CleanDNS

Evidencing reports of DNS Abuse

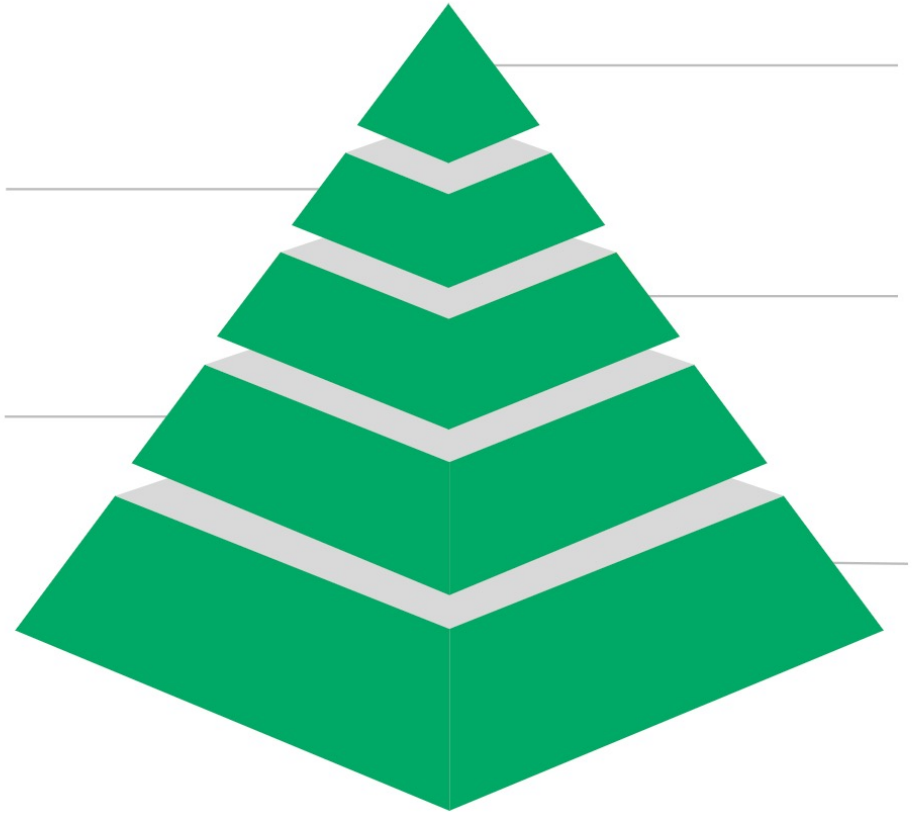
Chris Lewis-Evans

CleanDNS

Receive reports

Abuse Lists
Phishlabs, OpenPhish, SURBL, Spamhaus, APWG, Maldatabase, abuse.ch

Abuse@
Clients provide access to their abuse email box.



NetBeacon
Reports from NetBeacon are directly fed into CleanDNS.

Abuse Ingest Form
Embedded abuse form on clients site fed directly into CleanDNS. Managed by a CRM.

Reporters
Researchers, Cybersecurity organizations, CERTS

CleanDNS

- All abuse reports received by CleanDNS from *any* source, for *any* Rr/Ry/Host are processed and enriched

- All reports that cannot be resolved via CleanDNS due to a lack of client relationship are relayed to the appropriate party via DNS Abuse Institute's NetBeacon (to be then relayed to the appropriate party)

- Feedback on actions taken on the reported domain – facilitating better outcomes for reporters

- By determination at time of report whether a domain is registered for abusive purposes or in fact a compromised host, the case can be directed to appropriate party faster (Rr/Ry vs Host) allowing for shorter uptime and thus less victimisation

CleanDNS

Evidencing Requirements:

Each type of abuse has different types of evidence available to qualify the specific harm. The evidence can often be captured in a visual context. Where it is not, it is important to be able to detail the activity or resources used that contributed to the harm caused.

- Report
- Screenshots
- Header information
- Log data
- Record Full URLs: harmful websites or posts.
- Content or a Hash of the content
- Preserve Metadata

CleanDNS

Is PII used?

- In evidencing reports?
- In taking appropriate action?

CleanDNS

Questions?

Chris Lewis-Evans
chris@cleandns.com