DNS Abuse - Decisive Mitigation Based on Evidence

James Galvin, Ph.D.
Identity Digital

ROW12 - 20 June 2023

Pro-Active Abuse Mitigation

- Anti-Abuse Report 2022Q2
  - https://identity.digital/wp-content/uploads/2022/09/Anti-Abuse-Report-Q2-2022.pdf
- Anti-Abuse Report 2022Q3
  - https://identity.digital/wp-content/uploads/2022/12/Anti-Abuse-Report-Q3-2022.pdf
- Anti-Abuse Report 2022Q4
  - https://identity.digital/wp-content/uploads/2023/03/Anti-Abuse-Report-Q4-2022.pdf
- Anti-Abuse Report 2023Q1
  - https://identity.digital/wp-content/uploads/2023/06/Anti-Abuse-Report-Q1-2023.pdf

Upleveling First Principles

- Clear stand on non-arbitrary, evidence-based decisions
  - Allegations or reports are insufficient
  - Evidence is required
- Decisive
  - Mitigate and disrupt
  - Reduce severity and duration of victimization
- Focus
  - **Behavior and activity - not registration data**
  - Thoughtful, multi-layered, and remaining aggressive

CleanDNS®

- Cornerstone tool - relatively new entrant in anti-abuse industry
    - Ingest reports
    - **Gather evidence - includes only public information**
    - Create cases
- Building on First Principles, we focus on cases and actions

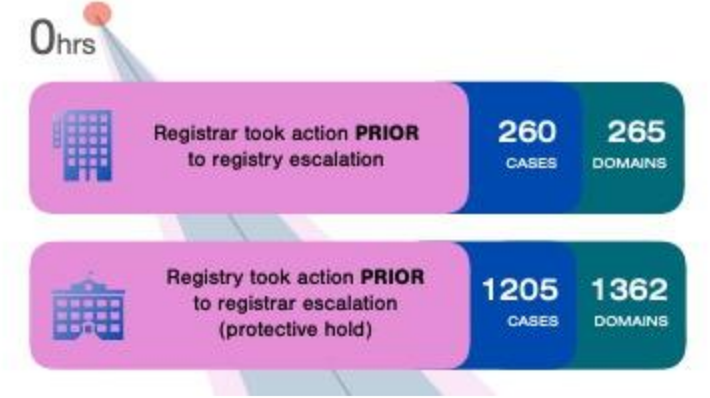
Key Definitions

- DNS Abuse
  - Phishing, Pharming, Malware, Botnets
  - Spam - when used for delivery of abuse
- Content - no, except for clear and present danger
  - CSAM
  - Inciting violence
- Trusted Notifiers
  - IWF

Effectiveness

	2022Q2	**2022Q3**	**2022Q4**	**2023Q1**
Phishing	2794	2794	2487	2224
Spam	124	124	66	23
Malware	49	49	77	88
Pharming	11	11	0	0
Botnet	4	4	0	0
Other	25	25	35	29

Action Timeline - 2023Q1

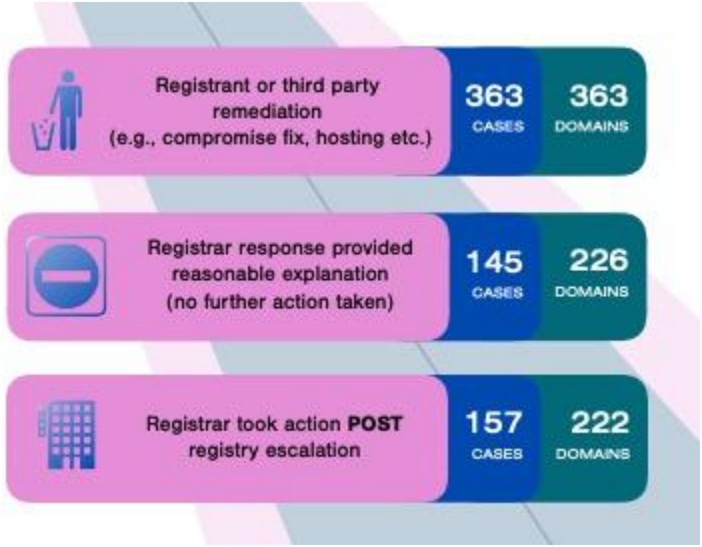


0hrs

Registrar took action **PRIOR** to registry escalation — 260 CASES — 265 DOMAINS

Registry took action **PRIOR** to registrar escalation (protective hold) — 1205 CASES — 1362 DOMAINS

24hrs



Registrant or third party remediation (e.g., compromise fix, hosting etc.) — 363 CASES — 363 DOMAINS

Registrar response provided reasonable explanation (no further action taken) — 145 CASES — 226 DOMAINS

Registrar took action **POST** registry escalation — 157 CASES — 222 DOMAINS

- 66% of cases addressed in less than 24 hours
- 96% of cases addressed in less than 72 hours

Credit: Getty Images/iStockphoto