CyberTOOLBELT

Version 3.x Version 4.x

Migration Guide

Revision: 1.0 7/1/2017

CONTENTS

INTRODUCTION

This document describes the differences between versions 3.x and versions 4.x of the CyberTOOLBELT (CTB) restful API access to the CTB database. There are a number of differences between the two versions that make them incompatible both in API usage and data formats. Note that the 3.6 version of the API is still available and will be until at least 12/31/2017. However, it will not be upgraded.

The primary driver of the data format changes to the API returned results is that a number of optimizations and enhancements to the available data were made with the 2.0 version of the CTB web server ("https://www.cybertoolbelt.com"). These changes were reflected in the backend.

The program changes were driven by the desire to have a more consistant and easy to modify set of API commands as well as improving performance.

The documentation has been substantially rewritten. It has increased from 53 to 92 pages in size. It's better organized. It more clearly explains the input parameters and results. It is available at https://www.cybertoolbelt.com/documentation/ctb-restful-api-version4.pdf.

The number of API endpoints increased from XXX to YYY even with removal of two toolsets.

GENERAL CHANGES

A number of changes were made to the API that affect all calls as follows:

- The URL changed from https://api.cybertoolbelt.com:2475 to https://rest-api.cybertoolbelt.com:2476. Notice the port number changed from 2475 to 2476 in addition to the subdomain changing from "api" to "rest-api".
- The PHP interface class we provide changed from "int_dm.php" to "int_ctb.php".
- All calls are "POST" calls. 3.x had a mixture of GET and POST calls.
- Performance in most cases should be much better than the 3.x releases. A level of middleware was removed (translation of our restful API call to our internal API). The API processing code is now written in a much faster language with more parallel operations being performed to satisfy requests. The API also works with its own copy of the CTB database in 95% of all calls on the same server the API is located on. This reduces both data access time and the eliminates internet latancy. The internet latency has been replaced by LAN latency when required.
- More calls return JSON-formated results.
- Better information is returned when an error occurs.

CALL TRANSLATION TABLE

The following table lists the translation of 3.x calls to their 4.x versions:

3.x API Call Format	4.x API Call Format	Notes	Toolset
/POST /domains/find	/domains/match/		do
n/a	/domain/lookup/	New	do
/GET /domains/ips/	/domain/info/	what=ip	do
n/a	/domain/info/	New	do
n/a	/domain/all_info/	New	do
/GET /datamine/email/{:email}	/domain/emails/		do
or:	/domain/info/	what=base	do
n/a	/domain/ip/	New	do
n/a	/domain/all_ips/	New	do
n/a	/domain/by_id/	New	do
n/a	/domain/get_id/	New	do
/GET /domains/subdomains/{:domain}	/domain/info/	what=host	do
or:	/subdomain/domain/	New	do
n/a	/subdomain/ip/	New	do
n/a	/subdomain/search/	New	do
n/a	/domains/ns/	New	do
n/a	/domains/mx/	New	do
/GET /whois/{:id}	/whois/by_id/		whois
n/a	/whois/raw/	New	whois
n/a	/whois/all_contacts/	New	whois
n/a	/whois/get_page/	New	dm

/POST /datamine/whois/	/whois/datamine/		dm
/GET /whois/ip/{:ip}	/ip/whois/		ipwho
/POST /ip/issue/	/ip/issue		issue
n/a	/ip/asn_number/	New	io
n/a	/ip/asns/	New	io
n/a	/ip/by_id/	New	io
n/a	/ip/translate	New	io
/GET /ip/domains/{:ip}	/ip/domains/		io
/GET /ip/geolocate/{:ip}	/ip/geolocate/		io
/POST /ip/issue/	/ip/save_issue/		up
n/a	/ip/issue/	New	issue
/GET /ip/asn/	/ip/asn_info/		io
/POST /datamine/ip_whois/	/ip/datamine/		ipdm
n/a	/ip/blocklist/	New	up
n/a	/ip/get_rdns/	New	io
/GET /ip/is_tor/{:ip}	/ip/is_tor/		io
/GET /ip/is_proxy/{:ip}	/ip/is_proxy/		io
n/a	/ip/type/	New	io
n/a	/ip/asn_badness/	New	io
/POST /report/cyber/	/report/cyber/		up

The toolset abbrevations are: “do” > Domain Operations; “io” > IP operations; “whois” > Domain Whois; “ipwho” > IP Whois; “dm” > Domain datamining; “ipdm” > IP datamining; “up” > Update Operations; “issue” > IP/Domain issues;

REMOVED ITEMS

In almost all cases items were removed for one good reason: no one really used them.

This is the list of removed items:

- The Social Media toolset was removed.
- The Person Search toolset was removed. This toolset was developed primiarly for a single client. We have since developed a different solution for them.
- The "/domains/zone_history/" endpoint was removed.

NEW FEATURES AND CHANGES

The primary additions were to add new endpoints to various toolsets. The following is a brief, 30,000 foot overview of the new items:

- The format of the Whois record returned changed somewhat. Before it was returned as an array that always only had a single record in it. The array wrapper has been removed. See Appendix A of the new documentation for the format of the current Whois record.
- The following major changes were made to existing calls:
  - The "whois/datamine/" call now allows you to specify that you want paginated results.
- Many new endpoints were added. See the *Call Translation Table* for details.
- The "domain/info/" call can return a number of items that were not available under the 3.x API including current live IP(s) for the domains as well as current live name servers. It will also return an indicator as to whether or not the domain is currently "live".
- Information about an IP address has had ASN badness added.
- The IP Issues endpoints are now fully implemented in the Issues Toolset.
- The "domain/info/" and "domain/all_info" endpoints were added in order to provide access to a number different data details about a domain.
- The "ip/info/" endpoint was added to get a number of different data details about an IP address.
- Increased support for Ipv6 was added to the API
- Additional data is returned for many of the calls.

Please review the documentation for more detailed information about functionality and data results.

ROADMAP FOR 4.X

The following is some of what to expect for development of future releases of the API:

- More extensive IPv6 integration.
- Bulk operations.
- Monitoring capabilities.
- Further performance enhancements.
- More access to our abuse data.