

# Mitigating threats associated with your TLD

Moving from passive, complaints-based action to pro-active measures

**Primary Goal:** To identify and take action against domains that may violate the TLD's Acceptable Use Policy or that have otherwise been flagged by third parties as potentially harmful.

**Secondary Goal:** Identify and share information on other domains registered by those individuals for closer inspection. Privacy concerns ? We only share data with the secure domain foundation that is publicly available under CoCCA WHOIS / RDDS policy. The Secure Domain Foundation connects as a "CERT" client type and able to query by EPP ( read only ) and dedicated WHOIS query .

**Our First Attempt** – Contracted a reputable security company to do periodic scanning of the websites of domains in the registry. Outcome ? Expensive and not overly useful...

- Most AUP violations / criminal activity is in lower level domains created by Registrants - names that do not appear in the registry and were not scanned, very few "hits". No "drill-down" on the data. Difficult to extract and store information locally.
- People are generally less than thrilled about having their websites scanned. Detection may be overly intrusive and may impact web applications and/or disrupt services provided to end users -as well as invite angry emails from systems administrators.

**Current Attempt** – Compare domains ( and hosts, contacts, emails ) in the registry against databases that contain data that has identifies potentially harmful host names or actors.

More useful, it identifies subordinate domains not in the registry ( baddomain.domain.tld ) and has none of the side effects of active scanning.

**Configuration Procedure** ? Simple...

Configure CoCCA to connect to and external DB, via an API and continuously “walk through” registry records ( domain / email / name servers ) and look for a match, if one is found, import the data and make it part of the domains history.

CoCCA can be configured to automatically email and/or send SMS to Administrators, Registrars, Registrants or CERT’s and automatically lock (or suspend) the domain when there is a match.

Future versions will allow users to configure the automated actions based on reputation variables - severity of the issue, number of reports, sources of the data etc.

Automation allows operators of even the smallest ccTLD’s with limited human or technical resources to take pro-active measures to identify and react to threats that are associated with domains in their TLDs.

Username / API Key	External Verification System	Description
cocca	CHIP	CHIP verification
4199b068b94716a347e4aa866f5ab504	SECURE_DOMAINS	Secure Test

[Delete](#)

[Edit Record \(Secure Test\)](#) [Cancel](#)

Verification Type

SECURE\_DOMAINS

API Key

4199b068b94716a347e4aa

Description

Secure Test

Host

api.thesesecuredomain.org

Port

1222

[Save](#)

Fast Flux Mitigation Settings for .cx CoCCA Registry Services (NZ) Limited | Public Registrar (CoCCA) - garth\_miller - 49.50.209.148 EN | FR EPP WHOIS

You are currently acting on behalf of CoCCA. Any action you take will be logged against their account.

Home Register Portfolio Name Servers Contacts Logins Clients **Zones** Reports Maintenance Configuration Info Account Sign Out

**Please select what you'd like to do when domains in this zone have security warnings**

- Modify the domain (lock / suspend / exclude)
- Notify people about the problem

**Modification** *Please choose the action you'd like to perform on the domain*

Lock  
Lock  
Suspend  
Exclude

**Notification Settings**

**SMS Notification** *Enter the phone numbers you want to send notification SMS messages to*

**From:** do-not-reply@coccaregistry.net  
**Bcc:** bcc@coccaregistry.net , bcc@coccaregistry.net  
**To:**  Zone Admins

CERT / Law Enforcement (enter the address)

Registrant Contact  Administrative Contacts

Domains Awaiting Approval [+]  
 Domains Pending Activation [+]  
 Pending Superlock [+]  
 Domains With Security Issues [+]  
 Account Balance Negative [+]  
 Search Domains    
 All Zones  
 Create Zone  
 Administrative Actions  
 Build Zone Files  
 Zone File Processing Defaults  
 Zone File Automation  
 Clone Zone  
 Update Pricing  
 Clone Pricing

Easy to configure actions and notifications... will be expanded on in future versions.

Links to any other databases that have an API will be incorporated in future builds as resources allow. CoCCA is "neutral" we just make it easy for users to connect.

You are currently acting on behalf of CoCCA. Any action you take will be logged against their account.

[Home](#)
[Register](#)
[Portfolio](#)
[Name Servers](#)
[Contacts](#)
[Logins](#)
[Clients](#)
[Zones](#)
[Reports](#)
[Maintenance](#)
[Configuration](#)
[Info](#)
[Account](#)
[Sign C](#)

If you would like to clear the outstanding security warnings, please enter a note and press Accept

**Note**

[Accept](#)

These security violations have been recorded regarding this domain

Violation Type	Date Recorded	Date Reported	MD5 Signature	Accepted By (Registrar)	Accepted By (Login)	Date Accepted
CnC	2012-10-02	2012-10-15	353dbd5b67f70236fd11b178afceeed8			

The following security-related notes are on file

Note	Note Type	Made By (Registrar)	Made By (Login)	Date
No notes made for this domain				

Domains Awaiting Approval [+]

Domains Pending Activation [+]

Pending Superlock [+]

Domains With Security Issues [+]

Account Balance Negative [+]

Search Domains

 [go](#)

Import Domains

Transfer Request

Recent Transfer Activity

WHOIS

Download Droplist

View Domain

Summary

## CoCCA will ...

- store all unique reports it finds and associate them with the domains history
- automatically “clear” domains if issues are resolved
- allow drill-down for all domains registered using the same email or hosts
- send notices to admins if a new domain is registered by an individual who is listed as a contact for a domain that has been flagged.

**For more information - [garth.miller@cocca.org.nz](mailto:garth.miller@cocca.org.nz)**