

knipp

mambo+ funds program



Linda Müller
Dr. Michael Bauland

26th of June 2017

agenda

1. introduction

2. abuse monitoring

a. domain name abuse

b. needed information and tools

c. lessons learned

3. mambo⁺ funds program

agenda

1. introduction

2. abuse monitoring

a. domain name abuse

b. needed information and tools

c. lessons learned

3. mambo⁺ funds program

2.a. domain name abuse (1/3)



2.b. domain name abuse (2/3)

- Registries ► Registrars ► Hosters ► Registrant
- Registry can
 - monitor domains in zone
 - inform Registrars, Hosters, Registrants, third parties
 - technical handling, e.g. server hold, delete, suspend Registrar account

2.b. domain name abuse (3/3)

- ICANN's stand-point
 - regulation for ngTLDs: Spec 11 3b
 - working groups and activities:
 - Spec 11 3b Advisory
 - Security Framework
 - ITHI
 - DART

2.b. needed information and tools

- information
 - abuse information from various sources (free / with costs, pull / push)
 - zone file (e.g. AXFR, for ngTLDs: CZDS)
 - registrar and registrant information (e.g. whois, escrow)
- abuse handling tools
 - statistics
 - overview and details on abuse cases
 - action tracking
 - history of information
 - automatization as far as possible, e.g. alerts via email or mobile phone
 - immediate and periodic reports

2.c. lessons learned

- most recent information
- user-friendly accessibility key to successful abuse mitigation
- many benefits by data combination
- details important

Domains | mambo+ x +

https://mambo.plus/domains

mambo+ Dashboard Domain Views Report History Configuration

Linda Müller Domain Portfolio Owner Logout

Domain 67 Attributes

Domain	ALL ABUSE CASES	ALEXA RANKING	PROBLEMS	A	AAAA	MX	NS
cekuj.net		632,779		88.86.120.114	2a01:28:ca:63:120:114:0:0	2	2
chytrak.cz		491,342		88.86.117.145		2	2
clk.im	5	265,540		2		5	4
computerline.hk		612,467		91.135.67.202		mx1.computerline.net	3
comxa.com	1	229,157		54.243.232.177			2
crackspider.us	1	811,029		109.201.131.15		mail.crackspider.us	2
darktech.org	1	195,611		209.240.78.125		5	3
doodlekit.com	1	120,311		23.21.133.143		7	4
doubleclick.net		279		172.217.18.174	2a00:1450:4001:806:0:0:200e	5	4
earthlink.net	4	4,007	1				
easily.co.uk				185.26.229.205		2	2
fabioalbini.com	1			195.110.128.11		2	2
fanatiksport.ro				85.9.35.138		fanatiksport.ro	3
fashioncapital.co.uk	1						2
favorit-network.com			1	54.72.9.51		mail.b-io.co	4
fc2.com	3	110		2		mx01.fc2.com	4
fh-worms.de		314,120		143.93.160.29	2001:4c80:81:a000:0:0:0:1d	2	2
filepicker.io		36,095		54.87.148.91		5	4
focus.de		984		23.57.22.242		4	6

Subcategory MALWARE
 Added on 2016-08-30T11:08:21Z
 Abused URL http://www.fabioalbini.com/7o7agb
 Ransomware Locky Distribution Site

Filter Sort by: Domain Name (ascending) Page: 1

Domain Abuse Alexa Ranking Problems DNS Domain is in Zone

All Date Time Update Save Report Download E-Mail

agenda

1. introduction
2. abuse monitoring
 - a. domain name abuse
 - b. needed information and tools
 - c. lessons learned
3. mambo⁺ funds program

3. mambo⁺ funds program (1/5)

- our goal:
Make the advantages of an abuse monitoring system available to Registries that currently do not have the financial resources to pay for such a service.

3. mambo⁺ funds program (2/5)

- we provide:
 - monitoring of zone
 - identification of abuse cases (e.g. Spam, Phishing, Botnets, Malware)
 - additional data available (ranking, DNS information, etc.)
 - view historical data
 - data storage on servers located in Germany
 - compliance with European Data Protection
 - immediate alerts
 - automated reports

3. mambo+ funds program (3/5)

- Who provides the solution?

Knipp Medien und Kommunikation GmbH

- specialized software company from Germany
- over 20 years of experience in the domain industry
- other products:  
- highest standards of Data Protection
 - ISO 27001 certified
 - own data centers in Germany
 - all solutions are developed and operated under strict German Data Protection laws

3. mambo⁺ funds program (4/5)

- Who can apply?
 - You are a **ccTLD Registry**
 - You are a **nonprofit organization**
 - You have less than **5.000 domains**
 - You are from a **non-OECD country**

3. mambo⁺ funds program (5/5)

- How to apply?
 - Unbureaucratic process
 - Contact us:
info@mambo.plus
<https://mambo.plus>