Network Telescopes Revisited
From Loads of Unwanted Traffic to Threat Intelligence

Piotr Bazydło, Adrian Korczak, Paweł Pawliński

Research and Academic Computer Network
(NASK, Poland)
Who are we

**Piotr Bazydło**
Head of Network Security Methods Team NASK
@chudyPB
piotr.bazydlo@nask.pl

**Adrian Korczak**
Network Security Methods Team NASK
adrian.korczak@nask.pl

**Paweł Pawliński**
CERT Polska
pawel.pawlinski@cert.pl
Network Telescope

• Also known as **darknet** or blackhole.

• Unused IP address space.

• No legitimate network traffic should be observed.

• First (?) & largest telescope (approx /8): **caida**
Network Telescope

In practice, we can see a lot of different activities:

- Misconfiguration of network devices/applications.
- Scanning.
- Backscatter from DoS attacks.
- Exploitation attempts (UDP).
- Weird stuff.
DoS attacks (backscatter)
What we want to achieve?

• Detect large-scale malicious events (botnets, exploits).
• Detect attacks on interesting targets.
• Track activities of specific actors responsible.
• Understand the dynamics (trends).
Problems

• How to group packets?
• How to classify them into events?
• How to find interesting events?
• How to identify actors?
• How to analyze trends?
Our approach

1. Monitored IPv4 space: > 100,000 addresses
2. Analyze captured traffic every 5 minutes.

Stats:

~ 10,000 pps
~ 25,000,000,000 packets per month
80% = TCP
Two parsing scripts:

- **Parser L4** – up to 4\textsuperscript{th} OSI layer. written in C++, uses libtins library.

- **Parser L7** – parsing of 7\textsuperscript{th} OSI layer. written in python, uses dpkt library.
Traffic going to network telescope

Parser up to L4

Parser L7

Initial aggregation

Aggregator 1

Aggregator ...

Aggregator N

Redis
Traffic going to network telescope

Parser up to L4

Parser L7

Initial aggregation

Aggregator 1
Aggregator ...
Aggregator N

Analysis

Analyzer TCP
Analyzer UDP
Analyzer DNS
Analyzer amplifiers
Analyzer ...
Analyzer SIP

Redis
Traffic going to network telescope

Parser up to L4 → Parser L7

Initial aggregation
- Aggregator 1
- Aggregator ...
- Aggregator N

Analysis
- Analyzer TCP
- Analyzer UDP
- Analyzer DNS
- Analyzer amplifiers
- Analyzer ...
- Analyzer SIP

Elastic Search

Redis
Case study 1
Botnet Fingerprinting
Botnet fingerprinting
Botnet fingerprinting

Do you see port 8080 scan going up sharply as of now? Satori is coming back with a new variant, will provide more detail tonight (tomorrow morning Beijing time)
Botnet fingerprinting

In total, about 45,000 unique IP addresses were identified.

Distribution of source IPs

- Vietnam: 24,830
- China: 3,540
- Korea, Republic of: 3,186
- Thailand: 2,728
- Japan: 1,467
- Mexico: 1,189
- United States: 936
- Hong Kong: 670
- Russian Federation: 621
- Ireland: 578
Case study 2
Memcached
Memcached
UDP SCANS ON PORT 11211

Github 1.3 Tbps DoS
Reported 1.7 Tbps DoS

Packet Count
0 1M 2M 3M 4M 5M 6M 7M 8M
Day 1 – 20.02 (first scan)

- Only 4 IP addresses
- Source: DigitalOcean, UK
- Duration: 25 minutes
- Constant source port per source IP
- One payload used (memcached statistics)
Day 5 – 24.02 (new actor)

• Only 1 IP addresses
• Source: AS 27176, DataWagon LLC, US
• Small hosting with anti-DDoS
• Randomized source ports
• New payload
• Scan lasted longer: 3 hours
And so on… Pre-GitHub scanners

■ About 60 IP addresses.
■ Several scanning patterns.
And so on… Post-GitHub scanners

Distribution of source IPs

- About 315 IP addresses.
- Multiple scanning patterns.
Looking deeper into packets
PGA

• PGA = custom code to generate packets

• Usually simple operations, examples
  • constant values
  • byte swap
  • incrementation

• Leaves patterns that can be used for IDS

• Our tool detects patterns and creates new signatures
PGA examples

1. Mirai:
   \[ TCP\_SEQ = IP\_DST \]

2. XoR.DDoS PGA:
   \[ IP\_ID = SPORT \]
   \[ TCP\_SEQ[1:2] = IP\_ID \]
### PGA Example

<table>
<thead>
<tr>
<th>IP SRC</th>
<th>IP DST</th>
<th>IP ID</th>
<th>SPORT</th>
<th>DPORT</th>
<th>DNS ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>6b d6</td>
<td>a1 c6</td>
<td>6b 4a</td>
<td>80 35</td>
<td>CF 6b</td>
<td>35</td>
</tr>
</tbody>
</table>
Signatures everywhere

SYN FLOOD on IP belonging to Google – full of PGA signatures.

PGA signatures detected during SYN FLOOD
Signatures everywhere

SYN FLOOD on IP belonging to Google – full of PGA signatures.

PGA signatures detected during SYN FLOOD

1. SPORT = TCP_SEQ[1:2]
2. TCP_SEQ[3:4] = 0xFFFF
3. SPORT = IP_SRC[3:4]
Operations
Operational value of network telescopes

- Raw output from analyzers is not actionable (too many events)
- **Scans** → abuse notifications (automated for high confidence events)
- **PGA fingerprinting** → Shadowserver remediation feeds
- **DoS attacks** → situational awareness & alerts
- Automated feeds provide limited “intelligence”
DoS backscatter for the Polish IPv4 space (color = PGA fingerprint)
Sharing threat information

- Automated distribution of abuse reports & IoCs
- Free
- > 100 active participating entities
- > 50 data sources
- Formats: JSON & CSV & more
Interested in getting the data?

- Network owners: send an email to n6@cert.pl to sign up
- Usually working with national CSIRTs
Aiming for actual intelligence

- In-depth analysis of events extracted from the traffic
  - insight into TTP
  - more difficult to automate
- Anomaly / trend detection:
  - forecast exploitation campaigns.
  - new campaigns
- Attribute activities to botnets / actors
Future plans

• Combine network telescopes with other data sources
  Honeypots, sandboxes, botnet tracking

• Research collaboration:
  Looking for help in linking PGA signatures to tools / malware
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 700176.

https://sissden.eu