

New nDPI flow risks: Fragmented DNS traffic Large DNS packets (over 512 bytes)

Relazione di Debora Cerretini – A. A 2020/2021

nDPI and flow risks.

nDPI® is an open source LGPLv3 library for deep-packet inspection based on OpenDPI and it includes ntop extensions.

In nDPI flows can be inspected to find particular conditions needing attention, which are reported at the end of the analysis. These conditions are called “flow risks”. Every flow risk has a severity, which determines the reported risks order.

Fragmented DNS traffic.

It can be useful to detect flows with fragmented DNS traffic!

Like reported in <https://blog.powerdns.com/2018/09/10/spoofing-dns-with-fragments/>, fragmented DNS responses can be used for cache poisoning, so it is possible to spoof fake DNS responses using fragmented datagrams.

Large DNS packets (over 512 bytes).

There are problems with DNS resolvers that cannot receive large responses.

The maximum reply size between a DNS server and resolver may be limited by a number of factors, reported in <https://www.dns-oarc.net/oarc/services/replysizetest>. With the use of DNSSEC (DNS extensions that help providing security and reliability of information by DNS systems) this limit can be an issue.

Flow risk implementation.

To implement a flow risk, first the flow risk must be defined in these files:

- src/include/ndpi_typedefs.h (in ndpi_risk_enum)
- wireshark/ndpi.lua
- python/ndpi.py (in ndpi_risk_enum)
- src/lib/ndpi_main.c (in ndpi_known_risks)
- src/lib/ndpi_utils.c (in ndpi_risk2str)

In this case, I added two new definitions: NDPI_DNS_DIMENSION_ALERT e NDPI_DNS_FRAGMENTED. Then the protocol file related to the new flow risk must be updated with the risk test and call of the procedure ndpi_set_risk.

Flow risk testing.

I tested both flow risks with the file DNS-capture-FINAL.pcap that can be downloaded from <https://weberblog.net/dns-capture-udp-tcp-ip-fragmentation-edns-ecs-cookie/>.

The output is:

nDPI Memory statistics:

nDPI Memory (once):	221.05 KB
Flow Memory (per flow):	2.94 KB
Actual Memory:	2.14 MB
Peak Memory:	2.14 MB
Setup Time:	60 msec
Packet Processing Time:	20 msec

Traffic statistics:

Ethernet bytes:	23786	(includes ethernet CRC/IFC/trailer)
Discarded bytes:	872	
IP packets:	62	of 66 packets total
IP bytes:	22298	(avg pkt size 337 bytes)
Unique flows:	27	
TCP Packets:	20	
UDP Packets:	42	
VLAN Packets:	0	
MPLS Packets:	0	
PPPoE Packets:	0	
Fragmented Packets:	4	
Max Packet size:	1764	
Packet Len < 64:	28	
Packet Len 64-128:	18	
Packet Len 128-256:	4	
Packet Len 256-1024:	3	
Packet Len 1024-1500:	7	
Packet Len > 1500:	2	
nDPI throughput:	3.03 K pps / 8.87 Mb/sec	
Analysis begin:	27/May/2019 10:40:08	
Analysis end:	18/Jun/2019 10:58:36	
Traffic throughput:	0.00 pps / 0 b/sec	
Traffic duration:	1901908.500 sec	
Guessed flow protos:	7	

DPI Packets (TCP):	12	(6.00 pkts/flow)
DPI Packets (UDP):	42	(1.68 pkts/flow)

Detected protocols:

Unknown	packets: 3	bytes: 603	flows: 3
DNS	packets: 53	bytes: 16888	flows: 21
Google	packets: 6	bytes: 4807	flows: 3

Protocol statistics:

Acceptable	16888 bytes
Tracker/Ads	4807 bytes
Unrated	603 bytes

Risk stats [found 9 (33.3 %) flows with risks]:

DNS packet is larger than 512 bytes	9 [69.2 %]
DNS message is fragmented	4 [30.8 %]

NOTE: as one flow can have multiple risks set, the sum of the last column can exceed the number of flows with risks.

