Open Threat Partner Exchange (OpenTPX)

Version 2.2.0

Tables Index

Figures Index

1 Introduction

This document provides the specification of the Open Threat Partner Exchange (OpenTPX) data schema and data elements for threat intelligence, security and network data sharing.

OpenTPX consists of multiple categories of information that may be shared as shown in the following diagram.

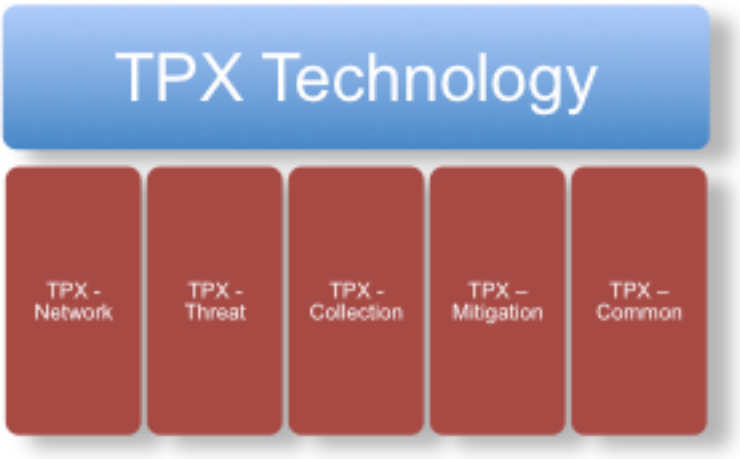

Figure 1: TPX Overview

- TPX Common
  - Aspects of sharing common to all elements of TPX including source, distribution dates…etc
- TPX Network
  - Network topology, routing, packet traces….etc
- TPX Threat
  - Threat observables, confidence scoring, meta data, observable descriptions….etc.
- TPX Collection
  - Sectors, incidents, actors, domains
- TPX Mitigation
  - Recommendations on threat mitigation

1.1 License

OpenTPX specification and software are distributed under Apache 2.0 License.

```
“Copyright 2015 Lookingglass Cyber Solutions

Licensed under the Apache License, Version 2.0 (the "License"); you may not
use this file except in compliance with the License. You may obtain a copy of
the License at

http://www.apache.org/licenses/LICENSE-2.0
```

1.2 Version

Date	Version	Change
10/08/15	2.2.0	• Initial open source distribution

1.3 Definitions

The following definitions are used in this document.

Table 1: Definitions

Term	Definition
BGP	Border Gateway Protocol
Classification	A categorization of risk that defines the form of risk
Collection	A named group of network elements, host elements, actors, incident or observables
Criticality	A numerical, linear measurement of risk based on a scale of 0 (no risk) to 100 (highest possible critical risk)
Observable	A name associated with a measurement of risk including a description of the risk and one or more classifications associated with one or more network elements
TLP	Traffic Light Protocol
TPX	Threat Partner Exchange
TPX Provider	A system that generates TPX content
TPX Consumer	A system that consumes TPX content

2 Overview

TPX may be used in a variety of ways to exchange information relevant to Threat Analysis, Security Operations and Incident Response.

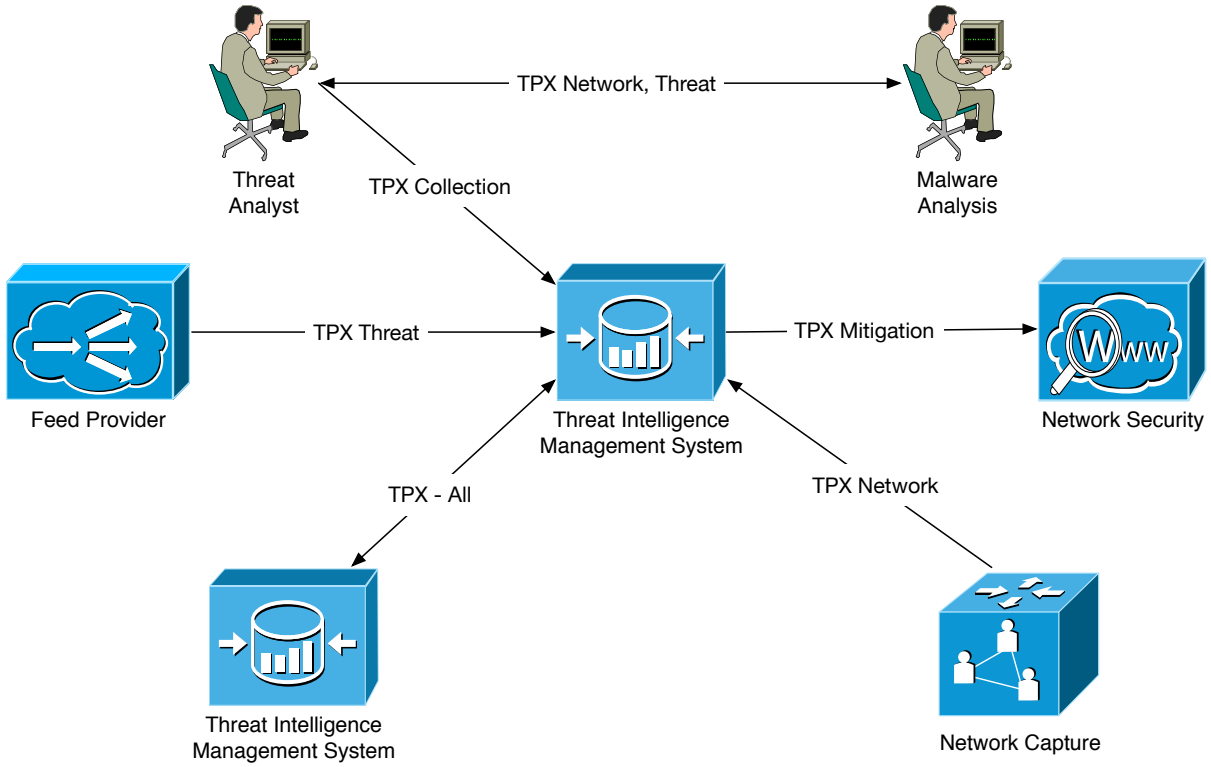

Figure 2: Example TPX Providers and Consumers

There are multiple use cases where TPX content may be exchanged and the schema is deliberately designed to be extensible to enable further use cases to be defined without requiring an overhaul on the schema.

- **Source**: Threat Analyst, **Destination**: Threat Intelligence Management System
  - Threat Analyst sends a manually defined Collection containing sector and/or company specific information to the TIMS to enable the system to correlate threats associated with a sector or company
- **Source**: Malware Analysis, **Destination**: Threat Analyst
  - Automated Malware Analysis system sends results of malware analysis including network packet captures, threat observables to threat analyst directly via email
  - Threat Analyst sends signature information for malware analyst system to hunt for specific aspects of malware
- **Source**: Feed Provider, **Destination**: TIMS
  - A feed provider has a set of threats that they have observed certain threat attributes every 24 hours and wishes to publish this information to other consumers to improve their security posture.
- **Source**: TIMS, **Destination**: TIMS
  - Organization X has their own TIMS and wishes to exchange complete threat context associated with an incident including network, threat and actor information with Organization Y.

- **Source**: Network Capture, **Destination**: TIMS
  - Network switch or router captures packets and flows and sends summarized results every 5 minutes to threat intelligence analysis system for correlation with other threat intelligence data
- **Source**: TIMS, **Destination**: Network Security
  - The TIMS identifies with high confidence a known threat and IP to block and sends the mitigation rule to the network security device asynchronously

TPX is a JSON-based payload and can be transmitted using any number of transport protocols and interfaces:

- Via Email
- Via SCP File transfer
- Via HTTP File Transfer
- Via HTTP RESTful API

TPX sources and recipients can choose which transport of providing their data best suits their needs.

2.1 Threat Observables

We define the term 'threat observable' loosely to be **any observation** that ***may*** have an **associated threat score** and ***may*** be associated with **one or more elements of interest**

It is deliberate that OpenTPX has a very loose definition of the threat observable to ensure increased flexibility and extensibility. Thereby removing some of the rigidity of a more structured approach.

A threat observable can be one or more of the following:

- An Indicator Of Compromise (IOC)
- An Originating or Destination Network
- A network topology
- A Target Network, domain
- A Command & Control behavior
- An application (malware or otherwise)
- An actor
- A behavior
- A TTP
- A report
- A human defined note or description

Threat observables ***may*** be combined into collections and reference each other.

Threat observables comprise an identifying name, and one or more key/value attributes that capture the observation's data.

Threat observable attributes keys may come from a pre-defined dictionary or may introduce new terms

2.2 TPX Conventions

TPX files follow certain conventions to allow ease of parsing, readability and efficient data ingestion.

2.2.1 Syntax

The following naming conventions have been used:

- TPX uses lowercase terms throughout the schema
- Where appropriate use underscores "_" to separate terms

2.2.2 Examples

Throughout this document the OpenTPX examples may show comments in the JSON that are not JSON compliant but are included in the examples to help the reader understand the examples.

Before using any of the examples displayed in this document with a JSON grammar checker please remove all comments.

For example, remove all text shown in **red** below.

```
{
  //
  // SECTION: Intro
  // DESCRIPTION: Provides the attribute of the list, provider name, date of distribution ...etc.
  // There is only one source_observable per TPX file.
  // If a provider has multiple feeds then there will be one file per feed
  //
  "schema_version_s": "2.2.0",
  "provider_s": "Intel Provider Company",
```

2.2.3 Types

A key/value pair typically defines TPX data. The key is comprised of a descriptive name of the value and a suffix that identifies the type of the value. There are 2 types of keys used in TPX that allow the TPX content to convey more or less encoding information for the value.

General key types are keys that are not specific network elements.

Table 2: General TPX Types

Suffix	Description	Key Example
_t	A key that is represented as a unix Epoch timestamp in milliseconds	a_time_t
_s	A key that is represented as a string	schema_vers_s
_i	A key that is represented as an integer (big int included)	filesize_i
_ui	A key that is represented as an unsigned integer (big uint included)	ipv4_ui
_h	A key that is represented as a hexadecimal string	hash_h
_l	A key that is represented as a long	a_value_l

_ll	A key that is represented as a long long	ipv6_ll
_f	A key that is represented as a floating point number	lat_f
_c_array	A key that represents data as an array of complex data objects	dns_req_c_array
_c_map	A key that represents data as an map of complex data objects	observable_c_map
_s_array	A key that represents data as an array of string objects	lstring_s_array

Encoded types are:

Table 3: Specific Encoding TPX Types

Suffix	Description	Key Example
_id_i	An integer identifier	_obs_id_i
_id_s	A string identifier	_classification_id_s
_id_h	A hexadecimal identifier	_mac_id_h
_id_f	A floating point identifier	_lat_id_f
_ipv4_ui	An IPv4 object represented as an unsigned integer	c2server_ipv4_ui
_ipv4_s	An IPv4 object represented as a string	c2server_ipv4_s
_cidrv4_s	A CIDR v4 object represented as a string	c2network_cidrv4_s
_ipv6_ll	An IPv6 object represented as an long long	c2server_ipv6_ll
_ipv6_s	An IPv6 object represented as a string	c2server_ipv6_s
_cidrv6_s	A CIDR v6 object represented as a string	c2network_cidrv6_s
_fqdn_s	A FQDN represented as a string	c2server_fqdn_s
_asn_number_ui	An ASN represented as an unsigned number	home_asn_number_ui
_asn_s	An ASN represented as a string	home_asn_s
_md5_h	An MD5 hash represented as a hex string	hash_md5_h
_sha1_h	An SHA1 hash represented as a hex string	hash_sha1_h
_sha256_h	An SHA256 hash represented as a hex string	hash_sha256_h
_sha512_h	An SHA512 hash represented as a hex string	hash_sha512_h

Notes:

- **Ipv4_i** (IP as a signed integer) use is deprecated in 2.2.0.
    - Pre-2.2.0 files **ipv4_i** will continue to be supported but all new implementations should use **ipv4_uii** instead

2.2.4Timestamps

All timestamp information in TPX is UTC unless otherwise stated.

2.2.5Maximum File Size

It is recommended that TPX files **should** not be greater than 1GB. If files exceed this size, they **should** be split into partial files and represented via the TPX manifest (cf. section 3.1 for manifest details).

2.2.6 Dictionary Ordering

TPX files that contain a dictionary for observables **should** include the dictionary prior to any observables that refer or require that dictionary in their definition. This is primarily for readability of the TPX file if a human is reading the file.

3 Content Introduction

TPX allows the conveyance of network topology, network routing, network ownership and threat intelligence observables, threat observable associations and threat confidence information attributed to the threat observables for network, application and users.

The TPX Context define the following optional information that is sharable:

- A **Context Introduction** that defines the data necessary to identify the source of the information and other identifying attributes of the source
- A **threat observable dictionary** and associated definitions
    - Including observable names, their associated criticality, description and the set of classifications to which the observable belongs to
    - The dictionary allows the provider to define observables once and then refer to that observable name for each subject, thereby associating the criticality, description and classifications defined in the header dictionary to the tagged subject element.
    - The dictionary must occur in the TPX file prior to any observable associations using that dictionary
- A set of **threat observable associations** to one or more subjects (i.e. elements) including network, host or user subjects
    - Network subjects include IP, CIDR, ASN, FQDN
    - Host subjects include file hashes, application identifiers, malware indicators
    - User subjects include user name, user identity, alias, email address
    - Threat subjects may have multiple threat observables associated with them
    - There is no limit to the type of subject that may be identified provided that the subject is supported by the LG threat ingestion capability.
    - A threat observable may have one or more mitigation recommendations.
- A set of **collections** where each collection may define country information, named grouping of network, host elements and observables
    - A collection may contain zero or more collections
    - Observables referenced by a collection must be defined in the threat observable dictionary
- A set of **networks** where each network may define network membership, routing topology, ownership, network announcements

The TPX top-level objects are shown below:

```
"schema_version_s": "2.2.0",
"provider_s": "Intel Provider Company",
"list_name_s": "Intel Provider Company List Data",
"source_observable_s": "PROV_IND_NAME",
"source_file_s": "/var/lg/data/json/list_name/2014/06/01/202data.csv",
"source_description_s": "This is a description of the feed and the information it provides",
"distribution_time_t": 1221312312,
"last_updated_t": 121232134,
"score_i": 90,

"observable_dictionary_c_array": [
        …the set of observables defined in this TPX file
]

"element_observable_c_array": [
        …the set of network/host/application elements associated with observables
        …with elements as the key (i.e. element centric organization)
```

```
]

"collection_c_array": [
        ...a set of collections
]

"asn_c_array": [
        ...a set of networks
]
```

3.1 TPX Context Introduction

The TPX Context introduction represents the overall description of the TPX content that a producer is sharing. The TPX producer can provide content in 3 forms:

1) A single TPX payload containing all aspects of the TPX content typically in a single file
2) Multiple files that split each key section of the TPX across one or more files and then include a manifest in the introduction part of the TPX content.
3) A single TPX event that is transported over syslog, smtp and other well-defined transport protocols

As certain large TPX content may require splitting the content across multiple files the manifest mechanism provides maximum flexibility.

The content introduction section has a set of key/value pairs of information that describes the overall TPX content, followed by the set of manifest arrays that point to the files used for the **Observable Dictionary**, the **Observable Elements**, the **Collections** and the **Networks**. Where each of those entries points to the specific TPX objects for those aspects of the TPX schema.

```
{
  //
  // SECTION: Intro
  // DESCRIPTION: Provides the attribute of the list, provider name, date of distribution ...etc.
  // There is only one source_observable per TPX file.
  // If a provider has multiple feeds then there will be one file per feed
  //
  "schema_version_s": "2.2.0",
  "provider_s": "Intel Provider Company",
  "list_name_s": "Intel Provider Company List Data",
  "source_observable_s": "PROV_IND_NAME",
  "source_file_s": "/var/lg/data/json/list_name/2014/06/01/202data.csv",
  "source_description_s": "This is a description of the feed and the information it provides",
  "distribution_time_t": 1221312312,
  "last_updated_t": 121232134,
  "score_i": 90,

  //
  // SECTION: Manifest for dictionary files
  //
  "dictionary_file_manifest": [
    "/var/data/json/202data_dictionary_1.json", "/var/data/json/202data_dictionary_2.json"
    ],

  //
  // SECTION: Manifest for observable element files
  //

  "observable_element_file_manifest": [
    "/var/data/json/202data_1.json", "/var/data/json/202data_2.json"
```

```
  ],

  //
  // SECTION: Manifest for collection files
  //
  "collection_file_manifest": [
    "/var/data/json/collection_1.json", "/var/data/json/collection_2.json"
  ]

  //
  // SECTION: Manifest for network files
  //
  "network_file_manifest": [
    "/var/data/json/asn_1.json", "/var/data/json/asn_2.json"
  ]
}
```

3.2 Observable Dictionary and Associations over Time

TPX supports a Threat Observable dictionary entry and zero or more Threat Observable associations with elements. The dictionary entry provides description and classification information associated with the Threat Observable independent of that observable associated with an element. The association is a specific event in time when that observable was associated with an element.

The following diagram shows the event observables occurring in time:

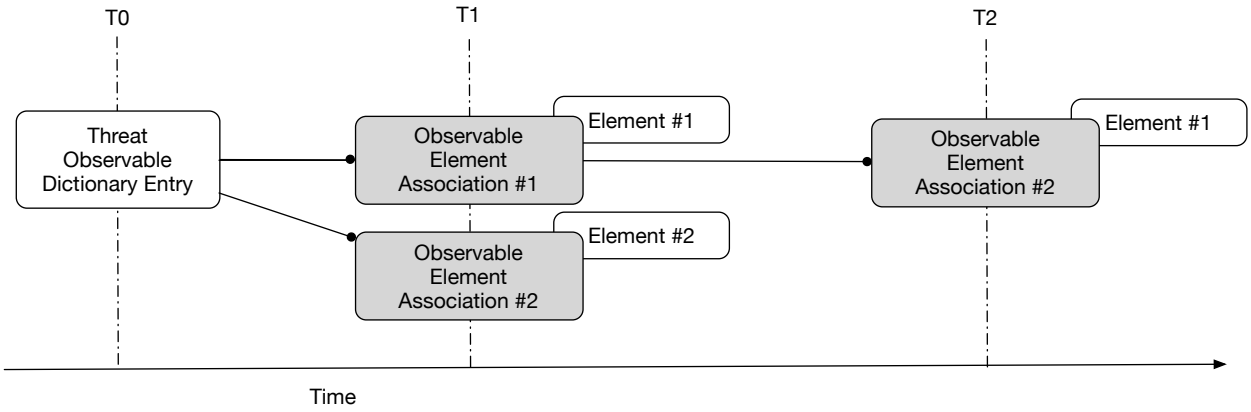

Figure 3: Observable Timeline

- T0: The dictionary entry is created by the provider.
  - The provider defines the description and the classification of the threat
- T1: The 1st instance of the Observable associated with Element #1
  - The provider observes the Threat **associated with** an element
- T1: The 1st instance of the Observable associated with Element #2
  - The provider observes the Threat associated with **another** element
- T2: The 2nd instance of the Observable associated with Element #1
  - The provider observes the Threat **again on the same element**

3.3 Observable Dictionary

This section provides details of each observable that are common across all instances of that observable.

The Threat Observable dictionary entry provides the description and classification information that is shared across all observation instances of that Threat Observable.

Example:

```
 //
 // SECTION: Observable Dictionary
 // DESCRIPTION: Provides the dictionary of all observables in this file. For each observable there is a name, criticality,
classification list
 //
 "observable_dictionary_c_array": [
  {
    "observable_id_s" : "Conficker A",
    "criticality_i": 70,
    “summary_s”: “This is a summary of the observable description”,
    "description_s": "If an IP address or domain has been associated with this tag, it means that Intel Provider Company
has identified the IP address or domain to be associated with the Conficker botnet variant A.",
    “notes_s”: “These are user defined notes providing additional background to the description”,
    "reference_s_array": [
       "http://www.thisisareference.com/observablereference", "http://www.anotherreference.com/2ndrefererence"
    ],
    "classification_c_array" : [
     {
       "classification_id_s": "Bot”,
       “classification_family_s”: “Malware”,
       "score_i": 70,
       “score_24hr_decay_i”: 2
     }
    ],
  },
]
```

3.4 Observable Association

An important part of the TPX content (within a single file or as a separate file if manifests are being used), is the association of observables to elements. It allows the provider to define network elements (e.g. IP, FQDN, CIDR, ASN), host/application elements (e.g MD5, SHA1) and then associated one or more threat observables with that element. In this section the observable is referenced by its unique identifier and where appropriate unique attributes of that observation associated with the element.

There are 3 parts to an observable association.

- At the top level there is an array that defines a list of subjects. This is defined as the “element_observable_c_array”.
- Within that array there is a list of subjects that define the network or application elements where each subject is prefixed by “subject_<type>_<id>”.
- For each subject there is a threat observable map, named “threat_observable_c_map” that defines the set of observables associated with that particular subject.

Example:

```
//
// SECTION: Observable Association List
// DESCRIPTION: Provides the association from elements to their list of observables.
```

```
// For each subject, type there is a list of threat observables and associated attributes for that observable
when the association took place on that element
//

 "element_observable_c_array": [
  {
    "subject_ipv4_s": "123.123.123.132",
    "score_i": 90,
    "threat_observable_c_map": {
          "Conficker A": {
                    "occurred_at_t": 4355545,
                    "last_seen_t": 13123,
                    "country_code_s": "IR",
                    "dest_fqdn_s": "ddd.com",
                    "score_i": 70,
                    "mitigation_c_array": [
                              { "action": "log destination 1.1.1.1" },
                              { "action": "drop" },
                    ],
          },
          "Clicker": {
                    "occurred_at_t": 4355545,
                    "last_seen_t": 13123,
                    "country_code_s": "CH",
                    "dest_fqdn_s": "aaa.com",
                    "mitigation_c_array": [
                              { "action": "log 1/1" },
                    ],
          }
},},]
```

3.5 Network Definition

The network information may be described in TPX:

- ASN Ownership
- ASN Router Members
- ASN Router Topology
- ASN CIDR Announcements
- ASN Upstream and Downstream Topology
- ASN Communities

BGP Network Example:

```
{
 "schema_version_s": "2.2.0",
 "provider_s": "CompanyName",
 "list_name_s": "LG BGP",
 "source_description_s": "This feed contains BGP routing and topology data.",
 "workspace_s": "lg-system",
 "distribution_time_t": 1429894284,
 "observed_at_t": 1429894284,
 "asn_c_array": [
  {
    //
    // This information is for ASN = 1
    //
    "asn_number_ui": 1,
    "asn_owner_s": "ABC Corp",

    //
    // The list of routers that are part of the ASN
    //
```

```
    "asn_routers_ipv4_array" : [
      1231231, 12312313214, 12131311241, 12312423414
    ],

    //
    // The router interconnections in the ASN
    //
    "asn_router_conns_c_array": [
      { "router_1_ui": 1231232112, "router_2_ui": 121435523 },
      { "router_1_ui": 2314123434, "router_2_ui": 4523423432}
    ],

    //
    // The CIDR announcements from the ASN
    //
    "asn_cidr_announcements_c_array": [
      { "start_ipv4_ui": 1234567890, "end_ipv4_ui": 2234567890, "aggregator_ipv4_ui": 12332144,
"observed_at_t": 213232232 },
      { "start_ipv4_ui": 3234567890, "end_ipv4_ui": 4234567890, "aggregator_ipv4_ui": 12332144 },
    ],

    //
    // The downstream ASNs for this ASN
    //
    "asn_downstream_ui_array": [
      2, 53, 5, 66
    ],

    //
    // The upstream ASNs for this ASN
    //
    "asn_upstream_ui_array": [
      3, 4
    ],

    //
    // The community pairs for this ASN
    //
    "asn_community_c_array": [
      { "asn_1_ui": 2323, "asn_2_ui": 2 },
      { "asn_1_ui": 3, "asn_2_ui": 4}
    ]
  },}
```

3.6 Collection Definition

A collection in TPX is a group of related entities. There are no limitations to what entities TPX could include in a collection and currently the following are defined:

- Country Codes
  - Geographic information associated with countries
- Element groups and observables
  - Threat intelligence collections define a grouping of elements and observables. They can represent market-segments, companies, organizational entities…etc. and the collections may have associated attributes.

Country Code Example:

```
{
  "schema_version_s": "2.2.0",
  "provider_s": "CompanyName",
```

```
 "list_name_s": "LG Country Codes",
 "source_description_s": "This collection is ISO-2 and ISO-3 country codes.",
 "distribution_time_t": 1429894284,
 "observed_at_t": 1429894284,
 "collection_c_array": [
   { "name_id_s": "Aruba", "iso_3_s": "abw", "iso_2_s": "aw", "region_code_ui": 0, "continent_code_ui": 6,
"continent_code_s": "na", "country_code_ui": 533 },
   { "name_id_s": "Afghanistan", "iso_3_s": "afg", "iso_2_s": "af", "region_code_ui": 1, "continent_code_ui": 4,
"continent_code_s": "as", "country_code_ui": 4 },
   { "name_id_s": "Angola", "iso_3_s": "ago", "iso_2_s": "ao", "region_code_ui": 1, "continent_code_ui": 1,
"continent_code_s": "af", "country_code_ui": 24 },
   { "name_id_s": "Anguilla", "iso_3_s": "aia", "iso_2_s": "ai", "region_code_ui": 0, "continent_code_ui": 6,
"continent_code_s": "na", "country_code_ui": 660 },
   { "name_id_s": "Aland Islands", "iso_3_s": "ala", "iso_2_s": "ax", "region_code_ui": 0, "continent_code_ui": 5,
"continent_code_s": "eu", "country_code_ui": 248 },
   { "name_id_s": "Albania", "iso_3_s": "alb", "iso_2_s": "al", "region_code_ui": 1, "continent_code_ui": 5,
"continent_code_s": "eu", "country_code_ui": 8 },
}
```

Element Collection Example:

```
 // the version of the schema being used
 "schema_version_s": "2.2.0",
 // the source provider of this collection definition
 "provider_s": "CompanyName",
 // UTC timestamp for the most recent change across the entire collection
 "last_updated_t": 343423324324,

 // collections is a grouping of references to other elements
 // the TPX format already has the definition of elements such as observables
 // these structures 'refer' and group

 "collection_c_array": [
  {
   // a top level collection
   "name_id_s": "MarketSeg1",
   // each element *may* have their own last updated timestamp
   // to indicate when the specific element was changed, no timestmap means the element was last changed
as the master list
   "last_updated_t": 1212312323,
   // each collection can have an optional description
   "description_s": "This collection is related to MarketSeg1",
   // each collection may have optional individual authors for collaboration identification
   "author_s": "Allan Thomson",
   // the optional workspace that this collection is assigned to. No workspace means the collection is a
system level
   "workspace_s": "lg-system",
   // the score of the MarketSeg1 collection
   "score_i": 90,
   "collection_c_array": [
   {
    // a 2nd level collection MarketSeg1 -> NCR10205
    // with FQDN, IP, CIDR, ASN and sub-collection defined
    "name_id_s": "NCR10205",
    "description_s": "This is NCR10205 sub-collection",
    "last_updated_t": 12123132322323,
    "author_s": "Gerry Eaton",
    "score_i": 70,
    "fqdn_ref_c_array": [
     { "fqdn_s": "seguintexas.gov" },
     { "fqdn_s": "tenaska.com" },
    ],
    "ip_ref_c_array": [
     { "ip_ipv4_s": "12.1.1.1" },
     { "ip_ipv4_s": "13.1.1.1" },
    ],
    "cidr_ref_c_array": [
     { "cidr_cidrv4_s": "208.191.120.72/29" },
```

```
    { "cidr_cidrv4_s": "208.191.120.64/29" },
   ],
   "asn_ref_c_array": [
    { "asn_number_ui": 393265 },
   ],
   // the observable list is a reference to observable definitions already in TPX file
   "observable_c_array": [
    { "observable_id_s": "Conficker A" },
    { "observable_id_s": "Tracker" },
   ],
   "collection_c_array": [
   {
    // a 3rd level collection MarketSeg1 -> NCR10205 -> 10205-SubGroup
    // With only 1 domain defined
    "name_id_s": "10205-SubGroup",
    "score_i": 50,
    "fqdn_ref_c_array": [
     { "fqdn_s": "test.gov" },
    ],
   },
   ],
},
```

4 Schema Elements

4.1 Content Introduction Elements

Table 4: Top-Level Elements

Element Term	Description	Example	Status
asn_c_array	An array of ASN network information	See examples	Optional
collection_c_array	An array of Collections	See examples	Optional
collection_file_manifest	An array of filenames (fully qualified path) where the collection files are	See examples	Optional
dictionary_file_manifest	An array of filenames (fully qualified path) where the dictionary files are	See examples	Optional
distribution_time_t	The Epoch UTC timestamp this file was distributed by the provider	123123213	Optional
element_observable_c_array	An array of Element Threat Observables	See examples	Optional
last_updated_t	The Epoch UTC timestamp this file was last changed by the provider	123123213	Mandatory
list_name_s	The threat feed list name	“list 1”	Mandatory
network_file_manifest	An array of filenames (fully qualified path) where the network files are	See examples	Optional
observable_dictionary_c_array	An array of observable definitions	See examples	Optional
observable_element_file_manifest	An array of filenames (fully qualified path) where the element observable files are	See examples	Optional
provider_s	The provider’s company name	“mycompany”	Mandatory (list only)
schema_version_s	The provider’s version of their schema	“2.2.0”	Mandatory
score_i	The score of the source feed accuracy. As assessment of the source feed’s accuracy between 1 and 100 where 100 is completely accurate	90	Optional
source_description_s	A description of the source feed that provides background to the type of data, the types of information available to the user	“The feed provides information on botnets that target data extraction from infected Windows laptops. The information available includes the botnet CC, the URLs used to extract	Optional

		information."	
source_file_s	The file containing the original feed information	[a file url]	Optional
source_observable_s	The prefix associated with this threat list	"myprefix"	Mandatory

A TPX provider should either:

- Have all content within a single file and use observable_dictionary_c_array, element_observable_c_array, collection_c_array and asn_c_array within that single TPX file
- OR
- Use the manifest options (dictionary_file_manifest..etc) where the dictionary, elements observables and collections are split across separate files.
- They should not mix single file vs multiple files.

4.2 Observable Dictionary

Table 5: Observable Dictionary Elements

Element Term	Description	Example	Status
attribute_c_map	An map of attributes associated with the observable that are common across all subjects	See examples	Optional
classification_c_array	An array of classification of this threat observable.	See examples	At least 1 required
criticality_i	The threat observable's relative criticality between 1 and 100	75	Optional
description_s	A user displayable description of the observable. This description may be a URL reference to where the content is defined.	See examples	Mandatory
notes_s	A user defined set of notes that provide background to the description	"this observable is useful in our environment for tagging unknowns "	Optional
observable_id_s	The name of the observable	"ConfickerAB"	Mandatory
reference_s_array	An array of string URL references to background information on the observable	["http://www.thisisaref.com/obsref", "http://www.anotherreference.com/2ndref"],	Optional
score_i	Optional overridden threat score between 1 and 100.	64	Optional
score_calc_setting_s	Optional parameter that defines whether the score was calculated based on a manual or automatic calculation. Default: auto	"Auto" or "Manual"	Optional
score_24hr_decay_i	Optional parameter that defines the percentage of the	2	Optional

	score decays over time if no new observation. A valid decay is between 0 and 100. A value of 0 switches off decay due to time.		
summary_s	A user displayable summary of the observable description	See Examples	Optional

4.2.1 Criticality Notes

A criticality is a TPX provider's assessment of risk associated with a particular observable. This information is sometimes referred to as reputation score, confidence, risk factor….etc.

Lookingglass recommends that TPX vendors use a scale number between 1 and 100 where a value of 100 represents the most serious risk associated and a value of 1 represents the lowest risk.

An observable may have a criticality associated with it in the dictionary in which case all subjects associated with that observable receive that criticality unless the observable + subject associated has an overridden value.

4.2.2 Classification Notes

An observable may have one or more classifications depending on the type of observable represented. The TPX data format supports any string for classification but Lookingglass recommends that TPX partners use one or more of the following classifications where possible.

The TPX classifications are based on a tree structure where there are sets of top-level classifications that identify a course grained definitions. Within each top-level classification, there are sets of additional sub-classifications that further identify specific aspects of a classification.

The TPX provider may provide an observable definition with one or more top-level classifications as well as one or more fine-grained sub-classifications. The resultant set of classification information is known as the **Observable Classification List**.

Table 6: Course-Grained Top Level Classifications

Classification	Description	Score
Malware	Malicious software, often installed without a users consent or knowledge	50
Recon	The process of information and intelligence collection, often used to orchestrate attacks	30
Malicious	Software, motives, and/or infrastructure which is intentionally harmful	30
Attack	A malicious action or event	30
Infrastructure	Physical and virtual entities that comprise a network	10
Intel	Information about a subject matter with appropriate context	70
Actions	An observed event	50

Watchlist	Items of interest	30
Actor	An individual or group with malicious intent	75

At least one of the above classifications must be provided for each Observable.

For each of the course-grained top-level classifications there are finer-grained classifications that may be provided in addition to the top-level classification for an observable.

Table 7: Fine-Grained Classifications

Classification	Description	Score
Adware	Adware is software that displays advertising. It is typically not malicious but is often a nuisance	40
Anonymization	A service that aids in the obfuscation of traffic or user activities	10
AOL	A proxy operated by America Online (AOL)	5
APT	Relating to a campaign or group using advanced and/or previously unknown techniques to attain persistence, avoid detection, exfiltrate information, and/or cause destruction/disruption	90
Automated Transfer Script	A toolset to automate the covert execution of financial transactions	70
Backdoor	Software that allows for the unauthorized bypass of authentication systems	60
BGP	BGP (Border Gateway Protocol) is a protocol designed to allow routers to exchange routing information. A BGP Hijack is the malicious, often inadvertent, advertisement of a valid route by a legitimate ISP for the purpose of traffic redirection	60
Black hat	A hacker who uses their skills with malicious intent	60
Bot	A compromised host under the control of a threat actor, often one of many such hosts, collectively called a 'Botnet'	60
Brand or Image Degradation	An action that damages the reputation of an organization	75
Bruteforce	Bruteforce, or Brute forcing, is when a compromised host or attacker attempts to break into a service through user enumeration and password guessing. It is often a dictionary attack leveraging a predefined set of easily guessed or common usernames and passwords. Prevalent attacks are aimed at FTP servers (TCP/20 and 21), secure shell (SSH TCP/22), and websites accounts (HTTP TCP/80 and HTTPS TCP/443)	30
Bulletproof Hosting/Rogue Hosting	Bulletproof Hosting, also known as BP or rogue hosting, is a server that resides in a company and/or country that does not comply with takedown notices and are usually more expensive than normal hosting providers. Some of the hosting providers go to lengths of protecting their clients for a fee. BP Hosting is notorious for hosting spam, illegal material, and command and control servers	40
C2	A Command and Control (C2 or C&C) is a centralized connection point where infected hosts obtain tasks and provide updates	75
Campaign	Interesting and/or relevant facets that help to describe an attack	70

Characteristics	campaign	
Chat Server	A server that allows for the relay of communications, frequently textual in nature	5
Click Fraud	A compromised machine performing automated 'clicking' of URLs and advertisements for the purpose of ad revenue generation	40
Cloud Hosting	A third-party provider of hosting services, typically web and storage	5
Collective Threat Intel	Threat Intelligence gathered from multiple sources about multiple subjects	70
Communications	A method for communicating information	5
Compromised Server	A server that has been illegally accessed	40
Confidential Information	Related to the loss of private information	75
Corporate	Proxies set up by organizations as a gateway for their employees to reach the Internet	5
CBRN Chemical, biological, radiological, nuclear	An individual or group who has expressed an interest in one of these areas	75
Credential Theft	Illegitimately obtaining login information	60
Credential Theft Botnet Operator	An individual or group operating a network of compromised machines whose intent is to steal account information, especially financial	50
Credential Theft Botnet Service	An individual or group operating a network of compromised machines who lease usage of the network	50
Cryptocurrency	A digital currency, backed by faith and pseudo-anonymity, which relies on advanced math and donated computing power to maintain stability and volume. Bitcoin is one such currency	5
Cyber Espionage Operations	A sophisticated individual or group whom use digital means to illegally obtain corporate, economic, political, or military information. These campaigns often go on for years before being uncovered	99
Darknet	A variant of the Internet accessible only via specialized means, whose goal is anonymity and secrecy. An example would be Tor	20
Data breach	The illegal access of a network or device resulting in the loss of proprietary and/or confidential information	75
DDoS	A distributed denial of service attack in which multiple (often compromised) hosts attack a single target	60
Degradation of Service	An event or action that causes a poor user experience	75
Destruction	An event or action that causes a poor user experience The act or process of damaging something to the extent that it is no longer usable	75
Dialer	A dialer is malware designed to automatically dial a telephone number	40
Disgruntled User	Related to an insider threat, a Disgruntled User is a legitimate	75

	user of a network or service who, for one reason or another, has malicious intent	
Disruption of Service	Potentially the result of a DDoS, is an interruption in the services offered by an organization, either causing a poor user experience or complete downtime of the service	75
DNS	The Domain Name System (DNS) is a system that allows for the translation of a domain name to an IP address. DNS Servers are servers that handle the actual translation, running on UDP/53 for queries and TCP/53 for queries and server to server administration	60
Domain Watchlist	A list of domains that have been identified as being of interest	30
DoS	A denial of service attack in which access to services are hindered	60
DoS Tools	A tool that allows for the ability to perform a denial of service attack	60
Downloader	Frequently a component of Trojans, responsible for downloading stage two payloads	50
Dropper	Frequently a component of Trojans, drops additional self-contained (obfuscated and/or packed) malware	50
Dynamic DNS	Dynamic DNS (DDNS or DynDNS) is a way to maintain domain name resolution with a dynamic IP address. DDNS is often abused by threat actors due to ease of creation of subdomains that point to changing and arbitrary IP addresses	10
Economic	An attack intent on identifying economic strategies	75
eCrime Actor	An individual or group known to be associated with various forms of digital crimes	50
Education	A proxy operated by an educational institution	5
Electronic Payment Methods	Infrastructure associated with digital payment systems	5
Email	An electronic message used by most people on the Internet. This is a delivery method of text, images, and files. Emails can contain tracking information used to identify the user opening the email	15
Endpoint Characteristics	Interesting and/or relevant facets that help to describe a client device	40
Exfiltration	The process of covertly stealing information, generally moving (copying) it from a compromised network to a staging area to be analyzed and disseminated	75
Exit Node	In Tor, an exit node is a host where Tor traffic exits the Tor network, destined for the Internet. Exit nodes aren't single purpose - they can also be an entrance to the Tor network as well as a relay, relaying Tor traffic between nodes	50
Exploit Attempt	An attempt to exploit a vulnerability	60
Exploit Kit	An Exploit Kit (EK) is a web based toolkit used by threat actors, which contains a myriad of exploits against an arbitrary number of applications. EKs target software such as Adobe Reader, Flash, and the users' browser and are set up by a threat actor on a compromised server. When a user visits the compromised	50

	server, data is gathered by the EK to determine which exploit to deliver. Once delivered, if the exploit is successful, custom code will be executed on the system which leads to an infection of some kind	
Fast Flux Botnet Hosting	Fast Flux is a DNS technique used to conceal phishing and malware distribution points through a large array of rapidly changing compromised hosts	60
File Hash Watchlist	A list of file hashes that have been identified as being of interest	30
Financial	Relating to the theft of finances or financial account information	60
Financial Loss	Having to do with the loss of currency	75
Forums	Also known as a message board, a Forum is a place where users can communicate in an email-style discussion with other users	5
Gray Hat	A hacker who uses their skills unethically to attain ethical goals	30
Hacker	An individual or group that gains access to a networked device or service. 'Hacker' is generally used to refer to individuals/groups that have gained said access without the owner or operators' consent	50
Hacktivism	Hacktivism is the act of hacking, or breaking into a computer system, for a politically or socially motivated purpose. The individual who performs an act of hacktivism is said to be a hacktivist.	40
Hijack	Capturing data in transit to be used for one's own purpose	60
Honeypot	A decoy network or device set up to deliberately distract an attacker, often times with the purpose of gaining information and insight into an attackers means and motives. Frequently, honeypots have falsified data on them that appears legitimate so as to entice an attacker	5
Host Characteristics	Interesting and/or relevant facets that help to describe a networked device when being viewed (eg: scanned) from another device	40
Hosting	This generally refers to an individual, group, or organization that provides the infrastructure for a service. For example, a VPS company hosts Virtual Private Servers for individuals who can then utilize them in any way they see fit. The term "hosting" is also commonly used to promote web site space. A company handles all of the infrastructure and maintenance, and a user need only upload their documents to begin serving website content.	5
I2P	An anonymous network, akin to Tor, that enables users to mask the source of their Internet traffic	5
Illegal Activity	Any action that falls outside the law, either foreign or domestic	15
Information Loss	The loss of access to information	75
Injection	An attempt to exploit a known or unknown vulnerability via a purposefully crafted request	45
Insider Threat	An internal danger to a company or organization, typically in the form of an employee (vs. a visitor)	75
Intellectual	Information and/or tangible items that contribute to a company's	75

Property	competitive strategy.	
IP Watchlist	A list of IP addresses and/or IP Ranges, generally in CIDR notation, that are of interest	30
IRC	Internet Relay Chat (IRC) is a client/server based chat protocol designed for text-based chat and file transfers that is commonly used. It can be used by malicious actors to control malware, as well as exfiltrate data. Typically, IRC runs over ports TCP/6667-6670 with an optional SSL layer	5
Jabber	A chat server which utilizes XMPP as its communications protocol	5
Jihadist	An Islamic militant	75
Legitimate Domain Registration Services	An organization who, for a fee, registers domain names with a Top Level Registrar on behalf of the client	1
Loss of Competitive Advantage	The loss of information or property that is detrimental to a company's success over competition	75
Malicious Domain Registrars	A domain registrar known to be tolerant of malicious domains registered by threat actors, typically by being unresponsive to formal abuse complaints	20
Malicious Email	A email designed to entice the user to unknowingly open something malicious	15
Malicious Host	A host known to be exhibiting malicious behavior of some sort.	10
Malvertising	The combined form of Malicious Advertising, refers to malicious advertisements that are unknowingly displayed by legitimate ad networks on websites	40
Malware Artifacts	A file, configuration, or system modification left behind by malware. These are commonly referred to as Indicators of Compromise (IOCs)	30
Malware Developer	The author of malicious software	60
Military	An attack intent on identifying military strategies	75
Mobile Communications	Related to infrastructure designed to provide communications services to mobile devices	5
Mobile Device	Indicates a compromised mobile device, hand-held, tablet, etc.	60
Money Laundering Network	A group of individuals attempting to legitimize illegal income from digital crimes	40
Organized Crime Actor	A group of individuals that has some form of an organized structure who's intent is to commit digital crimes	60
P2P	A group of protocols that enables individual clients to communicate directly with one another	5
Participant	A compromised host taking part in an attack	60
Password cracking	The process of programmatically attempting to recover a password	40
Phishing	A crafted, unsolicited email that entices and/or tricks users to enter personal information or deliver malware	50
Political	An attack intent on identifying political strategies	75
Port Scanner	A tool or tool suite designed to discover open channels of	20

	communication on networked host	
POS – ATM	Malware designed to target Point of Sale or Automated Teller Machine devices with the intent of stealing Credit Card information and funds	75
Probes	An exploration of network infrastructure for reconnaissance purposes	30
Proprietary Information	Related to the loss of privately owned data	75
Proxy	A network device that acts as a gateway between a client and a service or the Internet at large	5
Public	A proxy that is openly accessible	5
Ransomware	Malware designed to encrypt personal data which requires a fee to unlock	70
Regulatory, Compliance or Legal Impact	An event or sequence of events that is detrimental to the adherence of rules or laws	75
Remote Access Trojan	Malware designed to provide a persistent foothold in a device for a threat actor, allowing them to easily remotely control it	80
Rogue Antivirus	Malicious software designed to imitate an anti-virus program, scaring the user into downloading additional malicious components and/or paying an illegitimate fee to have their device 'cleaned'	40
Rootkit	Persistent malware that is difficult to detect and remove which operates at the kernel level	60
Router	A hardware device identified as a routing platform	5
Russian Business Network	The Russian Business Network was a Russian cybercrime organization that focused on identity theft. Currently it is a bulletproof hosting provider that hosts cyber crime and espionage	20
SCADA	Standing for Supervisory Control and Data Acquisition, SCADA generally refers to groups of interconnected devices that utilize coded signals to communicate, and are responsible for gathering, analyzing, and reacting to real-time data	75
Scanning	The process of gathering information about a network topology	30
Script	A text document containing commands that perform a task. These commands are usually language specific and require an interpreter to execute, such as Python, Perl, or Ruby	10
Sending Spam	Sending an unsolicited email	20
Sinkhole	A sinkhole is a dead-end destination where malicious traffic is routed. Security researchers utilize sinkholes to aid in tracking the spread of infections and to neutralize portions of malicious infrastructure	5
SMTP Abuse	Exploiting misconfigured SMTP servers to relay unsolicited email on behalf of a threat actor	20
Social Networks	Commonly websites, social networks are comprised of groups of individuals communicating and exchanging information electronically	5
Spam	Unsolicited email	5
Spam Service	A paid-for service that will send unsolicited emails to an arbitrary list of recipients	20

Spyware	A classification of Malware that is designed steal personal information and track a users usage of the infected device	40
State Actor or Agency	Refers to a Threat Actor that is sponsored/supported by a Nation State	85
Stress Test Tool	A tool or suite of tools designed to push the physical limits of a device or network	60
Threat Actor Characterization	The descriptive profiling of an individual or group that is suspect of malicious intent	70
Threat Report	An informational document describing a specific threat or campaign, commonly accompanied by an in-depth technical analysis	70
Top-Level Domain Registrars	One of eight organizations responsible for delegating TLDs on the Internet. The Public Root (http://inaic.com/index.php?p=public-root-servers) resolves all TLDs registered through any of these organizations, meaning that anyone, anywhere can perform the same DNS query and get the same result	1
Tor	Tor is free software that enables users to remain anonymous on the Internet via the use of encryption and advanced traffic routing techniques	10
Transparent	Often used in conjunction with 'Proxy', indicates a networking layer that is invisible to the user	5
Trojan	Software that appears to be one thing, generally harmless, but in actuality is malicious in nature	50
TTP	Tactics, Techniques, and Procedures (TTPs) are individual patterns of behavior of a particular malicious activity, or a particular malicious organization	70
Unintended Access	Accidentally gaining access to something, often a networked service or device, without the owners permission	75
URL Watchlist	A list of potentially malicious URLs	30
User Data Loss	When users' access to their data is lost	75
User-Generated Content Websites	Websites that allow users to create their own content, such as blogs	5
VPN	An acronym standing for 'Virtual Private Network', is a technology that allows a user to connect to a remote network. Frequently, VPNs are used as tunnels to proxy traffic with the intent of anonymizing their traffic	5
Vulnerability Scanner	An automated tool that scans networks, devices, and/or services for weaknesses, frequently done for the purpose of exploitation	40
Vulnerable Service	A service identified as being vulnerable to a known exploit	40
Web Panel	A web-based UI located on a C2 server that allows threat actors to control their bots	75
Web Shell	Simple or complex executable code, commonly PHP or .NET, running on a compromised web server providing remote access to attackers to perform malicious actions on or with the host. One of the most commonly used web shells is the PHP/c99shell	65
White Hat	A hacker who uses their skills legally, ethically, and professionally	5

White Supremacist	An extremist whom believes that white people are superior to all other races	65
Worm	A type of malware that spreads on its own via network and removable devices	60

4.3 Observable Association

An observable association is the association of one or more threat observables with a subject entity (i.e. IP, FQDN, Malware Hash…etc)

Table 8: Observable Association Map

Element Term	Description	Example	Status
score_i	The element's overridden score if not derived from scoring of the observables	80	Optional
score_calc_setting_s	Optional parameter that defines whether the score was calculated based on a manual or automatic calculation. Default: auto	"Auto" or "Manual"	Optional
score_24hr_decay_i	The element's overridden score decay if not derived from the observable's decay parameter. 0 indicates this particular element's score will not change due to time decay alone.	0	Optional
subject_<type>_s	An <typed> element subject identifier	"12.1.1.1"	Mandatory
threat_observable_c_map	A map of Threat Observables that is associated with the subject. The threat observable must already be defined in the observable dictionary to be referenced by this map.	See examples	At least 1 required

4.3.1 Type Notes

The subject of the element has a type that is combined with subject_<type>_s to define the key name.

The TPX data format supports any string for type but OpenTPX recommends use one of the following types where possible.

- ipv4
- ipv6
- fqdn
- cidrv4

- cidrv6
- asn
- md5
- sha1
- sha256
- sha512
- registrykey
- filename
- filepath
- mutex
- actor
- email
- account

4.4 Threat Observable Elements

A Threat Observable is a named observation associated at a specific time against a network element.

Table 9: Threat Observable Elements

Element Term	Description	Example	Status
<key>	The threat observable's name as a key in the map	"c2s"	Mandatory
attribute_c_map	A map of attributes associated with this threat observable	See examples	At least one attribute

4.5 Classification List Elements

Table 10: Classification List Elements

Element Term	Description	Example	Status
classification_family_s	The top-level family of this classification. This value must be a top-level classification.	"malware"	Optional
classification_id_s	The name of the classification. This value must be a fine-grained classification.	"C2"	Mandatory
score_i	The criticality/score of the classification between 1 and 100 where a higher number is a higher risk classification	74	Optional

4.6 Common Attribute List Elements

The following attributes are shared across multiple complex types within TPX.

Every attribute is a 3-tuple with name, type, value where the name and type are combined into a single key enabling optimized parsing. A TPX provider may add additional attributes to the list where an existing term does not cover the attribute being communicated.

Table 11: Attribute List Elements

Element Term	Description	Example	Status
access_count_ui	The number of times a site, malware or request has occurred	12	Optional
account_c_array	The list of user account key/value pairs	“user@company.com”	Optional
browser_id_s	The browser identifier	“Firefox”	Optional
city_s	The name of the city	“Edinburgh”	Optional
classification_id_s	The name of the classification	“c2s”	Optional. Only if overriding the dictionary
continent_code_ui	The continent code for the country code file	6	Optional
continent_code_s	The continent name for the country code file	“na”	Optional
country_code_ui	The country identifier as part of the country code file	533	Optional
country_code_s	The 2 or 3 digit country code associated with the threat observable	US	Optional
country_s	The full name of the country	Austria	Optional
description_s	The description of the observable or element or collection	This observable represents that the infected host is communicating with a command and control server	Optional
dest_port_i	A destination protocol port	{ “dest_port_i”: 12 }	Optional
dest_ipv4_s	A destination IP v4 address as a string	{ “dest_ipv4_s”: “12.1.1.1” }	Optional
dest_ipv4_ui	A destination IP v4 address as an unsigned integer	{ “dest_ipv4_ui”: 1213223 }	Optional
dest_fqdn_s	The domain that a particular botnet or peer to peer communication threat was destined to	Ddd.com	Optional
dns_request_c_array	The list of DNS requests made	"req_fqdn": "irc.freenode.net" }	Optional
dns_response_c_array	The list of DNS responses where each response is { Dns-record-type : Dns-value}	{ "record_s": "A", "resp_ip": "12.1.1.1" },	Optional
filepath_s_array	The filepaths used by malware	filepath_s_array": ["C:\\DOCUME~1\\Me\\LOCALS~1\\Temp\\nsj1.tmp"]	Optional
filesize_i	The size of a file used to convey some behavior	123133	Optional
fqdn_c_array	The list of FQDN mappings in the PCAP	{ "fqdn": "eff.com", "ip": "12.1.1.1" },	Optional

geoloc_lat_f	The latitude of the observable if known	{ “geoloc_lat_f”: -10.2 }	Optional
geoloc_long_f	The longitude of the observable if known	{ “geoloc_long_f”: 9.9 }	Optional
hash_md5_h	The MD5 hash of a file	See example	Optional
hash_sha1_h	The SHA1 hash of a file	See example	Optional
hash_sha256_h	The SHA256 hash of a file	See example	Optional
hash _sha512_h	The SHA512 hash of a file	See example	Optional
host_c_array	The list of hosts in the PCAP	{ "host_fqdn": "badguy.com" },	Optional
http_c_array	The list of HTTP key/value pairs in the PCAP	{ "body_s": "", "method_s": "GET", "version_s": "1.1", "user_agent_s": "Battle.net/1.2.4.5383"}	Optional
imei_s	The IMEI	359688052678595	Optional
imsi_s	The IMSI	460023871086752	Optional
iso_3_s	The ISO 3 letter code for the country	Abw	Optional
iso_2_s	The ISO 2 letter code for the country	Aw	Optional
internal_ipv4_s	A private/internal IP v4 address as a string	{ “internal_ipv4_s”: “10.1.1.1” }	Optional
isp_name_s	The ISP name	“Comcast”	Optional
last_seen_t	The Epoch UTC timestamp of the last update when this threat observable was observed associated with the subject	12312312	Optional
magic_s	The description of the file	"tcpdump capture file (little-endian) - version 2.4 (Ethernet, capture length 65535)"	Optional
malware_version_s	The version of malware or botnet if known	“2.2”	Optional
mime_type_s	The mime type of the file	"application/vnd.tcpdunmp.pcap"	Optional
mitigation_c_array	The list of mitigation actions	"mitigation_c_array": [{ "action": "log 1.1.1.1"}, { "action": "drop" }]	Optional
mobile_network_operator_s	The mobile network operation	“British Telecom”	Optional
msisdn_s	The MS ISDN	+436803315878	Optional
mutex_s_array	The mutex used by malware as an array	"mutex_s_array": ["CTF.TimListCache.FMPDefaultS-1-5-21-2025429265-1580436667-1957994488-1003MUTEX.DefaultS-1-5-21-2025429265-1580436667-1957994488-1003"]	Optional
naics_code_i	The NAICS code	{ “naics_code_i”: 22 }	Optional
naics_code_s	The NAICS code as a string	{ “naics_code_s”: “Utilities”	Optional
name_id_s	The name of the country provided	“Aruba”	Optional

	as part of a country code file		
netblock_fqdn_s	The netblock FQDN	“telekom.at”	Optional
occurred_at_t	The Epoch UTC timestamp when this particular threat observable was first observed associated with the subject	12332322	Mandatory
organization_name_s	The organization’s name of a network asset	“MyCompany Inc”	Optional
os_s	The operating system identifier string	“MacOs 10.1”	Optional
postal_code_s	The postal code or ZIP code or equivalent	“CA95134”	Optional
protocol_s	The protocol	“UDP”, “HTTP”, “TCP”, “P2P”	Optional
query_s	A query that is associated with an observable or element. Syntax of supported queries are defined in the OpenTPX QL syntax	“score:[90 to 100]”	Optional
region_code_ui	The regional code for the country code file	1	Optional
referrer_s	The referrer URL	“http://www.google.com”	Optional
registrykey_s_array	The list of registry keys	"registrykey_s_array": ["HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet001\\Services\\PDRELI\\ObjectName"]	Optional
request_path_s	The request path of a HTTP request	“/feff/eee”	Optional
score_i	The criticality/score of the classification between 1 and 100 where a higher number is a higher risk observable	74	Optional. Only if overriding the dictionary value of the criticality for this observable
score_calc_setting_s	Optional parameter that defines whether the score was calculated based on a manual or automatic calculation. Default: auto	“Auto” or “Manual”	Optional
size_i	A size in bytes of a communication or entity	{ “size_i”: 12312313 }	Optional
smtp_c_array	The list of SMTP key/value pairs in the PCAP		Optional
src_port_i	A source protocol port	{ “src_port_i”: 12 }	Optional
src_ipv4_s	A source IP v4 address as a string	{ “src_ipv4_s”: “12.1.1.1” }	Optional
src_ipv4_ui	A source IP v4 address as an unsigned integer	{ “src_ipv4_ui”: 1213223 }	Optional
ssl_c_array	The list of SSL key/value pairs in	{ "session_start_t":	Optional

	the PCAP	123123123, "session_info_s": "session started on port 1232" },	
tcp_c_array	The list of SMTP key/value pairs in the PCAP	{ "src_port_i": 58463, "src_ip": "172.16.246.6", "dest_port_i": 22, "dest_ip": "10.0.50.3"},	Optional
tlp_i	The Traffic Light Protocol value. 0 – White, 1 – Green, 2 – Amber, 3 – Red	{ “tlp_i”: 1 }	Optional
transport_protocol_s	The transport layer protocol for applications or malware that have an application protocol within a transport protocol	“UDP”, “HTTP”, “TCP”	Optional
url_s	The url associated with the observable	www.badstuff.com/badwebpage	Optional
user_agent_s	The user agent within HTTP	"user_agent_s": "Battle.net/1.2.4.5383"	Optional

Note:

- Mitigation action key is defined to be “action” but the value of the action can be anything that a recipient understands or can translate to their local mitigation syntax.
- Mitigation actions may be combined to allow the recipient to perform sequential mitigation actions
- Recommended mitigation action values include:
  - drop
    - Drop the specific subject’s traffic
  - log <ip | url | slot/port | filename | smtp>
    - Log (i.e. copy) the subject’s traffic matching the threat observable to the chosen destination
  - rate-limit <bps-rate>
    - Rate-limit the traffic to a specific bits-per-sec
  - forward [slot/port]
    - Forward the subject’s traffic. Optionally redirect the traffic to a specific slot/port if provided otherwise the default forwarding decision will be chosen based on the platform’s switch/route state

4.7 Network Elements

In addition to the common attributes, the following attributes may be specified for network specific elements.

Table 12: Network Elements

Element Term	Description	Example	Status
asn_cidr_announcements_c_array	The array of CIDR announcements in this ASN	See example	Optional
asn_community_c_array	The array of communities within this ASN	See example	Optional
asn_downstream_ui_array	The array of downstream ASNs from this ASN	See example	Optional
asn_owner_s	The owner of the ASN	“utp”	Optional
asn_routers_ipv4_array	The array of routers that	See example	Optional

	make up this ASN		
asn_router_conns_ipv4_array	The array of router interconnections in this ASN	See example	Optional
asn_upstream_ui_array	The array of upstream ASNs from this ASN	See example	Optional

4.8 Collection Elements

In addition to the common attributes, the following attributes may be specified for collections.

Table 13: Collection Elements

Element Term	Description	Example	Status
author_s	A name associated with the last team, group, company or person making the change	“Allan”	Optional
asn_ref_c_array	An array of ASN elements referenced by this collection	See examples	Optional
cidr_ref_c_array	An array of CIDR elements referenced by this collection	See examples	Optional
collection_c_array	An array of children collections contained within this collection	See examples	Optional
fqdn_ref_c_array	An array of FQDN elements referenced by this collection	See examples	Optional
ip_ref_c_array	An array of IP (v4 and v6) elements referenced by this collection	See examples	Optional
last_updated_t	The UTC Epoch time of the last update to this collection	23232232	Optional
name_id_s	The name of the collection	“MyCompanyX”	Mandatory
observable_ref_c_array	An array of observables referenced by this collection	See examples	Optional
workspace_s	A collaboration space this collection is associated with	“incidentResponseTeamWS”	Optional

5 OpenTPX Query Language (OpenTPX QL)

The syntax is a dialect of Solr Lucene, with extensions that ease querying network elements. OpenTPX QL supports advanced query grouping, ranges, and wildcarding of values passed to terms.

The following is a description of the syntactical elements for this dialect in EBNF notation:

```
whitespace = { " " | "\t" | "\n" | "\r" } ;
string = '"' , { characters } , '"' ;
integer = { '0', '1', '2', '3', '4','5', '6', '7', '8', '9' },
field-separator = ':' ;
group-begin = '(', [ whitespace ] ;
group-end = ')', [ whitespace ] ;
range-begin = '[', [ whitespace ] ;
range-end = [ whitespace ], ']' ;
range-to = whitespace, 'TO', whitespace ;
wildcard = '*' ; wildcard_single = '?' ;
and-token = [ whitespace ], 'AND', [ whitespace ] ;
or-token = [ whitespace ], 'OR', [ whitespace ] ;
not-token = [ whitespace ], 'NOT' | '!', [ whitespace ] ;
symbol = [ whitespace | symbol ] | begin-of-input, {characters} , [
whitespace | end-of-input ];
range = range-begin, [ integer, string, symbol, wildcard ], whitespace,
range-to, whitespace, [ integer, string, symbol, wildcard ];
term = symbol, field-separator, [ string, symbol, integer, range ] ;
and = { term, group, and, or, not }, and-token, { term, group, and, or, not
};
or = { term, group, and, or, not }, or-token, { term, group, and, or, not };
not = not-token, { term, group, and, or, not } ;
group = group-begin, { group, term, and, or, not }, group-end ;
```

5.1 Basic Queries

The most basic `Query` in OpenTPX QL is a single `Term`. `Terms` are in the following format: `field:value` which is a `Field`, followed by a `:`, followed by a `Value`. Examples:

- `foo:bar` - searches `foo` for `String` "`bar`".
- `foo:5` - searches `foo` for `Integer` 5.

All `Fields` in queries against a data store is typed explicitly as either an `Integer` or `String`. The `Field` in a query is typed by appending the relevant type indicator to the `Field`:

- `Integer` - `_i`
- `String` - `_s`

`Values` in a `Term` in a basic query can be one of the following types:

- `Symbol` - `Symbols` will be evaluated as `Strings`, as a convenience. However, any special characters that would be evaluated as OpenTPX QL syntax would need to be quoted in a `String`, including `Values` with whitespace.
- `Strings` - Anything between two `"` double-quote or `'` single-quote characters are `Strings`.
- `Integer` - Any non-floating `Numeric`.

Example queries might be:

- `observable_s:Zeus` - return all entities where `observable_s` matches `Zeus`.
- `timestamp_i:1414503194` - return all entities with an exact `timestamp_i` match.
- `observable_s:'Banking Trojan'` - return all entities where `observable_s` matches `Banking Trojan`.

5.2 Wildcard Queries

In OpenTPX Solr, the following wildcards are supported in `Values`:

- `*` - `Wildcard` - multi-character
- `?` - `WildcardChar` - single-character

Wildcards have the following restrictions:

- Wildcards are not permitted for `Integers`.
- `Values` cannot start with a wildcard. i.e. left-anchored wildcards in strings such as `*foobar` will not be accepted.
- `Values` can themselves be a single `Wildcard` to express a query that wishes to select for the existence of a `Field`.
- `Fields` cannot contain wildcards.

Example queries might be:

- `observable_s:Banking*` - return all entities where `observable_s` begins with `Banking`.
- `sha1_s:????f4f4e4cf2f9669cc61e2565effcd8f923d28` - return all entities where the last 36 characters of the `sha1_s` match the provided hex digest.
- `url_s:http://msn*.com` - return all entities where the URL begins with `msn` and ends with `.com`.

5.3 Range Queries

`Values` in a `Term` can also be a `Range`. `Ranges` are expressed in the following format: `[begin TO end] begin` and `end` can either be an `Integer` or a `Wildcard`. `Ranges` currently only support `Numeric` ranges currently.

The equivalent of <= or `less than or equal` would be beginning a range with a `Wildcard` and terminating with an `Integer`:

- `x <= 10` is `x:[* TO 10]`

The opposite, >= or `greater than or equal` would be beginning a range with an `Integer` and terminating with a `Wildcard`:

- `x >= 10` is `x:[10 to *]`

Using the above, we can construct queries such as:

- `timestamp_i:[1414503194 TO *]` - return all entities which were last updated sooner than `1414503194`.
- `timestamp_i:[* to 1414503194]` - return all entities whose last updates were older than `1414503194`.

5.4 Booleans

OpenTPX QL supports `Boolean` operators as part of the query language. They are:

- `NOT` or `!` - `NOT` can be applied before any `Term`, including `Ranges`.
- `OR` - `OR` can be applied between any `Groups` or `Terms`.
- `AND` - `AND` can be applied between any `Groups` or `Terms`.

Please note that unlike Apache Solr, OpenTPX QL resolves Booleans in Boolean Algebraic precedence; `NOT` is resolved before `OR` is resolved before `AND`.

Examples of `Booleans` in use:

- `NOT observable_s:Banking*` - return all entities where `observable_s` does `NOT` begin with `Banking`.
- The above can also be written as `!observable_s:Banking*`.
- `observable_s:Banking* AND timestamp_i:[1414503194 TO *]` - return all entities where `observable_s` begins with `Banking` and was last updated past `1414503194`.
- `observable_s:Banking* OR observable_s:Trojan*` - return all entities where `observable_s` either begins with `Banking` or `Trojan`.

OpenTPX QL supports implicit `AND`; that is, `Terms` and `Groups` that do not have any tokens or symbols in between are resolved as if they have `AND` joining them.

The second example above could instead be written as, leveraging implicit `ANDs`:

- `observable_s:Banking* timestamp_i:[1414503194 TO *]`

5.5 IPv4 and CIDR Types

OpenTPX QL supports IPv4 addresses and IPv4 networks written with CIDR netmasks as the `Value` for any `Term`, and will translate into the appropriate `Range` and `Integer` types internally.

- IPv4 notation - `192.168.0.1`
- CIDR notation - `192.168.0.0/24`

Example usage of the above notation forms are:

- Individual IPs - `ip_i:10.0.0.1`
- multiple IPs - `ip_i:10.0.0.1 OR ip_i:10.0.0.2`
- CIDR searches against IP field - `ip_i:10.0.0.0/8`
- IP range searches, specified as - `ip_i:[10.0.0.0 TO 10.255.255.255]`
- Multiple IPranges - `ip_i:10.0.0.0/8 OR ip_i:192.168.0.0/16`
- Search for CIDRs that encompass this CIDR: `cidr_i:10.0.0.0/24`
- Any indicators with a non-null IP: `ip_i:*`

OpenTPX QL does *not* support wildcarding in IPs, such as:

- `ip_i:10.0.0.*`

5.6 Grouping

OpenTPX QL also supports sub query grouping, which can be useful for altering the order and precedence of the Boolean statements. Groups are begun with the `(`character and terminated with the) character. Groups can also be nested to an arbitrary depth, as needed.

For example:

Default: `a:1 b:2 OR c:3` would evaluate as an implicit `AND` in between `a:1` and `b:2`. `OR` takes precedence before `AND` in Boolean Algebra, so this would evaluate as `(a:1 AND (b:2 OR c:3))`.

Grouped: The above statement can be written as: `(a:1 b:2) OR c:3` to alter the order of evaluation, and will evaluate as `(a:1 AND b:3) OR c:3`

Complex possibilities are:

- `(ip_i:10.0.0.1 AND observable_s:Banking*) OR (ip_i:10.0.0.2 AND observable_s:Trojan*)`
- `(ip_i:10.0.0.0/24 indicator_s:*) OR (ip_i:10.1.1.0/24 observable_s:Firewall*)`

•

6 Single File Examples

The following example files describe both the dictionary of the observable and the observable associations to network elements in one file. This would typically be useful for smaller amounts of data to be conveyed.

6.1 Observations IP, FQDN, MD5 Example

This example shows how the TPX vendor “Intel Provider Company” has a list of IP, FQDN elements that have a variety of threat observables associated with them.


```
{
  "schema_version_s": "2.2.0",
  "provider_s": "Intel Provider Company",
  "list_name_s": "Intel Provider Company List Data",
  "source_observable_s": "PROV_IND_NAME",
  "source_file_s": "/var/lg/data/json/list_name/2014/06/01/202data.csv",
  "source_description_s": "This is a description of the feed and the information it provides",
  "distribution_time_t": 1221312312,
  "last_updated_t": 121232134,
  "score_i": 90,
  "observable_dictionary_c_array": [
    {
      "observable_id_s" : "Conficker A",
      "criticality_i": 70,
      "score_i": 72,
      "summary_s": "This is a summary of the observable",
      "description_s": "If an IP address or domain has been associated with this tag, it means that Intel Provider Company
has identified the IP address or domain to be associated with the Conficker botnet variant A.",
      "notes_s": "User defined notes",
      "reference_s_array": [
         "http://www.thisisareference.com/observablereference", "http://www.anotherreference.com/2ndrefererence"
      ],
      "classification_c_array" : [
        {
          "classification_id_s": "Worm",
          "classification_family_s": "Malware",
          "score_i": 70
        }
      ]
    },
    {
      "observable_id_s": "Clicker",
      "criticality_i": 70,
      "score_i": 72,
      "summary_s": "This is a summary of the observable",
      "description_s": "If an IP address or domain has been associated with this tag, it means that Intel Provider Company
has identified the IP address or domain to be associated with the Clicker botnet.",
      "notes_s": "User defined notes",
      "reference_s_array": [
         "http://www.thisisareference.com/observablereference", "http://www.anotherreference.com/2ndrefererence"
      ],
      "classification_c_array": [
        {
          "classification_id_s": "Bot",
          "classification_family_s": "Malware",
          "score_i": 70
        }
      ]
    },
    {
      "observable_id_s": "Sality",
```

```
    "criticality_i": 70,
    "score_i": 72,
    "summary_s": "This is a summary of the observable",
    "description_s": "If an IP address or domain has been associated with this tag, it means that Intel Provider Company
has identified the IP address or domain to be associated with the Sality botnet variant 1.",
    "notes_s": "User defined notes",
    "reference_s_array": [
       "http://www.thisisareference.com/observablereference", "http://www.anotherreference.com/2ndrefererence"
    ],
    "classification_c_array": [
     {
       "classification_id_s": "Bot",
       "classification_family_s": "Malware",
       "score_i": 70
     }
    ]
   }
 ],
 "element_observable_c_array": [
   {
    "subject_ipv4_s": "123.123.123.132",
    "score_i": 90,
    "threat_observable_c_map": {
       "Conficker A": {
            "occurred_at_t": 4355545,
            "last_seen_t": 13123,
            "country_code_s": "IR",
            "dest_fqdn_s": "ddd.com",
            "score_i": 70
          },
       "Clicker": {
            "occurred_at_t": 4355545,
            "last_seen_t": 13123,
            "country_code_s": "CH",
            "dest_fqdn_s": "aaa.com"
          }
     }
   },
   {
    "subject_fqdn_s": "www.badguy.com",
    "threat_observable_c_map": {
       "Conficker A" : {
            "occurred_at_t": 4355545,
            "last_seen_t": 13123
       }
    }
   },
   {
    "subject_md5_h": "bb1bb053843ca7a03152790a79ac64bd",
    "threat_observable_c_map":
     {
       "Conficker A" : {
            "occurred_at_t": 4355545,
            "last_seen_t": 13123
       }
     }
   }
 ]
}
```

6.2 Malware Report Example

This example shows a report on malware determined by a sandbox technology and potentially a list of IP and FQDNs that have been seen distributing the malware. The malware dictionary definition defines the IOCs as observed on the malware.


```
{
   "schema_version_s": "2.2.0",
   "provider_s": "LookingGlass",
   "last_updated_t": 1441402033,
   "list_name_s": "Automated Malware Analysis",
   "score_i": 95,
   "source_observable_s": "LG CTIG",
   "source_description_s": "This feed provides data collected from the automated behavioral analysis of malware by the
LookingGlass Cyber Threat Intelligence Group",
   "observable_dictionary_c_array": [
      {
         "observable_id_s": "Automated Malware Analysis Report -
08cffe1eceda66e81f6bed4ddadb08f1566a091b7bdb157778f147112151068c",
         "criticality_i": 60,
         "classification_c_array": [
            {
               "score_i": 30,
               "classification_id_s": "Malware Artifacts",
               "classification_family_s": "Malware"
            }
         ],
         "description_s": "A report containing the summary of an automated malware analysis on a specific piece of
malware, which includes behavioral analysis data such as outbound communication destinations and host based
indicators of compromise",
         "attribute_c_map" : {
            "hash_md5_h": "25e2c09e64df62a7a735b670e0ad42a3",
            "hash_sha1_h": "fb5e7302949bd85797badf8ccfb090b89ee88758",
            "hash_sha256_h": "08cffe1eceda66e81f6bed4ddadb08f1566a091b7bdb157778f147112151068c",
            "hash_sha512_h":
"5ee9c830f9f349220f71e99d7f992731d8836485e41d93e1bc4065d95721580d8e36a1099b63079feb9f9ee27ab39c7d
fc40562cd431f2474252efda6039b5df",
            "magic_s": "PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive",
            "last_seen_t": 12312312,
            "tlp_i": 1,
            "filepath_s_array": [
               "C:\\DOCUME~1\\Me\\LOCALS~1\\Temp\\nsj1.tmp",
               "C:\\DOCUME~1\\Me\\LOCALS~1\\Temp\\nsj1.tmp",

"C:\\DOCUME~1\\Me\\LOCALS~1\\Temp\\08cffe1eceda66e81f6bed4ddadb08f1566a091b7bdb157778f14711215106
8c",
               "C:\\DOCUME~1\\Me\\LOCALS~1\\Temp\\oo9.ddbcabfcdbhc",
               "C:\\DOCUME~1\\Me\\LOCALS~1\\Temp\\nsx2.tmp",
               "C:\\DOCUME~1\\Me\\LOCALS~1\\Temp\\nsx2.tmp\\frqss.dll",
               "C:\\DOCUME~1\\Me\\LOCALS~1\\Temp\\ddbcabfcdbhc.zip",
               "C:\\DOCUME~1\\Me\\LOCALS~1\\Temp\\nsx2.tmp\\nsisunz.dll",
               "C:\\DOCUME~1\\Me\\LOCALS~1\\Temp\\oo9.exe",
               "C:\\DOCUME~1\\Me\\LOCALS~1\\Temp\\ddbcabfcdbhc.exe"
            ],
            "registrykey_s_array": [
               "HKEY_LOCAL_MACHINE\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\Explorer",
               "HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\Explorer",

"HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\ShellCompatibility\\Objects\\{20D04FE0-
3AEA-1069-A2D8-08002B30309D}"
            ],
            "mutex_s_array": [
               "CTF.TimListCache.FMPDefaultS-1-5-21-2025429265-1580436667-1957994488-1003MUTEX.DefaultS-1-5-
21-2025429265-1580436667-1957994488-1003"
            ],
            "dest_ipv4_s_array": [
```

```
                "8.8.8.8", "12.1.1.1"
            ],
            "dest_fqdn_s_array": [
                "twitter.com", "google.com", "gree.ck"
            ]
        }
    },
    {
        "observable_id_s": "Observed Malware Distribution",
        "criticality_i": 65,
        "classification_c_array": [
            {
                "score_i": 30,
                "classification_id_s": "Malware Artifacts",
                "classification_family_s": "Watchlist"
            },
            {
                "score_i": 30,
                "classification_id_s": "IP Watchlist",
                "classification_family_s": "Malware"
            },
            {
                "score_i": 30,
                "classification_id_s": "Domain Watchlist",
                "classification_family_s": "Malware"
            }
        ],
        "description_s": "An outbound destination for a specific piece of malware that was observed communicating
with it via DNS, HTTP, or other protocols"
    }
  ],
  "element_observable_c_array": [
    {
        "subject_ipv4_s": "8.8.8.8",
        "threat_observable_c_map": {
            "Observed Malware Distribution": {
                "occurred_at_t": 4355545,
                "last_seen_t": 13123
            }
        }
    },
    {
        "subject_ipv4_s": "74.125.34.46",
        "threat_observable_c_map": {
            "Observed Malware Distribution": {
                "occurred_at_t": 4355545,
                "last_seen_t": 13123
            }
        }
    },
    {
        "subject_fqdn_s": "gfff.google.com",
        "threat_observable_c_map": {
            "Observed Malware Distribution": {
                "occurred_at_t": 4355545,
                "last_seen_t": 13123
            }
        }
    }
  ]
}
```

6.3 Malware Report #2 Example

This example shows a report on malware determined by a sandbox technology. The malware dictionary definition defines the IOCs as observed on the malware.


```
{
   "source_observable_s": "LG CTIG",
   "list_name_s": "Automated Malware Analysis",
   "observable_dictionary_c_array": [
      {
         "criticality_i": 60,
         "classification_c_array": [
            {
               "score_i": 30,
               "classification_id_s": "Malware Artifacts",
               "classification_family_s": "Malware"
            }
         ],
         "observable_id_s": "Automated Malware Analysis Report -
947875388ff7e99613a58a3af3890d9304d912cb15b388f42875a212035e5f8a",
         "attribute_c_map": {
            "magic_s": "PE32 executable (console) Intel 80386, for MS Windows",
            "tlp_i": 1,
            "last_seen_t": 1442949180,
            "dest_fqdn_s_array": [
               "xthefo.com",
               "qyupbu.com",
               "sliyjy.com",
               "ewyaio.com",
               "bljwia.com",
               "ycdjui.com",
               "blovra.com",
               "zuyttv.com",
               "annume.com",
               "sb-ssl.google.com",
               "retuoi.com",
               "kivbwa.com",
               "avtgny.com",
               "zaoqad.com",
               "ant.trenz.pl",
               "ubonin.com",
               "ylfilr.com",
               "ilo.brenz.pl",
               "ooveyg.com",
               "qnunoe.com",
               "lbuyzo.com"
            ],
            "hash_md5_h": "0dd3f6a83347768b88f3013dce592d3d",
            "hash_sha512_h":
"5f199ae2df70ec1d73c9c43ece12350d9b50dab7c043264fee6ab4566be81a5c3b52328e006a9c90faba06f763b382ee5
a48d6cff2867a9aeb95e01fe4c446ee",
            "hash_sha256_h": "947875388ff7e99613a58a3af3890d9304d912cb15b388f42875a212035e5f8a",
            "filepath_s_array": [
               "C:\\WINDOWS\\system32\\ntkrnlpa.exe",
               "\\Device\\NamedPipe\\lsass"
            ],
            "virustotal_permalink_s":
"https://www.virustotal.com/file/947875388ff7e99613a58a3af3890d9304d912cb15b388f42875a212035e5f8a/analys
is/1442937524/",
            "registrykey_s_array": [
               "HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet001\\Services\\PDRELI\\ObjectName",
               "HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet001\\Services\\aic78u2\\ObjectName",
               "HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\WBEM\\CIMOM\\Logging",
               "HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet001\\Services\\ql1080\\ObjectName",
               "HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet001\\Services\\Atmarpc\\ObjectName",
               "HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet001\\Services\\Fdc\\ObjectName",
```

```
                "HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet001\\Services\\Cdaudio\\ObjectName",
                "HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet001\\Services\\hpn\\ObjectName",
                "HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet001\\Services\\adpu160m\\ObjectName",
                "HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet001\\Services\\ql12160\\ObjectName",
                "HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet001\\Services\\Atdisk\\ObjectName",
                "HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet001\\Services\\Modem\\ObjectName",
                "HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet001\\Services\\NwlnkFlt\\ObjectName",
                "HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet001\\Services\\RDPWD\\ObjectName",
                "HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet001\\Services\\CmdIde\\ObjectName",
                "HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet001\\Services\\AsyncMac\\ObjectName",
                "HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet001\\Services\\IpInIp\\ObjectName",

"HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet001\\Services\\SharedAccess\\Parameters\\FirewallPolicy\\StandardProfil
e\\AuthorizedApplications\\List\\\\??\\C:\\WINDOWS\\system32\\winlogon.exe",
                "HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet001\\Services\\PCIDump\\ObjectName",
                "HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet001\\Services\\Ql10wnt\\ObjectName",
                "HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet001\\Services\\Ibrtfdc\\ObjectName",
                "HKEY_LOCAL_MACHINE\\SYSTEM\\Setup\\SystemSetupInProgress",
                "HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\WBEM\\CIMOM\\Log File Max Size",
                "HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet001\\Services\\redbook\\ObjectName",
                "HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet001\\Services\\PDFRAME\\ObjectName",
                "HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet001\\Services\\Pcmcia\\ObjectName",
                "HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet001\\Services\\PDCOMP\\ObjectName",
                "HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet001\\Services\\asc\\ObjectName",
                "HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet001\\Services\\dpti2o\\ObjectName",
                "HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet001\\Services\\amsint\\ObjectName",
                "HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet001\\Services\\Ip6Fw\\ObjectName",
                "HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet001\\Services\\Fastfat\\ObjectName",
                "HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet001\\Services\\Cpqarray\\ObjectName",
                "HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet001\\Services\\IRENUM\\ObjectName",
                "HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet001\\Services\\abp480n5\\ObjectName",
                "HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet001\\Services\\ini910u\\ObjectName",
                "HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet001\\Services\\Secdrv\\ObjectName",
                "HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet001\\Services\\ql1280\\ObjectName",
                "HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet001\\Services\\Sfloppy\\ObjectName",
                "HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet001\\Services\\Abiosdsk\\ObjectName",
                "HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet001\\Services\\perc2\\ObjectName",
                "HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\CommonFilesDir",
                "HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet001\\Services\\PCIIde\\ObjectName",
                "HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet001\\Services\\AliIde\\ObjectName",
                "HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet001\\Services\\dac960nt\\ObjectName",
                "HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet001\\Services\\cbidf2k\\ObjectName",
                "HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet001\\Services\\NwlnkFwd\\ObjectName",
                "HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet001\\Services\\ql1240\\ObjectName",
                "HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet001\\Services\\Imapi\\ObjectName",
                "HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet001\\Services\\i2omp\\ObjectName",
                "HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet001\\Services\\cd20xrnt\\ObjectName",
                "HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet001\\Services\\asc3350p\\ObjectName",
                "HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet001\\Services\\IpFilterDriver\\ObjectName",
                "HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet001\\Services\\Flpydisk\\ObjectName",
                "HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet001\\Services\\Aha154x\\ObjectName",
                "HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet001\\Services\\aic78xx\\ObjectName",
                "HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\ProgramFilesDir",
                "HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet001\\Services\\Serial\\ObjectName",
                "HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet001\\Services\\mraid35x\\ObjectName",

"HKEY_LOCAL_MACHINE\\SYSTEM\\CurrentControlSet\\Services\\SharedAccess\\Parameters\\FirewallPolicy\\StandardP
rofile\\AuthorizedApplications\\List",
                "HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet001\\Services\\perc2hib\\ObjectName",
                "HKEY_LOCAL_MACHINE\\Software\\Microsoft\\WBEM\\CIMOM",
                "HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet001\\Services\\Changer\\ObjectName",
                "HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet001\\Services\\i2omgmt\\ObjectName",
                "HKEY_LOCAL_MACHINE\\SECURITY\\Policy\\SecDesc\\(Default)",
                "HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet001\\Services\\asc3550\\ObjectName",
                "HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet001\\Services\\ACPIEC\\ObjectName",
                "HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet001\\Services\\PDRFRAME\\ObjectName"
            ],
            "hash_sha1_h": "a2dbf3a419a0cf9f190b47ae624bf52196617c9c",
```

```
            "filesize_i": 56832,
            "dest_ipv4_s_array": [
               "50.63.202.29",
               "8.8.8.8",
               "148.81.111.121"
            ]
         },
         "description_s": "A report containing the summary of an automated malware analysis on a specific piece of
malware, which includes behavioral analysis data such as outbound communication destinations and host based
indicators of compromise"
      }
   ],
   "source_description_s": "This feed provides data collected from the automated behavioral analysis of malware by the
LookingGlass Cyber Threat Intelligence Group",
   "last_updated_t": 1442949180,
   "score_i": 95,
   "schema_version_s": "2.2.0",
   "provider_s": "LookingGlass"
}
```


6.4 Collections Example

This example shows a collection with a set of network elements and observables associated and multiple levels within the collection.


```
{
  "schema_version_s": "2.2.0",
  "provider_s": "A provider's name",
  "last_updated_t": 343423324324,
  "source_observable_s": "pr-short",
  "list_name_s": "Collections-US",
  "collection_c_array": [
   {
     "name_id_s": "MarketSeg1",
     "last_updated_t": 1212312323,
     "description_s": "This collection is related to MarketSeg1",
     "author_s": "Fred Jones",
     "workspace_s": "lg-system",
     "score_i": 90,
     "collection_c_array": [
     {
       "name_id_s": "NCR10205",
       "description_s": "This is NCR10205 sub-collection",
       "last_updated_t": 12123132322323,
       "author_s": "Gerry Freddy",
       "score_i": 70,
       "fqdn_ref_c_array": [
        { "fqdn_s": "seguintexas.gov" },
        { "fqdn_s": "tenaska.com" }
       ],
       "ip_ref_c_array": [
        { "ip_ipv4_s": "12.1.1.1" },
        { "ip_ipv4_s": "13.1.1.1" }
       ],
       "cidr_ref_c_array": [
        { "cidr_cidrv4_s": "208.191.120.72/29" },
        { "cidr_cidrv4_s": "208.191.120.64/29" }
       ],
       "asn_ref_c_array": [
        { "asn_asn_i": 393265 }
       ],
       "observable_ref_c_array": [
        { "observable_id_s": "Conficker A" },
        { "observable_id_s": "Tracker" }
       ],
       "collection_c_array": [
```

```
      {
        "name_id_s": "10205-SubGroup",
        "score_i": 50,
        "fqdn_c_array": [
          { "fqdn_s": "test.gov" }
        ]
      }
      ]
    },
    {
      "name_id_s": "NCR10112",
      "description_s": "this is a 2nd level collection",
      "workspace_s": "customer-prem-ws1",
      "score_i": 50,
      "fqdn_ref_c_array": [
        { "fqdn_fqdn_s": "wppienergy.org" }
      ],
      "ip_ref_c_array": [
        { "ip_ipv4_s": "62.189.96.254" }
       ],
      "observable_ref_c_array": [
        { "observable_id_s" : "md232312312123123" },
        { "observable_id_s" : "www.badguy.com"}
      ]
    }
    ]
  }
]
}
```

6.5 Data Exfiltration - Account Example

This example shows email accounts that have been captured as part of a data leak.


```
{
   "provider_s": "Cyber Threat Intelligence Group",
   "schema_version_s": "2.2.0",
   "source_description_s": "",
   "source_observable_s": "CTIG",
   "tlp_i": 2,
   "data_source_description_s": "Untitled4 Jul212015",
   "data_source_s": "http://pastebin.com/wdsbKddsYu",
   "distribution_time_t": 1437491489,
   "last_updated_t": 1437491489,
   "list_name_s": "Data Exfiltration",
   "observable_dictionary_c_array": [
   {
      "observable_id_s": "Data Leak Announcement",
      "classification_c_array": [
         { "classification_family_s": "Observed Actions", "classification_id_s": "Credential Theft", "score_i": 60 },
         { "classification_family_s": "Observed Actions", "classification_id_s": "Information Loss", "score_i": 15 },
         { "classification_family_s": "Observed Actions", "classification_id_s": "Public", "score_i": 5 }
      ],
      "criticality_i": 30,
      "description_s": "Potentially sensitive company information has been discovered in an unauthorized location. It was
collected through independent means of scanning multiple public third-party sites and data dumps."
   }
   ],
   "element_observable_c_array": [
      {
         "subject_fqdn_s": "twitter.com",
         "threat_observable_c_map": {
            "Data Leak Announcement": {
              "occurred_at_t": 4355545,
              "smtp_c_array" : [
                  { "email_s": "joelleey", "last_seen_t": 1437480000, "occurred_at_t": 1437480000, "password_s":
"jan15025" },
                  { "email_s": "chnesee", "last_seen_t": 1437480000, "occurred_at_t": 1437480000, "password_s":
"willmit2212" },
                  { "email_s": "dedelopeismed", "last_seen_t": 1437480000, "occurred_at_t": 1437480000, "password_s":
"ismedsofyan14" },
                  { "email_s": "ibnu_fahrezy", "last_seen_t": 1437480000, "occurred_at_t": 1437480000, "password_s":
"ilove03" }
              ]
            }
         }
      }
   ]
 }
```

6.6 Packet Capture Example

This example shows a packet capture with a set of network elements and observables associated and multiple levels within the collection. This shows the combination of a malware can be described partly as part of the dictionary and its behaviors on a single IP have been observed within the observable association itself as those behaviors were unique to that IP observed on rather than being common to the malware regardless of which host its executing on.


```
{
  "schema_version_s": "2.2.0",
  "provider_s": "Pcap Intel Provider Company",
  "list_name_s": "Pcap Provider Company List Data",
  "source_observable_s": "PCAP_IND_NAME",
  "source_file_s": "/var/lg/data/json/list_name/2014/06/01/2014.pcap",
  "source_description_s": "This feed provides information on PCAP behavior captured by X",
  "distribution_time_t": 1221312312,
  "last_updated_t": 121232134,
  "score_i": 90,

  "observable_dictionary_c_array": [
    {
      "observable_id_s" : "5013a954e6793d3610df43e761fd2deacdd3cd81dbc0ef902c5756bca61b5a94",
      "criticality_i": 90,
      "summary_s": "This is a summary of the observable",
      "description_s": "This is the observable associated with Detonation_Hash
5013a954e6793d3610df43e761fd2deacdd3cd81dbc0ef902c5756bca61b5a94",
      "notes_s": "User defined notes",
      "reference_s_array": [
         "http://www.thisisareference.com/observablereference", "http://www.anotherreference.com/2ndrefererence"
      ],
      "classification_c_array" : [
        {
          "classification_id_s": "Espionage",
          "score_i": 90
        }
      ],
      "attribute_c_map" : {
        "analysis_last_updated_t": 1421700366,
        "hash_md5_h": "12345678901234567890123456789012",
        "priority_i": 0,
        "submission_last_updated_t": 1421700366,
        "tlp_i": 1
      }
    },
    {
      "observable_id_s" : "PCAP_BASIC_FILEINFO_10000",
      "criticality_i": 90,
      "summary_s": "This is a summary of the observable",
      "description_s": "This is the observable associated with the PCAP file information. The observable name should be a
unique file",
      "notes_s": "User defined notes",
      "reference_s_array": [
         "http://www.thisisareference.com/observablereference", "http://www.anotherreference.com/2ndrefererence"
      ],
      "classification_c_array" : [
        {
          "classification_id_s": "Espionage",
          "score_i": 90
        }
      ],
      "attribute_c_map" : {
         "filesize_i": 4355545,
         "magic_s": "tcpdump capture file (little-endian) - version 2.4 (Ethernet, capture length 65535)",
         "country_code_s": "IR",
         "mime_type_s": "application/vnd.tcpdunmp.pcap",
```

```
        "hash_md5_h": "bb1bb053843ca7a03152790a79ac64bd",
        "hash_sha1_h": "bedb1987bc973b8bcf41a1a09143163928578b0b",
        "hash_sha256_h": "5013a954e6793d3610df43e761fd2deacdd3cd81dbc0ef902c5756bca61b5a94",
        "hash_sha512_h":
"236df7a6e29b9e0a10862a5ddf8b341355c47bacc278d975fd5dac4715aec64860cbc4d26a3510608ed937b36960fff15
c62f52d228b05b38ee74e6d202d6f7b"
      }
    }
  ],
  "element_observable_c_array": [
    {
      "subject_ipv4_s": "101.12.12.12",
      "score_i": 50,
      "threat_observable_c_map": {
         "PCAP_BASIC_FILEINFO_10000": {
             "occurred_at_t": 4355545,
             "last_seen_t": 13123
         },
         "Threat_Inject_tiger_mama": {
             "occurred_at_t": 4355545,
             "dns_request_c_array": [
               { "req_fqdn_s": "irc.freenode.net" }
               ],
             "dns_response_c_array": [
               { "record_s": "A", "resp_ipv4_s": "12.1.1.1" },
               { "record_s": "CNAME", "resp_fqdn_s": "chat.freenode.net"},
               { "record_s": "AAAA", "resp_ipv6_s": "2001:708:40:2001:a822:baff:fec4:2428"},
               { "record_s": "TXT", "resp_fqdn_s": "google-site-
verification=MrSWLn2NcqsbGduYWEr9F6Y0EuAU0MR_ANpGnA0mWEs"}],
             "fqdn_c_array": [
               { "fqdn_s": "eff.com", "ip_ipv4_s": "12.1.1.1" },
               { "fqdn_s": "isatap.f.sck.im", "ip_ipv4_s": "89.2.11.2"}
             ],
             "host_c_array": [
               { "host_fqdn_s": "badguy.com" }
             ],
             "http_c_array": [
               { "body_s": "", "method_s": "GET", "version_s": "1.1", "agent_s": "Battle.net/1.2.4.5383", "uri_fqdn_s":
"http://us.launcher.battle.net/service/wow/alert/en-us", "dest_port_i": 8653},
               { "body_s": "", "method_s": "GET", "version_s": "1.1", "agent_s": "Battle.net/1.2.4.5383", "uri_fqdn_s":
"http://us.launcher.battle.net/service/wow/alert/en-us", "dest_port_i": 8654}
             ],
             "icmp_c_array": [
               { "src_ipv4_s": "224.0.0.1", "dest_ipv4_s": "121.1.1.1", "type_i": 9 }
             ],
             "tcp_c_array": [
               { "src_port_i": 58463, "src_ipv4_s": "172.16.246.6", "dest_port_i": 22, "dest_ipv4_s": "10.0.50.3"},
               { "src_port_i": 12312, "src_ipv4_s": "172.16.246.7", "dest_port_i": 21, "dest_ipv4_s": "10.0.51.3"}
             ],
             "ssl_c_array" : [
               { "session_start_t": 123123123, "session_info_s": "session started on port 1232" }
             ],
             "smtp_c_array": [
               { "email_s": "fred@badguy.com", "mail_server_ipv4_s": "1.1.1.1"}
             ],
             "country_code_s": "IR",
             "score_i": 70
          }
       }
    }
  ]
}
```

6.7 BGP Network Information Example

This example shows an example with a set of BGP ASN information.


```
{
  "schema_version_s": "2.2.0",
  "provider_s": "Lookingglass Cyber Solutions",
  "list_name_s": "LG BGP",
  "source_description_s": "This feed contains BGP ownership, routing and topology data.",
  "workspace_s": "lg-system",
  "distribution_time_t": 1429894284,
  "last_updated_t": 343423324324,
  "source_observable_s": "LG",
  "asn_c_array": [
   {
    "asn_number_ui": 1,
    "asn_owner_s": "ABC Corp",

    "asn_routers_ipv4_array" : [
     1231231, 12312313214, 12131311241, 12312423414
    ],

    "asn_router_conns_c_array": [
     { "router_1_ui": 1231232112, "router_2_ui": 121435523 },
     { "router_1_ui": 2314123434, "router_2_ui": 4523423432}
    ],

    "asn_cidr_announcements_c_array": [
     { "start_ipv4_ui": 1234567890, "end_ipv4_ui": 2234567890, "aggregator_ipv4_ui": 12332144,
"observed_at_t": 213232232 },
     { "start_ipv4_ui": 3234567890, "end_ipv4_ui": 4234567890, "aggregator_ipv4_ui": 12332144 }
    ],

    "asn_downstream_ui_array": [
     2, 53, 5, 66
    ],

    "asn_upstream_ui_array": [
     3, 4
    ],

    "asn_community_c_array": [
     { "asn_1_ui": 2323, "asn_2_ui": 2 },
     { "asn_1_ui": 3, "asn_2_ui": 4}
    ]
   },

   {
    "asn_number_ui": 2,
    "asn_owner_s": "UTD Corp",
    "router_ipv4_ui": 123431,
    "routers_ipv4_array" : [
     76767676, 7676765, 333, 65657888
    ],
    "router_c_array": [
     { "router_1_ui": 6565656, "router_2_ui": 234324 },
     { "router_1_ui": 2346, "router_2_ui": 645645}
    ],
    "asncidr_c_array": [
     { "start_ipv4_ui": 23432423, "end_ipv4_ui": 234222, "aggregator_ipv4_ui": 12332144 },
     { "start_ipv4_ui": 3234567890, "end_ipv4_ui": 4234567890, "aggregator_ipv4_ui": 12332144 }
    ],
    "asn_downstream_ui_array": [
     5, 55, 7, 61
    ],
    "asn_upstream_ui_array": [
```

```
      3, 4
    ],
    "asn_community_c_array": [
      { "asn_1_ui": 1, "asn_2_ui": 2 },
      { "asn_1_ui": 3, "asn_2_ui": 4}
    ]
  }
  ]
}
```

6.8 Country Code Collection Example

This example shows a collection with a set of Country Code updates


```
{
  "schema_version_s": "2.2.0",
  "provider_s": "Company Name",
  "list_name_s": "Country Codes",
  "source_observable_s": "CompName",
  "source_description_s": "This collection is ISO-2 and ISO-3 country codes.",
  "distribution_time_t": 1429894284,
  "last_updated_t": 1429894284,
  "collection_c_array": [
    { "name_id_s": "Aruba", "iso_3_s": "abw", "iso_2_s": "aw", "region_code_ui": 0, "continent_code_ui": 6,
"continent_code_s": "na", "country_code_ui": 533 },
    { "name_id_s": "Afghanistan", "iso_3_s": "afg", "iso_2_s": "af", "region_code_ui": 1, "continent_code_ui": 4,
"continent_code_s": "as", "country_code_ui": 4 },
    { "name_id_s": "Angola", "iso_3_s": "ago", "iso_2_s": "ao", "region_code_ui": 1, "continent_code_ui": 1,
"continent_code_s": "af", "country_code_ui": 24 },
    { "name_id_s": "Anguilla", "iso_3_s": "aia", "iso_2_s": "ai", "region_code_ui": 0, "continent_code_ui": 6,
"continent_code_s": "na", "country_code_ui": 660 },
    { "name_id_s": "Aland Islands", "iso_3_s": "ala", "iso_2_s": "ax", "region_code_ui": 0, "continent_code_ui": 5,
"continent_code_s": "eu", "country_code_ui": 248 },
    { "name_id_s": "Albania", "iso_3_s": "alb", "iso_2_s": "al", "region_code_ui": 1, "continent_code_ui": 5,
"continent_code_s": "eu", "country_code_ui": 8 },
    { "name_id_s": "Andorra", "iso_3_s": "and", "iso_2_s": "ad", "region_code_ui": 1, "continent_code_ui": 5,
"continent_code_s": "eu", "country_code_ui": 20 },
    { "name_id_s": "Netherlands Antilles", "iso_3_s": "ant", "iso_2_s": "an", "region_code_ui": 0, "continent_code_ui": 6,
"continent_code_s": "na", "country_code_ui": 530 },
    { "name_id_s": "United Arab Emirates", "iso_3_s": "are", "iso_2_s": "ae", "region_code_ui": 1, "continent_code_ui": 4,
"continent_code_s": "as", "country_code_ui": 784 },
    { "name_id_s": "Argentina", "iso_3_s": "arg", "iso_2_s": "ar", "region_code_ui": 1, "continent_code_ui": 7,
"continent_code_s": "sa", "country_code_ui": 3 },
    { "name_id_s": "Armenia", "iso_3_s": "arm", "iso_2_s": "am", "region_code_ui": 1, "continent_code_ui": 4,
"continent_code_s": "as", "country_code_ui": 51 },
    { "name_id_s": "Asia (unknown Country)", "iso_3_s": "asi", "iso_2_s": "ap", "region_code_ui": 0, "continent_code_ui": 4,
"continent_code_s": "as", "country_code_ui": 994 },
    { "name_id_s": "American Samoa", "iso_3_s": "asm", "iso_2_s": "as", "region_code_ui": 0, "continent_code_ui": 3,
"continent_code_s": "au", "country_code_ui": 16 },
    { "name_id_s": "Antarctica", "iso_3_s": "ata", "iso_2_s": "aq", "region_code_ui": 0, "continent_code_ui": 2,
"continent_code_s": "an", "country_code_ui": 10 },
    { "name_id_s": "French Southern Territories", "iso_3_s": "atf", "iso_2_s": "tf", "region_code_ui": 0, "continent_code_ui":
2, "continent_code_s": "an", "country_code_ui": 260 },
    { "name_id_s": "Antigua And Barbuda", "iso_3_s": "atg", "iso_2_s": "ag", "region_code_ui": 1, "continent_code_ui": 6,
"continent_code_s": "na", "country_code_ui": 28 },
    { "name_id_s": "Australia", "iso_3_s": "aus", "iso_2_s": "au", "region_code_ui": 1, "continent_code_ui": 3,
"continent_code_s": "au", "country_code_ui": 36 },
    { "name_id_s": "Austria", "iso_3_s": "aut", "iso_2_s": "at", "region_code_ui": 1, "continent_code_ui": 5,
"continent_code_s": "eu", "country_code_ui": 40 },
    { "name_id_s": "Azerbaijan", "iso_3_s": "aze", "iso_2_s": "az", "region_code_ui": 1, "continent_code_ui": 4,
"continent_code_s": "as", "country_code_ui": 31 },
    { "name_id_s": "Burundi", "iso_3_s": "bdi", "iso_2_s": "bi", "region_code_ui": 1, "continent_code_ui": 1,
"continent_code_s": "af", "country_code_ui": 108 },
    { "name_id_s": "Belgium", "iso_3_s": "bel", "iso_2_s": "be", "region_code_ui": 1, "continent_code_ui": 5,
"continent_code_s": "eu", "country_code_ui": 56 },
    { "name_id_s": "Benin", "iso_3_s": "ben", "iso_2_s": "bj", "region_code_ui": 1, "continent_code_ui": 1,
"continent_code_s": "af", "country_code_ui": 204 },
    { "name_id_s": "Bonaire/sint Eustatius/saba", "iso_3_s": "bes", "iso_2_s": "bq", "region_code_ui": 1,
"continent_code_ui": 6, "continent_code_s": "na", "country_code_ui": 535 },
    { "name_id_s": "Burkina Faso", "iso_3_s": "bfa", "iso_2_s": "bf", "region_code_ui": 1, "continent_code_ui": 1,
"continent_code_s": "af", "country_code_ui": 854 },
    { "name_id_s": "Bangladesh", "iso_3_s": "bgd", "iso_2_s": "bd", "region_code_ui": 1, "continent_code_ui": 4,
"continent_code_s": "as", "country_code_ui": 50 },
    { "name_id_s": "Bulgaria", "iso_3_s": "bgr", "iso_2_s": "bg", "region_code_ui": 1, "continent_code_ui": 5,
"continent_code_s": "eu", "country_code_ui": 100 },
```

{ "name_id_s": "Bahrain", "iso_3_s": "bhr", "iso_2_s": "bh", "region_code_ui": 1, "continent_code_ui": 4, "continent_code_s": "as", "country_code_ui": 48 },
{ "name_id_s": "Bahamas", "iso_3_s": "bhs", "iso_2_s": "bs", "region_code_ui": 1, "continent_code_ui": 6, "continent_code_s": "na", "country_code_ui": 44 },
{ "name_id_s": "Bosnia And Herzegowina", "iso_3_s": "bih", "iso_2_s": "ba", "region_code_ui": 1, "continent_code_ui": 5, "continent_code_s": "eu", "country_code_ui": 70 },
{ "name_id_s": "Saint Barthelemy", "iso_3_s": "blm", "iso_2_s": "bl", "region_code_ui": 0, "continent_code_ui": 6, "continent_code_s": "na", "country_code_ui": 652 },
{ "name_id_s": "Belarus", "iso_3_s": "blr", "iso_2_s": "by", "region_code_ui": 1, "continent_code_ui": 5, "continent_code_s": "eu", "country_code_ui": 112 },
{ "name_id_s": "Belize", "iso_3_s": "blz", "iso_2_s": "bz", "region_code_ui": 1, "continent_code_ui": 6, "continent_code_s": "na", "country_code_ui": 84 },
{ "name_id_s": "Bermuda", "iso_3_s": "bmu", "iso_2_s": "bm", "region_code_ui": 0, "continent_code_ui": 6, "continent_code_s": "na", "country_code_ui": 60 },
{ "name_id_s": "Bolivia", "iso_3_s": "bol", "iso_2_s": "bo", "region_code_ui": 1, "continent_code_ui": 7, "continent_code_s": "sa", "country_code_ui": 68 },
{ "name_id_s": "Brazil", "iso_3_s": "bra", "iso_2_s": "br", "region_code_ui": 1, "continent_code_ui": 7, "continent_code_s": "sa", "country_code_ui": 76 },
{ "name_id_s": "Barbados", "iso_3_s": "brb", "iso_2_s": "bb", "region_code_ui": 1, "continent_code_ui": 6, "continent_code_s": "na", "country_code_ui": 52 },
{ "name_id_s": "Brunei Darussalam", "iso_3_s": "brn", "iso_2_s": "bn", "region_code_ui": 1, "continent_code_ui": 4, "continent_code_s": "as", "country_code_ui": 96 },
{ "name_id_s": "Bhutan", "iso_3_s": "btn", "iso_2_s": "bt", "region_code_ui": 1, "continent_code_ui": 4, "continent_code_s": "as", "country_code_ui": 64 },
{ "name_id_s": "Bouvet Island", "iso_3_s": "bvt", "iso_2_s": "bv", "region_code_ui": 0, "continent_code_ui": 2, "continent_code_s": "an", "country_code_ui": 74 },
{ "name_id_s": "Botswana", "iso_3_s": "bwa", "iso_2_s": "bw", "region_code_ui": 1, "continent_code_ui": 1, "continent_code_s": "af", "country_code_ui": 72 },
{ "name_id_s": "Central African Republic", "iso_3_s": "caf", "iso_2_s": "cf", "region_code_ui": 1, "continent_code_ui": 1, "continent_code_s": "af", "country_code_ui": 140 },
{ "name_id_s": "Canada", "iso_3_s": "can", "iso_2_s": "ca", "region_code_ui": 1, "continent_code_ui": 6, "continent_code_s": "na", "country_code_ui": 124 },
{ "name_id_s": "Cocos (keeling) Islands", "iso_3_s": "cck", "iso_2_s": "cc", "region_code_ui": 0, "continent_code_ui": 3, "continent_code_s": "au", "country_code_ui": 166 },
{ "name_id_s": "Switzerland", "iso_3_s": "che", "iso_2_s": "ch", "region_code_ui": 1, "continent_code_ui": 5, "continent_code_s": "eu", "country_code_ui": 756 },
{ "name_id_s": "Chile", "iso_3_s": "chl", "iso_2_s": "cl", "region_code_ui": 1, "continent_code_ui": 7, "continent_code_s": "sa", "country_code_ui": 152 },
{ "name_id_s": "China", "iso_3_s": "chn", "iso_2_s": "cn", "region_code_ui": 1, "continent_code_ui": 4, "continent_code_s": "as", "country_code_ui": 156 },
{ "name_id_s": "Cote D Ivoire", "iso_3_s": "civ", "iso_2_s": "ci", "region_code_ui": 1, "continent_code_ui": 1, "continent_code_s": "af", "country_code_ui": 384 },
{ "name_id_s": "Cameroon", "iso_3_s": "cmr", "iso_2_s": "cm", "region_code_ui": 1, "continent_code_ui": 1, "continent_code_s": "af", "country_code_ui": 120 },
{ "name_id_s": "Congo - The Democratic Rep Of", "iso_3_s": "cod", "iso_2_s": "cd", "region_code_ui": 1, "continent_code_ui": 1, "continent_code_s": "af", "country_code_ui": 180 },
{ "name_id_s": "Congo", "iso_3_s": "cog", "iso_2_s": "cg", "region_code_ui": 1, "continent_code_ui": 1, "continent_code_s": "af", "country_code_ui": 178 },
{ "name_id_s": "Cook Islands", "iso_3_s": "cok", "iso_2_s": "ck", "region_code_ui": 0, "continent_code_ui": 3, "continent_code_s": "au", "country_code_ui": 184 },
{ "name_id_s": "Colombia", "iso_3_s": "col", "iso_2_s": "co", "region_code_ui": 1, "continent_code_ui": 7, "continent_code_s": "sa", "country_code_ui": 170 },
{ "name_id_s": "Comoros", "iso_3_s": "com", "iso_2_s": "km", "region_code_ui": 1, "continent_code_ui": 1, "continent_code_s": "af", "country_code_ui": 174 },
{ "name_id_s": "Cape Verde", "iso_3_s": "cpv", "iso_2_s": "cv", "region_code_ui": 1, "continent_code_ui": 1, "continent_code_s": "af", "country_code_ui": 132 },
{ "name_id_s": "Costa Rica", "iso_3_s": "cri", "iso_2_s": "cr", "region_code_ui": 1, "continent_code_ui": 6, "continent_code_s": "na", "country_code_ui": 188 },
{ "name_id_s": "Cuba", "iso_3_s": "cub", "iso_2_s": "cu", "region_code_ui": 1, "continent_code_ui": 6, "continent_code_s": "na", "country_code_ui": 192 },
{ "name_id_s": "Curacao", "iso_3_s": "cuw", "iso_2_s": "cw", "region_code_ui": 0, "continent_code_ui": 6, "continent_code_s": "na", "country_code_ui": 531 },
{ "name_id_s": "Christmas Island", "iso_3_s": "cxr", "iso_2_s": "cx", "region_code_ui": 0, "continent_code_ui": 3, "continent_code_s": "au", "country_code_ui": 162 },
{ "name_id_s": "Cayman Islands", "iso_3_s": "cym", "iso_2_s": "ky", "region_code_ui": 0, "continent_code_ui": 6, "continent_code_s": "na", "country_code_ui": 136 },
{ "name_id_s": "Cyprus", "iso_3_s": "cyp", "iso_2_s": "cy", "region_code_ui": 1, "continent_code_ui": 5, "continent_code_s": "eu", "country_code_ui": 196 },

{ "name_id_s": "Czech Republic", "iso_3_s": "cze", "iso_2_s": "cz", "region_code_ui": 1, "continent_code_ui": 5, "continent_code_s": "eu", "country_code_ui": 203 },
{ "name_id_s": "Germany", "iso_3_s": "deu", "iso_2_s": "de", "region_code_ui": 1, "continent_code_ui": 5, "continent_code_s": "eu", "country_code_ui": 276 },
{ "name_id_s": "Djibouti", "iso_3_s": "dji", "iso_2_s": "dj", "region_code_ui": 1, "continent_code_ui": 1, "continent_code_s": "af", "country_code_ui": 262 },
{ "name_id_s": "Dominica", "iso_3_s": "dma", "iso_2_s": "dm", "region_code_ui": 1, "continent_code_ui": 6, "continent_code_s": "na", "country_code_ui": 212 },
{ "name_id_s": "Denmark", "iso_3_s": "dnk", "iso_2_s": "dk", "region_code_ui": 1, "continent_code_ui": 5, "continent_code_s": "eu", "country_code_ui": 208 },
{ "name_id_s": "Dominican Republic", "iso_3_s": "dom", "iso_2_s": "do", "region_code_ui": 1, "continent_code_ui": 6, "continent_code_s": "na", "country_code_ui": 214 },
{ "name_id_s": "Algeria", "iso_3_s": "dza", "iso_2_s": "dz", "region_code_ui": 1, "continent_code_ui": 1, "continent_code_s": "af", "country_code_ui": 12 },
{ "name_id_s": "Ecuador", "iso_3_s": "ecu", "iso_2_s": "ec", "region_code_ui": 1, "continent_code_ui": 7, "continent_code_s": "sa", "country_code_ui": 218 },
{ "name_id_s": "Egypt", "iso_3_s": "egy", "iso_2_s": "eg", "region_code_ui": 1, "continent_code_ui": 1, "continent_code_s": "af", "country_code_ui": 818 },
{ "name_id_s": "Eritrea", "iso_3_s": "eri", "iso_2_s": "er", "region_code_ui": 1, "continent_code_ui": 1, "continent_code_s": "af", "country_code_ui": 232 },
{ "name_id_s": "Western Sahara", "iso_3_s": "esh", "iso_2_s": "eh", "region_code_ui": 0, "continent_code_ui": 1, "continent_code_s": "af", "country_code_ui": 732 },
{ "name_id_s": "Spain", "iso_3_s": "esp", "iso_2_s": "es", "region_code_ui": 1, "continent_code_ui": 5, "continent_code_s": "eu", "country_code_ui": 724 },
{ "name_id_s": "Estonia", "iso_3_s": "est", "iso_2_s": "ee", "region_code_ui": 1, "continent_code_ui": 5, "continent_code_s": "eu", "country_code_ui": 233 },
{ "name_id_s": "Ethiopia", "iso_3_s": "eth", "iso_2_s": "et", "region_code_ui": 1, "continent_code_ui": 1, "continent_code_s": "af", "country_code_ui": 231 },
{ "name_id_s": "Europe (unknown Country)", "iso_3_s": "eur", "iso_2_s": "eu", "region_code_ui": 0, "continent_code_ui": 5, "continent_code_s": "eu", "country_code_ui": 995 },
{ "name_id_s": "Finland", "iso_3_s": "fin", "iso_2_s": "fi", "region_code_ui": 1, "continent_code_ui": 5, "continent_code_s": "eu", "country_code_ui": 246 },
{ "name_id_s": "Fiji", "iso_3_s": "fji", "iso_2_s": "fj", "region_code_ui": 1, "continent_code_ui": 3, "continent_code_s": "au", "country_code_ui": 242 },
{ "name_id_s": "Falkland Islands (malvinas)", "iso_3_s": "flk", "iso_2_s": "fk", "region_code_ui": 0, "continent_code_ui": 7, "continent_code_s": "sa", "country_code_ui": 238 },
{ "name_id_s": "France", "iso_3_s": "fra", "iso_2_s": "fr", "region_code_ui": 1, "continent_code_ui": 5, "continent_code_s": "eu", "country_code_ui": 250 },
{ "name_id_s": "Faroe Islands", "iso_3_s": "fro", "iso_2_s": "fo", "region_code_ui": 0, "continent_code_ui": 5, "continent_code_s": "eu", "country_code_ui": 234 },
{ "name_id_s": "Micronesia - Federated States Of", "iso_3_s": "fsm", "iso_2_s": "fm", "region_code_ui": 1, "continent_code_ui": 3, "continent_code_s": "au", "country_code_ui": 583 },
{ "name_id_s": "Gabon", "iso_3_s": "gab", "iso_2_s": "ga", "region_code_ui": 1, "continent_code_ui": 1, "continent_code_s": "af", "country_code_ui": 266 },
{ "name_id_s": "United Kingdom", "iso_3_s": "gbr", "iso_2_s": "uk", "region_code_ui": 1, "continent_code_ui": 5, "continent_code_s": "eu", "country_code_ui": 826 },
{ "name_id_s": "Georgia", "iso_3_s": "geo", "iso_2_s": "ge", "region_code_ui": 1, "continent_code_ui": 5, "continent_code_s": "eu", "country_code_ui": 268 },
{ "name_id_s": "Guernsey", "iso_3_s": "ggy", "iso_2_s": "gg", "region_code_ui": 0, "continent_code_ui": 5, "continent_code_s": "eu", "country_code_ui": 831 },
{ "name_id_s": "Ghana", "iso_3_s": "gha", "iso_2_s": "gh", "region_code_ui": 1, "continent_code_ui": 1, "continent_code_s": "af", "country_code_ui": 288 },
{ "name_id_s": "Gibraltar", "iso_3_s": "gib", "iso_2_s": "gi", "region_code_ui": 0, "continent_code_ui": 5, "continent_code_s": "eu", "country_code_ui": 292 },
{ "name_id_s": "Guinea", "iso_3_s": "gin", "iso_2_s": "gn", "region_code_ui": 1, "continent_code_ui": 1, "continent_code_s": "af", "country_code_ui": 324 },
{ "name_id_s": "Guadeloupe", "iso_3_s": "glp", "iso_2_s": "gp", "region_code_ui": 0, "continent_code_ui": 6, "continent_code_s": "na", "country_code_ui": 312 },
{ "name_id_s": "Gambia", "iso_3_s": "gmb", "iso_2_s": "gm", "region_code_ui": 1, "continent_code_ui": 1, "continent_code_s": "af", "country_code_ui": 270 },
{ "name_id_s": "Guinea-bissau", "iso_3_s": "gnb", "iso_2_s": "gw", "region_code_ui": 1, "continent_code_ui": 1, "continent_code_s": "af", "country_code_ui": 624 },
{ "name_id_s": "Equatorial Guinea", "iso_3_s": "gnq", "iso_2_s": "gq", "region_code_ui": 1, "continent_code_ui": 1, "continent_code_s": "af", "country_code_ui": 226 },
{ "name_id_s": "Greece", "iso_3_s": "grc", "iso_2_s": "gr", "region_code_ui": 1, "continent_code_ui": 5, "continent_code_s": "eu", "country_code_ui": 300 },
{ "name_id_s": "Grenada", "iso_3_s": "grd", "iso_2_s": "gd", "region_code_ui": 1, "continent_code_ui": 6, "continent_code_s": "na", "country_code_ui": 308 },

{ "name_id_s": "Greenland", "iso_3_s": "grl", "iso_2_s": "gl", "region_code_ui": 1, "continent_code_ui": 6, "continent_code_s": "na", "country_code_ui": 304 },
{ "name_id_s": "Guatemala", "iso_3_s": "gtm", "iso_2_s": "gt", "region_code_ui": 1, "continent_code_ui": 6, "continent_code_s": "na", "country_code_ui": 320 },
{ "name_id_s": "French Guiana", "iso_3_s": "guf", "iso_2_s": "gf", "region_code_ui": 0, "continent_code_ui": 7, "continent_code_s": "sa", "country_code_ui": 254 },
{ "name_id_s": "Guam", "iso_3_s": "gum", "iso_2_s": "gu", "region_code_ui": 0, "continent_code_ui": 3, "continent_code_s": "au", "country_code_ui": 316 },
{ "name_id_s": "Guyana", "iso_3_s": "guy", "iso_2_s": "gy", "region_code_ui": 1, "continent_code_ui": 7, "continent_code_s": "sa", "country_code_": 328 },
{ "name_id_s": "Hong Kong", "iso_3_s": "hkg", "iso_2_s": "hk", "region_code_ui": 0, "continent_code_ui": 4, "continent_code_s": "as", "country_cod_i": 344 },
{ "name_id_s": "Heard And Mc Donald Islands", "iso_3_s": "hmd", "iso_2_s": "hm", "region_code_ui": 0, "continent_code_ui": 3, "continent_code_s": "u", "country_code_ui": 334 },
{ "name_id_s": "Honduras", "iso_3_s": "hnd", "iso_2_s": "hn", "region_code_ui": 1, "continent_code_ui": 6, "continent_code_s": "na", "country_code_ui": 340 },
{ "name_id_s": "Croatia (local Name - Hrvatska)", "iso_3_s": "hrv", "iso_2_s": "hr", "region_code_ui": 1, "continent_code_ui": 5, "continent_code_s":"eu", "country_code_ui": 191 },
{ "name_id_s": "Haiti", "iso_3_s": "hti", "iso_2_s": "ht", "region_code_ui": 1, "continent_code_ui": 6, "continent_code_s": "na", "country_code_ui": 33 },
{ "name_id_s": "Hungary", "iso_3_s": "hun", "iso_2_s": "hu", "region_code_ui": 1, "continent_code_ui": 5, "continent_code_s": "eu", "country_code_ui": 34 },
{ "name_id_s": "Indonesia", "iso_3_s": "idn", "iso_2_s": "id", "region_code_ui": 1, "continent_code_ui": 4, "continent_code_s": "as", "country_code_ui": 360 },
{ "name_id_s": "Isle Of Man", "iso_3_s": "imn", "iso_2_s": "im", "region_code_ui": 0, "continent_code_ui": 5, "continent_code_s": "eu", "country_code_ui": 833 },
{ "name_id_s": "India", "iso_3_s": "ind", "iso_2_s": "in", "region_code_ui": 1, "continent_code_ui": 4, "continent_code_s": "as", "country_code_ui": 356 },
{ "name_id_s": "British Indian Ocean Territory", "iso_3_s": "iot", "iso_2_s": "io", "region_code_ui": 0, "continent_code_ui": 4, "continent_code_s": "as", "country_code_ui": 86 },
{ "name_id_s": "Ireland", "iso_3_s": "irl", "iso_2_s": "ie", "region_code_ui": 1, "continent_code_ui": 5, "continent_code_s": "eu", "country_code_ui": 372 },
{ "name_id_s": "Iran (islamic Republic Of)", "iso_3_s": "irn", "iso_2_s": "ir", "region_code_ui": 1, "continent_code_ui": 4, "continent_code_s": "as", "country_code_ui": 364 },
{ "name_id_s": "Iraq", "iso_3_s": "irq", "iso_2_s": "iq", "region_code_ui": 1, "continent_code_ui": 4, "continent_code_s": "as", "country_code_ui": 368 },
{ "name_id_s": "Iceland", "iso_3_s": "isl", "iso_2_s": "is", "region_code_ui": 1, "continent_code_ui": 5, "continent_code_s": "eu", "country_code_ui": 352 },
{ "name_id_s": "Israel", "iso_3_s": "isr", "iso_2_s": "il", "region_code_ui": 1, "continent_code_ui": 4, "continent_code_s": "as", "country_code_ui": 376 },
{ "name_id_s": "Italy", "iso_3_s": "ita", "iso_2_s": "it", "region_code_ui": 1, "continent_code_ui": 5, "continent_code_s": "eu", "country_code_ui": 380 },
{ "name_id_s": "Jamaica", "iso_3_s": "jam", "iso_2_s": "jm", "region_code_ui": 1, "continent_code_ui": 6, "continent_code_s": "na", "country_code_ui": 388 },
{ "name_id_s": "Jersey", "iso_3_s": "jey", "iso_2_s": "je", "region_code_ui": 0, "continent_code_ui": 5, "continent_code_s": "eu", "country_code_ui": 832 },
{ "name_id_s": "Jordan", "iso_3_s": "jor", "iso_2_s": "jo", "region_code_ui": 1, "continent_code_ui": 4, "continent_code_s": "as", "country_code_ui": 400 },
{ "name_id_s": "Japan", "iso_3_s": "jpn", "iso_2_s": "jp", "region_code_ui": 1, "continent_code_ui": 4, "continent_code_s": "as", "country_code_ui": 392 },
{ "name_id_s": "Kazakhstan", "iso_3_s": "kaz", "iso_2_s": "kz", "region_code_ui": 1, "continent_code_ui": 4, "continent_code_s": "as", "country_code_ui": 398 },
{ "name_id_s": "Kenya", "iso_3_s": "ken", "iso_2_s": "ke", "region_code_ui": 1, "continent_code_ui": 1, "continent_code_s": "af", "country_code_ui": 404 },
{ "name_id_s": "Kyrgyzstan", "iso_3_s": "kgz", "iso_2_s": "kg", "region_code_ui": 1, "continent_code_ui": 4, "continent_code_s": "as", "country_code_ui": 417 },
{ "name_id_s": "Cambodia", "iso_3_s": "khm", "iso_2_s": "kh", "region_code_ui": 1, "continent_code_ui": 4, "continent_code_s": "as", "country_code_ui": 116 },
{ "name_id_s": "Kiribati", "iso_3_s": "kir", "iso_2_s": "ki", "region_code_ui": 0, "continent_code_ui": 3, "continent_code_s": "au", "country_code_ui": 296 },
{ "name_id_s": "Saint Kitts And Nevis", "iso_3_s": "kna", "iso_2_s": "kn", "region_code_ui": 1, "continent_code_ui": 6, "continent_code_s": "na", "country_code_ui": 659 },
{ "name_id_s": "Korea - South", "iso_3_s": "kor", "iso_2_s": "kr", "region_code_ui": 1, "continent_code_ui": 4, "continent_code_s": "as", "country_code_ui": 410 },
{ "name_id_s": "Kuwait", "iso_3_s": "kwt", "iso_2_s": "kw", "region_code_ui": 1, "continent_code_ui": 4, "continent_code_s": "as", "country_code_ui": 414 },
{ "name_id_s": "Lao Peoples Democratic Republic", "iso_3_s": "lao", "iso_2_s": "la", "region_code_ui": 1, "continent_code_ui": 4, "continent_code_s": "as", "country_code_ui": 418 },

{ "name_id_s": "Lebanon", "iso_3_s": "lbn", "iso_2_s": "lb", "region_code_ui": 1, "continent_code_ui": 4, "continent_code_s": "as", "country_code_ui": 422 },
{ "name_id_s": "Liberia", "iso_3_s": "lbr", "iso_2_s": "lr", "region_code_ui": 1, "continent_code_ui": 1, "continent_code_s": "af", "country_code_ui": 430 },
{ "name_id_s": "Libyan Arab Jamahiriya", "iso_3_s": "lby", "iso_2_s": "ly", "region_code_ui": 1, "continent_code_ui": 1, "continent_code_s": "af", "country_code_ui": 434 },
{ "name_id_s": "Saint Lucia", "iso_3_s": "lca", "iso_2_s": "lc", "region_code_ui": 1, "continent_code_ui": 6, "continent_code_s": "na", "country_code_ui": 662 },
{ "name_id_s": "Liechtenstein", "iso_3_s": "lie", "iso_2_s": "li", "region_code_ui": 1, "continent_code_ui": 5, "continent_code_s": "eu", "country_code_ui": 438 },
{ "name_id_s": "Sri Lanka", "iso_3_s": "lka", "iso_2_s": "lk", "region_code_ui": 1, "continent_code_ui": 4, "continent_code_s": "as", "country_code_ui": 144 },
{ "name_id_s": "Lesotho", "iso_3_s": "lso", "iso_2_s": "ls", "region_code_ui": 1, "continent_code_ui": 1, "continent_code_s": "af", "country_code_ui": 426 },
{ "name_id_s": "Lithuania", "iso_3_s": "ltu", "iso_2_s": "lt", "region_code_ui": 1, "continent_code_ui": 5, "continent_code_s": "eu", "country_code_ui": 440 },
{ "name_id_s": "Luxembourg", "iso_3_s": "lux", "iso_2_s": "lu", "region_code_ui": 1, "continent_code_ui": 5, "continent_code_s": "eu", "country_code_ui": 442 },
{ "name_id_s": "Latvia", "iso_3_s": "lva", "iso_2_s": "lv", "region_code_ui": 1, "continent_code_ui": 5, "continent_code_s": "eu", "country_code_ui": 428 },
{ "name_id_s": "Macau", "iso_3_s": "mac", "iso_2_s": "mo", "region_code_ui": 0, "continent_code_ui": 4, "continent_code_s": "as", "country_code_ui": 446 },
{ "name_id_s": "Saint Martin", "iso_3_s": "maf", "iso_2_s": "mf", "region_code_ui": 0, "continent_code_ui": 6, "continent_code_s": "na", "country_code_ui": 663 },
{ "name_id_s": "Morocco", "iso_3_s": "mar", "iso_2_s": "ma", "region_code_ui": 1, "continent_code_ui": 1, "continent_code_s": "af", "country_code_ui": 504 },
{ "name_id_s": "Monaco", "iso_3_s": "mco", "iso_2_s": "mc", "region_code_ui": 1, "continent_code_ui": 5, "continent_code_s": "eu", "country_code_ui": 492 },
{ "name_id_s": "Moldova - Republic Of", "iso_3_s": "mda", "iso_2_s": "md", "region_code_ui": 1, "continent_code_ui": 5, "continent_code_s": "eu", "country_code_ui": 498 },
{ "name_id_s": "Madagascar", "iso_3_s": "mdg", "iso_2_s": "mg", "region_code_ui": 1, "continent_code_ui": 1, "continent_code_s": "af", "country_code_ui": 450 },
{ "name_id_s": "Maldives", "iso_3_s": "mdv", "iso_2_s": "mv", "region_code_ui": 1, "continent_code_ui": 4, "continent_code_s": "as", "country_code_ui": 462 },
{ "name_id_s": "Mexico", "iso_3_s": "mex", "iso_2_s": "mx", "region_code_ui": 1, "continent_code_ui": 6, "continent_code_s": "na", "country_code_ui": 484 },
{ "name_id_s": "Marshall Islands", "iso_3_s": "mhl", "iso_2_s": "mh", "region_code_ui": 1, "continent_code_ui": 3, "continent_code_s": "au", "country_code_ui": 584 },
{ "name_id_s": "Macedonia - The Frm Yugoslav Rep Of", "iso_3_s": "mkd", "iso_2_s": "mk", "region_code_ui": 1, "continent_code_ui": 5, "continent_code_s": "eu", "country_code_ui": 807 },
{ "name_id_s": "Mali", "iso_3_s": "mli", "iso_2_s": "ml", "region_code_ui": 1, "continent_code_ui": 1, "continent_code_s": "af", "country_code_ui": 466 },
{ "name_id_s": "Malta", "iso_3_s": "mlt", "iso_2_s": "mt", "region_code_ui": 1, "continent_code_ui": 5, "continent_code_s": "eu", "country_code_ui": 470 },
{ "name_id_s": "Myanmar", "iso_3_s": "mmr", "iso_2_s": "mm", "region_code_ui": 1, "continent_code_ui": 4, "continent_code_s": "as", "country_code_ui": 104 },
{ "name_id_s": "Montenegro", "iso_3_s": "mne", "iso_2_s": "me", "region_code_ui": 1, "continent_code_ui": 5, "continent_code_s": "eu", "country_code_ui": 499 },
{ "name_id_s": "Mongolia", "iso_3_s": "mng", "iso_2_s": "mn", "region_code_ui": 1, "continent_code_ui": 4, "continent_code_s": "as", "country_code_ui": 496 },
{ "name_id_s": "Northern Mariana Islands", "iso_3_s": "mnp", "iso_2_s": "mp", "region_code_ui": 0, "continent_code_ui": 3, "continent_code_s": "au", "country_code_ui": 580 },
{ "name_id_s": "Mozambique", "iso_3_s": "moz", "iso_2_s": "mz", "region_code_ui": 1, "continent_code_ui": 1, "continent_code_s": "af", "country_code_ui": 508 },
{ "name_id_s": "Mauritania", "iso_3_s": "mrt", "iso_2_s": "mr", "region_code_ui": 1, "continent_code_ui": 1, "continent_code_s": "af", "country_code_ui": 478 },
{ "name_id_s": "Montserrat", "iso_3_s": "msr", "iso_2_s": "ms", "region_code_ui": 0, "continent_code_ui": 6, "continent_code_s": "na", "country_code_ui": 500 },
{ "name_id_s": "Martinique", "iso_3_s": "mtq", "iso_2_s": "mq", "region_code_ui": 0, "continent_code_ui": 6, "continent_code_s": "na", "country_code_ui": 474 },
{ "name_id_s": "Mauritius", "iso_3_s": "mus", "iso_2_s": "mu", "region_code_ui": 1, "continent_code_ui": 1, "continent_code_s": "af", "country_code_ui": 480 },
{ "name_id_s": "Malawi", "iso_3_s": "mwi", "iso_2_s": "mw", "region_code_ui": 1, "continent_code_ui": 1, "continent_code_s": "af", "country_code_ui": 454 },
{ "name_id_s": "Malaysia", "iso_3_s": "mys", "iso_2_s": "my", "region_code_ui": 1, "continent_code_ui": 4, "continent_code_s": "as", "country_code_ui": 458 },
{ "name_id_s": "Mayotte", "iso_3_s": "myt", "iso_2_s": "yt", "region_code_ui": 0, "continent_code_ui": 1, "continent_code_s": "af", "country_code_ui": 175 },

{ "name_id_s": "Namibia", "iso_3_s": "nam", "iso_2_s": "na", "region_code_ui": 1, "continent_code_ui": 1, "continent_code_s": "af", "country_code_ui": 516 },
{ "name_id_s": "New Caledonia", "iso_3_s": "ncl", "iso_2_s": "nc", "region_code_ui": 0, "continent_code_ui": 3, "continent_code_s": "au", "country_code_ui": 540 },
{ "name_id_s": "Niger", "iso_3_s": "ner", "iso_2_s": "ne", "region_code_ui": 1, "continent_code_ui": 1, "continent_code_s": "af", "country_code_ui": 562 },
{ "name_id_s": "Norfolk Island", "iso_3_s": "nfk", "iso_2_s": "nf", "region_code_ui": 0, "continent_code_ui": 3, "continent_code_s": "au", "country_code_ui": 574 },
{ "name_id_s": "Nigeria", "iso_3_s": "nga", "iso_2_s": "ng", "region_code_ui": 1, "continent_code_ui": 1, "continent_code_s": "af", "country_code_ui": 566 },
{ "name_id_s": "Nicaragua", "iso_3_s": "nic", "iso_2_s": "ni", "region_code_ui": 1, "continent_code_ui": 6, "continent_code_s": "na", "country_code_ui": 558 },
{ "name_id_s": "Niue", "iso_3_s": "niu", "iso_2_s": "nu", "region_code_ui": 0, "continent_code_ui": 3, "continent_code_s": "au", "country_code_ui": 570 },
{ "name_id_s": "Netherlands", "iso_3_s": "nld", "iso_2_s": "nl", "region_code_ui": 1, "continent_code_ui": 5, "continent_code_s": "eu", "country_code_ui": 528 },
{ "name_id_s": "Norway", "iso_3_s": "nor", "iso_2_s": "no", "region_code_ui": 1, "continent_code_ui": 5, "continent_code_s": "eu", "country_code_ui": 578 },
{ "name_id_s": "Nepal", "iso_3_s": "npl", "iso_2_s": "np", "region_code_ui": 1, "continent_code_ui": 4, "continent_code_s": "as", "country_code_ui": 524 },
{ "name_id_s": "Nauru", "iso_3_s": "nru", "iso_2_s": "nr", "region_code_ui": 1, "continent_code_ui": 3, "continent_code_s": "au", "country_code_ui": 520 },
{ "name_id_s": "New Zealand", "iso_3_s": "nzl", "iso_2_s": "nz", "region_code_ui": 1, "continent_code_ui": 3, "continent_code_s": "au", "country_code_ui": 554 },
{ "name_id_s": "Oman", "iso_3_s": "omn", "iso_2_s": "om", "region_code_ui": 1, "continent_code_ui": 4, "continent_code_s": "as", "country_code_ui": 512 },
{ "name_id_s": "Pakistan", "iso_3_s": "pak", "iso_2_s": "pk", "region_code_ui": 1, "continent_code_ui": 4, "continent_code_s": "as", "country_code_ui": 586 },
{ "name_id_s": "Panama", "iso_3_s": "pan", "iso_2_s": "pa", "region_code_ui": 1, "continent_code_ui": 6, "continent_code_s": "na", "country_code_ui": 591 },
{ "name_id_s": "Pitcairn", "iso_3_s": "pcn", "iso_2_s": "pn", "region_code_ui": 0, "continent_code_ui": 3, "continent_code_s": "au", "country_code_ui": 612 },
{ "name_id_s": "Peru", "iso_3_s": "per", "iso_2_s": "pe", "region_code_ui": 1, "continent_code_ui": 7, "continent_code_s": "sa", "country_code_ui": 604 },
{ "name_id_s": "Philippines", "iso_3_s": "phl", "iso_2_s": "ph", "region_code_ui": 1, "continent_code_ui": 4, "continent_code_s": "as", "country_code_ui": 608 },
{ "name_id_s": "Palau", "iso_3_s": "plw", "iso_2_s": "pw", "region_code_ui": 1, "continent_code_ui": 3, "continent_code_s": "au", "country_code_ui": 585 },
{ "name_id_s": "Papua New Guinea", "iso_3_s": "png", "iso_2_s": "pg", "region_code_ui": 1, "continent_code_ui": 3, "continent_code_s": "au", "country_code_ui": 598 },
{ "name_id_s": "Poland", "iso_3_s": "pol", "iso_2_s": "pl", "region_code_ui": 1, "continent_code_ui": 5, "continent_code_s": "eu", "country_code_ui": 616 },
{ "name_id_s": "Puerto Rico", "iso_3_s": "pri", "iso_2_s": "pr", "region_code_ui": 0, "continent_code_ui": 6, "continent_code_s": "na", "country_code_ui": 630 },
{ "name_id_s": "Korea - North", "iso_3_s": "prk", "iso_2_s": "kp", "region_code_ui": 1, "continent_code_ui": 4, "continent_code_s": "as", "country_code_ui": 408 },
{ "name_id_s": "Portugal", "iso_3_s": "prt", "iso_2_s": "pt", "region_code_ui": 1, "continent_code_ui": 5, "continent_code_s": "eu", "country_code_ui": 620 },
{ "name_id_s": "Paraguay", "iso_3_s": "pry", "iso_2_s": "py", "region_code_ui": 1, "continent_code_ui": 7, "continent_code_s": "sa", "country_code_ui": 600 },
{ "name_id_s": "Palestinian Territories", "iso_3_s": "pse", "iso_2_s": "ps", "region_code_ui": 1, "continent_code_ui": 4, "continent_code_s": "as", "country_code_ui": 275 },
{ "name_id_s": "French Polynesia", "iso_3_s": "pyf", "iso_2_s": "pf", "region_code_ui": 0, "continent_code_ui": 3, "continent_code_s": "au", "country_code_ui": 258 },
{ "name_id_s": "Qatar", "iso_3_s": "qat", "iso_2_s": "qa", "region_code_ui": 1, "continent_code_ui": 4, "continent_code_s": "as", "country_code_ui": 634 },
{ "name_id_s": "Reunion", "iso_3_s": "reu", "iso_2_s": "re", "region_code_ui": 0, "continent_code_ui": 1, "continent_code_s": "af", "country_code_ui": 638 },
{ "name_id_s": "Romania", "iso_3_s": "rou", "iso_2_s": "ro", "region_code_ui": 1, "continent_code_ui": 5, "continent_code_s": "eu", "country_code_ui": 642 },
{ "name_id_s": "Russian Federation", "iso_3_s": "rus", "iso_2_s": "ru", "region_code_ui": 1, "continent_code_ui": 5, "continent_code_s": "eu", "country_code_ui": 643 },
{ "name_id_s": "Rwanda", "iso_3_s": "rwa", "iso_2_s": "rw", "region_code_ui": 1, "continent_code_ui": 1, "continent_code_s": "af", "country_code_ui": 646 },
{ "name_id_s": "Saudi Arabia", "iso_3_s": "sau", "iso_2_s": "sa", "region_code_ui": 1, "continent_code_ui": 4, "continent_code_s": "as", "country_code_ui": 682 },
{ "name_id_s": "Sudan", "iso_3_s": "sdn", "iso_2_s": "sd", "region_code_ui": 1, "continent_code_ui": 1, "continent_code_s": "af", "country_code_ui": 736 },

{ "name_id_s": "Senegal", "iso_3_s": "sen", "iso_2_s": "sn", "region_code_ui": 1, "continent_code_ui": 1, "continent_code_s": "af", "country_code_ui": 686 },
{ "name_id_s": "Singapore", "iso_3_s": "sgp", "iso_2_s": "sg", "region_code_ui": 1, "continent_code_ui": 4, "continent_code_s": "as", "country_code_ui": 702 },
{ "name_id_s": "South Georgia / South Sandwich Isl", "iso_3_s": "sgs", "iso_2_s": "gs", "region_code_ui": 0, "continent_code_ui": 7, "continent_code_s": "sa", "country_code_ui": 239 },
{ "name_id_s": "St. Helena", "iso_3_s": "shn", "iso_2_s": "sh", "region_code_ui": 1, "continent_code_ui": 1, "continent_code_s": "af", "country_code_ui": 654 },
{ "name_id_s": "Svalbard And Jan Mayen Islands", "iso_3_s": "sjm", "iso_2_s": "sj", "region_code_ui": 0, "continent_code_ui": 5, "continent_code_s": "eu", "country_code_ui": 744 },
{ "name_id_s": "Solomon Islands", "iso_3_s": "slb", "iso_2_s": "sb", "region_code_ui": 1, "continent_code_ui": 3, "continent_code_s": "au", "country_code_ui": 90 },
{ "name_id_s": "Sierra Leone", "iso_3_s": "sle", "iso_2_s": "sl", "region_code_ui": 1, "continent_code_ui": 1, "continent_code_s": "af", "country_code_ui": 694 },
{ "name_id_s": "El Salvador", "iso_3_s": "slv", "iso_2_s": "sv", "region_code_ui": 1, "continent_code_ui": 6, "continent_code_s": "na", "country_code_ui": 222 },
{ "name_id_s": "San Marino", "iso_3_s": "smr", "iso_2_s": "sm", "region_code_ui": 1, "continent_code_ui": 5, "continent_code_s": "eu", "country_code_ui": 674 },
{ "name_id_s": "Somalia", "iso_3_s": "som", "iso_2_s": "so", "region_code_ui": 1, "continent_code_ui": 1, "continent_code_s": "af", "country_code_ui": 706 },
{ "name_id_s": "St. Pierre And Miquelon", "iso_3_s": "spm", "iso_2_s": "pm", "region_code_ui": 0, "continent_code_ui": 6, "continent_code_s": "na", "country_code_ui": 666 },
{ "name_id_s": "Serbia", "iso_3_s": "srb", "iso_2_s": "rs", "region_code_ui": 1, "continent_code_ui": 5, "continent_code_s": "eu", "country_code_ui": 688 },
{ "name_id_s": "South Sudan", "iso_3_s": "ssd", "iso_2_s": "ss", "region_code_ui": 1, "continent_code_ui": 1, "continent_code_s": "af", "country_code_ui": 728 },
{ "name_id_s": "Sao Tome And Principe", "iso_3_s": "stp", "iso_2_s": "st", "region_code_ui": 1, "continent_code_ui": 1, "continent_code_s": "af", "country_code_ui": 678 },
{ "name_id_s": "Suriname", "iso_3_s": "sur", "iso_2_s": "sr", "region_code_ui": 1, "continent_code_ui": 7, "continent_code_s": "sa", "country_code_ui": 740 },
{ "name_id_s": "Slovakia (slovak Republic)", "iso_3_s": "svk", "iso_2_s": "sk", "region_code_ui": 1, "continent_code_ui": 5, "continent_code_s": "eu", "country_code_ui": 703 },
{ "name_id_s": "Slovenia", "iso_3_s": "svn", "iso_2_s": "si", "region_code_ui": 1, "continent_code_ui": 5, "continent_code_s": "eu", "country_code_ui": 705 },
{ "name_id_s": "Sweden", "iso_3_s": "swe", "iso_2_s": "se", "region_code_ui": 1, "continent_code_ui": 5, "continent_code_s": "eu", "country_code_ui": 752 },
{ "name_id_s": "Swaziland", "iso_3_s": "swz", "iso_2_s": "sz", "region_code_ui": 1, "continent_code_ui": 1, "continent_code_s": "af", "country_code_ui": 748 },
{ "name_id_s": "Sint Maarten", "iso_3_s": "sxm", "iso_2_s": "sx", "region_code_ui": 0, "continent_code_ui": 6, "continent_code_s": "na", "country_code_ui": 534 },
{ "name_id_s": "Seychelles", "iso_3_s": "syc", "iso_2_s": "sc", "region_code_ui": 1, "continent_code_ui": 1, "continent_code_s": "af", "country_code_ui": 690 },
{ "name_id_s": "Syrian Arab Republic", "iso_3_s": "syr", "iso_2_s": "sy", "region_code_ui": 1, "continent_code_ui": 4, "continent_code_s": "as", "country_code_ui": 760 },
{ "name_id_s": "Turks And Caicos Islands", "iso_3_s": "tca", "iso_2_s": "tc", "region_code_ui": 0, "continent_code_ui": 6, "continent_code_s": "na", "country_code_ui": 796 },
{ "name_id_s": "Chad", "iso_3_s": "tcd", "iso_2_s": "td", "region_code_ui": 1, "continent_code_ui": 1, "continent_code_s": "af", "country_code_ui": 148 },
{ "name_id_s": "Togo", "iso_3_s": "tgo", "iso_2_s": "tg", "region_code_ui": 1, "continent_code_ui": 1, "continent_code_s": "af", "country_code_ui": 768 },
{ "name_id_s": "Thailand", "iso_3_s": "tha", "iso_2_s": "th", "region_code_ui": 1, "continent_code_ui": 4, "continent_code_s": "as", "country_code_ui": 764 },
{ "name_id_s": "Tajikistan", "iso_3_s": "tjk", "iso_2_s": "tj", "region_code_ui": 1, "continent_code_ui": 4, "continent_code_s": "as", "country_code_ui": 762 },
{ "name_id_s": "Tokelau", "iso_3_s": "tkl", "iso_2_s": "tk", "region_code_ui": 0, "continent_code_ui": 3, "continent_code_s": "au", "country_code_ui": 772 },
{ "name_id_s": "Turkmenistan", "iso_3_s": "tkm", "iso_2_s": "tm", "region_code_ui": 1, "continent_code_ui": 4, "continent_code_s": "as", "country_code_ui": 795 },
{ "name_id_s": "Timor-leste", "iso_3_s": "tls", "iso_2_s": "tl", "region_code_ui": 1, "continent_code_ui": 4, "continent_code_s": "as", "country_code_ui": 626 },
{ "name_id_s": "Tonga", "iso_3_s": "ton", "iso_2_s": "to", "region_code_ui": 1, "continent_code_ui": 3, "continent_code_s": "au", "country_code_ui": 776 },
{ "name_id_s": "Trinidad And Tobago", "iso_3_s": "tto", "iso_2_s": "tt", "region_code_ui": 1, "continent_code_ui": 6, "continent_code_s": "na", "country_code_ui": 780 },
{ "name_id_s": "Tunisia", "iso_3_s": "tun", "iso_2_s": "tn", "region_code_ui": 1, "continent_code_ui": 1, "continent_code_s": "af", "country_code_ui": 788 },
{ "name_id_s": "Turkey", "iso_3_s": "tur", "iso_2_s": "tr", "region_code_ui": 1, "continent_code_ui": 5, "continent_code_s": "eu", "country_code_ui": 792 },

```
   { "name_id_s": "Tuvalu", "iso_3_s": "tuv", "iso_2_s": "tv", "region_code_ui": 1, "continent_code_ui": 3,
"continent_code_s": "au", "country_code_ui": 798 },
   { "name_id_s": "Taiwan - Province Of China", "iso_3_s": "twn", "iso_2_s": "tw", "region_code_ui": 1, "continent_code_ui":
4, "continent_code_s": "as", "country_code_ui": 158 },
   { "name_id_s": "Tanzania - United Republic Of", "iso_3_s": "tza", "iso_2_s": "tz", "region_code_ui": 1,
"continent_code_ui": 1, "continent_code_s": "af", "country_code_ui": 834 },
   { "name_id_s": "Uganda", "iso_3_s": "uga", "iso_2_s": "ug", "region_code_ui": 1, "continent_code_ui": 1,
"continent_code_s": "af", "country_code_ui": 800 },
   { "name_id_s": "Ukraine", "iso_3_s": "ukr", "iso_2_s": "ua", "region_code_ui": 1, "continent_code_ui": 5,
"continent_code_s": "eu", "country_code_ui": 804 },
   { "name_id_s": "Us Minor Outlying Islands", "iso_3_s": "umi", "iso_2_s": "um", "region_code_ui": 1, "continent_code_ui":
3, "continent_code_s": "au", "country_code_ui": 581 },
   { "name_id_s": "Uruguay", "iso_3_s": "ury", "iso_2_s": "uy", "region_code_ui": 1, "continent_code_ui": 7,
"continent_code_s": "sa", "country_code_ui": 858 },
   { "name_id_s": "United States", "iso_3_s": "usa", "iso_2_s": "us", "region_code_ui": 1, "continent_code_ui": 6,
"continent_code_s": "na", "country_code_ui": 840 },
   { "name_id_s": "Uzbekistan", "iso_3_s": "uzb", "iso_2_s": "uz", "region_code_ui": 1, "continent_code_ui": 4,
"continent_code_s": "as", "country_code_ui": 860 },
   { "name_id_s": "Holy See (vatican City State)", "iso_3_s": "vat", "iso_2_s": "va", "region_code_ui": 0, "continent_code_ui":
5, "continent_code_s": "eu", "country_code_ui": 336 },
   { "name_id_s": "Saint Vincent And The Grenadines", "iso_3_s": "vct", "iso_2_s": "vc", "region_code_ui": 1,
"continent_code_ui": 6, "continent_code_s": "na", "country_code_ui": 670 },
   { "name_id_s": "Venezuela", "iso_3_s": "ven", "iso_2_s": "ve", "region_code_ui": 1, "continent_code_ui": 7,
"continent_code_s": "sa", "country_code_ui": 862 },
   { "name_id_s": "British Virgin Islands", "iso_3_s": "vgb", "iso_2_s": "vg", "region_code_ui": 0, "continent_code_ui": 6,
"continent_code_s": "na", "country_code_ui": 92 },
   { "name_id_s": "Us Virgin Islands", "iso_3_s": "vir", "iso_2_s": "vi", "region_code_ui": 0, "continent_code_ui": 6,
"continent_code_s": "na", "country_code_ui": 850 },
   { "name_id_s": "Viet Nam", "iso_3_s": "vnm", "iso_2_s": "vn", "region_code_ui": 1, "continent_code_ui": 4,
"continent_code_s": "as", "country_code_ui": 704 },
   { "name_id_s": "Vanuatu", "iso_3_s": "vut", "iso_2_s": "vu", "region_code_ui": 1, "continent_code_ui": 3,
"continent_code_s": "au", "country_code_ui": 548 },
   { "name_id_s": "Wallis And Futuna Islands", "iso_3_s": "wlf", "iso_2_s": "wf", "region_code_ui": 0, "continent_code_ui": 3,
"continent_code_s": "au", "country_code_ui": 876 },
   { "name_id_s": "Samoa", "iso_3_s": "wsm", "iso_2_s": "ws", "region_code_ui": 1, "continent_code_ui": 3,
"continent_code_s": "au", "country_code_ui": 882 },
   { "name_id_s": "Yemen", "iso_3_s": "yem", "iso_2_s": "ye", "region_code_ui": 1, "continent_code_ui": 4,
"continent_code_s": "as", "country_code_ui": 887 },
   { "name_id_s": "South Africa", "iso_3_s": "zaf", "iso_2_s": "za", "region_code_ui": 1, "continent_code_ui": 1,
"continent_code_s": "af", "country_code_ui": 710 },
   { "name_id_s": "Zambia", "iso_3_s": "zmb", "iso_2_s": "zm", "region_code_ui": 1, "continent_code_ui": 1,
"continent_code_s": "af", "country_code_ui": 894 },
   { "name_id_s": "Zimbabwe", "iso_3_s": "zwe", "iso_2_s": "zw", "region_code_ui": 1, "continent_code_ui": 1,
"continent_code_s": "af", "country_code_ui": 716 }
 ]
}
```

7 Multiple File Examples

To enable distribute of larger data sets, TPX supports breaking data sets into smaller files indexed by a manifest file that provides the list of smaller file fragments that belong to a single feed.

7.1 Manifest File Example

This example shows a manifest introduction file that has references to multiple dictionary files, multiple element observable files and multiple collection files.

```
{
  //
  // SECTION: Intro
  // DESCRIPTION: Provides the attribute of the list, provider name, date of distribution ...etc. There is only one
source_observable per TPX file.
  // If a provider has multiple feeds then there will be one file per feed
  //
  "schema_version_s": "2.2.0",
  "provider_s": "Intel Provider Company",
  "list_name_s": "Intel Provider Company List Data",
  "source_observable_s": "PROV_IND_NAME",
  "source_file_s": "/var/lg/data/json/list_name/2014/06/01/202data.csv",
  "source_description_s": "This is a description of the feed and the information it provides",
  "distribution_time_t": 1221312312,
  "last_updated_t": 121232134,
  "score_i": 90,

  //
  // SECTION: Manifest for dictionary files
  //
  "dictionary_file_manifest": [
    "/var/data/json/202data_dictionary_1.json", "/var/data/json/202data_dictionary_2.json"
    ],

  //
  // SECTION: Manifest for observable element files
  //
  "observable_element_file_manifest": [
    "/var/data/json/202data_1.json", "/var/data/json/202data_2.json"
  ],

  //
  // SECTION: Manifest for collection files
  //
  "collection_file_manifest": [
    "/var/data/json/collection_1.json", "/var/data/json/collection_2.json"
  ]

  //
  // SECTION: Manifest for network files
  //
  "network_file_manifest": [
    "/var/data/json/asn_1.json", "/var/data/json/asn_2.json"
  ]
}
```

7.2 Observable Dictionary

This example shows a dictionary file that is referenced by the manifest introduction file. Note that there is no need for repeating the introductory information.


```
{
  //
  // SECTION: Observable Dictionary
  // DESCRIPTION: Provides the dictionary of all observables in this file. For each observable there is a name,
criticality, classififcation list
  //
  "observable_dictionary_c_array": [
    {
      "observable_id_s" : "Conficker A",
      "criticality_i": 70,
      "score_i": 72,
      "summary_s": "This is a summary of the observable",
      "description_s": "If an IP address or domain has been associated with this tag, it means that Intel Provider
Company has identified the IP address or domain to be associated with the Conficker botnet variant A.",
      "notes_s": "User defined notes",
      "reference_s_array": [
          "http://www.thisisareference.com/observablereference",
"http://www.anotherreference.com/2ndrefererence"
      ],
      "classification_c_array" : [
        {
          "classification_id_s": "Worm",
          "classification_family_s": "Malware",
          "score_i": 70
        }
      ],
    },
    {
      "observable_id_s": "Clicker",
      "criticality_i": 70,
      "score_i": 72,
      "summary_s": "This is a summary of the observable",
      "description_s": "If an IP address or domain has been associated with this tag, it means that Intel Provider
Company has identified the IP address or domain to be associated with the Clicker botnet.",
      "notes_s": "User defined notes",
      "reference_s_array": [
          "http://www.thisisareference.com/observablereference",
"http://www.anotherreference.com/2ndrefererence"
      ],
      "classification_c_array": [
        {
          "classification_id_s": "Bot",
          "classification_family_s": "Malware",
          "score_i": 70
        }
      ],
    },
    {
      "observable_id_s": "Sality",
      "criticality_i": 70,
      "score_i": 72,
      "summary_s": "This is a summary of the observable",
      "description_s": "If an IP address or domain has been associated with this tag, it means that Intel Provider
Company has identified the IP address or domain to be associated with the Sality botnet variant 1.",
      "notes_s": "User defined notes",
      "reference_s_array": [
          "http://www.thisisareference.com/observablereference",
"http://www.anotherreference.com/2ndrefererence"
      ],
      "classification_c_array": [
        {
```

```
        "classification_id_s": "Bot",
        "classification_family_s": "Malware",
        "score_i": 70
       }
     ],
    }
  ],
}
```


7.3 DDoS Manifest File Example

This example shows a manifest introduction file for a set of DDoS observations containing network observations of DDoS incidents detected by a sensor network


```
{
   "dictionary_file_manifest": [
      "tpx2-1-example-ddos-dictionary.json"
   ],
   "distribution_time_t": 1431340357,
   "last_updated_t": 1431340357,
   "list_name_s": "DDoS Sensors",
   "observable_element_file_manifest": [
      "ddos_tpx_20150725_155843.json",
      "ddos_tpx_20150725_145813.json"
   ],
   "provider_s": "Shadowserver",
   "schema_version_s": "2.2.0",
   "score_i": 90,
   "source_description_s": "Attempted DDoS attacks observed by DDoS sensor network",
   "source_observable_s": "network_ddos_sensors"
}
```


7.4 DDoS Observations Example

This example shows a dictionary file that is referenced by the manifest introduction file. Note that there is no need for repeating the introductory information.


```
{
 "element_observable_c_array":[
  {
   "subject_ipv4_s":"52.13.108.98",
   "threat_observable_c_map":{
    "DDoS":{
     "dns_c_array":[
      {
       "sensor_country_code_s":"US",
       "packet_count_i":10,
       "total_packet_size_i":530,
       "dest_port_i":53,
       "transport_protocol_s":"udp"
      }
     ],
     "ttl_i":60,
     "occurred_at_t":1437839923
    }
   },
   "asn_s":"Amazon Technologies Inc.",
   "country_code_s":"US",
   "asn_i":16509
  },
```

```
    {
      "subject_ipv4_s":"70.32.40.2",
      "threat_observable_c_map":{
        "DDoS":{
          "dns_c_array":[
            {
              "sensor_country_code_s":"US",
              "packet_count_i":9,
              "total_packet_size_i":408,
              "dest_port_i":53,
              "transport_protocol_s":"udp"
            }
          ],
          "ttl_i":60,
          "occurred_at_t":1437839923
        }
      },
      "asn_s":"Ubiquity Server Solutions New York",
      "country_code_s":"US",
      "asn_i":15003
    }
  ]
}
```