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
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 SIGINT CCI Discovery

Attribute
Characterize
Active Pursuit
CCNE Disco
ReplicantFarm
Cyber-CI Disco
SRE
GND Disco
Passive Pursuit
SlipStream
Report
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

- Kernel cloaking
- Schedule at
- Ntuninstall execution
- hidden

Other ideas....
Generic modules : example

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:**
- Dots ( . ) are single-character wildcards
- Dot-Star ( * ) means any number of characters
- Single WPID: 51: 8.1: 13
- Class C WPID: 51: 8.1: 13
- Newsarchive: /90/81/51

<table>
<thead>
<tr>
<th>Current Modules:</th>
<th>mod_1100_VD_Implant.p1</th>
<th>mod_1200_AF_ALLOGNMENT.p1</th>
<th>mod_1300_MM_DOUGHOUSE.p1</th>
<th>mod_1400_MM_WALKER.p1</th>
</tr>
</thead>
<tbody>
<tr>
<td>mod_1100_VD_Implant.p1</td>
<td>mod_1200_AF_ALLOGNMENT.p1</td>
<td>mod_1300_MM_DOUGHOUSE.p1</td>
<td>mod_1400_MM_WALKER.p1</td>
<td></td>
</tr>
<tr>
<td>mod_1210_RECOVERY.p1</td>
<td>mod_1220_SYSTEM52.p1</td>
<td>mod_1310_PASSWORDEXP.p1</td>
<td>mod_1410_MELANDT.p1</td>
<td></td>
</tr>
<tr>
<td>mod_1610_FACTORY.p1</td>
<td>mod_1620_MELANDT.p1</td>
<td>mod_1630_MELANDT.p1</td>
<td>mod_1640_MELANDT.p1</td>
<td></td>
</tr>
</tbody>
</table>

**Submit Query**

**ALERTS**

<table>
<thead>
<tr>
<th>WPID:</th>
<th>Module:</th>
<th>Date:</th>
<th>Tag:</th>
<th>File name:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>mod_103_MM_DOUGHOUSE.p1</td>
<td>2010-01-21T15:36:39+08:00</td>
<td>MM</td>
<td>/datastore/archive/2010/01/21/15/TXID000272485_18_Y2010M01D21_H15M28S59_MS642MU500NS0_RXID050_000_0</td>
</tr>
</tbody>
</table>

**Details:**
- Possible MM DOUGHOUSE driver file: C:\WINNT\SN-UninstallQ244598S.
- Possible MM DOUGHOUSE driver file: C:\WINNT\SN-UninstallQ244598saf.sys.
- Possible MM DOUGHOUSE driver file: C:\WINNT\SN-UninstallQ244598unet.sys.
- Possible MM DOUGHOUSE driver file: C:\WINNT\SN-UninstallQ244598tcpip.sys.
- Possible MM DOUGHOUSE driver file: C:\WINNT\SN-UninstallQ244598hotfix.inf.

----PULLEDPORK----
EONBLUE

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

Track Known Threats
Discover Unknown Threats
Defence at the core of the Internet
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:
    - 5-eyes accessible DONUTS
      - Discovery of New Unidentified Threats
      - CSEC / GCHQ right now
### CLASSIFICATION: TOP SECRET // COMINT // REL TO FFEY

Global Access Roadmap supporting SRSG and WISDEN Scenarios

<table>
<thead>
<tr>
<th>Topic</th>
<th>Desired Outcomes</th>
<th>Activity</th>
<th>Calendar Year: 2010</th>
<th>Calendar Year: 2011</th>
</tr>
</thead>
<tbody>
<tr>
<td>Metadata Sharing</td>
<td>Shared Situational Awareness</td>
<td>N. Build daily sharing of Cyber Event Metadata with 5-&lt;br&gt;M.3 Receive Metadata from partner agencies&lt;br&gt;M.3 Report on value of metadata sharing&lt;br&gt;M.3 Report instrument NRT sharing of CSEC Cyber Event Metadata&lt;br&gt;M.3 Report on RNT sharing (value / lessons learned / req's)&lt;br&gt;M.4 Enrich NRT feed with Geolocation / ASN&lt;br&gt;M.5 Add Impact Information to event metadata&lt;br&gt;M.8 Extend Deedea Live feed from CSEC to GCHQ&lt;br&gt;M.9 Receive FastFlux metadata (tip) b/w GCHQ/CSEC (see T.6/T.7)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Signatures and Target Knowledge</td>
<td>Replace current Signature Management System</td>
<td>S.1 Replace existing signature management with Herbaitch&lt;br&gt;S.2 Implement Impacts with DGI for Signatures (re-enter in HH)&lt;br&gt;S.3 Document/curate/curate process and replicate with HH&lt;br&gt;S.4 Report on HH (value / lessons learned / requirements / etc)&lt;br&gt;S.5 Open SIGINT IH repository to ITS for Signature Sharing&lt;br&gt;S.6 Open SIGINT IH repository to 5-eyes to retrieve signatures&lt;br&gt;S.7 Trial nSpaces with CTEC / TAC / NAC / DGI&lt;br&gt;S.8 Report on value of nSpaces to support Target Knowledge&lt;br&gt;S.9 Setup Collaborative Web Environment</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sharing Cyber Content</td>
<td>Create a shared environment to experiment with content sharing&lt;br&gt;- Develop requirements / lessons learned on sharing content&lt;br&gt;- Illustrate equitable processing in Cyber capability&lt;br&gt;- Trial XKS for content sharing built on existing metadata</td>
<td>C.1 Establish Cyber Play-lens&lt;br&gt;C.2 Upgrade EONBLUE for use in Cyber Play-lens&lt;br&gt;C.3 Assist in porting EONBLUE capability to PIP&lt;br&gt;C.4 Promote EONBLUE / PIP content to share XKS&lt;br&gt;C.5 Evaluate retrieving GHOQ content based on events from XKS&lt;br&gt;C.6 Trial feeding ofx and event at CSEC to a local XKS&lt;br&gt;C.7 Evaluate opening CSEC Cyber-XKS to GCHQ&lt;br&gt;C.8 Exploit CSEC Cyber-XKS Interface to 5-eyes&lt;br&gt;C.9 Report on content sharing experiments</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tipping and Cueing</td>
<td>Leverage EONBLUE's native messaging to extend national capability (within SIGINT / with ITS)&lt;br&gt;- Based on existing bilateral partnerships with Canadian friends / cutting to enhance content sharing / metadata sharing&lt;br&gt; - CSEC International EONBLUE and similar components with FASTFLUX as trial&lt;br&gt;- TIP to SIGINT events related to partner countries</td>
<td>T.1 Send EONBLUE cue’s across Canadian SGO circles&lt;br&gt;T.2 Send EONBLUE cue's between Canadian SIGINT Programs&lt;br&gt;T.3 Instrument Cyber Session Collection Domestically&lt;br&gt;T.4 Send tips on GCHQ activity to IT Security&lt;br&gt;T.5 Send EONBLUE cue's from Canadian SGO to ITS Sensors&lt;br&gt;T.6 Introduce and develop Cyber Session Collection Experiment&lt;br&gt;T.7 TIP FASTFLUX events from CSEC to GCHQ&lt;br&gt;T.8 Expand EONBLUE FastFlux cue's to GCHQ FastFlux Software&lt;br&gt;T.9 Receive cue's from GCHQ’s FastFlux Software at EONBLUE&lt;br&gt;T.10 Make FASTFLUX tips available to other 5-eyes agencies&lt;br&gt;T.11 TIP to NRT EONBLUE (message to 5-eyes based on IP-SGO)&lt;br&gt;T.12 Send EONBLUE cue's from CSEC EONBLUE to DSD EONBLUE&lt;br&gt;T.13 Based on equitable processing (EJ) send cue's tp GCHQ&lt;br&gt;T.14 Prepare report on Tipping / Cueing (requirements / value / etc)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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
CSEC Contacts

CCI (CNT1)

CCNE (K0G)

GND (GA4)

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