Released under the ATIA - unclassified information
Divulgé en vertu de la loi LAI - renseignements non classifiés

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

CSEC IT Security Operational Instructions ITSOI-1-1

Data Querying and Signatures in Cyber Defence Activities

IT Security

Canada

Released under the ATIA - unclassified information
Divulgé en vertu de la loi LAI - renseignements non classifiés

Table of Contents

Released under the ATIA - unclassified information
Divulgé en vertu de la LAI - renseignements non classifiés

1. Introduction

1.1 Objective These instructions provide direction on querying raw data (prior to use or retention) obtained by CSEC during cyber defence activities, including those conducted under Ministerial Authorization (MA), non-MA cyber defence activities using Data Provided by a System Owner (DPSO), and on the development and use of signatures.

Additionally, these instructions provide guidance on how to ensure querying is focused against suspected foreign cyber threats and not directed at Canadians.

1.2 Application These instructions apply to CSEC personnel and any other parties, including secondees, contractors and integrees, involved in conducting or supporting cyber defence activities.

2. Data Querying and Relevancy Requirements

2.1 Querying Data[1] querying refers to searching or scanning raw data; it can be automated or manual. Querying includes, but is not limited to the following:

Automated:

- Alert-driven – [redacted]
- Tools that capture sub-sets of data, such as [redacted]
- Anomaly-driven – [redacted]

Manual:

- Analysis-driven – e.g., an analyst can query data according to a set of criteria for the purpose of analyzing a particular alert, evaluating a hypothesis, or performing forensic analysis;
- Research-driven – e.g., queries created for brainstorming, workshops (e.g., Big Dig) and discovery work;
- Development-driven – [redacted]

[1] For cyber defence activities conducted under part (b) of CSE's mandate, "data" refers to [redacted] obtained from computer systems or networks of importance to the GC; it includes content and associated metadata (ITSOI-1-2, paragraph 2.1).

Released under the ATIA - unclassified information
Divulgé en vertu de la LAI - renseignements non classifiés

2.2 Auditing Requirement

Contact IPOC to determine whether a tool requires policy verification prior to deployment (through use of a CDO Service and Tool Pre-Deployment Form). If a tool undergoes policy verification, IPOC will determine whether the tool could have an impact on privacy. For example:

- will the tool intercept private communications?
- could use of the tool be directed against Canadians?
- will the tool collect personal information?

Queries run on tools that may impact privacy (as determined by IPOC) must be auditable (and backed-up as necessary).

2.3 Requirement to Query Data using Canadian Selectors

A foreign threat actor may use Canadian infrastructure to launch exploits against the GC. For example, websites ending in .ca can be registered by the threat actor and can receive beacons from infected computers. Canadian email addresses can be spoofed in order to mask the origins of a spear-phishing email.

In most cases, [redacted]

Data querying must not be directed at Canadians or persons in Canada. Canadian selectors may only be included in a query if that query is aimed at detecting, analyzing or mitigating foreign cyber threats.

Generally when querying, Canadian selectors must be coupled with other [redacted] to limit the risk of returning personal information about Canadians. For example, a Canadian email address [redacted]

In certain circumstances Canadian selectors may be used in signatures [redacted] See section 3.7 for more details.

Consult IPOC for assistance on what [redacted] to use to ensure a query is not directed at Canadians or persons in Canada.

2.4 Querying with Second Party Selectors

Unsuppressed Second Party selectors received from Second Parties can be used to query data (subject to any restrictions imposed by the Second Party). These selectors could come to CSEC via reporting or as a

Released under the ATIA - unclassified information
Divulgé en vertu de la LAI - renseignements non classifiés

[redacted]

Note: The use of all other Second Party selectors is subject to the policies of the relevant Second Party; contact IPOC.

2.5 Relevancy and Essentiality Requirements

All data used or retained as a result of querying must be relevant to providing advice, guidance and services to help ensure the protection of electronic information and of information infrastructures of importance to the Government of Canada (GC) (part (b) of CSEC's mandate).

Furthermore, all data from a private communication (intercepted under MA) retained as a result of querying must be essential to identify, isolate, or prevent harm to GC computer systems or networks.

The analyst determines the relevancy, and essentiality if required, of the query results at the time the decision is made to retain all or part of those results.

Note: Detached metadata is considered relevant for up to [redacted] **See ITSOI-1-2 for more information on handling detached metadata.**

3. Signatures and Selectors

3.1 What is a Signature

For these instructions, signatures refer to automated queries that scan traffic or data in order to detect malicious cyber activity.

Signatures are:

[redacted]

3.2 What is a Selector?

For these instructions, selectors are defined as:

- electronic infrastructure addresses that are used by a network or service provider for routing purposes (IP addresses, email addresses, and domain names.)
- any alphanumeric character stream applied to data in order to identify cyber threats.

Released under the ATIA - unclassified information
Divulgé en vertu de la loi LAI - renseignements non classifiés

3.3 What is a [redacted] Signature?

[redacted] signatures are defined, in the cyber threat context, as [redacted]

3.4 What is Considered a Canadian Selector?

How to identify a Canadian selector by type:

IP Addresses: If an IP address resolves to a Canadian internet service provider then it must be considered a Canadian selector. For GC networked systems, IP addresses that cannot be linked to an individual are not considered Canadian selectors.

Domain Names: If a domain is a recognizable Canadian company or is registered to a Canadian, it must be considered a Canadian selector. A .ca domain is to be considered a Canadian selector unless it is known to be registered by a foreign entity outside Canada.

Note: Domain names in the context of email addresses are treated as part of the email address following the guidelines below.

Email Addresses: If the domain of the email account (e.g., @live.ca, @rogers.com) is a recognizable Canadian communications provider, the entire email address is to be considered a Canadian selector, unless the sender is determined to be foreign based. For example, Foreign.Threat@live.ca is not a Canadian selector.

Note: In some circumstances spoofed Canadian email addresses may be considered foreign. Contact IPOC for guidance.

3.5 Running Signatures Comprised of Canadian Selectors

There are two types of signatures that may contain Canadian selectors:

- Type 1: Signatures that are comprised of a selector [redacted]
- Type 2: Signatures that are comprised of only selectors, such as an IP address.

In both of these cases, a Canadian selector might be used if an analyst believes it represents a Canadian victim or part of compromised Canadian infrastructure.

Attention: All signatures comprised of Canadian selectors must be tracked and reviewed by the cyber defence analyst every [redacted] Signatures must be detasked if obsolete or pulling in legitimate traffic.

Released under the ATIA - unclassified information
Divulgé en vertu de la loi LAI - renseignements non classifiés

Note: Use of Second Party selectors is subject to policies of the relevant Second Party; contact IPOC.

3.6 Approval of Type 1 Signatures

Type 1 signatures containing a Canadian selector require the approval of the cyber defence supervisor confirming that the selector is [redacted] linked to suspected foreign malicious activity before they can be run against collection.

For compliance purposes, IPOC must be able to access a record of all such signatures.

3.7 Approval of Type 2 Signatures

The process for deploying type 2 signatures containing Canadian selectors is as follows:

Run against ITS collection for a [redacted] period with cyber defence manager approval.	
If the signature [redacted]	If the signature [redacted]
[redacted]	
- the signature can continue deployment as is - sufficient documentation demonstrating the above must be available for compliance purposes - approval by cyber defence manager is required - IPOC is notified - automated use or retention (see 4.2 below) is not permitted for type 2 signatures.	- the signature must be turned into a type 1 signature based on the analytics collected - process outlined in 3.6 is followed.

Note: Following the initial [redacted] testing period, if a type 2 signature returns legitimate (i.e., non-malicious) activity, the signature must be turned into a type 1 signature, or detasked.

3.8 Additional Requirements for Signature Development using DPSO Data

Signatures can be developed from data received from DPSO activities. Permission from the client to share data must be stored in the Client File.

Signatures can only be created from [redacted] if they are intended to protect the System Owner's systems and networks or when the originator or recipient of the reported [redacted] has given express consent.

Released under the ATIA - unclassified information
Divulgé en vertu de la LAI - renseignements non classifiés

See ITSOI-1-2 for information on tagging DPSO data.

4. Automated Use or Retention for the Purpose of Sharing Data with Second Parties

4.1 Sharing Data

In order to share data with Second Parties, data must be relevant, and if from a private communication essential, to fulfilling part (b) of the mandate. It must also be used or retained prior to sharing. See ITSOI-1-3 for more information.

4.2 What is Meant by Automated Use or Retention?

Automated use or retention refers to the use of signatures that have been vetted to ensure output will always be relevant and essential, and may therefore be marked automatically as used or retained.

[redacted]

4.3 Requirements

In order for signatures to be considered as producing output that is automatically used or retained, the following must be in place (for certain data types - see "Note" below) :

1. Demonstrated link to a foreign threat actor,
   - via previous reporting by CSEC or our partners; or

[redacted]

2. Analyst review of initial results of the signature, in consultation with IPOC, [redacted] (see 3.2 of ITSOI-1-3).

3. Following the review and consultation, the signature is approved for automated relevancy, and essentiality if appropriate, by the Cyber Defence Manager.

All signatures that are approved as such must be available to IPOC for compliance purposes.

Released under the ATIA - unclassified information
Divulgé en vertu de la loi LAI - renseignements non classifiés

Notes:

- For each new data type (e.g., [redacted], prior consultation with IPOC is required in order to determine whether the above process must be followed).
- Type 2 signatures comprised only of Canadian selectors cannot be approved for automated use or retention.

4.4 Retention of Outputs

Data automatically marked as used or retained must be handled as any other data that has been used or retained; it is subject to Ministerial reporting requirements. Documentation of all output shared with Second Parties must be kept.
See ITSOI-1-3 for further details.

5. Additional Information

5.1 Accountability

This table establishes the areas of responsibilities as they relate to these instructions.

Who	What
Deputy Chief, IT Security	• Approving these instructions
Director, Program Management and Oversight	• Recommending these instructions for approval • Revising these instructions as necessary • Monitoring compliance with these instructions • Communicating guidance to those authorized to conduct cyber defence activities regarding any revisions to these instructions
Manager, Corporate and Operational Policy	• Reviewing these instructions to ensure compliance with CSEC policy

5.2 References

- OPS-1, *Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSEC's Activities*
- OPS-1-14, *Operational Procedures for Cyber Defence Operations Conducted under Ministerial Authorization*
- OPS-1-15, *Operational Procedures for Cyber Defence Activities Using System Owner Data*
- ITSOI-1-2, *Data Handling in Cyber Defence Activities*
- ITSOI-1-3, *Accessing and Sharing Cyber Defence Data*

Released under the ATIA - unclassified information
Divulgé en vertu de la loi LAI - renseignements non classifiés

5.3 Amendments Situations may arise where amendments to these instructions are required because of changing or unforeseen circumstances. Such amendments will be communicated to relevant staff, and will be posted on the IPOC website.

5.4 Enquiries Questions relating to these instructions should be directed to supervisors in the Cyber Defence Branch who in turn will contact IPOC.

6. Promulgation

I hereby approve Operational Instructions ITSOI-1-1, *Data Querying and Signatures in Cyber Defence Operations.*

These instructions are effective on June 28, 2013.
(Date)

Approved

28/6/13

Toni Moffa
Deputy Chief, IT Security

Date

Reviewed and Recommended for Approval

June 28/13

John Ommanney
Director, Program Management and Oversight

Date