

TARGET: Vitalik Buterin

Programmatore russo cresciuto in Canada residente a Toronto, co-fondatore di Ethereum.

GOOGLE DORCK:

query utilizzata: (site:github "Vitalik Buterin")

Utilizzando questa query ho trovato l'account certificato su github di ethereum e tramite quello osservando i vari progetti sono riuscito a risalire all'account github privato di Vitalik Buterin non trovando nulla di importante se non suoi progetti personali risalenti al 2013 fino ai giorni nostri, ho notato inoltre che lo sviluppatore segue solo una sola persona dal suo account github, ho provato a cercare qualcosa su questo account, ma a sua volta questa ricerca sembra non aver portato a qualcosa di importante, lascio questa parte in sospeso per provare a risalire al nome reale legato a quell'account github e cercare dei collegamenti fra i due.

ho provato ad utilizzare una query simile per quanto riguarda linkedin, non trovando nulla di particolarmente interessante, tra l'altro l'account linkedin che sembra appartenere al target dichiara di non utilizzare quell'account per uno scopo.

con la query (site:ethereum.org "Vitalik Buterin" filetype:pdf) son riuscito a risalire al whitepaper di ethereum scritto da Vitalik in persona, questo whitepaper pare essere il documento introduttivo al progetto ethereum pubblicato nel 2014 da Vitalik prima dell'uscita di ethereum avvenuta nel 2015

ho provato ad effettuare un site Crawling del sito web di ethereum per scovare i suoi eventuali sotto domini con la seguente query:
site:ethereum.org -site:www.ethereum.org


dalle mie ricerche ho notato che sono 2 i sottodomini principali del sito web di ethereum e sono rispettivamente
<https://launchpad.ethereum.org/> e <https://geth.ethereum.org/>

metodo utilizzato: ricerca su shodan:

dopo aver mappato il dominio principale di ethereum individuando i due sottodomini principali ho effettuato una ricerca su shodan utilizzando la seguente query:
hostname:*.ethereum.org

Da questa ricerca abbiamo ricavato qualche informazione utile ad esempio gli indirizzi ip dei server host dei servizi web, dove sono localizzati e alcuni protocolli abilitati:

TOP COUNTRIES



India	22
United States	12
Korea, Republic of	5
Netherlands	1

TOP PORTS

443	35
2083	2
8443	2
2087	1

TOP ORGANIZATIONS

Amazon.com, Inc.	29
Cloudflare, Inc.	10
DigitalOcean, LLC	1

TOP PRODUCTS

CloudFlare	4
nginx	1

403 Forbidden

104.18.176.152
ethereum.org
Cloudflare, Inc.
United States, San Francisco
cdn

SSL Certificate

Issued By: WE1
Issued To: ethereum.org
Supported SSL Versions: TLSv1, TLSv1.1, TLSv1.2

HTTP/1.1 403 Forbidden
Server: cloudflare
Date: Mon, 02 Dec 2024 21:17:53 GMT
Content-Type: text/html
Content-Length: 553
Connection: keep-alive
CF-RAY: 8ebe58a76986f987-SJC

2600:1f16:1a4:a000::1f4

launchpad.ethereum.org
Amazon.com, Inc.
United States, Columbus
cloud

SSL Certificate

Issued By: E5
Issued To: launchpad.ethereum.org
Supported SSL Versions: TLSv1.2, TLSv1.3

HTTP/1.1 200 OK
Accept-Ranges: bytes
Age: 0
Cache-Control: public,max-age=0,must-revalidate
Cache-Status: "Netlify Edge"; fwd=miss

443

35

2083

2

8443

2

2087

1

TOP ORGANIZATIONS

Amazon.com, Inc.	29
Cloudflare, Inc.	10
DigitalOcean, LLC	1

TOP PRODUCTS

CloudFlare	4
nginx	1

2600:1f16:1a4:a000::1f4

launchpad.ethereum.org
Amazon.com, Inc.
United States, Columbus
cloud

SSL Certificate

Issued By: E5
Issued To: launchpad.ethereum.org
Supported SSL Versions: TLSv1.2, TLSv1.3

HTTP/1.1 200 OK
Accept-Ranges: bytes
Age: 0
Cache-Control: public,max-age=0,must-revalidate
Cache-Status: "Netlify Edge"; fwd=miss

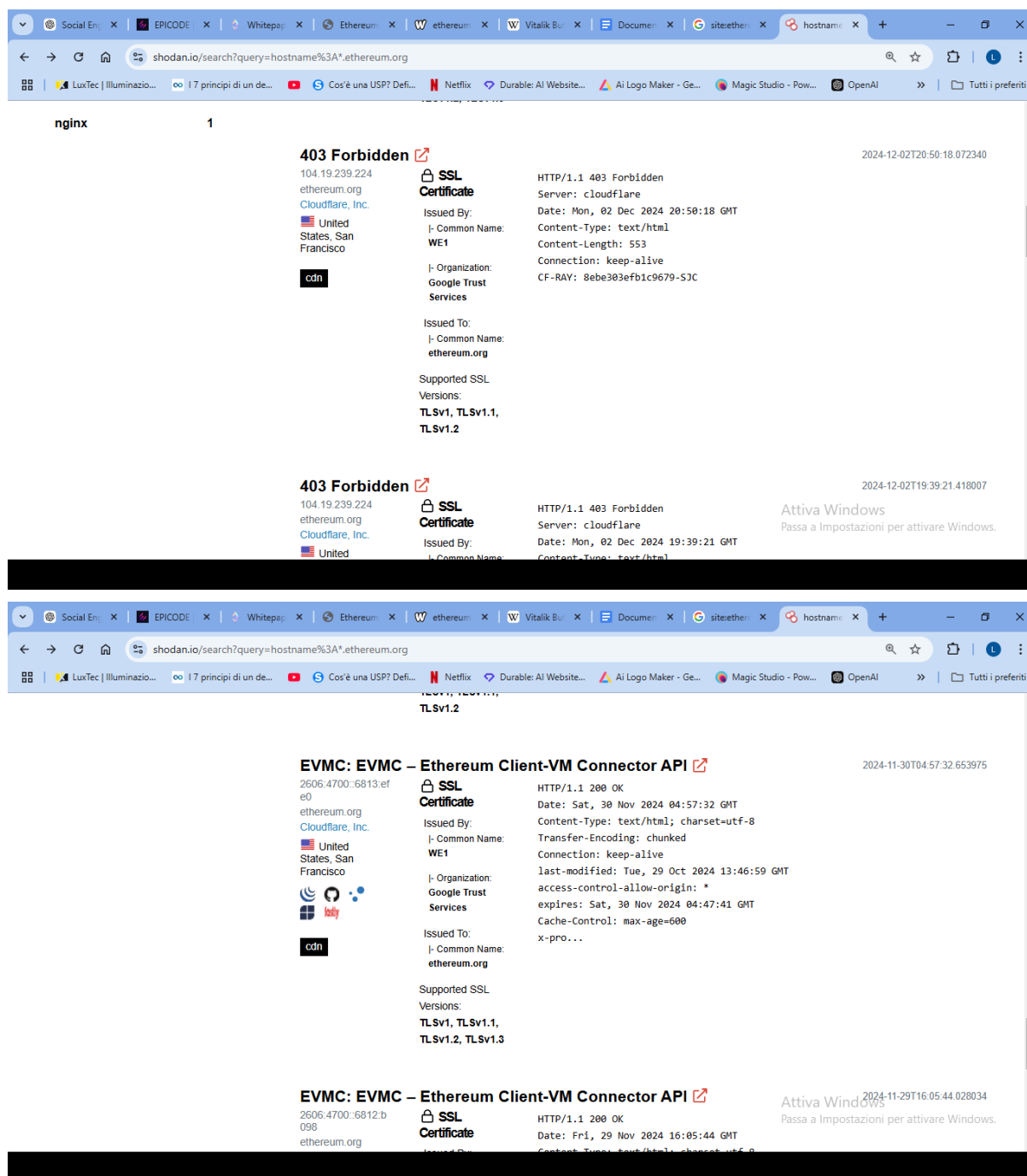
403 Forbidden

104.19.239.224
ethereum.org
Cloudflare, Inc.
United States, San Francisco

SSL Certificate

Issued By: WE1

HTTP/1.1 403 Forbidden
Server: cloudflare
Date: Mon, 02 Dec 2024 20:50:18 GMT
Content-Type: text/html
Content-Length: 553



Utilizzando maltego invece siamo riusciti a risalire ad eventuali email di contatto del sito web di ethereum e trovato altri indirizzi IPv4 e IPv6 confrontandoli con quelli trovati su shodan per lo stesso dominio, presumo che gli indirizzi IPv4 trovati su shodan rispondano a dei server proxy o server che fungono da reverse proxy, ho provato a scovare file importanti attraverso maltego cercando per piu estensioni di file non trovando nulla di nuovo, per quanto riguarda i contatti personali di Vitalik sembra non esserci materiali attendibili, oltre al suo profilo github e il suo profilo X inattivo da quasi 2 anni in seguito da un attacco hacker

Graph (Desktop) 4.8.1 - Community Edition

Investigate View Entities Collections Transforms Machines Collaboration Import/Export Windows

Entity Palette

- Person
- Cryptocurrency
- Bitcoin Cash Address
- Bitcoin Cash Block
- BitcoinCash Block Height
- Bitcoin Cash Transaction

Run View

Overview

Property View Hub Transform Inputs

Output - Transform Output

29 entities, 28 links

9°C Variabile 01:32 03/12/2024

Graph (Desktop) 4.8.1 - Community Edition

Investigate View Entities Collections Transforms Machines Collaboration Import/Export Windows

Entity Palette

- Person
- Cryptocurrency
- Bitcoin Cash Address
- Bitcoin Cash Block
- BitcoinCash Block Height
- Bitcoin Cash Transaction

Run View

Overview

Property View Hub Transform Inputs

Output - Transform Output

29 entities, 28 links

8°C Variabile 01:33 03/12/2024