UNDERSTANDING REPUTATION BLOCK LISTS and how they impact DNS Abuse regional practice

EURALO ROUNDTABLE DISCUSSION
JULY 6 2021

STEINAR GRØTTERØD
Recito AS
Board Member ISOC Norway

Why do I know something of this?

- Experience as ISP, Registrar and Registry Operator
- Dayjob handling abuse notices for iQ Global clients
- Consulting Registry Operators in creating their abuse policy
- Active in the DNS Abuse discussions within ICANN and At-Large

What is a Reputation Block List?

A list of domain names, Uniform Resource Locators (URLs), or Internet Protocol (IP) addresses that are known security threats. Security systems throughout the Internet use RBLs to keep malicious or unwanted material from reaching victims. In addition to filtering out billions of incoming spam messages a day, RBLs block outgoing requests to malicious or disreputable IP addresses.

RBLs are created and maintained by commercial service providers, researchers, and public interest communities.

ICANN Definition (https://www.icann.org/en/icann-acronyms-and-terms/reputation-block-list-en)

The data from the Reputation Block Lists (RBLs) are used by Contracted Parties, the Domain Abuse Activity Reporting (DAAR) system, and others in monitoring their namespace.

Some RBLs Providers

- SURBL lists (Spam –Phishing -Malware)
- Spamhaus Domain Block List (Spam -Phishing -Malware -Botnet C&C)
- Anti-Phishing Working Group (Phishing)
- Malware Patrol (Malware, Ransomware, Botnet C&C)
- Phishtank (Phishing domains)
- ABUSE.CH (Ransomware tracker, Feodotracker)

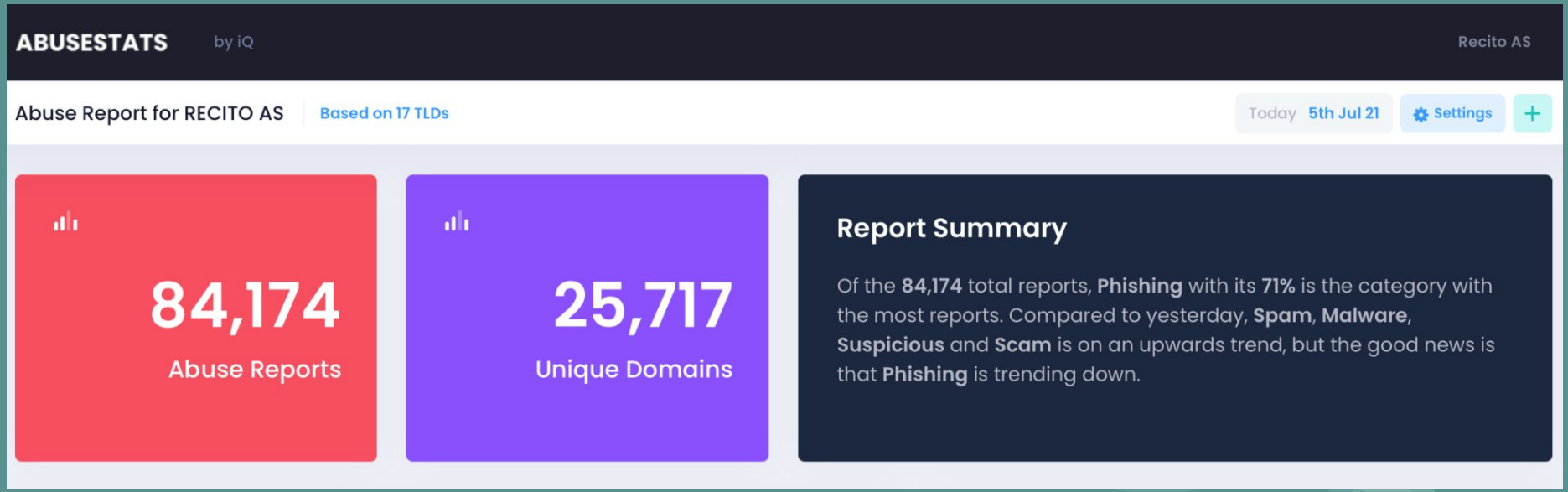
Abuse Mitigation

RBLs is a common “toolbox” for acting on security threats

Criteria #1: Terms and Conditions in agreement to act on suspicious behaviour

- New gTLDs: Registry Agreement Specification 11.3B
- 2013 Registrar Accreditation Agreement
- Various requirements to act on suspicious behaviour for European ccTLDs

Criteria #2: A system to identify security threats
Criteria #3: Communication



European ccTLDs RBL notices

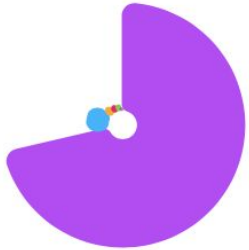
.FR, .CO.UK, .DE, .SE, .IT, .PL, .PT, .RO, CH, .NO, .AT, IS, .DK, .FI, .IE, LT & .LT

Report created using https://abusestats.com

https://abusestats.com/report/far-60d1a5bb07d47-wksnblrg

Abuse Reports by Categories

Click legend to toggle category on and off



Phishing	71.4%	Uncategorized	13.8%
Spam	5.3%	Malware	4.0%
Suspicious	3.4%	Botnet	1.0%
Scam	0.8%	Hacked	0.2%
Generated Domains	0.0%		

?

STEINAR@RECITO.NO