SNOWGLOBE:
From Discovery to Attribution

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
OVERVIEW
Overview

- Discovery
- Development
- Victimology
- Attribution
- SNOWGLOBE.
- Questions and Comments
**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 wmmgmt.exe and wmmgmt.dll (later called the SNOWBALL implant).
  – Creates a service → loads wmmgmt.exe → injects wmmgmt.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 = 491ffa2e746f2452608578761f6f0e2
flag
qKmP2amaqYHdIl7GE99nZrY qjmnpn9b634nKdp%2fiw44
6rlkHkgpWjupDerZmyg5%2 Fx7oWH3bfAmYvC1rULupS
M%2BqGeuP%2BV4eDk%2 4F3%2Fi7mYzLuQn4fe55z0
qWYnju2lZ6xO6uwqbbjou Z%2B9KlHVhAv5a1gd%2B
polW94N%2FiyuLfh%2FrMl Y3CsdYo6CmuYm60YxZ7
0KIlqAqZqQlkqoILTqN 7mgdW%2FxYGBwp2j6
%2Bu99Ctg8jGoseeh9% 2BY4sqsanyzekQj2n%FO
b3c6YbeHp5DCs4aqjYvN %2BLn69dbuxOfKlo2NqN
uc7rjnutmbvYWhiY611% 2FDYgO%2FYh1CZ%2F%
2Bz588et4W%2Bw3B3N 84Scw4L4hraE2LmM%2F
MiA8One3uzE6Nru0Yo3v TRivSC4OT86ue953xrdql
glD9lzd7MTotxBhuPE99 1k9lfX2aL70qe4ldPgxJWN
wrHcjouQ1qTK96FvYym 4rn9lMnD2ZjyvqRlo%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

<table>
<thead>
<tr>
<th>HashID</th>
<th>Last Visit</th>
<th>Next Visit</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>80e4b9537936b94b5f3f992c145006</td>
<td>36d 11h 29m 24s</td>
<td>No signal</td>
<td>Login/Domain (owner): SYSTEM\WT AUTHORITY (Geoff Group)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Computer name: SHIRAI</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Organization (countryy): Iran</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>OS version (ESR): 5.1 (Service Pack 3)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Default browser: ieexplorer.exe</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Portal: N/A</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>IR version: Mozilla/4.0 (compatible: MSIE 6.0, Win32)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Timeout: 5(min) 10(max)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>First launch: 04/10/2010 05:33:34</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Last launch: 05/07/2010 05:38:51</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Mode: Service Rights: Admin, UAC: N/A</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Time Left: Infinity days</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ID: shirai From: 85.198.6.130</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>c864a0b676ba577842a60c84517b8d4</th>
<th>26d 15h 30m 20s</th>
<th>No signal</th>
<th>Login/Domain (owner): SYSTEM\WT AUTHORITY (Star10)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>Computer name: N012</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Organization (countryy): United States</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>OS version (ESR): 5.1 (Service Pack 3)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Default browser: ieexplorer.exe</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Portal: N/A</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>IR version: Mozilla/4.0 (compatible: MSIE 6.0, Win32)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Timeout: 3500(min) 4900(max)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>First launch: 08/07/2010 18:45:26</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Last launch: 05/07/2010 17:09:19</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Mode: Service Rights: Admin, UAC: N/A</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Time Left: Infinity days</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ID: samadghi From: 217.218.61.34</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>5492a826c8293f14992b0b9e09466d</th>
<th>2mad 18h 3m 37s</th>
<th>No signal</th>
<th>Login/Domain (owner): SYSTEM\WT AUTHORITY (kemila)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>Computer name: HTM-2AV93634512</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Organization (countryy): Iran</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>OS version (ESR): 5.1 (Service Pack 3)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Default browser: ieexplorer.exe</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Portal: N/A</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>IR version: Mozilla/4.0 (compatible: MSIE 6.0, Win32)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Timeout: 3500(min) 4900(max)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>First launch: 04/10/2010 00:03:50</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Last launch: 04/07/2010 16:43:44</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Mode: Service Rights: Admin, UAC: N/A</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Time Left: Infinity days</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ID: y_kayat From: 79.132.202.100</td>
</tr>
</tbody>
</table>

Safeguarding Canada’s security through information superiority
Préserver la sécurité du Canada par la supériorité de l’information
Infrastructure: C2
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: 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.
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