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 verific		
4199b068b94716a347e4aa866f5ab504	SECURE_DOMAINS	Secure Tes		

Delete

Edit Record (Secure Test) Cancel

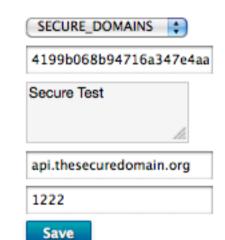
Verification Type

API Key

Description

Host

Port





Fast Flu	x Mitigation Se	ettings for .cx Co	CoCCA Registry Services (NZ) Limited Public Registrar (CoCCA)					garth_m	EN FR	EPP 🔵	WHOIS		
You are currently acting on behalf of CoCCA. Any action you take will be logged against their account.													
Home Regi	ster 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									Domains Awaiting Approval [+]				
✓ Modify the domain (lock / suspend / exclude) ✓ Notify people about the problem								Domains Pending Activation [+]					
Modification Please choose the action you'd like to perform on the domain Lock The state of the action you'd like to perform on the domain								Pending Superlock [+]					
Notification Settings SMS Notification Enter the phone numbers you want to send notification SMS messages to							Domains With Security Issues [+]						
							Account Balance Negative [+]						
							Search Domains go						
		Add									All Zones		
From: do-not-reply@coccaregistry.net									Create Zone				
Bcc:	bcc@coccaregistry.net , bcc@coccaregistry.net								Administrative Actions				
To:	Zone A	dmins								Build Zor	ne Files		
		CERT / Law Enforcement (enter the address)								Zone File Processing Defaults			
	CERT / Law									Zone File Automation			
										Clone Zone			
	□ Registra	ant Contact				■ Admini:	strative Cont	tacts		Update F	ricing		
									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 Portfo	Name Servers	Contacts L	ogins	Clients Zo	ones Rep	ports Mainter	nance Configuration	Info	Account	Sign (
If you would like to clear the outstanding security warnings, please enter a note and press Accept								Domains Awaiting Approval [+]					
Note										Domains Per	ding Activation	on [+]	
										Pending Sup	erlock [+]		
				la						Domains Wit	n Security Iss	ues [+]	
A	Accept									Account Balance Negative [+]			
These security violations have been recorded regarding this domain								Search Don	nains go				
Violation Type	Date Recorded	Date Reported	MD5 Signature		Acc	epted By (Regist	trar) Acce	pted By (Login)	Date Accepted	Import Doma	ins		
CnC	2012-10-02	2012-10-15	353dbd5b67f70236f	d11b178afceeed	18					Transfer Reg			
										Recent Trans			
The following secur	ity-related notes are	on file								WHOIS			
Note		No	ote Type		Made	By (Registrar)	Made By (Login) Date	•	Download D	roplist		
No notes made f	or this domain								// //	View Domai	n		
										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

