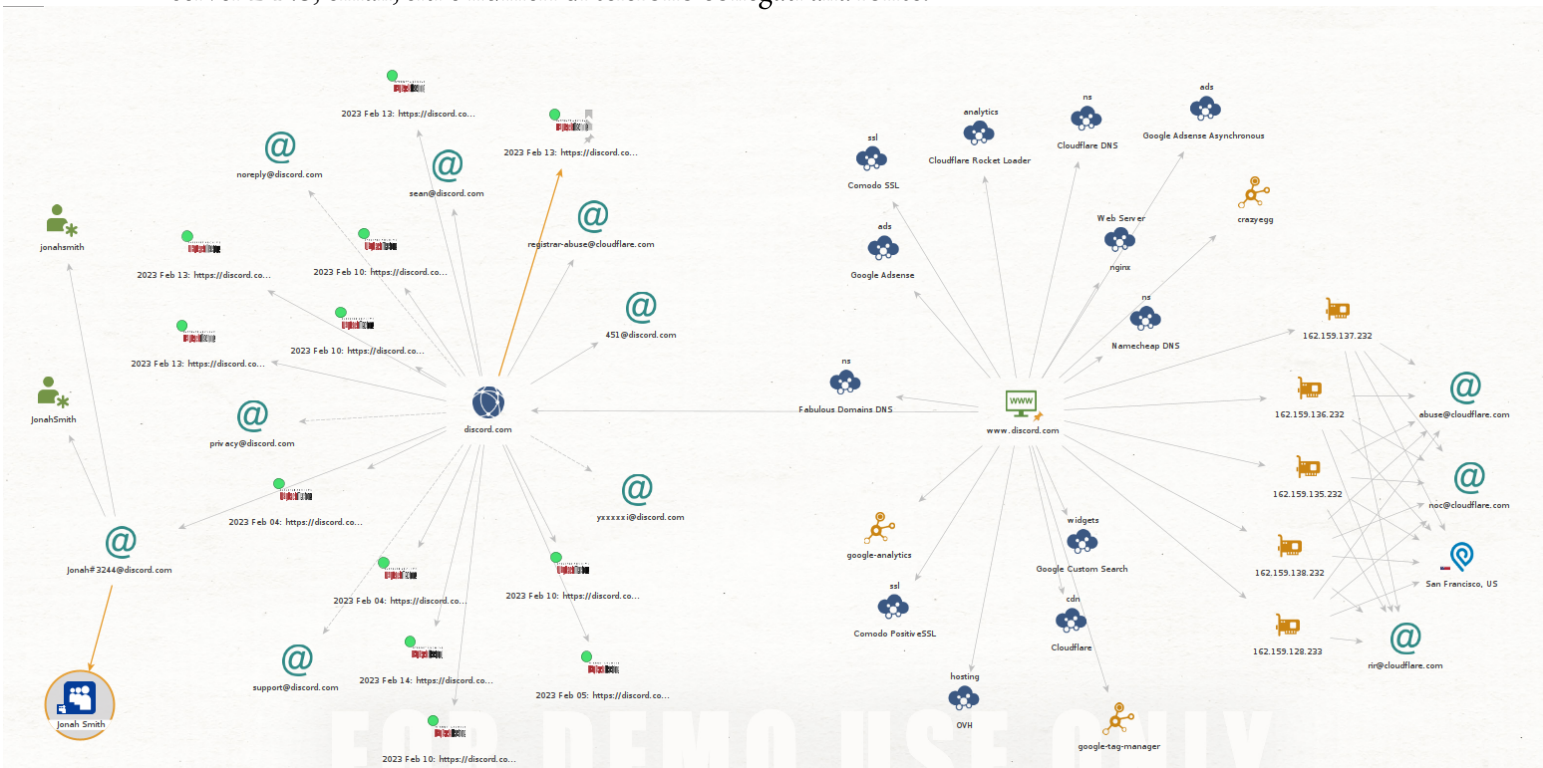
TARGET : Discord

Partendo da una scansione passiva con NQT, inserendo semplicemente il nome del sito da scansionare, possiamo estrapolare abbastanza informazioni come indirizzo ip e locazione geografica, quindi passiamo i risultati ad un tool più avanzato come maltego.

```
; <<>> DiG 9.2.4 <<>> any www.discord.com
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 58436
;; flags: qr rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;www.discord.com. IN ANY

;; ANSWER SECTION:
www.discord.com. 195 IN A 162.159.135.232
www.discord.com. 195 IN A 162.159.138.232
www.discord.com. 195 IN A 162.159.136.232
www.discord.com. 195 IN A 162.159.137.232
www.discord.com. 195 IN A 162.159.128.233
www.discord.com. 195 IN TYPE46 \# 95 00010D030000012C63F6438563F3

;; Query time: 32 msec
;; SERVER: 66.11.0.58#53(66.11.0.58)
;; WHEN: Tue Feb 21 10:44:14 2023
;; MSG SIZE rcvd: 220
```

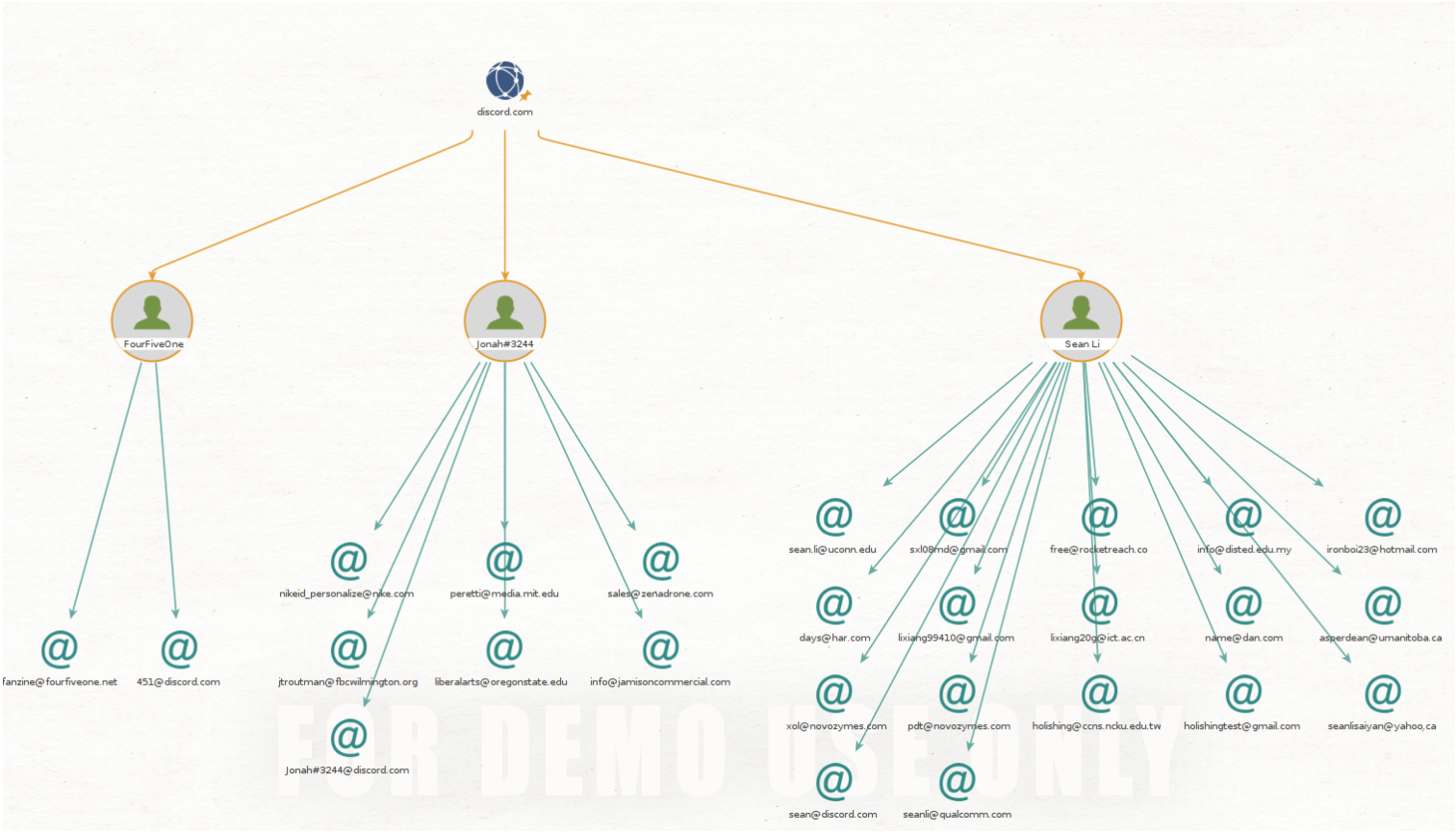
```
NetRange:       162.158.0.0 - 162.159.255.255
CIDR:           162.158.0.0/15
NetName:        CLOUDFLARENET
NetHandle:      NET-162-158-0-0-1
Parent:         NET162 (NET-162-0-0-0-0)
NetType:        Direct Allocation
OriginAS:       AS13335
Organization:   Cloudflare, Inc. (CLOUD14)
RegDate:        2013-05-23
Updated:        2021-05-26
Comment:        All Cloudflare abuse reporting can be done via https://www.cloudflare.com/abuse
Ref:            https://rdap.arin.net/registry/ip/162.158.0.0


OrgName:        Cloudflare, Inc.
OrgId:          CLOUD14
Address:        101 Townsend Street
City:           San Francisco
StateProv:      CA
PostalCode:     94107
Country:        US
RegDate:        2010-07-09
Updated:        2021-07-01
Ref:            https://rdap.arin.net/registry/entity/CLOUD14


OrgTechHandle: ADMIN2521-ARIN
OrgTechName:   Admin
OrgTechPhone:  +1-650-319-8930
OrgTechEmail:  rir@cloudflare.com
OrgTechRef:    https://rdap.arin.net/registry/entity/ADMIN2521-ARIN

OrgNOCHandle: CLOUD146-ARIN
OrgNOCName:   Cloudflare-NOC
OrgNOCPhone:  +1-650-319-8930
OrgNOCEmail:  noc@cloudflare.com
OrgNOCRef:    https://rdap.arin.net/registry/entity/CLOUD146-ARIN

OrgAbuseHandle: ABUSE2916-ARIN
OrgAbuseName:   Abuse
OrgAbusePhone:  +1-650-319-8930
OrgAbuseEmail:  abuse@cloudflare.com
OrgAbuseRef:    https://rdap.arin.net/registry/entity/ABUSE2916-ARIN

OrgRoutingHandle: CLOUD146-ARIN
OrgRoutingName:   Cloudflare-NOC
OrgRoutingPhone:  +1-650-319-8930
OrgRoutingEmail:  noc@cloudflare.com
OrgRoutingRef:    https://rdap.arin.net/registry/entity/CLOUD146-ARIN

RNOCHandle: NOC11962-ARIN
RNOCName:   NOC
RNOCPhone:  +1-650-319-8930
RNOCEmail:  noc@cloudflare.com
RNOCRef:    https://rdap.arin.net/registry/entity/NOC11962-ARIN

RAbuseHandle: ABUSE2916-ARIN
RAbuseName:   Abuse
RAbusePhone:  +1-650-319-8930
RAbuseEmail:  abuse@cloudflare.com
RAbuseRef:    https://rdap.arin.net/registry/entity/ABUSE2916-ARIN

RTechHandle: ADMIN2521-ARIN
RTechName:   Admin
RTechPhone:  +1-650-319-8930
RTechEmail:  rir@cloudflare.com
```

Grazie a maltego possiamo ottenere molte più informazioni sull'indirizzo vittima come eventuali sottodomini, server DNS, email, siti e numeri di telefono collegati alla fonte.



In questo caso abbiamo ottenuto, oltre alle informazioni di entità correlate al dominio, anche gli snapshot del sito, varie schede di rete connesse ed i servizi attivi sul sito.

Facendo una scansione più specifica possiamo notare anche tutte le mail e i nomi utente degli impiegati con ruolo superiore direttamente correlati al sito(admin)



In questa ultima evidenza notiamo invece tutti i server DNS, blocchi di network e le varie schede di rete