THE
SECURE DOMAIN
FOUNDATION

Norm Ritchie
ICANN Buenos Aires
November 2013
norm@thesecuredomain.org

Background

- Concept floated at ICANN Costa Rica (March, 2012)
  - Rampant recidivism in domain abuse can be curbed
  - We need to work together
- Initial concept has evolved considerably
  - Daily volume of of malware data doubled
  - Data feed idea became an API
  - API became a reputation system
  - SDF incorporated as a Canadian Non-Profit
- Official launch in January, 2014 … yeah!

THE SECURE DOMAIN FOUNDATION

About the Founders

Norm Ritchie
Domain Industry

The Canadian who holds the key to the Internet

It's housed in two high-security facilities separated by the North American landmass. The one authenticated map of the Internet.

Text size: Reset | Report an Error | + save to mystar

Chris Davis
Cyber Security

Canadian to receive FBI award for uncovering massive botnet scheme

JOHN GREENWOOD | 23/08/13 | Last Updated: 23/08/13 7:03 PM ET

More from John Greenwood

Republish Reprint

THE SECURE DOMAIN FOUNDATION

Some SDF Partners

What do Data Providers and Partners provide?

- Bad Guy Email Addresses
- ToS Breach Logs (Browser Fingerprint and Login IPs)
- Malware Data + Analysis
- Investigation Assistance
- Development Assistance
- Operational Assistance

Current Evolution

- Malware MD5 mapped to Domain Name + Category
  - Over 86M records
- Email Reputation Data
  - 7M+ records categorized
- Whois Data
  - 26M+ records categorized
- Browser Fingerprints
  - 315K collected
- ToS Violations logs
- Maltego Transforms
- Over 300M records in the Database

THE SECURE DOMAIN FOUNDATION

Coming Soon

- Postal Address Validation System - FREE
  - Dec, 2103 – Invite only Alpha
  - Jan, 2014 – Open Beta
- Phone Number Validation to follow
- Browser Fingerprint V2 Framework and Repository
- Registrar Rankings

THE SECURE DOMAIN FOUNDATION

Postal Address Validation

- Canada Post Partnership
- 150+ Countries
  - Last Name to Address Confidence Scoring
  - Multi-Format Fuzzy Logic
- UPS API approval for US addressing
- Google Maps API
- FREE!

THE SECURE DOMAIN FOUNDATION

Phone Number Validation

- Simple regex on current whois data = low fruit
- In the last 18 months, ~1.7 Million (gTLD) domains were registered with CC +1 and area codes that don't exist.
- Will publish findings

THE SECURE DOMAIN FOUNDATION

Browser Fingerprint DB

- Throwing away 300K current fingerprints at 94% unique
- New code is more accurate, better techniques
  - SDFPrint is a reversible 5 section hash
- Code is available now

THE SECURE DOMAIN FOUNDATION

Registrar Ranking

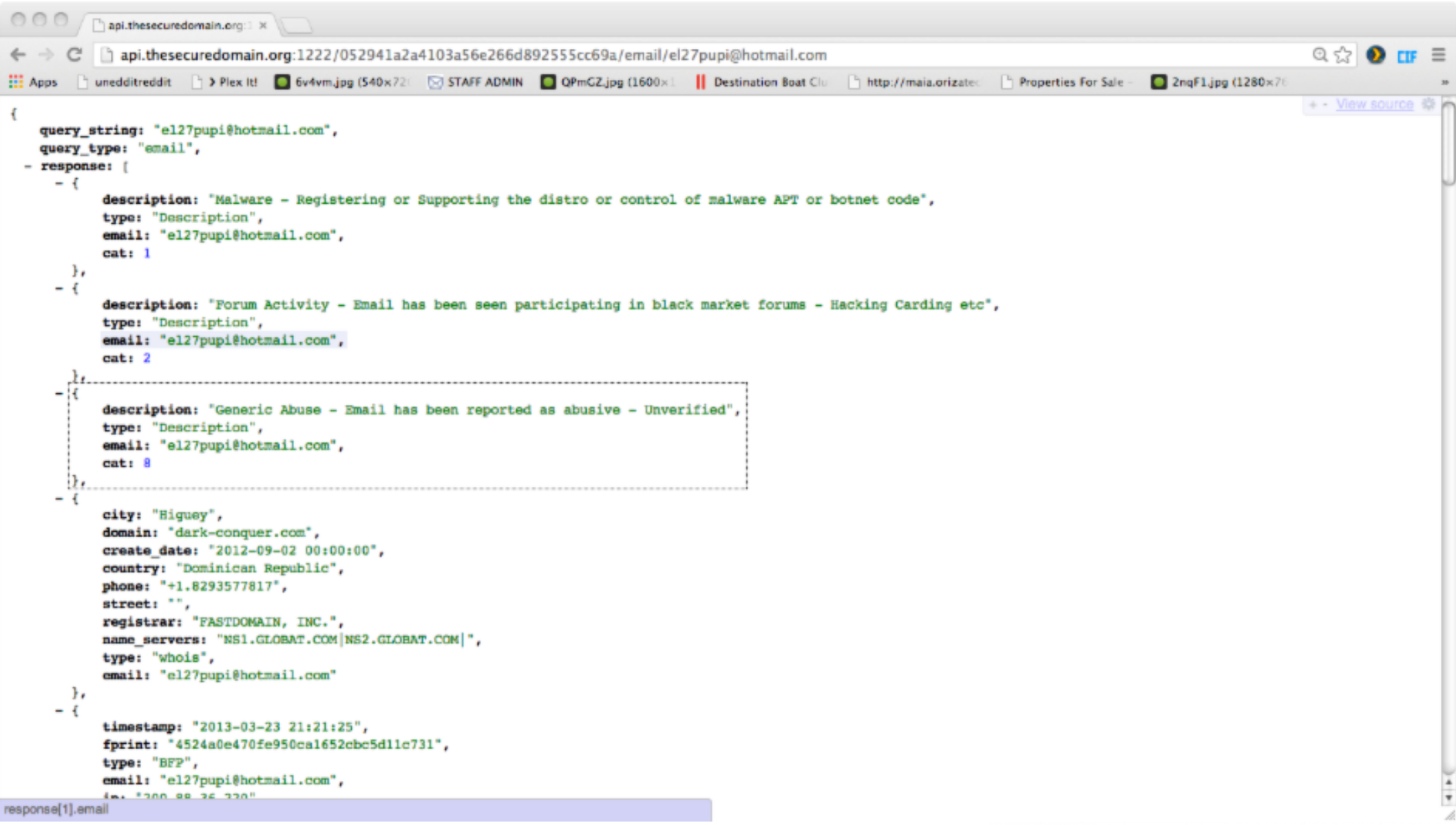
- Ranking based upon responsiveness to abuse complaints. NOT # of bad domains.
- Published record of turn around times on abuse complaints
- Apathetic and Malicious registrars will rise to the top

THE SECURE DOMAIN FOUNDATION

Synopsis of the API

- Validation scoring per data point for:
  Postal, Phone, Email
- Malicious reputation scoring per data point for:
  Email, Domain, IP, Postal, Phone, Fprint
- Simple or complex. JSON, XML, REST, CURL
- +details will present data after the score

THE SECURE DOMAIN FOUNDATION



THE SECURE DOMAIN FOUNDATION

Summary

- Free Postal Address Validation API covering 150+ Countries – Jan 2014
- Email, IP, and Fprint reputation data
- ccTLD daily feeds starting Nov1 2013
- Registrar reputation based on responsiveness
- This is a community effort! Always looking for more Partners!

www.thesecuredomain.org

THE SECURE DOMAIN FOUNDATION