Un mistero di censura all'italiana

10503 siti oscurati senza un motivo chiaro

Marco d'Itri
<md@seeweb.it>
@rfc1036

Seeweb s.r.l.

TOP-IX Technical Meeting - 27 maggio 2014

Chi

Dramatis personae:

- **`w-11.th.seeweb.it`**: un server web per 10503 domini.
- **Seeweb**: i gestori di `w-11.th`.
- **Interoute**: un grande carrier europeo.
- **ISP A**: un ISP italiano cliente di Interoute.
- **Nucleo Speciale Frodi Tecnologiche**: un reparto della Guardia di Finanza, già noto come **GAT**.
- **Decreto di sequestro preventivo**: emesso dal Tribunale di Roma nell'ambito del P.P. 14265/14 contro ignoti.

Che cosa

```
srv:~# wget www.telemestrino.it
--2014-05-20 17:34:56--  http://www.telemestrino.it/
Risoluzione di www.telemestrino.it (www.telemestrino.it)...
  217.64.195.204, 2001:4b78:1001::1101
Connessione a www.telemestrino.it↩
  (www.telemestrino.it)|217.64.195.204|:80... connesso.
Richiesta HTTP inviata, in attesa di risposta... 302 Found
Posizione: http://83.103.74.20/ [segue]
--2014-05-20 17:34:57--  http://83.103.74.20/
Connessione a 83.103.74.20:80... connesso.
Richiesta HTTP inviata, in attesa di risposta... 200 OK
Lunghezza: 94 [text/html]
Salvataggio in: "index.html"
2014-05-20 17:34:57 (15,6 MB/s) - "index.html" salvato [94/
```

217.64.195.204 = w-11.th.seeweb.it

83.103.74.20 = web.gat.gdf.it

seeweb

Quando

Cronologia dei fatti accertati:

- **18 aprile**: il GAT invia a diversi ISP, tra cui Seeweb e Interoute, un decreto di sequestro preventivo riguardante 38 siti stranieri.
- **20 maggio**: ISP A contatta Seeweb segnalando problemi nel raggiungere alcuni siti su un server del loro cliente Tophost.
- **20 maggio**: Seeweb determina che qualcuno tra loro e l'ISP A sta intercettando il traffico diretto a questo server.
- **20-21 maggio**: ISP A fornisce indicazioni secondo cui Interoute sta intercettando il traffico diretto a un certo IP di Seeweb.
- **21 maggio**: Seeweb chiede informazioni a riguardo a Interoute.
- **26 maggio**: dopo diversi solleciti, Interoute rifiuta di fornire qualsiasi informazione e suggerisce di contattare il GAT.
- **26 maggio**: il GAT conferma a Seeweb che il decreto non prevede di censurare alcun IP ma solo domini.

Prova numero 1

```
srv:~# tcptraceroute www.telemestrino.it
traceroute to www.telemestrino.it (217.64.195.204),↩
    30 hops max, 60 byte packets
 1  (omissis) 0.150 ms  0.123 ms  0.113 ms
 2  (omissis) 3.492 ms  3.532 ms  3.551 ms
 3  (omissis) 0.586 ms  0.611 ms  0.603 ms
 4  (omissis) 11.917 ms  12.024 ms  12.015 ms
 5  Gi0-2-249.mil-cal-access-2.interoute.net↩
    (195.81.190.105)  24.889 ms  24.887 ms  24.913 ms
 6  Gi0-1.mil-cal-access-5.interoute.net↩
    (212.23.41.14)  25.086 ms  24.929 ms  25.100 ms
 7  w-11.th.seeweb.it (217.64.195.204) <syn,ack>↩
    41.354 ms  41.495 ms  41.463 ms
```

seeweb

Prova numero 2

```
> show route protocol bgp 217.64.195.204 extensive hidden
inet.0: 492798 destinations, 2044991 routes (492737 active,
0 holddown, 214 hidden)
217.64.195.204/32 (1 entry, 0 announced)
     BGP                    /-101
         Next hop type: Router, Next hop index: 701
         Next-hop reference count: 567757
         Source: 195.81.190.105
         Next hop: 195.81.190.105 via ge-0/0/4.0, selected
         State: <Hidden Ext>
         Local AS: ..... Peer AS:  8928
         Age: 3w1d 11:26:27       Metric: 10
         Task: BGP_8928.195.81.190.105+179
         AS path: 8928 I
         Localpref: 100
         Router ID: 212.23.38.218
```

Riassumendo...

Interoute genera questa route che intercetta il traffico per un IP di terzi e fa rispondere un proprio server, che reindirizza gli utenti a una pagina della Guardia di Finanza.

- Ma non arriva a tutti i clienti.
- E non si vede nel loro looking glass.
- Rifiuta di giustificarla.
- Ma comunque ne riconosce l'esistenza.

A prima vista sembra un caso tipico di censura all'italiana, ma non è normale bloccare il traffico verso un IP italiano.

seeweb

Perché?

Interoute impedisce ad alcuni suoi clienti di raggiungere 10503 domini dei clienti di Tophost, e magari chissà quanti altri.

Interoute dice di contattare il GAT.

Il GAT dice di non avere mai chiesto di censurare questo IP.

Nessun magistrato italiano ha mai richiesto a ISP italiani di impedire l'accesso a siti su altre reti italiane.

Che fare?

seeweb

Domande?

`http://www.linux.it/~md/text/censura-interoute.pdf`

(Google . . . Marco d'Itri . . . I feel lucky)

CC BY SA

seeweb