# POLICY IN ACTION: What makes a Reputation Provider effective

**Nanog 92** | October, 2024

SPAMHAUS

# Meet the speaker

**Matthew Stith**
Industry Liaison

# Hello, we're Spamhaus

## STRENGTHENING TRUST AND SAFETY ON THE INTERNET

SPAMHAUS

# What we'll cover

1. **Policy**
2. **Importance of accuracy**
3. **Stellar Group SAS** | Scenario 1
4. **KDDI Corporation** | Scenario 2
5. **Community** | Sharing intelligence

# How Policy defines IP Reputation

- Research into suspicious IPs
- Indicators (good/bad) e.g., configuration
- Regular policy adjustments to address changes to the abuse landscape


Evidence is critical

# How Policy defines Domain Reputation

- Domain reputation score is a grayscale
- Multiple factors impact scoring
- Context is important in listing decisions


Evidence is critical

# Understanding escalations

- This is a last resort action
- Very few escalations
- Escalation triggers:
  - Failure to resolve a issue
  - Dishonesty in issue resolution
  - No response
  - Refusal to mitigate or remediate

**Evidence is critical**

# Importance of accuracy


Uncle Ben

# Stellar Group SAS

Scenario 1

**In this Spamhaus Blocklist (SBL) example, we identified who was behind this rogue ISP...**

- Stellar Group SAS, a France-based company.
- Running network infrastructure for bulletproof host.
- RDP[.]monster.
- Advertised RDP servers allowing anonymous registration.

# Stellar Group SAS

Scenario 1

## The plot thickens...

- AS203168, registered to a Dinant, Belgium-based strawman, Constant Moulin.
- Increased pressure through SBL listings and upstreams.
- Mistake revealed Stellar Group, not Constant Moulin.

# Stellar Group SAS

Scenario 1

## Time to DROP…

- Stellar Group relocated/obtained own AS, AS214961.
- DROP’d network leased from Neterra (Bulgaria-based IP broker)
- SBL648570 (178.215.236[.]0/24).
- Network ownership knowledge sufficient to preventively list.
- OpSec mistake key to link Stellar Group and RDP[.]monster.

# KDDI Corporation

Scenario 2

## A range of IP addresses on KDDI's Network

- Investigators manually discovered that a /22 was hosting malicious material
- A SBL listing was created to prevent further damage
- Thousands of domains were discovered on these IPs (All scams)

# KDDI Corporation

Scenario 2

## An ongoing problem of abuse...

- Continued abuse and new domain registrations on the malicious range
- Manually adding domains does not scale and increases gaps in protection against maliciousness

# KDDI Corporation

## Scenario 2

## Using automation to scale policy decisions...

- Researchers use multiple tools to find patterns
- Metadata for each domain is stored
- Associations are made from the domains observed on the listed range with the same attributes

# KDDI Corporation

## Scenario 2

## Automation in practice...

- After a pattern is identified any new domain observed will be automatically given the proper negative reputation and be put into the zone.
- All automated entries adhere to the policy in place

# Sharing intelligence

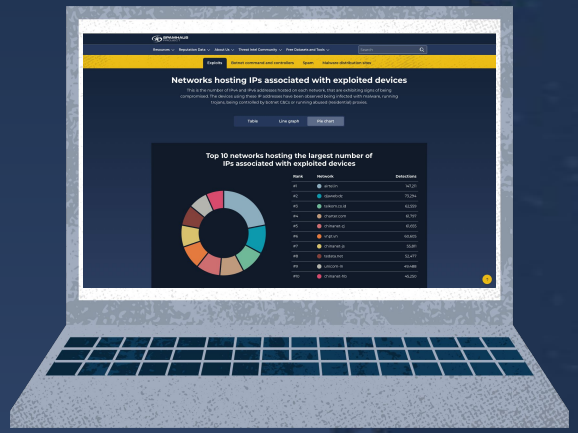
- We all have a role to play!
- Community = visibility and context
- Your insight is unique
- Reputation providers look at TTP (tactics, techniques & procedures) not users.

# Sharing intelligence

- Useful data: malware & phishing samples/URLs, unsolicited messages, passive DNS, connect data, etc.
- Your detections help strengthen trust and safety and improve provider’s policies.

# Free resources

## Available to Network Operators:



### DATA

**Don’t Route Or Peer (DROP) Lists**

### STATS

**Network Reputation Statistics**

### BLOG

**Avoid fraudulent sign ups**

# Any questions?

**Matthew Stith**

stith@spamhaus.com

SPAMHAUS