CSEC SIGINT Cyber Discovery
Summary of the current effort

Communications Security Establishment Canada
Covert Network Threats
Cyber-Counterintelligence

Discovery Conference
GCHQ – November 2010
Outline

- CSEC SIGINT Cyber
  - K0G (CCNE)
  - GA4 (GND)
  - CNT1 (CCI)
- CSEC SIGINT Cyber – Operational Discovery
  - Network Based Anomaly Detection
  - Host Based Anomaly Detection
- Contacts
CSEC Cyber Counterintelligence

- Target development
- Active collection
- Passive collection

- Attribute
- Persona
- Characterize
- Track
- Develop Collection
- Signatures

Safeguarding Canada’s security through information superiority
Préserver la sécurité du Canada par la supériorité de l’information
Counter CNE (K0G)

• Part of CSEC CNE operations (K0)
• Recently formed matrix team
• Analysts and operators from CNE Operations, Cyber-Counterintelligence and Global Network Detection
• Mandate:
  – Provide situational awareness to CNE operators
  – Discover unknown actors on existing CNE targets
  – Detect known actors on covert infrastructure
  – Pursue known actors through CNE
  – Review OPSEC of CNE operations
Global Network Detection (GND)

• Develop capabilities to improve the ability of the SIGINT collection system to detect Computer Network Exploitation and Computer Network Attack

• Help enable CSEC’s CNE program through timely identification of vulnerable computer systems and foreign CNE methodologies/activities

• Act as technical liaison between IT Security and SIGINT for CNO issues
Cyber Counterintelligence (CNT1)

• Covert Network Threats (New Directorate within CSEC)
  – CNT1 (Cyber Counterintelligence)
  – CNT2 (Traditional Counterintelligence)

• CNT1 Mission
  – To produce intelligence on the capabilities, intentions and activities of Hostile Intelligence Services to support Counterintelligence activities at home and abroad.

• Fusion of Cyber Analytic Skills with Traditional Counterintelligence Analytic Skills
  – All Cyber-Counterintelligence Investigations should lead to Traditional Counterintelligence investigations.
CSEC CNE (K) - WARRIORPRIDE

- **WARRIORPRIDE (WP):**
  - Scalable, Flexible, Portable CNE platform
  - Unified framework within CSEC and across the 5 eyes
  - WARRIORPRIDE@CSE/etc. == DAREDEVIL@GCHQ
  - xml command output to operators

- **Several plugins used for machine recon / OPSEC assessment**
  Several WP plugins are useful for CCNE:
  - Slipstream : machine reconnaissance
  - ImplantDetector : implant detection
  - RootkitDetector : rootkit detection
  - Chordflier/U_ftp : file identification / retrieval
  - NameDropper : DNS
  - WormWood : network sniffing and characterization
K0G – ReplicantFarm

- Created to leverage the WP XML output in a meaningful way
- Module based parser/alert system running on real-time CNE operational data
- Custom/module based analysis:
  - Actors
  - Implant technology
  - Host based signatures
  - Network based signatures
REPLICANTFARM generic modules

- Cloaked
- Recycler
- Rar password
- Tmp executable
- Packed
- Peb modification
- Privileges
- MS pretender
- System32 “variables”
- Strange DLL extensions

Other ideas....
Generic modules: example

```perl
my @runningProcs = xml_isProcessRunning( $xml, 'svchost.{1,3}\.exe',
    'winlogon.{1,3}\.exe',
    'services.{1,3}\.exe',
    'lsass.{1,3}\.exe',
    'spoolsv.{1,3}\.exe',
    'autochk.{1,3}\.exe',
    'logon.{1,3}\.scr',
    'rundll32.{1,3}\.exe',
    'chkdsk.{1,3}\.exe',
    'chkntfs.{1,3}\.exe',
    'logonui.{1,3}\.exe',
    'ntoskrnl.{1,3}\.exe',
    'ntvdm.{1,3}\.exe',
    'rdpclip.{1,3}\.exe',
    'taskmgr.{1,3}\.exe',
    'userinit.{1,3}\.exe',
    'wscntfy.{1,3}\.exe',
    'tcpmon.{1,3}\.dll' );

foreach my $runningProc (@runningProcs) {
    $alertText .= "Suspicious process detected, legitimate exe named appended with string: " .
    $runningProc . "\n";
}
```
CCNE/Opsec WPID Alerts

Note that the search is done with the fields as Perl regular expressions...

Examples:
- Dot (.) matches any character
- Dot Star (.*) matches any number of characters
- Single WPD: MM
- Class C WPD: 1.1.1
- Intermediate 2.2

---

**WID Request:**

**Module Request:** MM

**Alerts**

**WID:**
- **mod_123_MMD_DOGHOUSE.pl**
- **mod_124_MMD_DOGHOUSE.pl**
- **mod_125_MMD_DOGHOUSE.pl**
- **mod_126_MMD_DOGHOUSE.pl**

**Details:**
- Possible MM DOGHOUSE driver file: C:\WINNT\SNtUninstallQ244558S.
- Possible MM DOGHOUSE driver file: C:\WINNT\SNtUninstallQ244558S\netbsd.sys.
- Possible MM DOGHOUSE driver file: C:\WINNT\SNtUninstallQ244558S\sbin.sys.
- Possible MM DOGHOUSE driver file: C:\WINNT\SNtUninstallQ244558S\Cpep.sys.
- Possible MM DOGHOUSE driver file: C:\WINNT\SNtUninstallQ244558S\hotfix.inf.

---
EONBLUE

- CSEC cyber threat detection platform
- Over 8 years of development effort
- Scales to backbone internet speeds
- Over 200 sensors deployed across the globe
EONBLUE

Myricom (10Gbps)

Target Tracking (SNIFFLE)
Metadata Production (DNS / HTTP)

Target Discovery (SLIPSTREAM)

Packet Buffer (2GB)
Anomaly Detection Tools

• There are currently over 50 modules in Slipstream
  – RFC Validation
  – Heuristic Checks
  – Periodicity
  – Simple Encryption
  – Streaming Attack Detection
  – Analyst Utilities

• Not all of these tools are ‘YES/NO’, some will require some work.
Heuristic Example

- QUANTUM
  - It’s no lie, quantum is cool.
    - But its easy to find
  - Analyze first content carrying packet
    - Check for sequence number duplication, but different data size
    - If content differs within the first 10% of the pkt payload, alert.
What’s Next?

• Anomaly Discovery at scale
  – Multi-10G anomaly detection

• Cross Agency communication of anomalies
  – Sometimes signatures aren’t enough

• DONUTS!
  – Everyone likes them:
    • [Blank]
  – 5-eyes accessible DONUTS
    • Discovery of New Unidentified Threats
    • CSEC / GCHQ right now

Safeguarding Canada’s security through information superiority
Préserver la sécurité du Canada par la supériorité de l’information
### Classification: TOP SECRET // COMINT // ROYAL TO FVEY

#### Global Access Roadmap supporting SHO and WSOCN Scenarios

<table>
<thead>
<tr>
<th>Topic</th>
<th>Desired Outcomes</th>
<th>Activity</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Metadata Sharing</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Signature and Target Knowledge</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Sharing Cyber Content</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Tipping and Cueing</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Calendar Year 2010</th>
<th>Calendar Year 2011</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jan - Feb (Q2)</td>
<td>Jan - Mar (Q1)</td>
</tr>
<tr>
<td>Apr - May (Q2)</td>
<td>Jun - Jul (Q3)</td>
</tr>
<tr>
<td>Aug - Sep (Q4)</td>
<td>Oct - Nov (Q4)</td>
</tr>
</tbody>
</table>

- **Topic**
  - **Desired Outcomes**
  - **Activity**
CNT1 - Analysis

- Triage leads from K0G and GA4
  - Links to existing intrusion sets?
- Pursue interesting leads
  - Passive SIGINT collection
  - Technical analysis
- Produce reporting
- Attribute
Analytic Approach

1. Begin with lead
2. Apply to SIGINT
3. Apply to CCNE
4. Track, research and report
5. Generate persona lead
6. Coordinate with traditional CI
Cyber-Specifics of the Analytic Approach

Network Traffic Analysis
- We have access to Special Source, Warranted and 2nd Party collection in raw, unprocessed form
- Work very closely with protocol and crypt analysts

Malware Analysis and Reverse Engineering
- Samples are received through passive collection and human sources

Forensic Analysis
- Assist traditional CI investigations and others