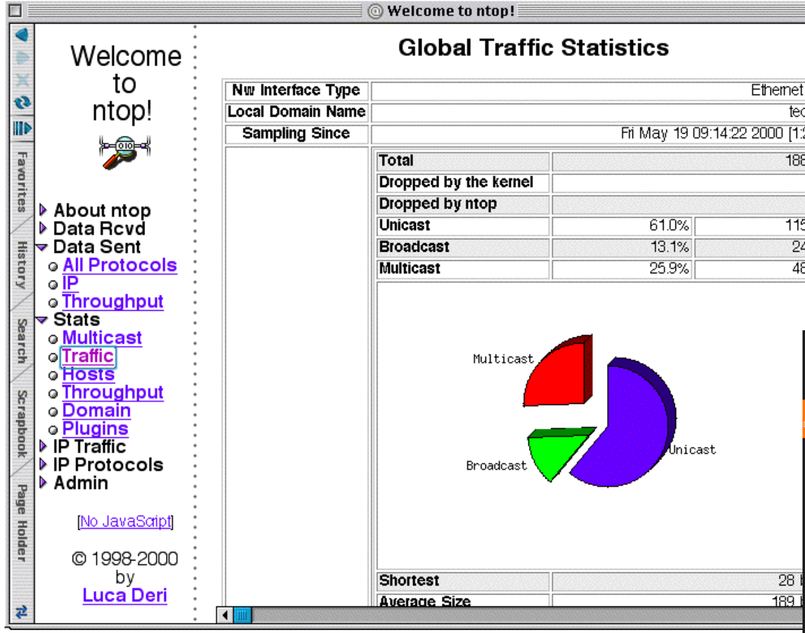
Network Visibility and Cybersecurity

Luca Deri <deri@ntop.org>
@lucaderi

20+ Years of OpenSource



Welcome to ntop!

Welcome to ntop!

- About ntop
- Data Rcvd
- Data Sent
  - All Protocols
  - IP
  - Throughput
- Stats
  - Multicast
  - Traffic
  - Hosts
  - Throughput
  - Domain
  - Plugins
- IP Traffic
- IP Protocols
- Admin

[No JavaScript]

© 1998-2000 by Luca Deri

Global Traffic Statistics

Nw Interface Type	Ethernet [eth0]
Local Domain Name	tecsiel.it
Sampling Since	Fri May 19 09:14:22 2000 [1:26:36]

Total		188,547
Dropped by the kernel		0
Dropped by ntop		0
Unicast	61.0%	115,090
Broadcast	13.1%	24,665
Multicast	25.9%	48,792

Shortest	28
Average Size	189

ntop for Wap

- Top Senders
- Top Receivers
- Stats

Options

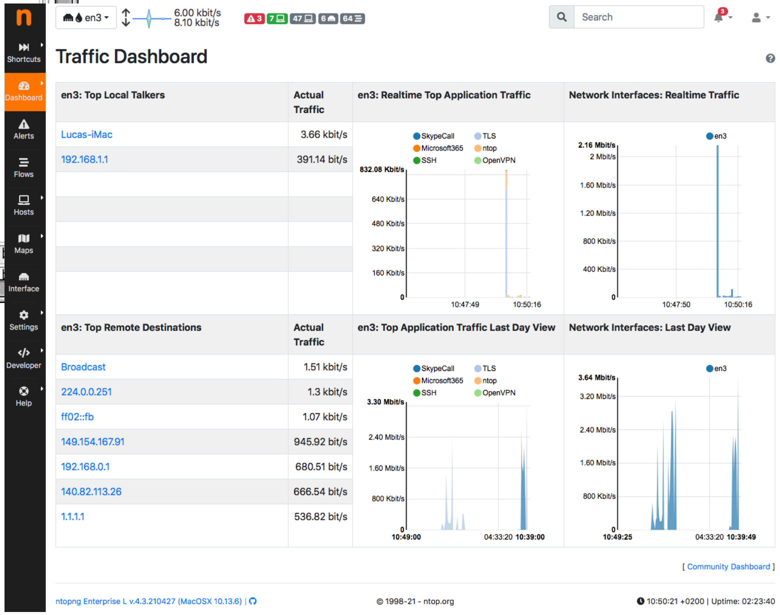
Top Senders

Host	Total
193.43.104	991.4

Options

Host 131.114.20.3

Name	ibook
Sent	312.5Kb



Traffic Dashboard

en3: Top Local Talkers	Actual Traffic
Lucas-iMac	3.66 kbit/s
192.168.1.1	391.14 bit/s

en3: Realtime Top Application Traffic

Network Interfaces: Realtime Traffic

en3: Top Remote Destinations	Actual Traffic
Broadcast	1.51 kbit/s
224.0.0.251	1.3 kbit/s
ff02::fb	1.07 kbit/s
149.154.167.91	945.92 bit/s
192.168.0.1	680.51 bit/s
140.82.113.26	666.54 bit/s
1.1.1.1	536.82 bit/s

en3: Top Application Traffic Last Day View

Network Interfaces: Last Day View

[Community Dashboard]

ntopng Enterprise L v.4.3.210427 (MacOSX 10.13.6) | © 1998-21 - ntop.org | 10:50:21 +0200 | Uptime: 02:23:40

Presentation Goals

- Show how open source software can monitor network traffic at high pace (10 Gbit+ using packets and commodity hardware,100 Gbit+ with hardware offload or NetFlow/sFlow) making it a mature technology.
- Demonstrate how cybersecurity threats can be detected without purchasing costly and closed-source software solutions.

20+ Years of Network Monitoring

- Increased speed:
  - 10Gbit is now commodity for companies.
  - 100 Gbit is standard for ISPs.
- Monitoring Protocols
  - Still NetFlow and sFlow, just at higher speed.
- Monitoring Metrics
  - Bytes and packets are still the main metrics for many network vendors.

Cybersecurity and Network Observability

- Observability: The ability to ask any question about your network, including security.
- Cybersecurity is an important piece of observability as this is unfortunately a popular topic in the news.
- Volumetric attacks (DDoS) and BGP traffic monitoring/hijacking are two hot topic for ISPs.
- We can safely assume that most (all ?) ISPs and and service providers already have mitigation solutions in place.

Cybersecurity and Network Edge

- As edge network speed is increasing, security threats on customer networks can propagate the issue to the core.
- Data centres with unhealthy customer traffic can affect neighbours and decrease the whole network reputation score.
- Limiting traffic observability to customer bandwidth usage is no longer wise: it is time to monitor customer traffic in an unobtrusive way in order to report users threats they have not detected, mitigate issues (as you do with DDoS) and implement a healthier Internet.

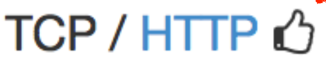
Welcome to nDPI

- In 2012 we decided to develop our own GNU LGPL DPI toolkit order to build an open source DPI layer.
- Protocols supported exceed 250+ and include:
  - P2P (BitTorrent)
  - Messaging (Viber, Whatsapp, Telegram, Facebook)
  - Multimedia (YouTube, Last.gm, iTunes)
  - Conferencing (Skype, Webex, Teams, Meet, Zoom)
  - Streaming (Zattoo, Disney, Netflix)
  - Business (VNC, RDP, Citrix)
  - Gaming

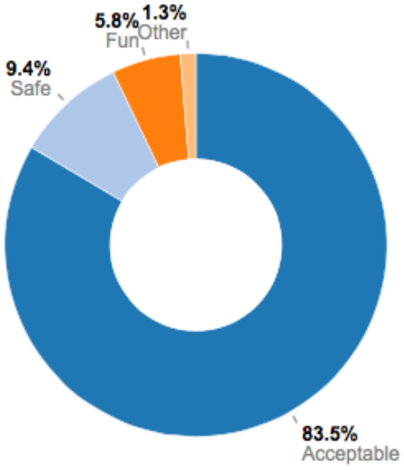
nDPI Traffic Analysis

Layer 4 Protocol

Good or Bad?



TCP / HTTP 👍



Layer 7 Protocol

nDPI in Cybersecurity

- Analyses encrypted traffic to detect issues hidden but un-inspectable payload content.
- Extracts metadata from selected protocols (e.g. DNS, HTTP, TLS..) and matches it against known algorithms for detecting selected threats (e.g. DGA hosts, Domain Generated Algorithm).
- Associates a “**risk**” with specific flows to identify communications that are affected by security issues.

nDPI: Flow Risks

- HTTP suspicious user-agent
- HTTP numeric IP host contacted
- HTTP suspicious URL
- HTTP suspicious protocol header
- TLS connections not carrying HTTPS (e.g. a VPN over TLS)
- Suspicious DGA domain contacted
- Malformed packet
- SSH/SMB obsolete protocol or application version
- TLS suspicious ESNI usage
- Unsafe Protocol used
- Suspicious DNS traffic
- TLS with no SNI
- XSS (Cross Site Scripting)
- SQL Injection

- Arbitrary Code Injection/Execution
- Binary/.exe application transfer (e.g. in HTTP)
- Known protocol on non standard port
- TLS self-signed certificate
- TLS obsolete version
- TLS weak cipher
- TLS certificate expired
- TLS certificate mismatch
- DNS suspicious traffic
- HTTP suspicious content
- Risky ASN
- Risky Domain Name
- Malicious JA3 Fingerprint
- Malicious SHA1 Certificate
- Desktop of File Sharing Session
- TLS Uncommon ALPN

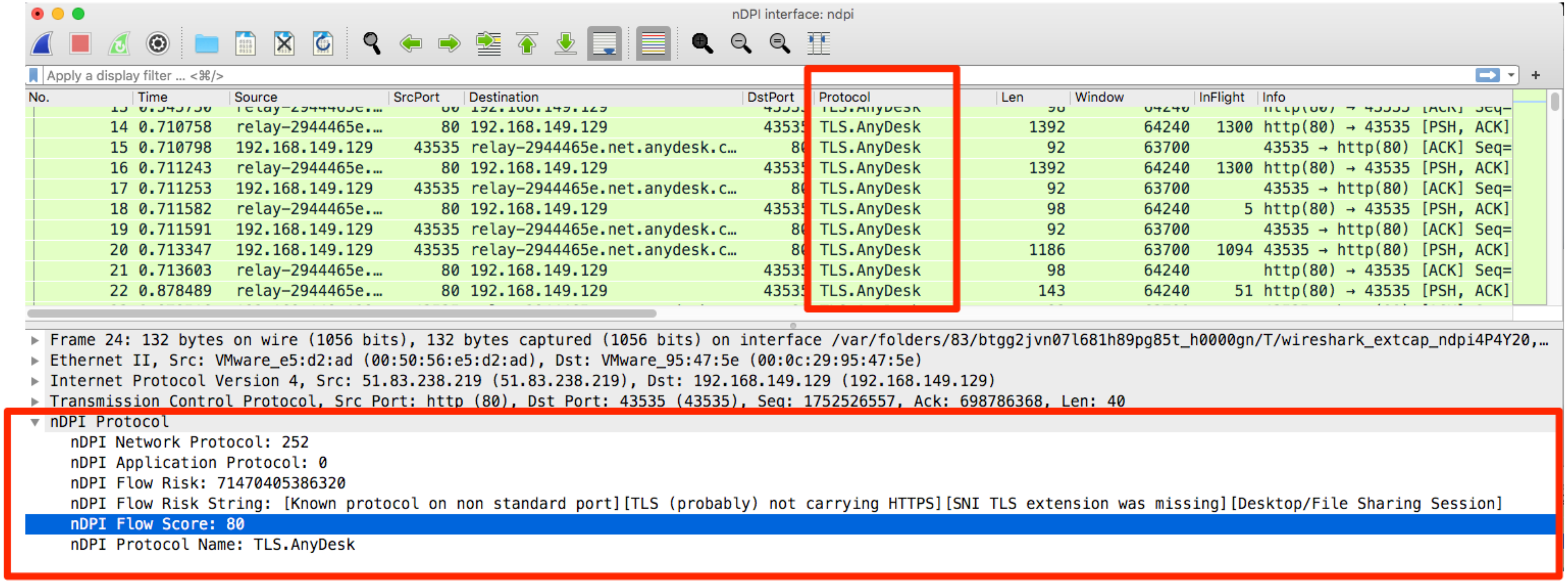
nDPI Encrypted Traffic Analysis

```
TCP 10.9.25.101:49184 <-> 187.58.56.26:449 [byte_dist_mean: 124.148883][byte_dist_std:
58.169660][entropy: 5.892724][total_entropy: 7124.302784][score: 0.9973][proto: 91/TLS]
[cat: Web/5][97 pkts/36053 bytes <-> 159 pkts/149429 bytes][Goodput ratio: 85/94][111.31
sec][bytes ratio: -0.611 (Download)][IAT c2s/s2c min/avg/max/stddev: 0/0 1129/662
19127/19233 2990/2294][Pkt Len c2s/s2c min/avg/max/stddev: 54/54 372/940 1514/1514
530/631][Risk: ** Self-signed Certificate **** Obsolete TLS version (< 1.1) **][TLSv1]
[JA3S: 623de93db17d313345d7ea481e7443cf][Issuer: C=AU, ST=Some-State, O=Internet Widgits
Pty Ltd][Subject: C=AU, ST=Some-State, O=Internet Widgits Pty Ltd][Certificate SHA-1:
DD:EB:4A:36:6A:2B:50:DA:5F:B5:DB:07:55:9A:92:B0:A3:52:5C:AD][Validity: 2019-07-23 10:32:39
- 2020-07-22 10:32:39][Cipher: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA]

TCP 10.9.25.101:49165 <-> 144.91.69.195:80 [byte_dist_mean: 95.694525][byte_dist_std:
25.418150][entropy: 0.000000][total_entropy: 0.000000][score: 0.9943][proto: 7/HTTP][cat:
Web/5][203 pkts/11127 bytes <-> 500 pkts/706336 bytes][Goodput ratio: 1/96][5.18 sec]
[Host: 144.91.69.195][bytes ratio: -0.969 (Download)][IAT c2s/s2c min/avg/max/stddev: 0/0
23/9 319/365 49/37][Pkt Len c2s/s2c min/avg/max/stddev: 54/54 55/1413 207/1514 11/134]
[URL: 144.91.69.195/solar.php[StatusCode: 200][ContentType: application/octet-stream]
[UserAgent: pwtyyEKzNtGatwnJjmCcBLb0veCVpc][Risk: ** Binary application transfer **][PLAIN
TEXT (GET /solar.php HTTP/1.1)]
```

Trickbot Traffic

nDPI in Wireshark



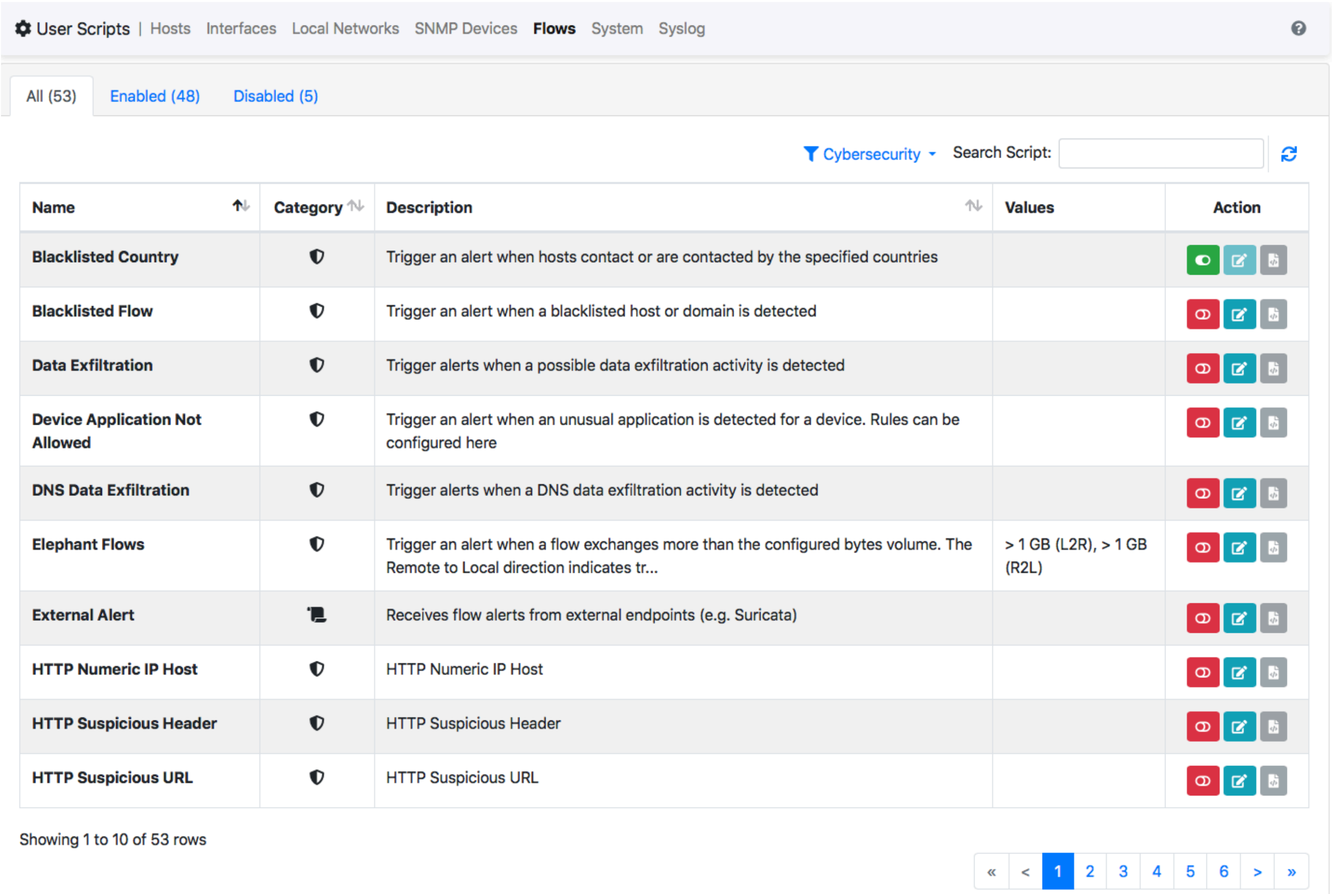
No.	Time	Source	SrcPort	Destination	DstPort	Protocol	Len	Window	InFlight	Info
14	0.710758	relay-2944465e.…	80	192.168.149.129	43535	TLS.AnyDesk	1392	64240	1300	http(80) → 43535 [PSH, ACK]
15	0.710798	192.168.149.129	43535	relay-2944465e.net.anydesk.c…	80	TLS.AnyDesk	92	63700		43535 → http(80) [ACK] Seq=
16	0.711243	relay-2944465e.…	80	192.168.149.129	43535	TLS.AnyDesk	1392	64240	1300	http(80) → 43535 [PSH, ACK]
17	0.711253	192.168.149.129	43535	relay-2944465e.net.anydesk.c…	80	TLS.AnyDesk	92	63700		43535 → http(80) [ACK] Seq=
18	0.711582	relay-2944465e.…	80	192.168.149.129	43535	TLS.AnyDesk	98	64240	5	http(80) → 43535 [PSH, ACK]
19	0.711591	192.168.149.129	43535	relay-2944465e.net.anydesk.c…	80	TLS.AnyDesk	92	63700		43535 → http(80) [ACK] Seq=
20	0.713347	192.168.149.129	43535	relay-2944465e.net.anydesk.c…	80	TLS.AnyDesk	1186	63700	1094	43535 → http(80) [PSH, ACK]
21	0.713603	relay-2944465e.…	80	192.168.149.129	43535	TLS.AnyDesk	98	64240		http(80) → 43535 [ACK] Seq=
22	0.878489	relay-2944465e.…	80	192.168.149.129	43535	TLS.AnyDesk	143	64240	51	http(80) → 43535 [PSH, ACK]

```
▶ Frame 24: 132 bytes on wire (1056 bits), 132 bytes captured (1056 bits) on interface /var/folders/83/btgg2jvn07l681h89pg85t_h0000gn/T/wireshark_extcap_ndpi4P4Y20,…
▶ Ethernet II, Src: VMware_e5:d2:ad (00:50:56:e5:d2:ad), Dst: VMware_95:47:5e (00:0c:29:95:47:5e)
▶ Internet Protocol Version 4, Src: 51.83.238.219 (51.83.238.219), Dst: 192.168.149.129 (192.168.149.129)
▶ Transmission Control Protocol, Src Port: http (80), Dst Port: 43535 (43535), Seq: 1752526557, Ack: 698786368, Len: 40
▼ nDPI Protocol
    nDPI Network Protocol: 252
    nDPI Application Protocol: 0
    nDPI Flow Risk: 71470405386320
    nDPI Flow Risk String: [Known protocol on non standard port][TLS (probably) not carrying HTTPS][SNI TLS extension was missing][Desktop/File Sharing Session]
    nDPI Flow Score: 80
    nDPI Protocol Name: TLS.AnyDesk
```

From Flow Risk To Score [1/2]

- Flow traffic analysis is too granular and it needs to be consolidated into:
  - Network Interface
  - Host/Network/Customer.
  - ASN/country
- In essence that is the pillar for creating a (client/server) numerical score that can be quickly used to spot issues (network, security…).

From Flow Risk To Score [2/2]

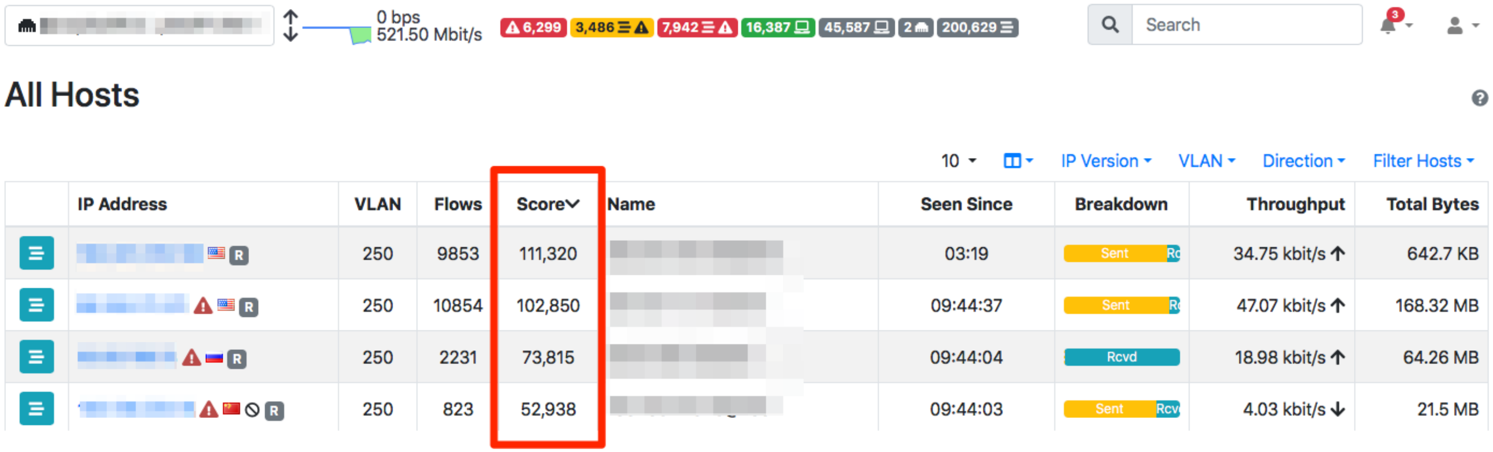


User Scripts | Hosts Interfaces Local Networks SNMP Devices Flows System Syslog
All (53) Enabled (48) Disabled (5)
Cybersecurity
Search Script:

Name	Category	Description	Values	Action
Blacklisted Country		Trigger an alert when hosts contact or are contacted by the specified countries		
Blacklisted Flow		Trigger an alert when a blacklisted host or domain is detected		
Data Exfiltration		Trigger alerts when a possible data exfiltration activity is detected		
Device Application Not Allowed		Trigger an alert when an unusual application is detected for a device. Rules can be configured here		
DNS Data Exfiltration		Trigger alerts when a DNS data exfiltration activity is detected		
Elephant Flows		Trigger an alert when a flow exchanges more than the configured bytes volume. The Remote to Local direction indicates tr...	> 1 GB (L2R), > 1 GB (R2L)	
External Alert		Receives flow alerts from external endpoints (e.g. Suricata)		
HTTP Numeric IP Host		HTTP Numeric IP Host		
HTTP Suspicious Header		HTTP Suspicious Header		
HTTP Suspicious URL		HTTP Suspicious URL		

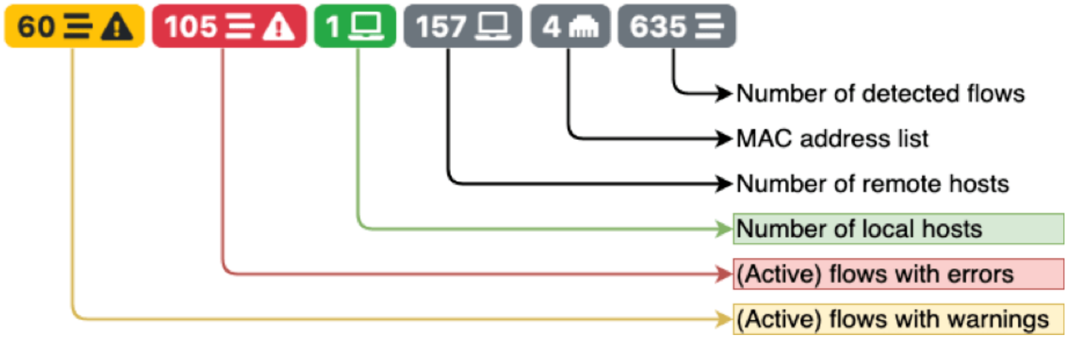
Showing 1 to 10 of 53 rows

Score At Work



All Hosts

	IP Address	VLAN	Flows	Score	Name	Seen Since	Breakdown	Throughput	Total Bytes
☰	[redacted] R	250	9853	111,320	[redacted]	03:19	Sent Rc	34.75 kbit/s ↑	642.7 KB
☰	[redacted] ⚠ R	250	10854	102,850	[redacted]	09:44:37	Sent R	47.07 kbit/s ↑	168.32 MB
☰	[redacted] ⚠ R	250	2231	73,815	[redacted]	09:44:04	Rcvd	18.98 kbit/s ↑	64.26 MB
☰	[redacted] ⚠ ⊘ R	250	823	52,938	[redacted]	09:44:03	Sent Rcv	4.03 kbit/s ↓	21.5 MB



Number of detected flows

MAC address list

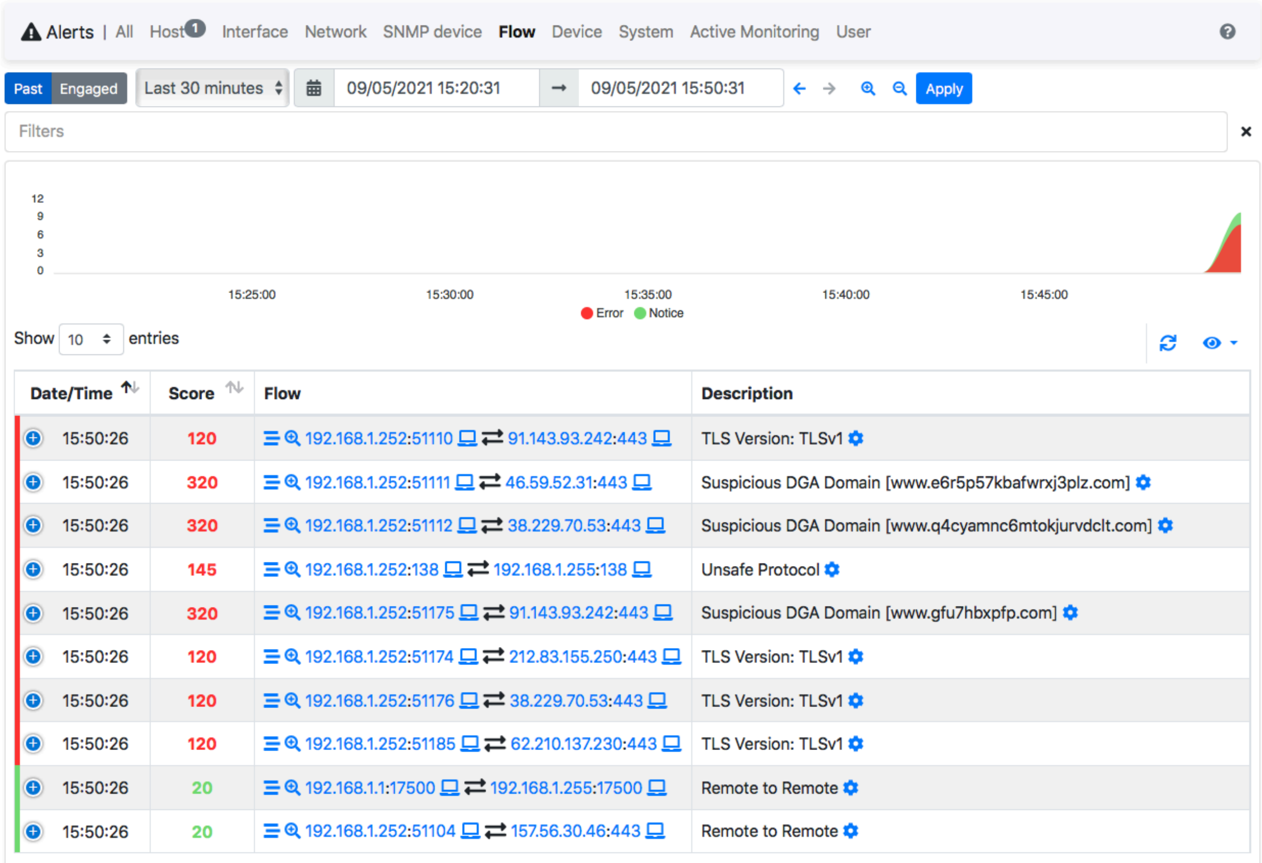
Number of remote hosts

Number of local hosts

(Active) flows with errors

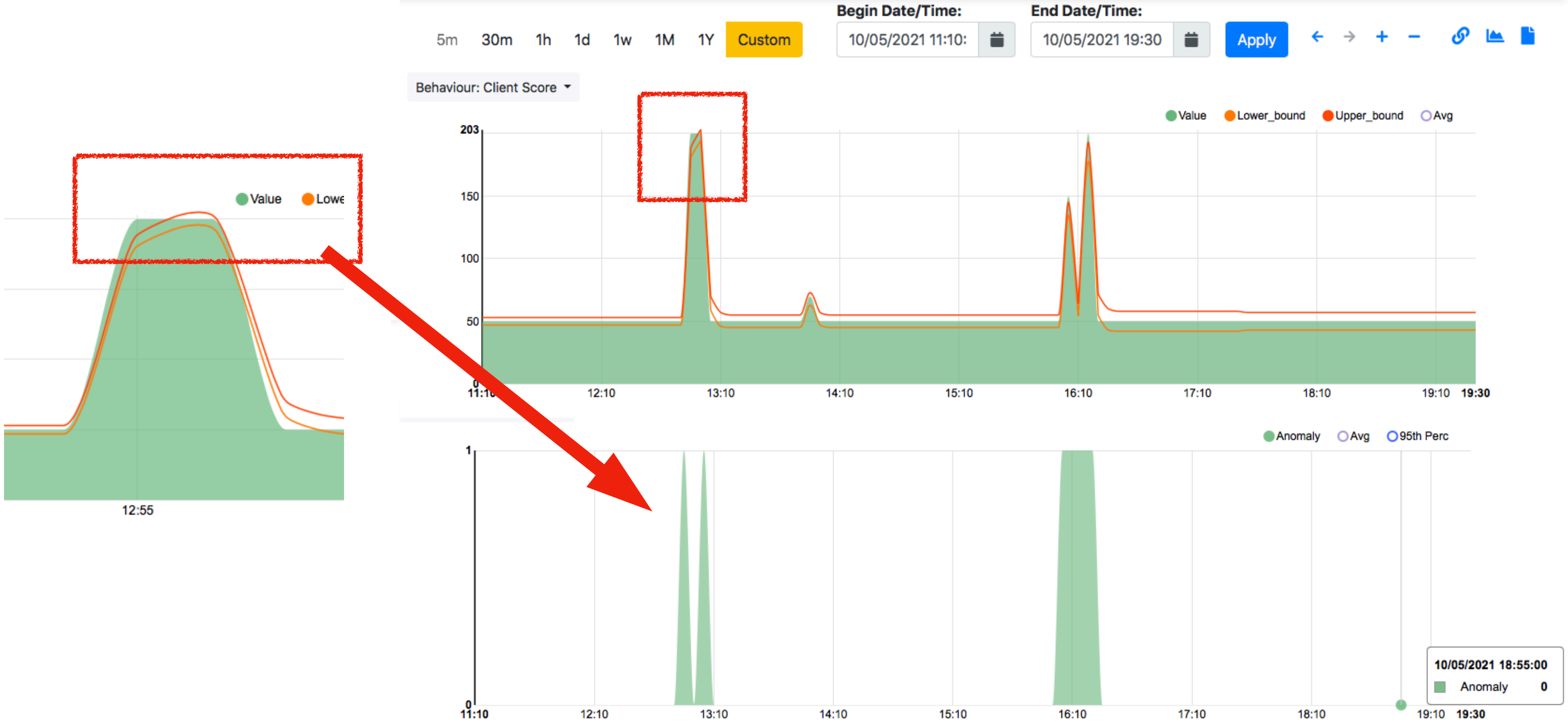
(Active) flows with warnings

Score-based Alerts



Date/Time	Score	Flow	Description
15:50:26	120	192.168.1.252:51110 ⇄ 91.143.93.242:443	TLS Version: TLSv1
15:50:26	320	192.168.1.252:51111 ⇄ 46.59.52.31:443	Suspicious DGA Domain [www.e6r5p57kbafwrxj3plz.com]
15:50:26	320	192.168.1.252:51112 ⇄ 38.229.70.53:443	Suspicious DGA Domain [www.q4cyamnc6mtokjurvdclt.com]
15:50:26	145	192.168.1.252:138 ⇄ 192.168.1.255:138	Unsafe Protocol
15:50:26	320	192.168.1.252:51175 ⇄ 91.143.93.242:443	Suspicious DGA Domain [www.gfu7hbxpfp.com]
15:50:26	120	192.168.1.252:51174 ⇄ 212.83.155.250:443	TLS Version: TLSv1
15:50:26	120	192.168.1.252:51176 ⇄ 38.229.70.53:443	TLS Version: TLSv1
15:50:26	120	192.168.1.252:51185 ⇄ 62.210.137.230:443	TLS Version: TLSv1
15:50:26	20	192.168.1.1:17500 ⇄ 192.168.1.255:17500	Remote to Remote
15:50:26	20	192.168.1.252:51104 ⇄ 157.56.30.46:443	Remote to Remote

Score-based Behaviour Analysis



Begin Date/Time: 10/05/2021 11:10:

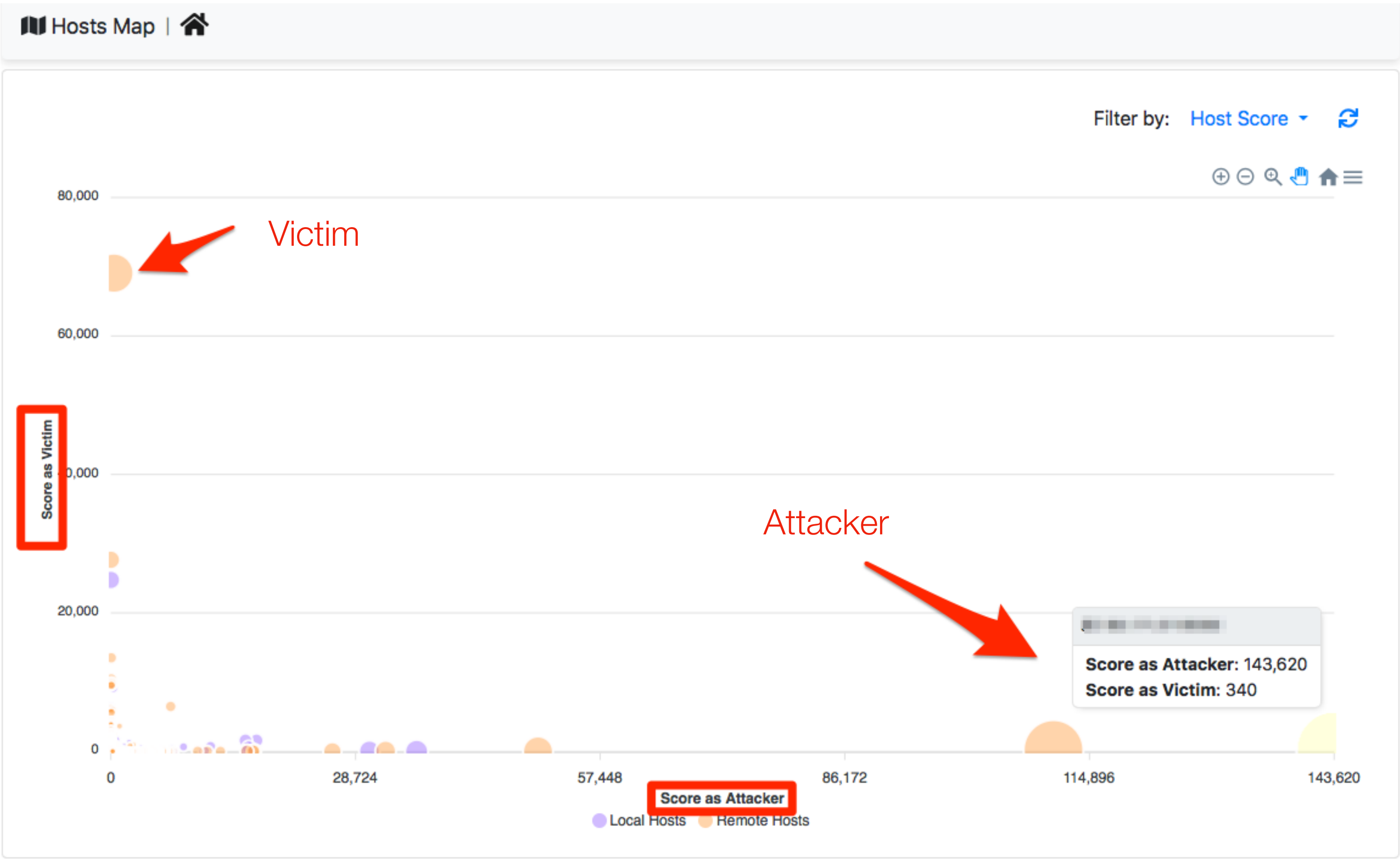
End Date/Time: 10/05/2021 19:30

Behaviour: Client Score

10/05/2021 18:55:00

Anomaly 0

Visualising Cybersecurity: Bubbles



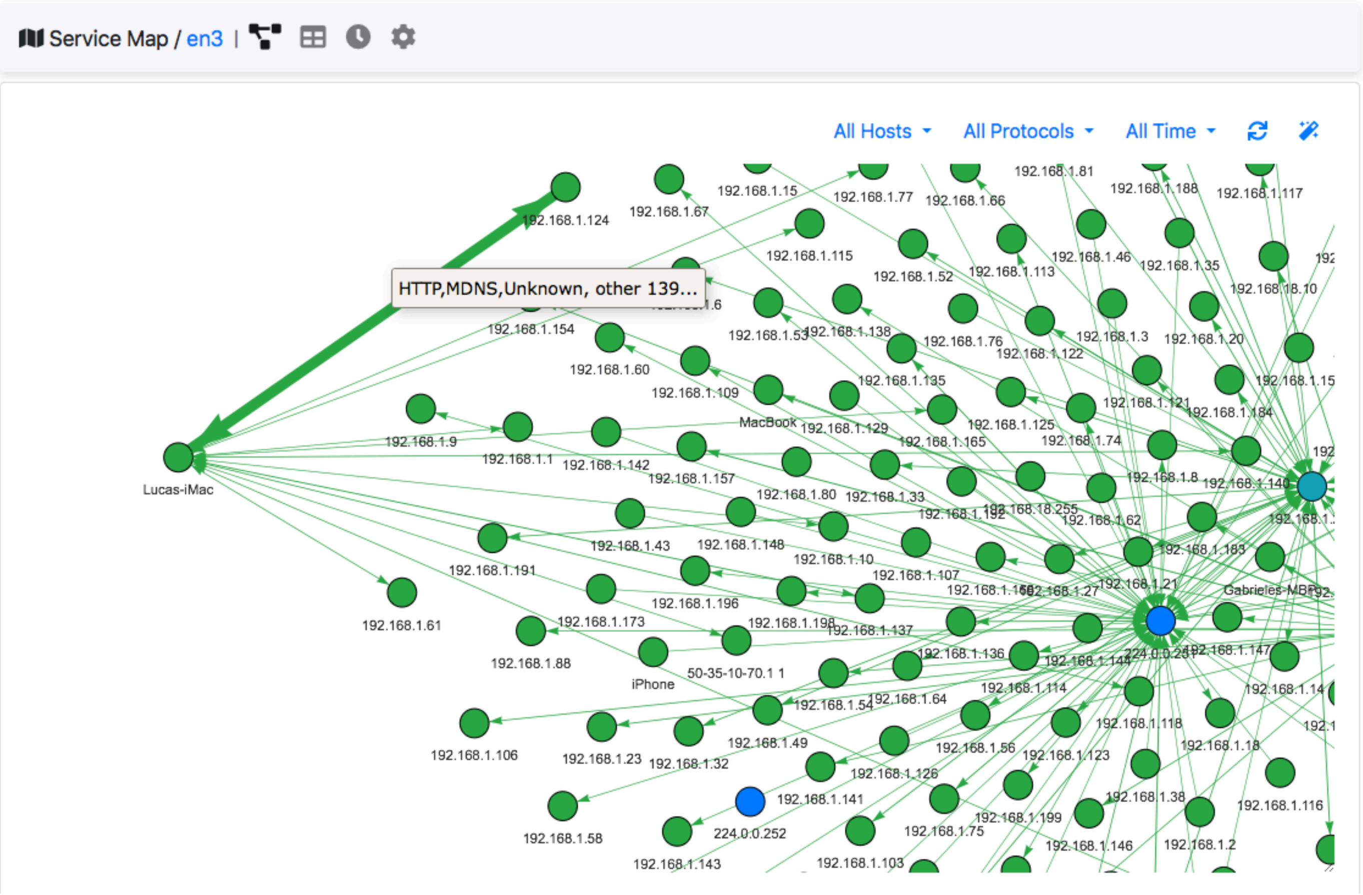
Victim

Attacker

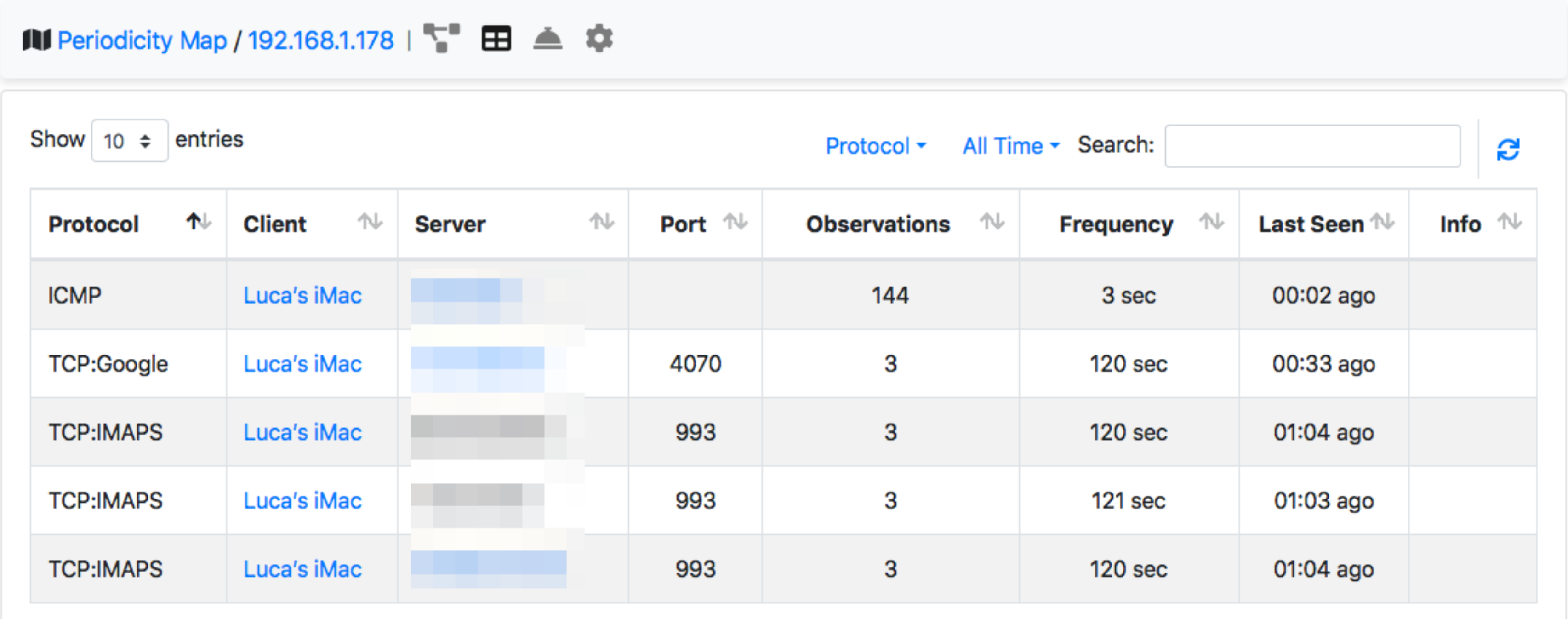
[redacted]

Score as Attacker: 143,620
Score as Victim: 340

Lateral Movement



Beaconing Detection



Periodicity Map / 192.168.1.178 |

Show 10 entries

Protocol ▾ All Time ▾ Search:

Protocol	Client	Server	Port	Observations	Frequency	Last Seen	Info
ICMP	Luca’s iMac	[redacted]		144	3 sec	00:02 ago	
TCP:Google	Luca’s iMac	[redacted]	4070	3	120 sec	00:33 ago	
TCP:IMAPS	Luca’s iMac	[redacted]	993	3	120 sec	01:04 ago	
TCP:IMAPS	Luca’s iMac	[redacted]	993	3	121 sec	01:03 ago	
TCP:IMAPS	Luca’s iMac	[redacted]	993	3	120 sec	01:04 ago	

From Software to Services

- Cybersecurity relies not just on traffic analysis but also on white-/black-lists (e.g. abuse.ch).
- What if all distributed network probe could report to a micro-MISP (per company, ISP or public) about public IP attackers with severe score and share this information (anonymously) for better security?
- Would you like to join this effort (verxo.it is the first one to participate) to make the Internet a better place?
  Please drop me a mail (deri@ntop.org) if interested.