SNOWGLOBE:

From Discovery to Attribution

[redacted] 2011

Safeguarding Canada's security through information superiority
Préserver la sécurité du Canada par la supériorité de l'information

Canada

VICTIMOLOGY

Discovery
Development
Victimology
Attribution
SNOWGLOBE
Questions

Victimology: Iran

- Iranian MFA
- Iran University of Science and Technology
- Atomic Energy Organization of Iran
- Data Communications of Iran
- Iranian Research Organization for Science Technology, Imam Hussein University
- Malek-E-Ashtar University

Victimology: Global

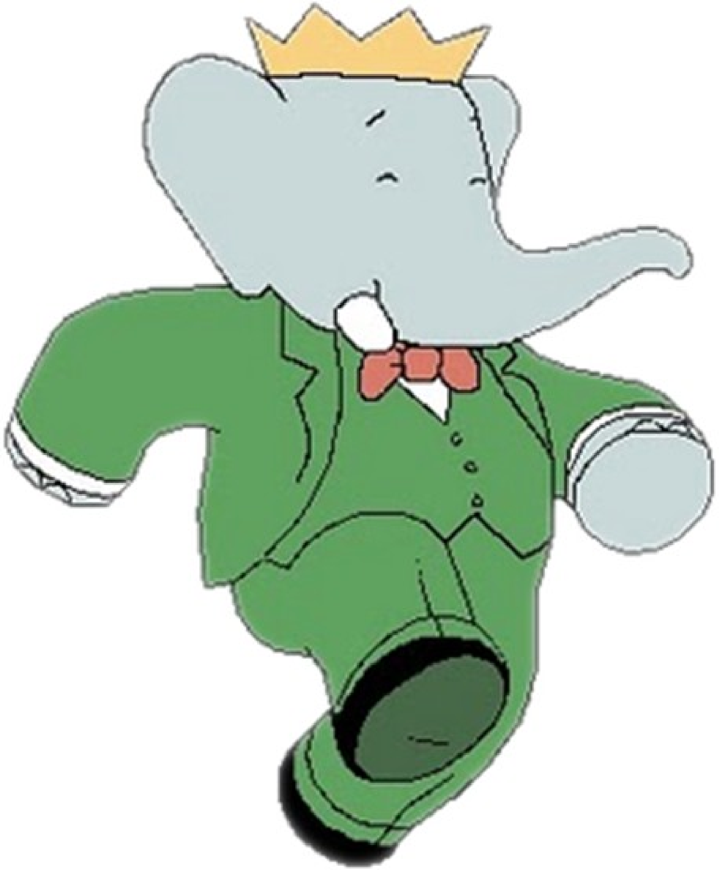
- Five Eyes
  - Possible targeting of a French-language Canadian media organization
- Europe
  - Greece
    - Possibly associated with European Financial Association
  - France
  - Norway
  - Spain
- Africa
  - Ivory Coast
  - Algeria

ATTRIBUTION

Discovery
Development
Victimology
Attribution
SNOWGLOBE
Questions

Attribution: Binary Artifacts

- ntrass.exe
  - DLL Loader uploaded to a victim as part of tasking seen in collection
  - Internal Name: Babar
  - Developer username: titi
- Babar is a popular French children's television show
- Titi is a French diminutive for Thiery, or a colloquial term for a small person



Attribution: Intelligence Priorities

- Iranian science and technology
  - Notably, the Atomic Energy Organization of Iran
  - Nuclear research
- European supranational organizations
  - European Financial Association
- Former French colonies
  - Algeria, Ivory Coast
- French-speaking organizations/areas
  - French-language media organization
- Doesn't fit cybercrime profile