Trinity College Dublin
Coláiste na Tríonóide, Baile Átha Cliath
The University of Dublin

Localised Internet Scanning Infrastructure

Supervisor: Dr. Stephen Farrell

Jordan Myers

26/04/2019

Background
Internet Scanning

- Internet scanning uses:

  - System Administrators, Researchers, Commercial Entities:

    - Studying and analysing the Internet

    - Finding security & privacy issues

      - Vulnerabilities, protocol adoption, cipher suite usage

  - Attackers:

    - Vulnerable host detection

This Project

- Motivation:

  - Internet-wide scanning is widespread but more local scans could produce more actionable results using local knowledge and relationships with local asset-owners

- Goal:

  - Build an infrastructure to do such scans (overall project)

  - Create data store for scan data that supports easy data analysis and visualisation (my project)
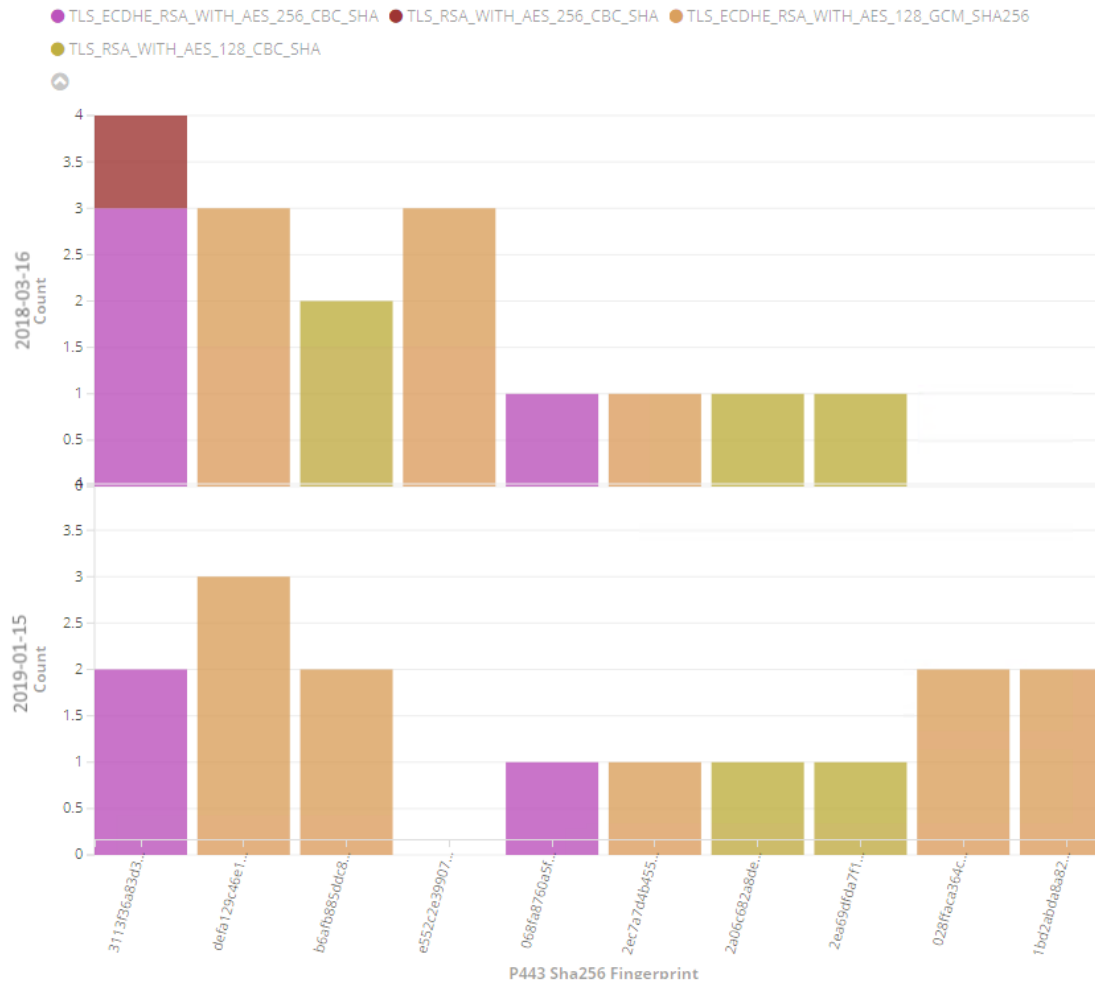
The Data

- Results from scanning hosts in a specific country that listen on port 25 (mail servers)

- Data collected for additional ports when the same host is used for multiple services

  - P22 (SSH)

  - P25 (SMTP)

  - P110 (POP3)

  - P143 (IMAP)

  - P443 (HTTPS)

  - P587 (SMTP)

  - P993 (IMAPS)

4

Results
Cipher Suites and Cryptographic Key Re-Use

AV P443 Sha256 Fingerprint, Cipher Suite

● TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA   ● TLS_RSA_WITH_AES_256_CBC_SHA   ● TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
● TLS_RSA_WITH_AES_128_CBC_SHA

Trinity College Dublin
Coláiste na Tríonóide, Baile Átha Cliath
The University of Dublin

Thank You