Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

SNOWGLOBE:

From Discovery to Attribution

[redacted]2011[redacted]

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

Canada

VICTIMOLOGY

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

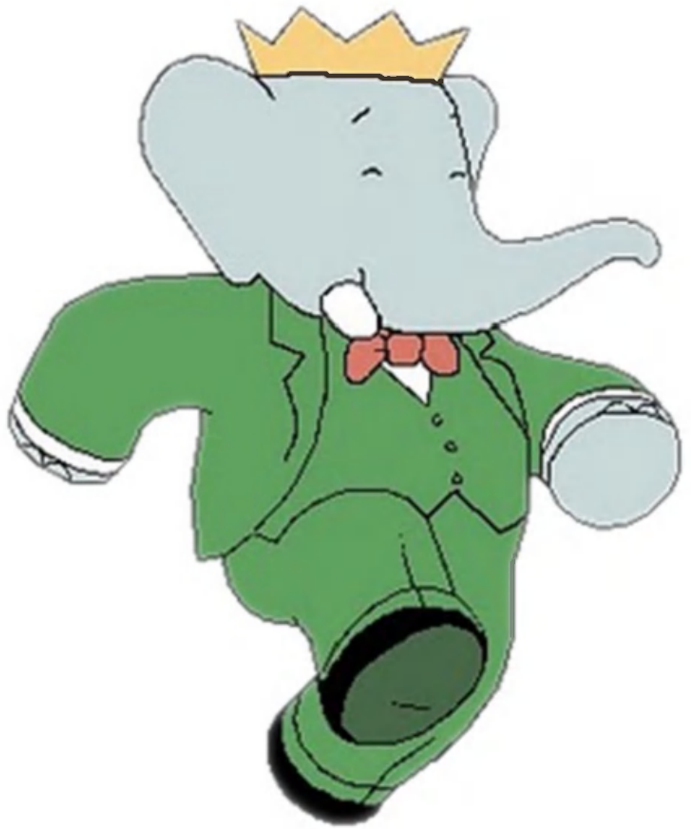
Victimology: Global

- 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

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

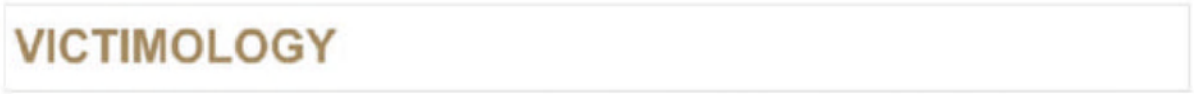
La traque de Babar

7 Pages - Contributed by Martin Untersinger , Le Monde - Mar 21, 2014

CSEC (p. 1)

Le CSEC est l'agence canadienne chargée des télécommunications, l'équivalent de la NSA.

Victimologie (p. 2)



Cette partie du document est dédiée aux victimes du programme informatique sur lequel s'est penché le CSEC.

Informations sensibles (p. 2)

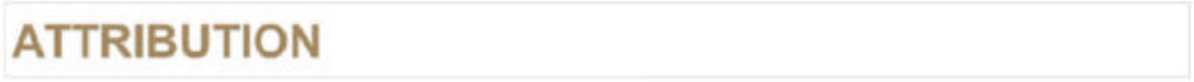
Nous avons choisi de ne publier qu'une partie du document sur lequel nous avons travaillé, ce dernier contenant des informations relatives à une opération de renseignement potentiellement encore en cours.

Ministère des affaires étrangères iranien (p. 3)

Medias canadiens (p. 4)

Des médias canadiens francophones pourraient faire partie des victimes du programme malveillant.

Attribution (p. 5)



Les pages qui suivent sont destinées à déterminer qui se cache derrière "Snowglobe".

DLL (p. 6)

Il s'agit ici d'un programme, une composante de "Snowglobe", conçu pour être inséré dans l'ordinateur de la cible.

Priorités (p. 7)

Attribution: Intelligence Priorities

Sur cette page, le CSEC résume les cibles de "Snowglobe" pour en faire apparaître les principales priorités.