Description	4106/SSH
Port	4106
Service banner	SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.9
Service	4106:SSH

Censys Host Information

[Open service on Censys dashboard](#)

Extended Service Name	SSH
Source IP	167.248.133.49
Port	4106
Transport Protocol	TCP
Observed At	2023-10-04T19:46:15.259995829Z

Incoming (1)

 IPv4 Address	45.63.92.252
--	--------------



Censys Service Details

maltego.censys.ServiceDetails

8888/HTTPS


Weight	0
IP Address	45.63.92.252
Banner Hex	485454502f312e31203430302042616420526571756573740d0a5365727665723a2073717569642f342e31300d0a4d696d652d56657273696f6e3a20312e300d0a446174653a20203c524544411435445443e0d0a436f6e74656e742d547970653a20746578742f68746d6c3b636861727365743d7574662d380d0a436f6e74656e742d4c656e6774683a20333531300d0a582d53717569642d4572726f723a204552525f494e56414c49445f55524c20300d0a566172793a204163636570742d4c616e67756167650d0a436f6e74656e742d4c616e67756167653a20656e0d0a582d43616368653a204d4953532066726f6d205553572d53462d3167622d32340d0a582d43616368652d4c6f6f6b75703a204e4f4e452066726f6d205553572d53462d3167622d32343a333132380d0a5669613a20312e31205553572d53462d3167622d3234202873717569642f342e3130290d0a436f6e6e656374696f6e3a20636c6f73650d0a
Perspective ID	PERSPECTIVE_NTT
Transport Protocol	TCP
Description	8888/HTTPS
Port	8888
Service banner	HTTP/1.1 400 Bad Request Server: squid/4.10 Mime-Version: 1.0 Date: <REDACTED> Content-Type: text/html; charset=utf-8 Content-Length: 3510 X-Squid-Error: ERR_INVALID_URL 0 Vary: Accept-Language Content-Language: en X-Cache: MISS from USW-SF-1gb-24 X-Cache-Lookup: NONE from USW-SF-1gb-24:3128 Via: 1.1 USW-SF-1gb-24 (squid/4.10) Connection: close
Service	8888:HTTPS

Censys Host Information

[Open service on Censys dashboard](#)

Extended Service Name	HTTPS
Source IP	167.248.133.38
Port	8888
Transport Protocol	TCP
Observed At	2023-10-05T17:28:53.362485981Z

Incoming (1)

 IPv4 Address	45.63.92.252
--	--------------





IPQS Tag
maltego.ipqs.Tag
Proxy


Weight	100
Text	Proxy

IPQS Info

Indicates this IP address is suspected to be a proxy (SOCKS, Elite, Anonymous, VPN, Tor, etc.).

Incoming (1)		
	IPv4 Address	45.63.92.252

	DNS Name maltego.DNSName usw3.theepicbrowser.com	
Weight	100	
DNS Name	usw3.theepicbrowser.com	
Incoming (1)		
	IPv4 Address	45.63.92.252



IPQS Tag

maltego.ipqs.Tag


Vpn


Weight	100
Text	Vpn

IPQS Info

Indicates this IP is suspected of being part of a VPN. This can include data center ranges which can become active VPNs at any time. The "proxy" status will always be true when this value is true.

Incoming (1)

	IPv4 Address	45.63.92.252
---	--------------	--------------



IPQS Tag

maltego.ipqs.Tag


Tor


Weight	100
Text	Tor

IPQS Info

Indicates this IP suspected is of being part of TOR. This can include previously active TOR nodes and exits which can become active TOR exits at any time. The "proxy" status will always be true when this value is true.

Incoming (1)

	IPv4 Address	45.63.92.252
---	--------------	--------------

 <div> IPQS Tag maltego.ipqs.Tag Recent Abuse </div>		
Weight	100	
Text	Recent Abuse	

IPQS Info

This value will indicate if there has been any recently verified abuse across IPQS' network for this IP address. Abuse could be a confirmed chargeback, compromised device, fake app install, or similar malicious behavior within the past few days.

Incoming (1)

 IPv4 Address	45.63.92.252
--	--------------



IPQS Tag

maltego.ipqs.Tag

Bot Status

Weight	100
Text	Bot Status

IPQS Info

Indicates if bots or non-human traffic has recently used this IP address to engage in automated fraudulent behavior. Provides stronger confidence that the IP address is suspicious.

Incoming (1)

 IPv4 Address	45.63.92.252
--	--------------



IPQS Tag

maltego.ipqs.Tag

Active Vpn

Weight	100
Text	Active Vpn

IPQS Info

Identifies active VPN connections used by popular VPN services and private VPN servers.

Incoming (1)

 IPv4 Address	45.63.92.252
--	--------------




IPQS Tag

maltego.ipqs.Tag

Abuse velocity: high

Weight	100
Text	Abuse velocity: high

Incoming (1)

 IPv4 Address	45.63.92.252
--	--------------



Censys Software

maltego.censys.Software

Squid

Weight	0
Component Uniform Resource Identifiers	
Edition	
Language	
Other Key	
Other Value	
Other Family	Squid
Part	a
Product	Squid
Source	OSI_APPLICATION_LAYER
SW Edition	
Target HW	
Target SW	
Uniform Resource Identifier	cpe:2.3:a:squid\-cache:squid:4.10:*:*:*:*:*
Update	
Vendor	Squid Cache
Version	4.10

Incoming (1)



maltego.Location

Weight	100
Name	United States
Country	United States
City	
Street Address	
Area	
Area Code	
Country Code	US
Longitude	0.0
Latitude	0.0
Continent	North America

Information retrieved from the Maxmind GeoLite2 DB.
[Available Here](#).



Censys Software
maltego.censys.Software
openssh

Weight	0
Component Uniform Resource Identifiers	
Edition	
Language	
Other Key	
Other Value	
Other Family	
Part	
Product	openssh
Source	OSI_APPLICATION_LAYER
SW Edition	
Target HW	
Target SW	
Uniform Resource Identifier	
Update	
Vendor	
Version	

Censys Software Information

[Open product on Censys dashboard](#)

Incoming (1)

IPv4 Address	45.63.92.252
--------------	--------------



Censys Software
maltego.censys.Software
OpenSSH

Weight	0
Component Uniform Resource Identifiers	
Edition	
Language	
Other Key	
Other Value	
Other Family	OpenSSH
Part	a
Product	OpenSSH
Source	OSI_APPLICATION_LAYER
SW Edition	
Target HW	
Target SW	
Uniform Resource Identifier	cpe:2.3:a:openbsd:openssh:8.2:p1:*****
Update	p1
Vendor	OpenBSD
Version	8.2

Censys Software Information

[Open product on Censys dashboard](#)

[Open CPE on nvd.nist.gov](#)

Incoming (1)

 IPv4 Address	45.63.92.252
--	--------------



WHOIS Record

maltego.WHOISRecord

45.63.92.252

Weight	0
Name	45.63.92.252
WHOIS Info	# # ARIN WHOIS data and services are subject to the Terms of Use # available at: https://www.arin.net/resources/registry/whois/tou/ # # If you see inaccuracies in the results, please report at # https://www.arin.net/resources/registry/whois/inaccuracy_reporting/ # # Copyright 1997-2023, American Registry for Internet Numbers, Ltd. # The Constant Company, LLC CONSTANT (NET-45-63-0-0-1) 45.63.0.0 - 45.63.127.255 Vultr Holdings, LLC NET-45-63-92-0-23 (NET-45-63-92-0-1) 45.63.92.0 - 45.63.93.255 # # ARIN WHOIS data and services are subject to the Terms of Use # available at: https://www.arin.net/resources/registry/whois/tou/ # # If you see inaccuracies in the results, please report at # https://www.arin.net/resources/registry/whois/inaccuracy_reporting/ # # Copyright 1997-2023, American Registry for Internet Numbers, Ltd. #
Registry Domain ID	
Domain Name	45.63.92.252
Created Date	
Registry Expiry Date	
Updated Date	
Transfer Date	
Nameservers	
Name Server IP Addresses	
Maintainer	
Created By	
Updated By	
DNSSEC	
Domain Status	NETWORK
ENS AuthId	
Registry Registrant ID	
Registrant Name	
Registrant Organization	
Registrant Address	
Registrant Street	
Registrant City	
Registrant State/Province	
Registrant Country	
Registrant Country Code	
Registrant Postal Code	
Registrant Phone	
Registrant Phone Ext	
Registrant Fax	
Registrant Fax Ext	
Registrant Email	
Admin ID	

Admin ID	
Admin Name	
Admin Organization	
Admin Address	
Admin Street	
Admin City	
Admin State/Province	
Admin Country	
Admin Country Code	
Admin Postal Code	
Admin Phone	
Admin Phone Ext	
Admin Fax	
Admin Fax Ext	
Admin Email	
Tech ID	
Tech Name	
Tech Organization	
Tech Address	
Tech City	
Tech State/Province	
Tech Country	
Tech Postal Code	
Tech Phone	
Tech Phone Ext	
Tech Fax	
Tech Fax Ext	
Tech Email	
Registrar ID	
Registrar IANA ID	778
Registrar	ARIN
Registrar Registration Expiration Date	
Registrar URL	
Registrar WHOIS Server	whois.arin.net
Registrar Status	
Registrar Address	
Registrar City	
Registrar State/Province	
Registrar Country	
Registrar Postal Code	
Registrar Phone	
Registrar Fax	
Registrar Fax Ext	
Registrar Email	
Registrar Abuse Contact Email	
Registrar Abuse Contact Phone	
Sponsoring Registrar	

WhoisXML audit information

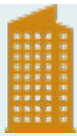
p { line-height:50% !important; }

Created Date 2023-10-06 13:27:09 UTC

Updated Date 2023-10-06 13:27:09 UTC

Incoming (1)

 IPv4 Address 45.63.92.252



Company

maltego.Company

American Registry for Internet Numbers, Ltd.

Weight 66
Name American Registry for Internet Numbers, Ltd.

Info

Relevance: 0.663278

Count: 2

Incoming (1)

 IPv4 Address 45.63.92.252



SSL Certificate

pt.SSLCertificate

40e313630ea5fe1fde5ce98dc4cf0240be58ea10

Weight 100
SSL Certificate 40e313630ea5fe1fde5ce98dc4cf0240be58ea10


Display Information



ThreatMiner
Data Mining for Threat Intelligence

[READ FULL REPORT FOR 40e313630ea5fe1fde5ce98dc4cf0240be58ea10](#)

Incoming (1)

 IPv4 Address 45.63.92.252



IPv4 Address

maltego.IPv4Address

45.63.0.0

Weight	46
IP Address	45.63.0.0
Internal	false

Info

Relevance:	0.468668
Count:	1

Incoming (1)

 IPv4 Address	45.63.92.252
--	--------------



IPv4 Address
maltego.IPv4Address
45.63.127.255

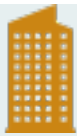
Weight	45
IP Address	45.63.127.255
Internal	false

Info

Relevance:	0.456049
Count:	1

Incoming (1)

 IPv4 Address	45.63.92.252
--	--------------



Company
maltego.Company
Constant Company, LLC

Weight	50
Name	Constant Company, LLC

Info

Relevance:	0.506713
Count:	1

Incoming (1)

 IPv4 Address	45.63.92.252
--	--------------



IPv4 Address
maltego.IPv4Address
45.63.93.255

Weight	37
IP Address	45.63.93.255
Internal	false

Info

Relevance:	0.378281
Count:	1

Incoming (1)

 IPv4 Address	45.63.92.252
--	--------------



IPv4 Address

maltego.IPv4Address

45.63.92.0

Weight	39
IP Address	45.63.92.0
Internal	false

Info

Relevance:	0.391631
Count:	1

Incoming (1)

 IPv4 Address	45.63.92.252
--	--------------



Location

maltego.Location

Santa Clara, United States

Weight	0
Name	Santa Clara, United States
Country	United States
City	Santa Clara
Street Address	
Area	California
Area Code	95054
Country Code	US
Longitude	-121.9623
Latitude	37.3924

Censys Location Information

[Open location on Censys dashboard](#)

Incoming (1)

 IPv4 Address	45.63.92.252
--	--------------



STIX2 Ipv4 Addr

maltego.STIX2.ipv4-addr

45.63.92.252

Weight	100
type	ipv4-addr
spec_version	2.1
object_marking_refs	[]
granular_markings	[]
defanged	
id	ipv4-addr--c340377e-9e07-5eff-b12a-4433dced9ddd
extensions	
ipv4-address	45.63.92.252
resolves_to_refs	[]
belongs_to_refs	[]
x_maltego_recovery_property_map	{"ipv4-address": ["value"]}
ping	
Internal	false
x_maltego_marking_color	
x_maltego_marking_text	

Incoming (1)



IPv4 Address

45.63.92.252



Location

maltego.Location

Santa Clara

Weight	100
Name	Santa Clara
Country	
City	Santa Clara
Street Address	
Area	California
Area Code	
Country Code	
Longitude	-121.962
Latitude	37.3931

Google Maps

[Google Maps Link](#)

Incoming (1)



IPv4 Address

45.63.92.252



DNS Name

maltego.DNSName

quickvol.work.gd

Weight	46
DNS Name	quickvol.work.gd
DNSDB JSON Output	{"count": 46, "time_first": 1681386995, "time_last": 1693325142, "rrname": "quickvol.work.gd.", "rrtype": "A", "rdata": "45.63.92.252"}

DNSDB JSON Output

```
{"count": 46, "time_first": 1681386995, "time_last": 1693325142, "rrname": "quickvol.work.gd.", "rrtype": "A", "rdata": "45.63.92.252"}
```

Incoming (1)

 IPv4 Address	45.63.92.252
--	--------------



Organization

maltego.Organization

Choopa, LLC

Weight	100
Name	Choopa, LLC

Incoming (1)

 IPv4 Address	45.63.92.252
--	--------------



DNS Name

maltego.DNSName


45-63-92-252.ipv4.nknlabs.io

Weight	6
DNS Name	45-63-92-252.ipv4.nknlabs.io
DNSDB JSON Output	{"count": 6, "time_first": 1624336325, "time_last": 1660351102, "rrname": "45-63-92-252.ipv4.nknlabs.io.", "rrtype": "A", "rdata": "45.63.92.252"}

DNSDB JSON Output

```
{"count": 6, "time_first": 1624336325, "time_last": 1660351102, "rrname": "45-63-92-252.ipv4.nknlabs.io.", "rrtype": "A", "rdata": "45.63.92.252"}
```

Incoming (1)

 IPv4 Address	45.63.92.252
--	--------------



DNS Name

maltego.DNSName

57546881.coridas.ru

Weight	1
DNS Name	57546881.coridas.ru
DNSDB JSON Output	{"count": 1, "time_first": 1652351481, "time_last": 1652351481, "rrname": "57546881.coridas.ru.", "rrtype": "A", "rdata": "45.63.92.252"}

DNSDB JSON Output

```
{"count": 1, "time_first": 1652351481, "time_last": 1652351481, "rrname": "57546881.coridas.ru.", "rrtype": "A", "rdata": "45.63.92.252"}
```

Incoming (1)

 IPv4 Address 45.63.92.252



DNS Name

maltego.DNSName

80738215.coridas.ru

Weight	1
DNS Name	80738215.coridas.ru
DNSDB JSON Output	{"count": 1, "time_first": 1652351781, "time_last": 1652351781, "rrname": "80738215.coridas.ru.", "rrtype": "A", "rdata": "45.63.92.252"}

DNSDB JSON Output

```
{"count": 1, "time_first": 1652351781, "time_last": 1652351781, "rrname": "80738215.coridas.ru.", "rrtype": "A", "rdata": "45.63.92.252"}
```

Incoming (1)

 IPv4 Address 45.63.92.252



DNS Name

maltego.DNSName

api.bestrdp.me

Weight	7
DNS Name	api.bestrdp.me
DNSDB JSON Output	{"count": 7, "time_first": 1536938627, "time_last": 1536938628, "rrname": "api.bestrdp.me.", "rrtype": "A", "rdata": "45.63.92.252"}

DNSDB JSON Output

```
{"count": 7, "time_first": 1536938627, "time_last": 1536938628, "rrname": "api.bestrdp.me.", "rrtype": "A", "rdata": "45.63.92.252"}
```

Incoming (1)

 IPv4 Address 45.63.92.252



DNS Name

maltego.DNSName


2378984.coridas.ru

Weight	1
DNS Name	2378984.coridas.ru
DNSDB JSON Output	{"count": 1, "time_first": 1652345007, "time_last": 1652345007, "rrname": "2378984.coridas.ru.", "rrtype": "A", "rdata": "45.63.92.252"}

DNSDB JSON Output

```
{"count": 1, "time_first": 1652345007, "time_last": 1652345007, "rrname": "2378984.coridas.ru.", "rrtype": "A", "rdata": "45.63.92.252"}
```

Incoming (1)

 IPv4 Address 45.63.92.252



DNS Name
maltego.DNSName
188727861.coridas.ru

Weight	1
DNS Name	188727861.coridas.ru
DNSDB JSON Output	<pre>{"count": 1, "time_first": 1652351478, "time_last": 1652351478, "rrname": "188727861.coridas.ru.", "rrtype": "A", "rdata": "45.63.92.252"}</pre>

DNSDB JSON Output

```
{"count": 1, "time_first": 1652351478, "time_last": 1652351478, "rrname": "188727861.coridas.ru.", "rrtype": "A", "rdata": "45.63.92.252"}
```

Incoming (1)

IPv4 Address	45.63.92.252
--------------	--------------



DNS Name
maltego.DNSName
198455199.coridas.ru

Weight	1
DNS Name	198455199.coridas.ru
DNSDB JSON Output	<pre>{"count": 1, "time_first": 1652346530, "time_last": 1652346530, "rrname": "198455199.coridas.ru.", "rrtype": "A", "rdata": "45.63.92.252"}</pre>

DNSDB JSON Output

```
{"count": 1, "time_first": 1652346530, "time_last": 1652346530, "rrname": "198455199.coridas.ru.", "rrtype": "A", "rdata": "45.63.92.252"}
```

Incoming (1)

IPv4 Address	45.63.92.252
--------------	--------------



DNS Name
maltego.DNSName
109278637.coridas.ru

Weight	2
DNS Name	109278637.coridas.ru
DNSDB JSON Output	<pre>{"count": 2, "time_first": 1652353453, "time_last": 1652353500, "rrname": "109278637.coridas.ru.", "rrtype": "A", "rdata": "45.63.92.252"}</pre>

DNSDB JSON Output

```
{"count": 2, "time_first": 1652353453, "time_last": 1652353500, "rrname": "109278637.coridas.ru.", "rrtype": "A", "rdata": "45.63.92.252"}
```

Incoming (1)

IPv4 Address	45.63.92.252
--------------	--------------



DNS Name
maltego.DNSName
166247104.coridas.ru

Weight	1
DNS Name	166247104.coridas.ru
DNSDB JSON Output	<pre>{"count": 1, "time_first": 1652344701, "time_last": 1652344701, "rrname": "166247104.coridas.ru.", "rrtype": "A", "rdata": "45.63.92.252"}</pre>

DNSDB JSON Output

```
{"count": 1, "time_first": 1652344701, "time_last": 1652344701, "rrname": "166247104.coridas.ru.", "rrtype": "A", "rdata": "45.63.92.252"}
```

Incoming (1)

 IPv4 Address	45.63.92.252
--	--------------



DNS Name
maltego.DNSName
222447903.coridas.ru

Weight	1
DNS Name	222447903.coridas.ru
DNSDB JSON Output	<pre>{"count": 1, "time_first": 1652350874, "time_last": 1652350874, "rrname": "222447903.coridas.ru.", "rrtype": "A", "rdata": "45.63.92.252"}</pre>

DNSDB JSON Output

```
{"count": 1, "time_first": 1652350874, "time_last": 1652350874, "rrname": "222447903.coridas.ru.", "rrtype": "A", "rdata": "45.63.92.252"}
```

Incoming (1)

 IPv4 Address	45.63.92.252
--	--------------




DNS Name
maltego.DNSName
229381994.coridas.ru

Weight	1
DNS Name	229381994.coridas.ru
DNSDB JSON Output	<pre>{"count": 1, "time_first": 1652348131, "time_last": 1652348131, "rrname": "229381994.coridas.ru.", "rrtype": "A", "rdata": "45.63.92.252"}</pre>

DNSDB JSON Output

```
{"count": 1, "time_first": 1652348131, "time_last": 1652348131, "rrname": "229381994.coridas.ru.", "rrtype": "A", "rdata": "45.63.92.252"}
```

Incoming (1)

 IPv4 Address	45.63.92.252
--	--------------



PolySwarm Scan

maltego.polyswarm.PolyswarmScan

45.63.92.252

Weight	100
Name	45.63.92.252
Artifact ID	21676605293440648
Polyscore	0.23213458159978606
First Seen	2023-10-06T13:27:24.247337
Last Scanned	2023-10-06T13:27:24.247337
MIME Type	text/plain
Extended Type	ASCII text, with no line terminators
MD5	7932232443c747e134d5843487786143
SHA-1	66c86113327141d80ec71f51356c4a940651abdc
SHA-256	21e89d4811c6519049c31ec238e6788f8f2ed20e195cec5f816c1b249463f2a8
ssdeep	
TLSH	
Tags	[]
Size	12
Guest Paths	[]

Scan URL

[Go to Scan Page on Polyswarm](#)

Detections

Benign	3
Total	3

Incoming (1)

IPv4 Address	45.63.92.252
--------------	--------------