CSEC SIGINT Cyber Discovery: Summary of the current effort

[redacted]

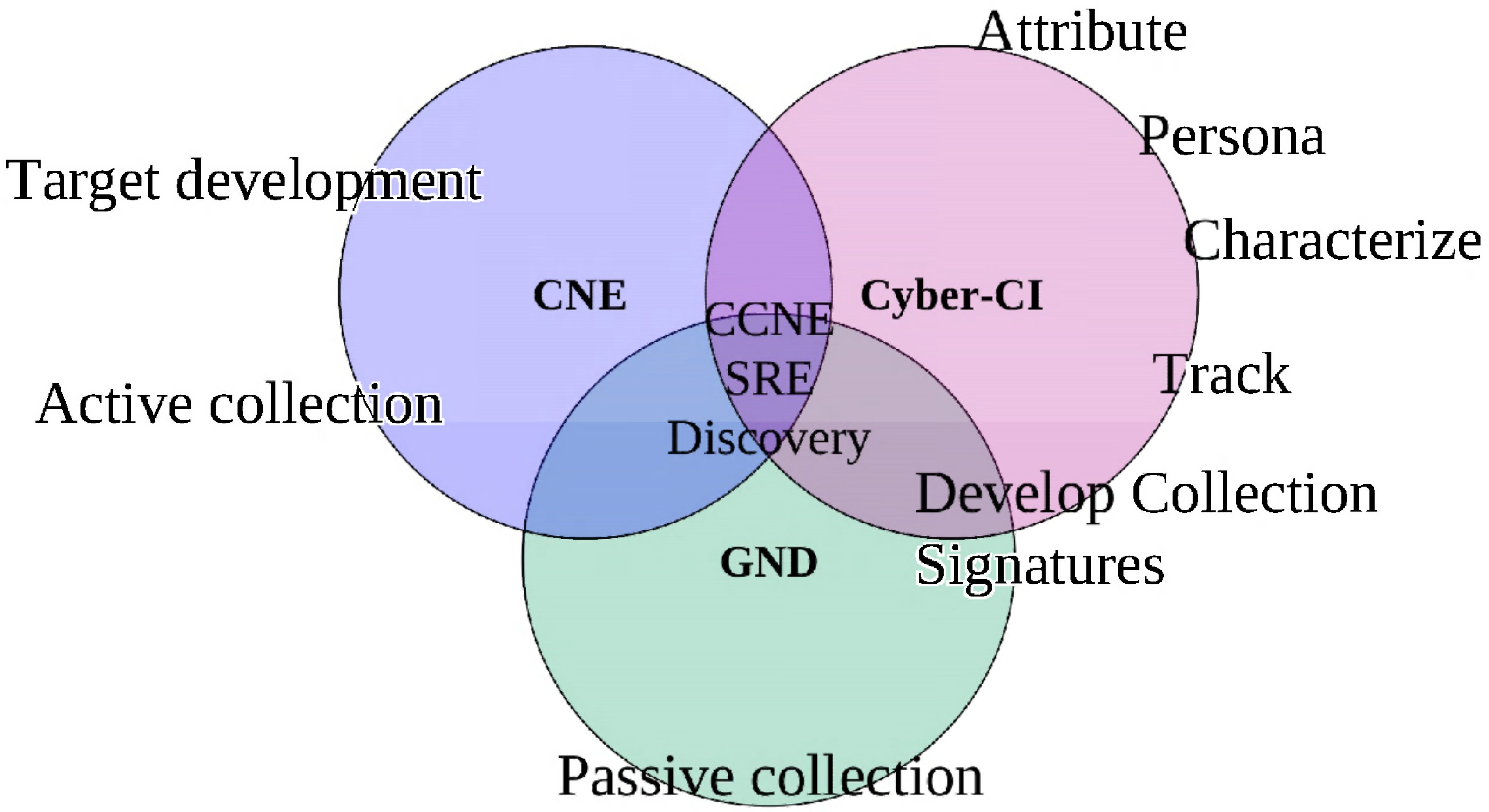
Communications Security Establishment Canada
Covert Network Threats
Cyber-Counterintelligence

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

CNE

CCNE
SRE
Discovery

Cyber-CI

Attribute

Persona

Characterize

Track

Develop Collection
Signatures

GND

Passive collection

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

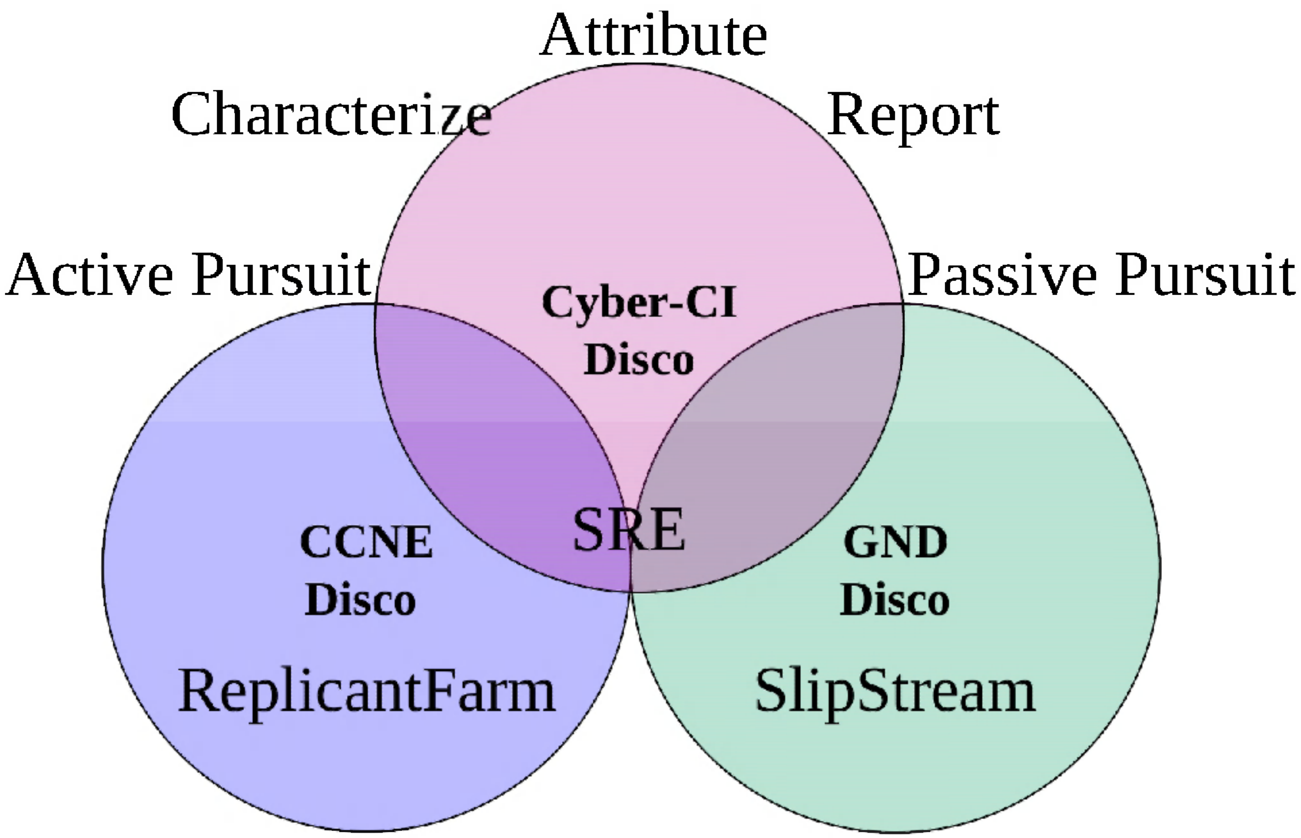
- Help enable CSEC's CNE program through timely identification of vulnerable computer systems and foreign CNE methodologies/activities

- 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



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

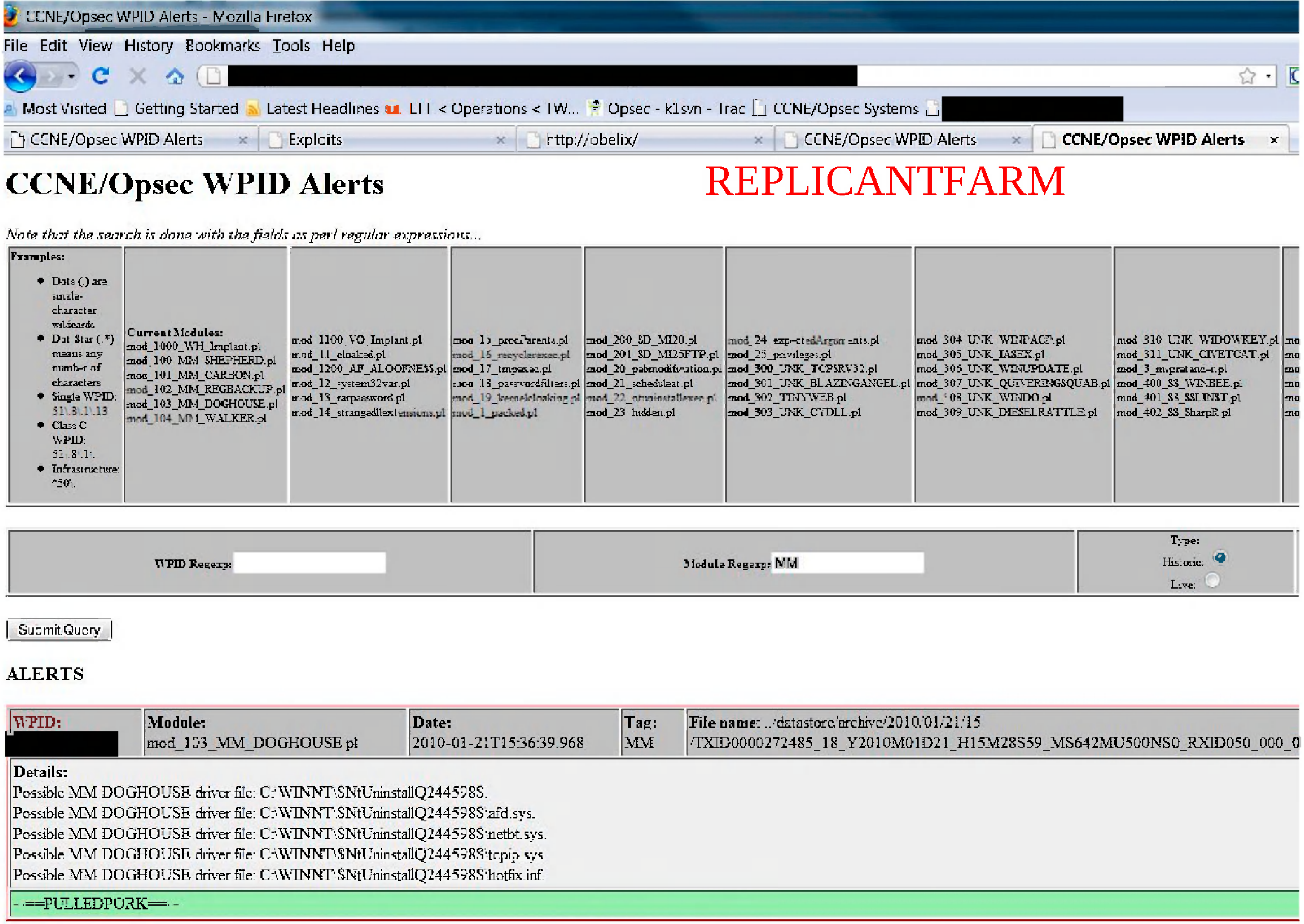
- Kernel cloaking
- Schedule at
- Ntuninstall execution
- hidden

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}\\.dil' );

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



CCNE/Opsec WPID Alerts - Mozilla Firefox
File Edit View History Bookmarks Tools Help
[redacted]
Most Visited Getting Started Latest Headlines LTT < Operations < TW... Opsec - k1svn - Trac CCNE/Opsec Systems [redacted]
CCNE/Opsec WPID Alerts Exploits http://obelix/ CCNE/Opsec WPID Alerts CCNE/Opsec WPID Alerts

CCNE/Opsec WPID Alerts

REPLICANTFARM

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

Examples:	**Current Modules:**							
• Dots (.) are single-character wildcards • Dot-Star (.*) means any numb-r of characters • Single WPID: 51\.8\.1\.13 • Class C WPID: 51\.8\.1\. • Infrastructure: ^50\.	mod_1000_WH_Implant.pl mod_100_MM_SHEPHERD.pl mod_101_MM_CARBON.pl mod_102_MM_REGBACKUP.pl mod_103_MM_DOGHOUSE.pl mod_104_MM_WALKER.pl	mod_1100_VO_Implant.pl mod_11_cloaked.pl mod_1200_AF_ALOOFNESS.pl mod_12_system32var.pl mod_13_earpassword.pl mod_14_strangedllextensions.pl	mod_15_procParents.pl mod_16_recycleexec.pl mod_17_tmpexec.pl mod_18_passwordfilters.pl mod_19_kernelcloaking.pl mod_1_packed.pl	mod_200_SD_MI20.pl mod_201_SD_MI25FTP.pl mod_20_pebmodification.pl mod_21_scheduleat.pl mod_22_uninstallexec.pl mod_23_hidden.pl	mod_24_expectedArguments.pl mod_25_privileges.pl mod_300_UNK_TCPSRV32.pl mod_301_UNK_BLAZINGANGEL.pl mod_302_TINYWEB.pl mod_303_UNK_CYDLL.pl	mod_304_UNK_WINPACP.pl mod_305_UNK_IASEX.pl mod_306_UNK_WINUPDATE.pl mod_307_UNK_QUIVERINGSQUAB.pl mod_308_UNK_WINDO.pl mod_309_UNK_DIESELRATTLE.pl	mod_310_UNK_WIDOWKEY.pl mod_311_UNK_CIVETCAT.pl mod_3_msprotancer.pl mod_400_SS_WINBEE.pl mod_401_SS_SSLINST.pl mod_402_SS_SharpR.pl	mo mo mo mo mo mo

WPID Regexp:	**Module Regexp:** MM	**Type:** Historic: ● Live: ○

Submit Query

ALERTS

WPID:	**Module:**	**Date:**	**Tag:**	**File name:**
[redacted]	mod_103_MM_DOGHOUSE.pl	2010-01-21T15:36:39.968	MM	../datastore/archive/2010/01/21/15 /TXID0000272485_18_Y2010M01D21_H15M28S59_MS642MU500NS0_RXID050_000_0

Details:

Possible MM DOGHOUSE driver file: C:\WINNT\$NtUninstallQ244598$.
Possible MM DOGHOUSE driver file: C:\WINNT\$NtUninstallQ244598$\afd.sys.
Possible MM DOGHOUSE driver file: C:\WINNT\$NtUninstallQ244598$\netbt.sys.
Possible MM DOGHOUSE driver file: C:\WINNT\$NtUninstallQ244598$\tcpip.sys
Possible MM DOGHOUSE driver file: C:\WINNT\$NtUninstallQ244598$\hotfix.inf

- -==PULLEDPORK==- -

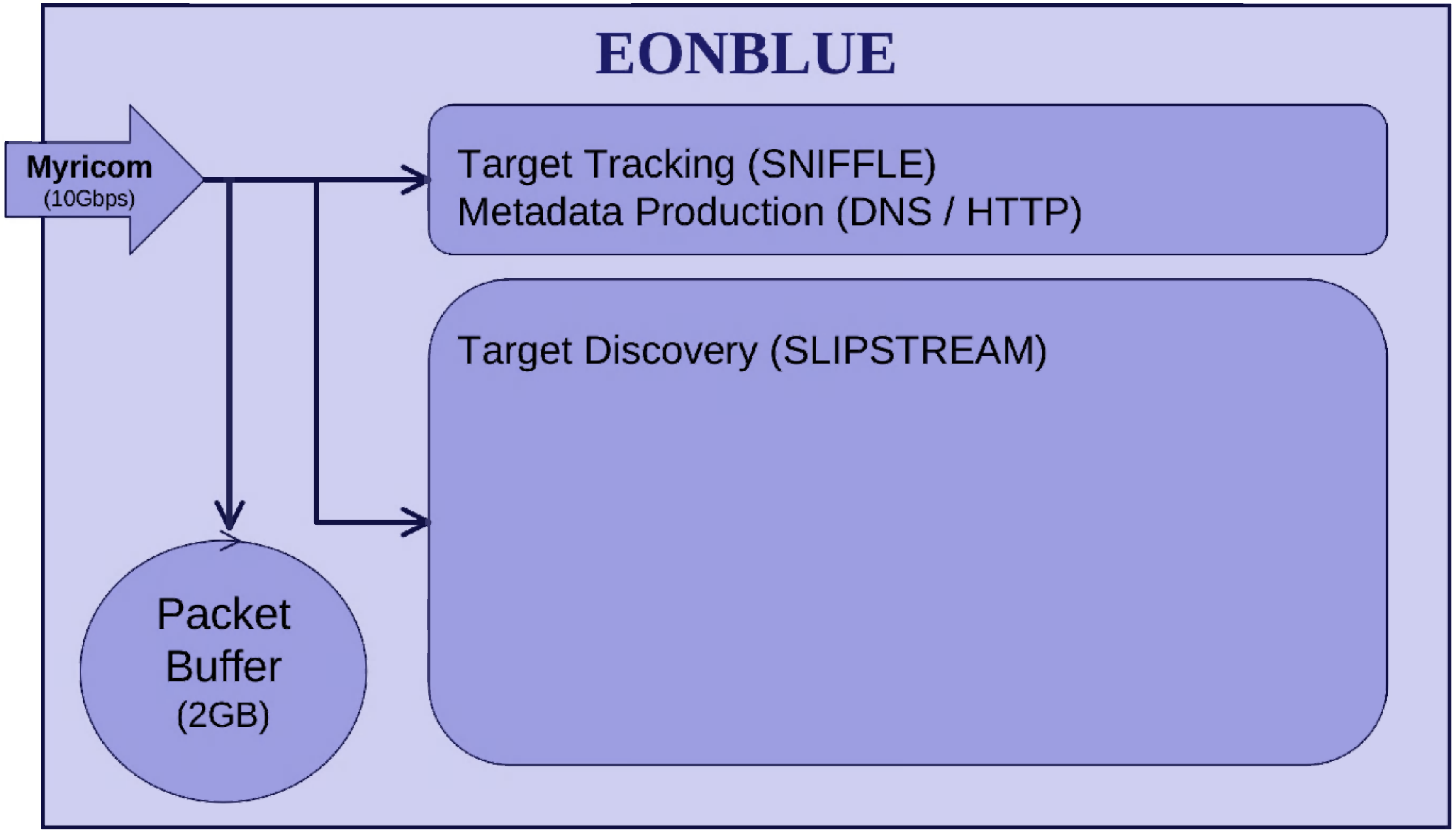
EONBLUE

- 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:
    - [redacted]
  - 5-eyes accessible DONUTS
    - Discovery of New Unidentified Threats
    - CSEC / GCHQ right now

CLASSIFICATION: TOP SECRET // COMINT // REL TO FVEY

Global Access Roadmap supporting SRSG and WISDEN Scenarios

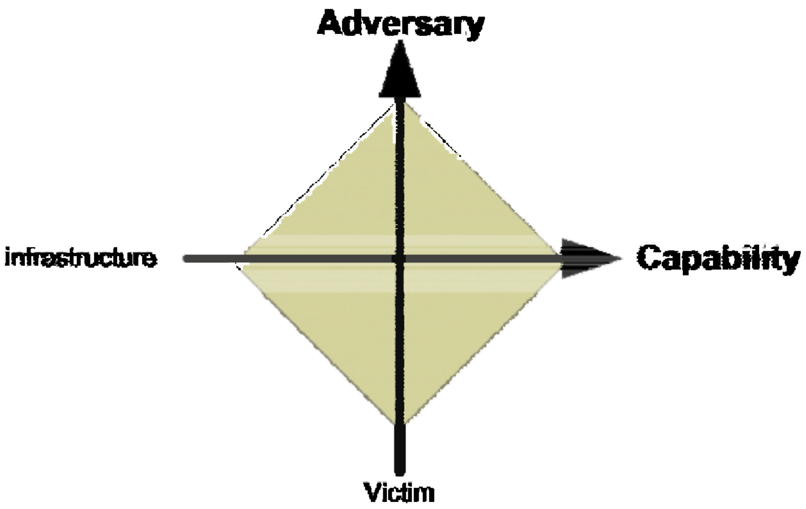
				Calendar Year: 2010		Calendar Year 2011			
Topic	**Desired Outcomes**	**#**	**Activity**	July - Sep (Q3)	Oct - Dec (Q4)	Jan - Mar (Q1)	Apr - Jun (Q2)	July - Sep (Q3)	Oct - Dec (Q4)
Metadata Sharing	- Shared Situational Awareness - Assess value of metadata sharing Develop Use Cases for Sharing - Develop Requirments for NRT Lipping	M.	Bulk daily sharing of Cyber Event Metadata with 5-	■					
		M.2	Receive Metadata from partner agencies	■					
		M.3	Report on value of metadata sharing		■				
		M.4	Instrument NRT sharing of CSEC Cyber Event Metadata	DSD/GCHQ					
		M.5	Report on NRT sharing (value / lessons learned / reqt's)		■				
		M.6	Enrich NRT feed with Geolocation / ASN	■	■				
		M.7	Add Impact information to event metadata		■				
		M.8	Extend Deadsea Live feed from CSEC to GCHQ		■				
		M.9	Receive FastFlux metadata (tip) b/w GHCQ/CSEC (see T.6/T.7)					■	
Signatures and Target Knowledge	- Replace current Signature Management system - Impacts to support Action-on / Cueing and enhance Metadata feed - Provide context to metadata - Experiment with TKB to gather requirments - Create baseline of Cyber knowledge	S.1	Replace existing signature management with HalterHitch	■	■				
		S.2	Implement Impacts with DGI for Signatures (re-enter in HH)		■				
		S.3	Decommission current targetting process and replace with HH		■				
		S.4	Report on HH (value / lessosn learned / requirments / etc)		■				
		S.5	Open SIGINT HH repository to ITS for Signature Sharing			■			
		S.6	Open SIGINT HH repository to 5-eyes to retrieve signatures			■			
		S.7	Trial nSpaces with CTEC / TAC / NAC / DGI		■				
		S.8	Report on value of nSpaces to support Target Knowledge			■			
		S.9	Set-up Collaborative Web Environment	■	■				
Sharing Cyber Content	- Create a shared environment to experiment with content sharing - Develop requirments / lessons learned on sharing content - Illustrate equitable processing in Cyber capability - Trial XKS for content sharing built on existing metadata	C.1	Establish Cyber Play-Pen	CTE / CND					
		C.2	Upgrade EONBLUE for use in Cyber Play-Pen	GTE/GND	■				
		C.3	Assist in porting EONBLUE capability to PPF		GTE/GND				
		C.4	Promote EONBLUE / PPF content to shared XKS		GTE / GND	■			
		C.5	Evaluate retrieving GHCO content based on events from XKS			GTE/GND	■		
		C.6	Trial feeding EONBLUE events at CSEC to a local XKS			CSEC NAC	■		
		C.7	Evaluate opening CSEC Cyber-XKS to GCHQ				GTE / GND		
		C.8	Expose CSEC Cyber-XKS interface to 5-eyes				■	■	
		C.9	Report on content sharing experiments					■	
Tipping and Cueing	- Leverage EONBLUE's native messaging to extend national capability (within SIGINT / with ITS) - Based on existing bilateral partnerships trial tipping / cueing to enhance content sharing / metadata sharing - Cue international EONBLUE and similar components with FASTFLUX as trial - Tip in NRT SIGINT events related to partner countries	T.1	Send EONBLUE cue's across Canadian SSO Sites	■					
		T.2	Send EONBLUE cue's between Canadian Passive Programs		■				
		T.3	Instrument Cyber Session Collection Domestically		SPOC				
		T.4	Send tips on GoC activity to IT Security		■				
		T.5	Send EONBLUE cue's from Canadian SSO to ITS Sensors		■				
		T.6	Introduce and develop Cyber Session Collection Experiment		■	Across 5-Eyes	■	■	
		T.7	Tip FASTFLUX events from CSEC to GCHQ		■	■			
		T.8	Extend EONBLUE FastFlux cue's to GCHQ FastFlux Software			GTE/GND	■		
		T.9	Receive cue's from GCHQ's FastFlux Software at EONBLUE				GTE/GND	■	
		T.10	Make FASTFLUX tips available to other 5-eyes agencies					■	
		T.11	Tip in NRT EONBLUE messages to 5-eyes based on IP-Geo					■	■
		T.12	Send EONBLUE cue's from CSEC EONBLUE to DSD EONBLUE						■
		T.13	Based on equitable processing (C.3) send cue's tp GCHQ						■
		T.14	Prepare report on Tipping / Cueing (requirments / value / etc)						■

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)

[redacted]

[redacted]@cse

[redacted]

[redacted]@cse

[redacted]

[redacted]@cse

CCNE (K0G)

[redacted]

[redacted]@cse

[redacted]

[redacted]@cse

[redacted]

[redacted]@cse

GND (GA4)

[redacted]

[redacted]@cse

[redacted]

[redacted]@cse

[redacted]