



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

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

Canada



Overview

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



DISCOVERY

Discovery

Development

Victimology

Attribution

SNOWGLOBE

Questions

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

Canada



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 initial comms analysis to allow signature deployment in passive collection



DEVELOPMENT

Discovery
Development
Victimology
Attribution
SNOWGLOBE
Questions

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

Canada



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

```

crc= 491ffa2e746f2452608578761f6fbe02
4293
flag
qKMnP2amaqYHdI7GE99nZrY qjmpn9lb6346Kdp%2Fiw44
6rlKHkgpWjupDerZmyg5%2 FX7oWH3bfAmYvC1raLupS
M%2BqGeuP%2BV4eDk%2 F4S%2Fi7mYzLuQrdfe552O
gcWYrJiu2Iz6xO6uwqbbjou Z%2B9KhNHAy5a1gd%2B
plcW94N%2FiyuLfh%2FrMI Y3CsdvOi5CmuYm80YXz7
oKN1qbAgZqQlKqFoILTqN 7mgdW%2FxYGBwpP2j6
%2BUu9Ctg8jGoseeh9% 2BY4sqansyziKqJn%2FO
b3c6YlbeHp5DCs4aqjYvn %2BL6n9dbuxOfKlo2NqN
uC7rjnutmbvYWihYz61% 2FDYgO%2FYhICZ%2F%
2BzS58Get4W%2Bwb3N 84Scw4L4hraE2LmM%2F
MiA8One3uzE6Nr0Yfo3v TRivSC4OT8l6ue953Xr4ql
gJD9ldzf7MTotuXBhuPE99 iK9IfX2oL70qe4ldPgxDWN
wrHcjouQ1qTK96PfvYym 4rn9ImD2Zj4yqvRlo%2Blh
dKQiZqs47q%2FnND3wY 7r3PLIkOeV

```



Meaning/decrypt

a 32-byte checksum
 beacon size in bytes
 Description field. Values can be: flag, segment, len

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

No	Reload	Get all histories	Delete sessions	DISMANTLE
	HashID	Last Visit	Next Visit	Data
	8ee4b93a7c3e3b89aeb9f8b9ad43cc006	36d 18h 20m 24s	No signal	Login/Domain (owner): SYSTEM/NT AUTHORITY (Guest Group) Computer name: SIRIUS Organization (country): www.IBMCT.com (Iran) OS version (SP): 5.1 (Service Pack 3) Default browser: iexplore.exe Proxy: N/A IE version: Mozilla/4.0 (compatible; MSIE 8.0; Windows 7) Timeout: 5min (10max) First launch: 04/15/2010 05:33:34 Last launch: 05/24/2010 05:38:59 Mode: Service + Rights: Admin + SAC: N/A Time left: infinity days ID: shirazi From: 85.196.6.190
	cdd6a04f7d6b437fb43ab0ca647188a	36d 19h 2am 20s	No signal	Login/Domain (owner): SYSTEM/NT AUTHORITY (Guest) Computer name: HELA Organization (country): galaxy (United States) OS version (SP): 5.1 (Service Pack 3) Default browser: iexplore.exe Proxy: N/A IE version: Mozilla/4.0 (compatible; MSIE 8.0; Windows 7) Timeout: 30min (4500max) First launch: 05/02/2010 18:49:29 Last launch: 05/20/2010 17:09:19 Mode: Service + Rights: Admin + SAC: N/A Time left: infinity days ID: sadeghi From: 217.218.81.34
	5499a806c893df4299bab9bcbef94688	ned 18h 3m 37s	No signal	Login/Domain (owner): SYSTEM/NT AUTHORITY (Guest) Computer name: HOM-24F05000013 Organization (country): home (Iran) OS version (SP): 5.1 (Service Pack 2) Default browser: iexplore.exe Proxy: N/A IE version: Mozilla/4.0 (compatible; MSIE 6.0; Windows 7) Timeout: 5min (10max) First launch: 04/19/2010 00:03:50 Last launch: 05/07/2010 16:43:44 Mode: Service + Rights: Admin + SAC: N/A Time left: infinity days ID: y_bayat From: 79.132.202.100
				Login/Domain (owner): STU/HOSTIN-E72A9E048 (all) Computer name: HOSTIN-E72A9E048 Organization (country): home (United Kingdom) OS version (SP): 5.1 (Service Pack 3) Default browser: Firefox.exe Proxy: N/A IE version: Mozilla/4.0 (compatible; MSIE 8.0; Windows 7) Timeout: 30min (4500max) First launch: 05/14/2010 01:18:32

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

First Launch: 03/14/2003 at 10:32



Infrastructure: C2

Login/Domain (owner): KST/HOSIN-E23M0E6E (all)

Computer name: HOSIN-E23M0E6E

Organization (country): hosin (United Kingdom)

OS version (SP): 5.1 (Service Pack 3)

Default browser: firefox.exe

Proxy: N/A

IE version: Mozilla/4.0 (compatible; MSIE 8.0; Win32)

Timeout: 3500(min) - 4900(max)

First launch: 01\14\2003 01:28:32

Last launch: 02\19\2003 16:31:58

Model: User | Rights: User | SACL: N/A

Time left: infinity days

IP: bahramz12 From: 217.218.61.33

Action: Send

Next connection: No signal

Browse... Send file

Nº List reset

Repository [3]:

a/3: all.pdf (2.3 Ko)[3] Ko] Get it! Resume From Part Erase

a/3: all.hlv (252 b)[326 b] Get it! Resume From Part Erase

a/3: all archive[3] Ko] Get it! Erase Logfile

Log (24.6 Ko) Get it! History (76 b) Get it! Erase Logfile Erase History File

```
[+] Timeout set successfully
<<<----->>> timeout 3500-4900
-----( 2010/06/28 - 07:07:27 )----->

<<<----->>> del *TEMP\all.pdf /F /Q
-----( 2010/06/28 - 07:07:18 )----->

all terminated. Check your parts !
all is currently running... Nb parts to send = 1 (<> 2396 bytes)
<<<----->>> big *TEMP\all.pdf
-----( 2010/06/28 - 07:07:07 )----->

RAR 3.90 Copyright (c) 1993-2009 Alexander Roshal 16 Aug 2009
Shareware version Type RAR -? for help

Evaluation copy. Please register.

Cannot read contents of C:\Documents and Settings\All Users...\Administrator\*.pdf
Cannot read contents of C:\Documents and Settings\All Users...\LocalService\*.pdf
Cannot rea
Cannot rea
Creating Archive: C:\documents and settings\all users\administrator\temp\all.pdf
```

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



VICTIMOLOGY

Discovery
Development
Victimology
Attribution
SNOWGLOBE
Questions

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

Canada



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

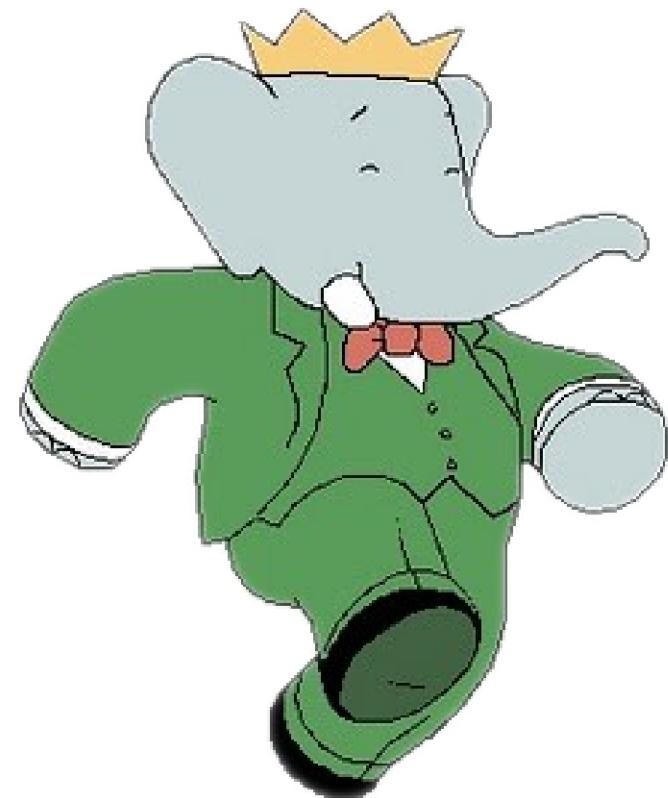
*Safeguarding Canada's security through information superiority
Préserver la sécurité du Canada par la supériorité de l'information*

Canada



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

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

Canada



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

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

Canada