The Void
A technical perspective to black-hole monitoring

CIRCL
Computer Incident
Response Center
Luxembourg

Alexandre Dulaunoy, CIRCL-

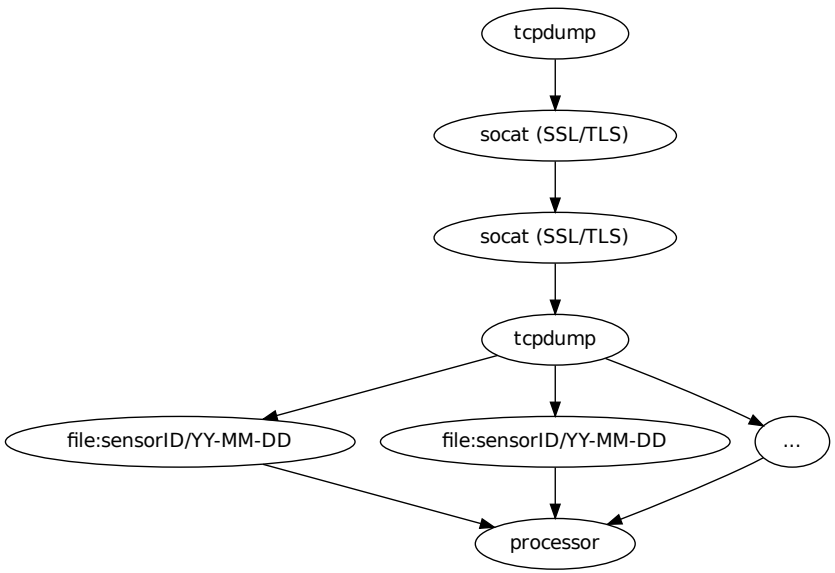
TLP:WHITE

info@circl.lu

19 November 2013 LORIA
Seminar

IP-Darkspace: Data Collection

Implementation



- Minimal sensor collecting IP-Darkspace networks (close to RFC1918 address space).
- Raw pcap are captured with the full payload.
- Netbeacon[a] developed to ensure consistent packet capture.

[a] `www.github.com/adulau/netbeacon/`

Challenges

- Erratic behavior of network packets captured.
- Peak usage can be huge (10 times bigger than baseline traffic is usual).
- Deviation is common and render traffic analysis more difficult.
- Reallocation of IPv4 subnet is regular and part of the difficulties in the analysis.

Data Storage (raw pcap)

```
circl@ccm:/sensors/chp-x-1/files/2013/11$ du -h
146M    ./01
138M    ./02
145M    ./03
166M    ./04
182M    ./05
177M    ./06
155M    ./07
163M    ./08
176M    ./09
142M    ./10
177M    ./11
170M    ./12
167M    ./13
174M    ./14
167M    ./15
144M    ./16
133M    ./17
158M    ./18
2.9G    .
```

Data Storage (raw pcap)

Files are stored in 5 minutes compressed pcap files:

```
circl@ccm:/sensors/chp-x-1/files/2013/11/18$ ls -1 | tail -n 4
chp-x-1-20131118222102.cap.gz
chp-x-1-20131118222602.cap.gz
chp-x-1-20131118223102.cap.gz
chp-x-1-20131118223602.cap.gz
```

Parallel processing of pcap files with tcpdump or other tools:

```
ls -1 | tail -n 4 | parallel "zcat {} | tcpdump -r - -n port 53"
22:45:57.005496 IP 184.65.36.185.32776 > A.B.100.1.53: 56718+ A? livezebra.
    zebralogic.ca.HPADOMAIN. (51)
22:45:57.058976 IP 91.54.224.11.56023 > A.B.100.1.53: 60602+ A? a26.ms.akamai.net.
    (35)
22:45:57.374134 IP 41.229.54.252.1025 > A.B.66.10.53: 45391+ A? dnl-09.geo.
    kaspersky.com. (42)
22:45:57.375793 IP 41.229.54.252.1025 > A.B.66.11.53: 45391+ A? dnl-09.geo.
    kaspersky.com. (42)
```

```
ls -1 | parallel "ipsumdump -t --payload-md5-hex -r {}"
```

Network Forensic Analysis Processing

- To allow concurrent processing, a non-blocking data store is required.
- To allow flexibility, a schema-free data store is required.
- To allow fast processing, you need to scale horizontally and to know the cost of querying the data store.
- To allow streaming processing, write/cost versus read/cost should be equivalent.

Redis key/value store provides a schema-free data store in memory for network forensic analysis[1].

[1] `http://www.foo.be/cours/dess-20112012/Redis-Introduction.pdf`

netbeacon - monitoring your network capture

netbeacon[2] is a set of free software tools to send beacons over the network to test the accuracy and the precision of your network capture framework.

- How long it takes for a packet to reach your monitoring.
- Time inconsistencies between devices.
- Finding missing packets or its (re)ordering.
- Watchdog to verify an operational network capture.

[2] `https://github.com/adulau/netbeacon/`

netbeacon - packet format

Netbeacon format (UDP):

```
header;epoch;sequence;hmac
nb;1354960619;101;335540bf3dae684c3d5cd5795fd09b9097bad656
nb;1354960619;102;56fc82c066644f179b58eb84a47e577bf92adc47
nb;1354960619;103;854207f54c1c4be97bdf4cd4a0d1068731848698
```

Sending 3 beacons to your sensor:

```
python nb_send.py -s -i 3 -d 1.2.3.4
```

Receiving beacons and verify them (sequence and time delta):

```
python nb_collect.py -i dag0 | python nb_verify.py -s -t
```