CERT Australia CTI Toolkit Documentation

Release 0.1

CERT Australia, Australian Government

November 07, 2015

CONTENTS

This package contains cyber threat intelligence (CTI) tools created by CERT Australia.

Contents:

CHAPTER

ONE

INSTALLATION

This document describes how to install the CERT Australia CTI Toolkit.

Installation is streamlined using Python's setuptools. The following installation process has been tested on clean install of Ubuntu 14.04.

1. Install prerequisites required by setuptools and libtaxii:

   ```
   $ sudo apt-get install python-pip python-dev libxml2-dev libxslt1-dev libz-dev
   ```

2. Clone the cti-toolkit repository (prompts for github username and password):

   ```
   $ git clone https://github.com/certau/cti-toolkit.git
   ```

3. Run the setup.py script to build and install the tools (and pip dependencies):

   ```
   $ cd cti-toolkit
   $ sudo python setup.py install
   ```

That's it. You should now be able to run utilities, such as stixtransclient.py:

```
$ stixtransclient.py -h
```

1.1 Documentation

To build the documentation you need Sphinx:

```
$ sudo pip install Sphinx sphinxcontrib-napoleon
$ cd docs
$ make html
```

This will create an HTML version of the documentation in docs/_build/html.

CHAPTER

TWO

STIXTRANSCLIENT.PY

Few systems can utilise indicators and observables when stored in STIX packages. CERT Australia has developed a utility (stixtransclient.py) that allows the atomic observables contained within a STIX package to be extracted and presented in either a text delimited format, or in the Bro Intel Framework format.

2.1 stixtransclient.py overview

Example usage::

```
$ stixtransclient.py -a -s -b --file ca-XXXX-YYY-stix.xml

++++++++++++++++++++++++++++++++++++
Summary statistics for XXXX-YYY
++++++++++++++++++++++++++++++++++++
File related observables:       9
Email related observables:      8
Domain related observables:     3
Address related observables:    3
URL related observables:        533
++++++++++++++++++++++++++++++++++++

#fields indicator       indicator_type  meta.source     meta.url        meta.do_notice  meta.if_
216.213.78.72   Intel::ADDR     CERT    https://yeti.host.tld/XXXX-YYY  T       -       -
88.211.147.62   Intel::ADDR     CERT    https://yeti.host.tld/XXXX-YYY  T       -       -
73.189.141.135  Intel::ADDR     CERT    https://yeti.host.tld/XXXX-YYY  T       -       -
38stalprof.com.ua/includes/domit/src.php        Intel::URL      CERT    https://yeti.host.tld/XX
ferma.az/incfiles/classes/iddx.php      Intel::URL      CERT    https://yeti.host.tld/XXXX-YYY
intimit.ru/includes/phpmailer/source.php        Intel::URL      CERT    https://yeti.host.tld/XX
jetc.com/illegal_access_folder/source.php       Intel::URL      CERT    https://yeti.host.tld/XX
keeleux.com/wp/wp-includes/idx.php      Intel::URL      CERT    https://yeti.host.tld/XXXX-YYY
shopcode.net/wp-includes/pomo/idx.php   Intel::URL      CERT    https://yeti.host.tld/XXXX-YYY
simpsons.freesexycomics.com/wp06/wp-includes/po.php     Intel::URL      CERT    https://yeti.hos
topstonet.ru/modules/mod_search/source.php      Intel::URL      CERT    https://yeti.host.tld/XX
zhayvoronok.com/wp-includes/pomo/idx.php        Intel::URL      CERT    https://yeti.host.tld/XX

$ stixtransclient.py -b --config ~/src/cti-toolkit/config/ctitoolkit.conf.sample-hailataxii \
                     --begin-timestamp `date +%Y-%m-%dT00:00:00.000000+00:00`

http://ebay.x10host.com/ws/NeBayISAPI.dl/oo_login.php   Intel::URL      HAT     hailataxii.com
http://golden-corner.com/make/bookmark/ii.php?rand.13InboxLight.aspxn.1774256418=       Intel::U
http://redbankplainsvet.com/324432423/192317148/        Intel::URL      HAT     hailataxii.com
http://www.gallecarhire.com/Admin/k/isx007/gdd.htm      Intel::URL      HAT     hailataxii.com
http://www.ibankservice-us.com/e49b438be1a419630a52f4792726351a/        Intel::URL      HAT
```

```
http://www.kaliluana.com/wp-includes/images/media/view/secure-dropbox/document/ Intel::URL
http://www.myownboss.co.zw/ab/ggdc/     Intel::URL      HAT     hailataxii.com  T       -
http://www.performance2.co.uk/wp-content/senn/  Intel::URL      HAT     hailataxii.com  T
http://www.toldosuniao.com.br/wp-admin/user/wp-config/user/config.inc/  Intel::URL      HAT
```

2.2 stixtransclient.py help

The command line (and configuration) options for stixtransclient.py are displayed below:

```
$ stixtransclient.py -h
```

usage: stixtransclient.py [-h] [-a] [-c] [-n] [-v] [-d] [-b] [–bro_no_notice] [–misp] [-t] [-f FIELD_SEPARATOR] [-s] [–base_url BASE_URL] [–source SOURCE] [–header] [–config CONFIG] [–hostname HOSTNAME] [–username USERNAME] [–password PASSWORD] [–key KEY] [–cert CERT] [–soltra] [–ssl] [–path PATH] [–collection COLLECTION] [–begin-timestamp BEGIN_TS] [–end-timestamp END_TS] [–subscription-id SUBSCRIPTION_ID] [–misp_url MISP_URL] [–misp_key MISP_KEY] [–misp_distribution MISP_DISTRIBUTION] [–misp_threat MISP_THREAT] [–misp_analysis MISP_ANALYSIS] [–misp_info MISP_INFO] [–misp_published] [–file FILE | –taxii]

Utility to extract observables from local STIX files or a TAXII server Args that start with '–' (eg. –aus) can also be set in a config file (/etc/ctitoolkit.conf or ~/.ctitoolkit or specified via –config) by using .ini or .yaml-style syntax (eg. aus=value). If an arg is specified in more than one place, then command-line values override config file values which override defaults.

optional arguments:

-h, --help	show this help message and exit
--config CONFIG	Configuration file to use
--file FILE	Full path to XML file to process
--taxii	TAXII server and arguments for poll client

input:

-a, --aus	input is CERT Australia formatted STIX
-c, --ca	input is CCIRC formatted STIX
-n, --nccic	input is NCCIC formatted STIX

output:

-v, --verbose	verbose output
-d, --debug	Enable debug output
-b, --bro	output bro intel framework formatted text
--bro_no_notice	Suppress bro intel notice framework messages
--misp	Feed output to MISP
-t, --text	output delimited text
-f FIELD_SEPARATOR	Field separation character to use
-s, --stats	display summary stats
--base_url BASE_URL	Base URL for indicator source - used in bro and MISP output
--source SOURCE	Source of indicators - eg Hailataxii, CERT-AU

--header Include header row for text output

taxii:

--hostname HOSTNAME Hostname of TAXII server. Defaults to taxii.host.tld

--username USERNAME Username for TAXII authentication

--password PASSWORD Password for TAXII authentication. Default value: guest

--key KEY PEM Key for TAXII authentication

--cert CERT PEM Certiificate file for authenticating to TAXII

--soltra TAXII server is a SoltraEdge appliance

--ssl Use SSL to connect to TAXII server

--path PATH Path on TAXII server. Defaults to /services/poll/

--collection COLLECTION Data Collection to poll. Defaults to 'default'.

--begin-timestamp BEGIN_TS The begin timestamp (format: YYYY-MM-DDTHH:MM:SS.ssssss+/-hh:mm) for the poll request. Defaults to None.

--end-timestamp END_TS The end timestamp (format: YYYY-MM-DDTHH:MM:SS.ssssss+/-hh:mm) for the poll request. Defaults to None.

--subscription-id SUBSCRIPTION_ID The Subscription ID for the poll request. Defaults to None.

misp:

--misp_url MISP_URL URL of MISP server. Defaults to misp.host.tld

--misp_key MISP_KEY Token for accessing MISP instance

--misp_distribution MISP_DISTRIBUTION Distribution group in MISP. Defaults to Your organisation only (0)

--misp_threat MISP_THREAT Threat level in MISP. Defaults to undefined (4)

--misp_analysis MISP_ANALYSIS Analysis phase in MISP. Defaults to initial (0)

--misp_info MISP_INFO MISP event description. Defaults to STIX package title or Automated STIX ingest

--misp_published Set MISP published state to True

CHAPTER

THREE

CTITOOLKIT.CONF

The stixtransclient.py utility can read its configuration parameters from the command line or configuration files located at:

- /etc/ctitoolkit.conf
- ~/.ctitoolkit

Any options that can be specified on the command line can be specified in a configuration file. Command line options will always take precedence.

3.1 ctitoolkit.conf examples

Some examples follow:

YETI:

```
# Connect to the CERT Australia taxii server
# Authenticate using certificate and user credentials
# Poll indicators from the 'advisories' collection
# Output data in Bro intel framework format
source: YETI
hostname: yeti.host.tld
cert: /path/cert.pem
key: /path/key.pem
username: _USER_
password: _PASSWORD_
collection: advisories
base_url: https://source.host.com/advisories/
ssl: true
taxii: true
bro: true
aus: true
```

SoltraEdge:

```
source: HAT
hostname: hailataxii.com
username: guest
password: guest
path: /taxii-data
collection: guest.dataForLast_7daysOnly
taxii: true
soltra: true
bro: true
```

FILE:

```
# Process an STIX file and output to MISP
source: FILE
file: /path/to/stix/file.xml
misp: true
misp_url:http://misp.host.tld
misp_key:keykeykeykeykeykeyke
```

CHAPTER

FOUR

API REFERENCE

Contents:

4.1 certau.transform.stixtrans Module

This module provides the certau.transform.StixTransform class which supports converting indicators (observables) from a STIX package into various other formats, including one suitable for importing indicators into the Bro Intelligence Framework.

class certau.transform.**StixTransform**(*options*)

When called with a STIX package and set of command line options this class will generate and output indicators appropriate to the arguments provided

Parameters **options** – an options object containing configuration options (see below)

Options used by this class are listed under the heading 'Other Parameters' below (these are attributes of the options object).

Other Parameters

- **stats** – generate summary statistics for the STIX Package
- **bro** – generate output in the Bro Intel format
- **text** – generate raw text output
- **aus** – input is a CERT Australia STIX package
- **nccic** – input is a US-CERT (NCCIC) STIX package
- **ca** – input is a Canadian (CCIRC) STIX package
- **soltra** – input has been obtained from a Soltra TAXII instance
- **field_separator** – delimiter to use in output
- **header** – include header row in text output

display_delimited_results()

Construct a delimited list of observables using options included in args.

Returns a string containing the output

generate_stats()

Returns the summary statistics for the STIX package as a string. Requires that the results array has already been populated.

4.2 certau.client.taxii Module

This module provides a simple TAXII client for polling a TAXII server.

The certau.client.SimpleTaxiiClient class provides a simple interface for polling a collection on a TAXII server and returning the response. It supports SSL (certificate-based) authentication in addition to a username and password.

class certau.client.**SimpleTaxiiClient**(*options*)

A simple interface to the libtaxii libraries for polling a TAXII server.

Parameters **options** – an options object containing configuration options (see below)

Options used by this class are listed under the heading 'Other Parameters' below (these are attributes of the options object).

Other Parameters

- **hostname** – the name of the TAXII server
- **collection** – the collection on the TAXII server to poll
- **path** – the URL path for the collection
- **ssl** – use SSL when connecting to the TAXII server
- **username** – a username for password-based authentication
- **password** – a password for password-based authentication
- **key** – a private key file for SSL certificate-based authentication
- **cert** – a certificate file for SSL certificate-based authentication
- **begin_ts** – a timestamp to describe the earliest content to be returned by the TAXII server
- **end_ts** – a timestamp to describe the most recent content to be returned by the TAXII server
- **subscription_id** – a subscription ID to include with the poll request

send_poll_request()

Send a poll request to the configured server/collection and return the poll response.

Returns a TAXII poll response message. On failure None is returned and an error logged.

CHAPTER

FIVE

INDICES AND TABLES

- *genindex*
- *modindex*
- *search*

C

C

D

G

S