Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

SNOWGLOBE:

From Discovery to Attribution

[redacted]
CSEC CNT / Cyber CI
SIGDEV 2011 Cyber Thread

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

Canada

OVERVIEW

Overview

- Discovery
- Development
- Victimology
- Attribution
- SNOWGLOBE.
- Questions and Comments

DISCOVERY

Discovery

- Discovered in November 2009
- Existing CNE Access
- WARRIORPRIDE as a sensor
  - REPLICANTFARM for anomaly detection
    - XML info from implant
    - Signature-based detection of anomalous activity and known techniques
    - Noticed: Command-line to create password protected RAR
      - Always the same password
- Retrieved files associated with activity
  - Identified unknown malware through reverse engineering
    - Collecting email from specific, targeted accounts
    - “Felt like” a FI-collecting tool
    - Pointed to first discovered LP
    - Provided intial comms analysis to allow signature deployment in passive collection

DEVELOPMENT

Implant

- SNOWBALLs
  - Found and identified wmimgmt.exe and wmimgmt.dll (later called the SNOWBALL implant).
  - Creates a service → loads wmimgmt.exe → injects wmimgmt.dll into IE.
  - Later upgraded SNOWBALL to SNOWBALL 2
    - Very similar beaconing.
- SNOWMAN
  - More sophisticated implant, discovered mid-2010
  - Less is known about SNOWMAN, but efforts against it continue.

SNOWBALL Beacons

Content	Meaning/decrypt
crc= 491ffa2e746f2452608578761f6fbe02	a 32-byte checksum
4293	beacon size in bytes
flag	Description field. Values can be: flag, segment, len
qKmP2amaqYHdl7GE99nZrY qjmpn9lb6346Kdp%2Fiw44 6rlKHkgpWjupDerZmyg5%2 FX7oWH3bfAmYvC1raLupS M%2BqGeuP%2BV4eDk%2 F4S%2Fi7mYzLuQr4fe552O gcWYrJiu2Iz6xO6uwqbbjou Z%2B9KlhNHAv5a1gd%2B plcW94N%2FiyuLfh%2FrMl Y3CsdyOi5CmuYm80YXz7 oKN1qbAgZqQlKqFoILTqN 7mgdW%2FxYGBwpP2j6 %2BUu9Ctg8jGoseeh9% 2BY4sqansyziKqJn%2FO b3c6YlbeHp5DCs4aqjYvn %2BL6n9dbuxOfKlo2NqN uC7rjnutmbvYWihYz61% 2FDYgO%2FYhICZ%2F% 2BzS58Get4W%2Bwb3N 84Scw4L4hraE2LmM%2F MiA8One3uzE6Nru0Yfo3v TRivSC4OT8l6ue953Xr4ql gJD9ldzf7MTotuXBhuPE99 iK9IfX2oL70qe4ldPgxJWN wrHcjouQ1qTK96PfvYyym 4rn9ImD2Zj4yqvRlo%2Blh dKQiZqs47q%2FnND3wY 7r3PLIkOeV	Login/Domain (owner): SYSTEM/AUTORITE NT (user) Computer name: EXPORT Organization (country): (France) OS version (SP): 5.1 (Service Pack 3) Default browser: iexplore.exe IE version: Mozilla/4.0 (compatible; MSIE 6.0; Win32) Timeout: 3600(min)4800(max) First launch: 07\30\2009 12:29:37 Last launch : 11\20\2009 10:32:42 Mode: Service | Rights: Admin | UAC: N/A ID: 08184

User-Agent: Mozilla/4.0 (compatible; MSI 6.0; Windows NT 5.1; .NET CLR 1.0.3705; .NET CLR 1.1.4322)

Passive Collection

- EONBLUE
  - Global Access capability deployed across collection programs, including SPECIALSOURCE and CANDLEGLOW (FORNSAT).
  - Provides passive cyber-threat detection.
  - Allowed us to find additional infrastructure by using signatures for known SNOWGLOBE beacons
- Traditional
  - As always, a huge asset
  - With passive access, we were able to see an operator log in to an LP
    - Single-token authentication + weak hash = breakthrough.
    - Seeing the operator log in provided enough to get into the LPs for ourselves.

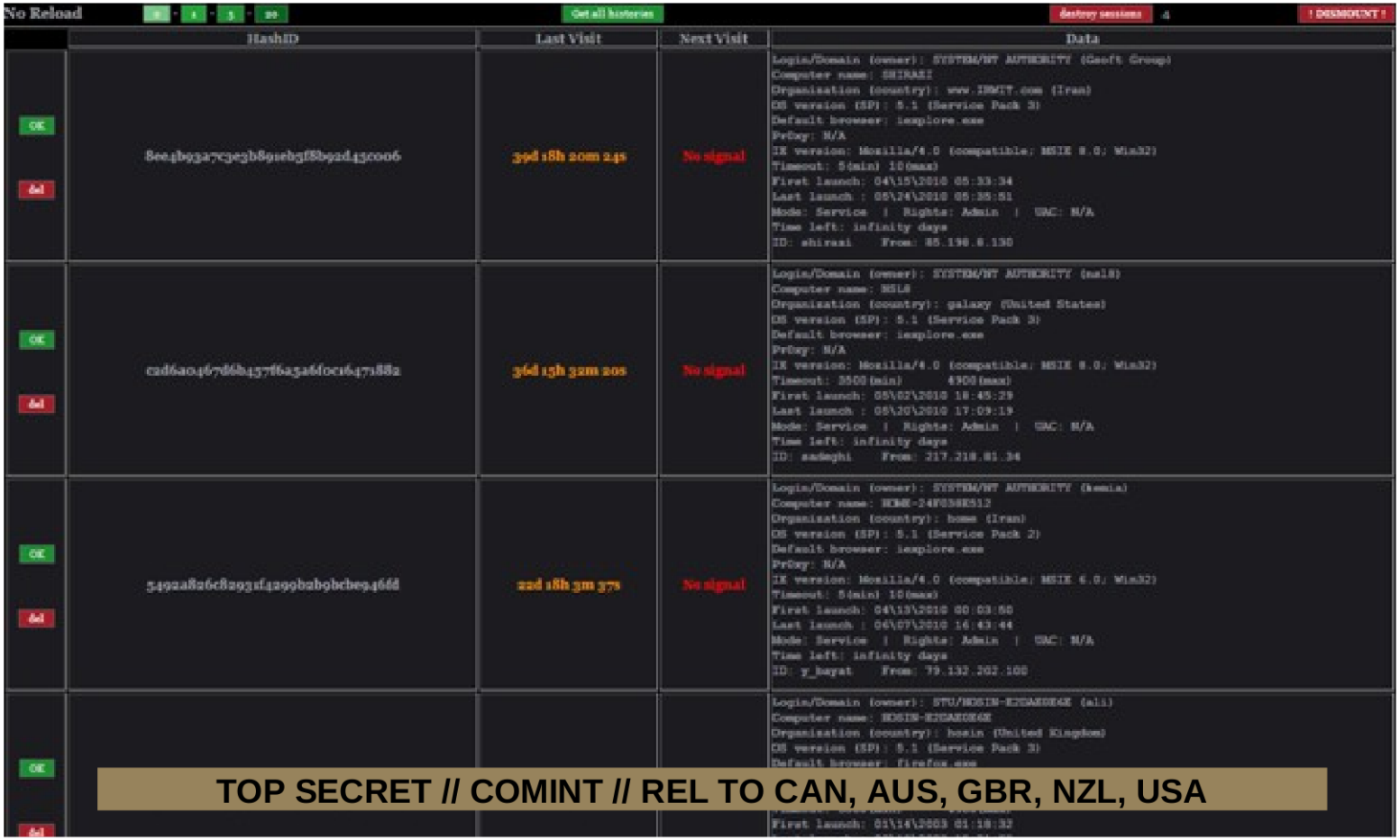
Infrastructure

- Most infrastructure hosted in FVEY nations
- US, Canada, UK, Czech Republic, Poland, Norway
- Two types of infrastructure:
  - Parasitic
    - outbase.php or register.php LP nested in a directory under root domain
    - Unsure if this infrastructure is acquired via exploitation, some sort of special-source access, or some combination of the two
    - This type seems to be found primarily, but not exclusively, on French-language sites
  - Free hosting
    - outbase.php or register.php LP directly under root

Infrastructure

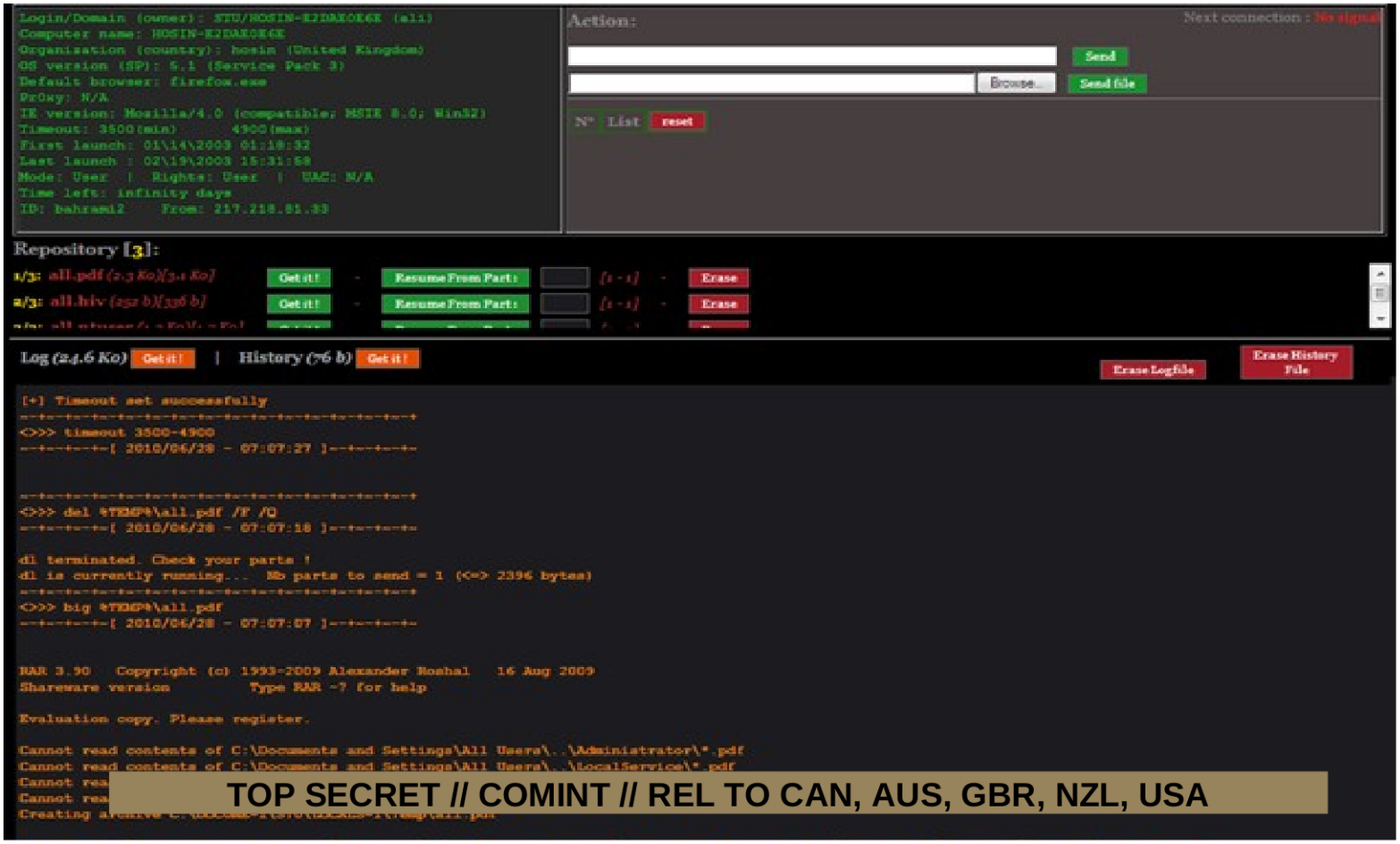
- Most infrastructure hosted in FVEY nations
- US, Canada, UK, Czech Republic, Poland, Norway
- Two types of infrastructure:
  - Parasitic
    - outbase.php or register.php LP nested in a directory under root domain
    - Unsure if this infrastructure is acquired via exploitation, some sort of special-source access, or some combination of the two
    - This type seems to be found primarily, but not exclusively, on French-language sites
  - Free hosting
    - outbase.php or register.php LP directly under root

Infrastructure: C2



TOP SECRET // COMINT // REL TO CAN, AUS, GBR, NZL, USA

Infrastructure: C2



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

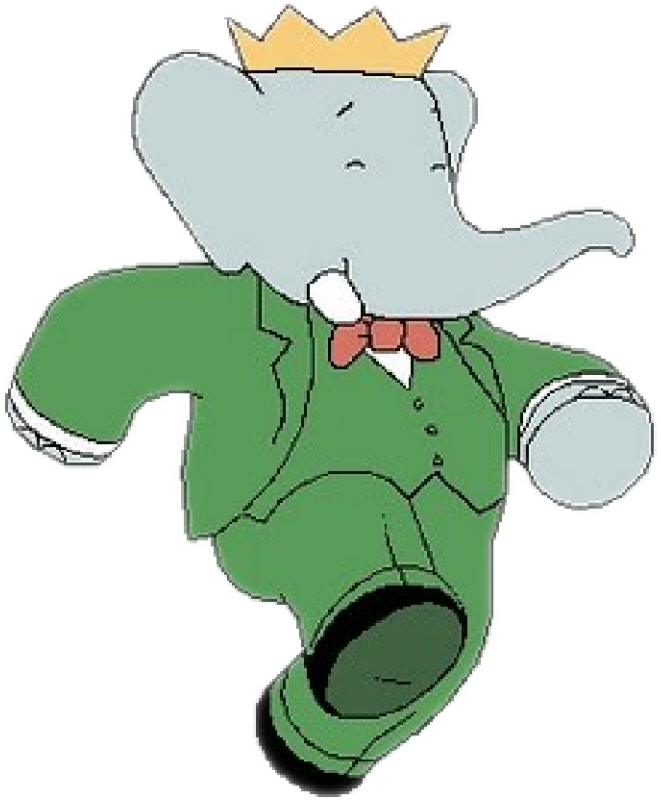
Victimology: Global

- 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

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: Language

- ko used instead of kB – a quirk of the French technical community
- English used throughout C2 interface, BUT phrasing and word choice are not typical of a native English speaker
  - An attempt at obfuscation?
- Locale option of artifact within spear-phishing attack set to "fr_FR"

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

SNOWGLOBE.

- Discovery
- Development
- Victimology
- Attribution
- SNOWGLOBE
- Questions

SNOWGLOBE.

- CSEC assesses, with moderate certainty, SNOWGLOBE to be a state-sponsored CNO effort, put forth by a French intelligence agency

SNOWGLOBE Program

- C2 nodes worldwide (including Canada, US, UK)
  - Free hosting
  - Compromised
- 3 implants
  - SNOWBALL 1
  - SNOWBALL 2
  - SNOWMAN
- Victims in Spain, Greece, Norway, France, Algeria, Cote d'Ivoire
  - Intense focus on Iranian science and technology organizations
- Likely French intelligence
  - Specific agency unknown

What We Don't Know

- Any persona details
- How they get their non-free LPs
  - Exploitation?
  - Special source?
- Last hop (operator to infrastructure)
  - Believed to be Tor-based…
- Which agency within the French intelligence community might be responsible
  - Who's driving the intelligence requirements
- Efforts against the SNOWMAN crypt continue

QUESTIONS AND COMMENTS

- Discovery
- Development
- Victimology
- Attribution
- SNOWGLOBE
- Questions