New nDPI flow risk for TLS certificate validity length

Antonio Pace

A.A 2020/21

1 TLS certificate limit

Since 01/09/2020, the lifespan of new TLS certificates is limited to 13 months (398 days) from the previous lifespan of 27 months. After that, most popular browsers like Safari, Chrome and Firefox, started to reject certificates that expire in more than 13 months.

2 nDPI

nDPI is a open-source library for deep packet inspection based on OpenDPI.

2.1 Flow risk

Each flow analysed by nDPI has an associated numerical flow risk (score). Every risk has a severity, and every severity has a value, at this point the score can be calculated as the sum of each risk's value. It may be useful to add a new flow risk for the length of TLS certificates.

3 TLS flow risk implementation

3.1 New flow risk definition

Flow risks are defined in *ndpi_risk_enum* (*ndpi_typedefs.h*), so *NDPI_TLS_CERT_VALIDITY_TOO_LONG* has been added to the enum. After defining a flow risk, you need to update:

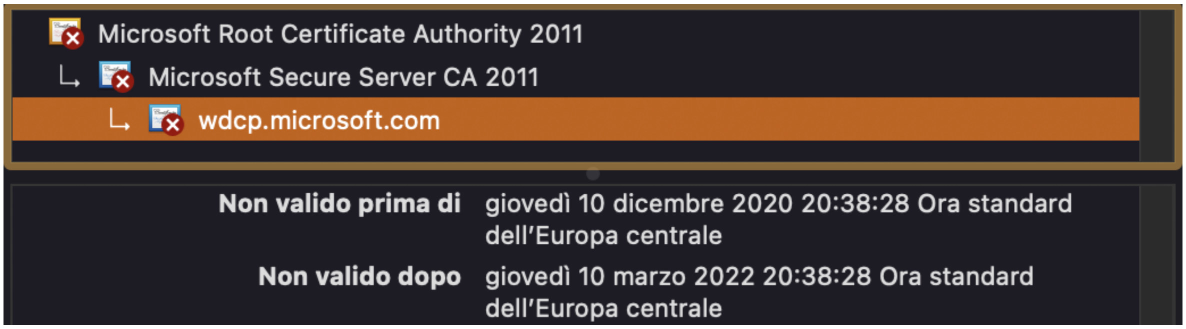
- ndpi.lua (script for whiteshark).
- ndpi_risk2str (textual description of the risk).
- ndpi_risk_enum (ndpi.py).
- ndpi_known_risk (risk's severity definition).

3.2 Update protocol file

Every protocol has a dedicated file under *src/lib/protocols*, so it's necessary to update *tls.c*. *processCertificateElements* dissects a TLS packet, extracting informations about the certificate. Checking the TLS certificate, if the lifespan is longer than 398 days (only for certificates issued after 01/09/2020), the new flow risk is set with *ndpi_set_risk*.

4 Testing

For reproducing the TLS certificate issue, it was made a capture with Wireshark by visiting https://wdcp.microsoft.com/.



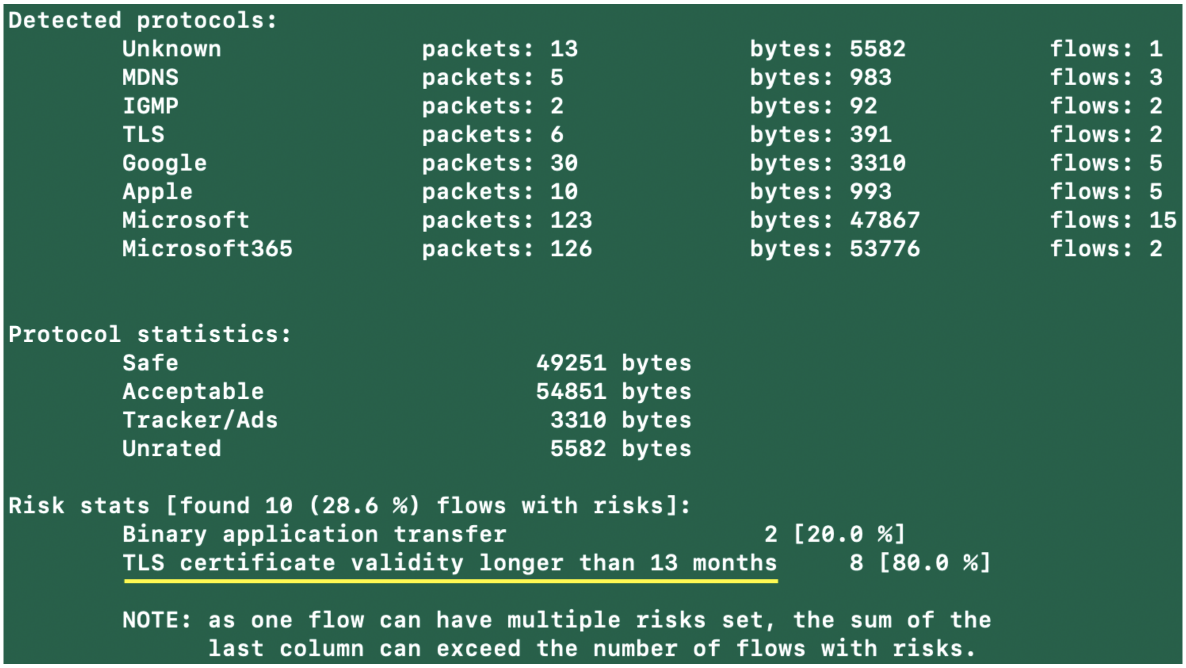
Microsoft Root Certificate Authority 2011
↳ Microsoft Secure Server CA 2011
↳ wdcp.microsoft.com

Non valido prima di giovedì 10 dicembre 2020 20:38:28 Ora standard dell'Europa centrale

Non valido dopo giovedì 10 marzo 2022 20:38:28 Ora standard dell'Europa centrale

Figure 1: https://wdcp.microsoft.com/ certificate (longer than 13 months)

The result below is obtained by analyzing the pcap file with ndpireader.



```
Detected protocols:
        Unknown              packets: 13            bytes: 5582          flows: 1
        MDNS                 packets: 5             bytes: 983           flows: 3
        IGMP                 packets: 2             bytes: 92            flows: 2
        TLS                  packets: 6             bytes: 391           flows: 2
        Google               packets: 30            bytes: 3310          flows: 5
        Apple                packets: 10            bytes: 993           flows: 5
        Microsoft            packets: 123           bytes: 47867         flows: 15
        Microsoft365         packets: 126           bytes: 53776         flows: 2


Protocol statistics:
        Safe                         49251 bytes
        Acceptable                   54851 bytes
        Tracker/Ads                   3310 bytes
        Unrated                       5582 bytes

Risk stats [found 10 (28.6 %) flows with risks]:
        Binary application transfer                  2 [20.0 %]
        TLS certificate validity longer than 13 months     8 [80.0 %]

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

Figure 2: Ndpireader output

nDPI has detected the new flow risk.