Measuring Domain Abuse

Stop Counting Abuse, Start Truly Measuring Abuses' Impact

March 3, 2024
CleanDNS.com

CleanDNS

…there must be a better method

To tackle the problem space around measuring harms and abuse, **we need to be able to understand if and what effects the mitigative and preventative actions make**. There are several techniques used to measure DNS abuse and online harms, each with its own strengths and weaknesses.

In this presentation we'll explore the methods for measure and determination of harms:

- domain volume analysis

- response time monitoring

- harm-based analysis

- barrier-to-entry analysis

CleanDNS

domain volume analysis

The current standard of measurement

Several methods to this technique but generally involves analyzing a group of domains (e.g. under management; per TLD) and plotting them against **block lists** or other **markers of malicious activity** to provide a **ratio of bad vs good**.

.

CleanDNS

missing the impact

Life Cycle vs Counting

- If one domain has 200K phishing domains on the 3rd level annually
- If one domain has live harms for an extended period
- If one domain serves as a service for provisioning of harms URL strings

- Do you count it once?
- Do you count all the abuse url's on the domain?
- How does that impact the actual measurement of the harm?

CleanDNS

Wide variability in measurement

Due to different systems of measurement variability comes into play as different abuse types or campaigns may utilize different domain usage techniques such as:

- Third level sub-domains for phishing in volume on one domain
- Multiple abuse URL strings as part of one domain

Domain volume analysis can be useful for giving an overview of a large domain space however, it may not be effective at giving a consistent and accurate measure to base mediative or proactive actions.

Interisle/Cybercrime Info Center:

- https://www.cybercrimeinfocenter.org/phishing-landscape-studies/#pl2023

ICANN DAAR:

- https://www.icann.org/octo-ssr/daar-faqs/#daar

APWG Phishing Trends:

- https://rb.gy/rmak32

CleanDNS

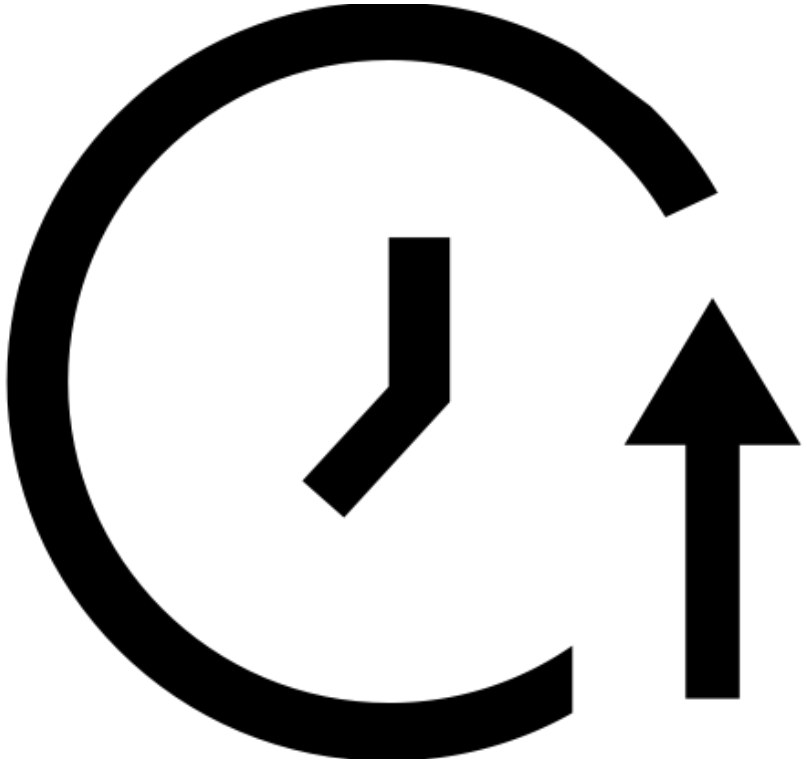
Can we do better?

There are better ways to measure the effectiveness and impacts of online harms.

uptime monitoring

How long was the impact of the potential harm live?

- This technique involves monitoring the availability of a malicious domain against the time to action an abuse report.



CleanDNS

time to live

As per SSAC 115 reporting to primary point of responsibility to act on the harm is a key element to reducing this time as it prevents the time taken in transferring the report between parties. Additionally, and most important, it reduces potential harms.

Reducing HARMS is the key measurement Point...
Reducing uptime or “time to live” helps determine the impact and effectiveness of any abuse/harms reduction program.

Time Measurements:

- first appearing on a block list -> mitigated
- first being reported (and after confirming actionable evidence) -> mitigated

The key benefit is that this provides a very repeatable measurement. Being able to focus on reducing this time allows for improvements in process to have large impacts.

CleanDNS

harm-based analysis

Analyzing the number and severity of harms caused by online harms

- Harm-based analysis can be useful for determining harms that cause significant harm to users or the internet as a whole.
- Prioritization of actions based on level or severity of harm

Difficulties:
Reporting: with low levels of reporting from victims and inconsistent definitions and measures makes this method more suited to trend reporting rather than basing activity from it.
Suggestions:
Correlation of victim report losses tied to domains involved to measure impact/losses

under reporting harms

Where are the harms?

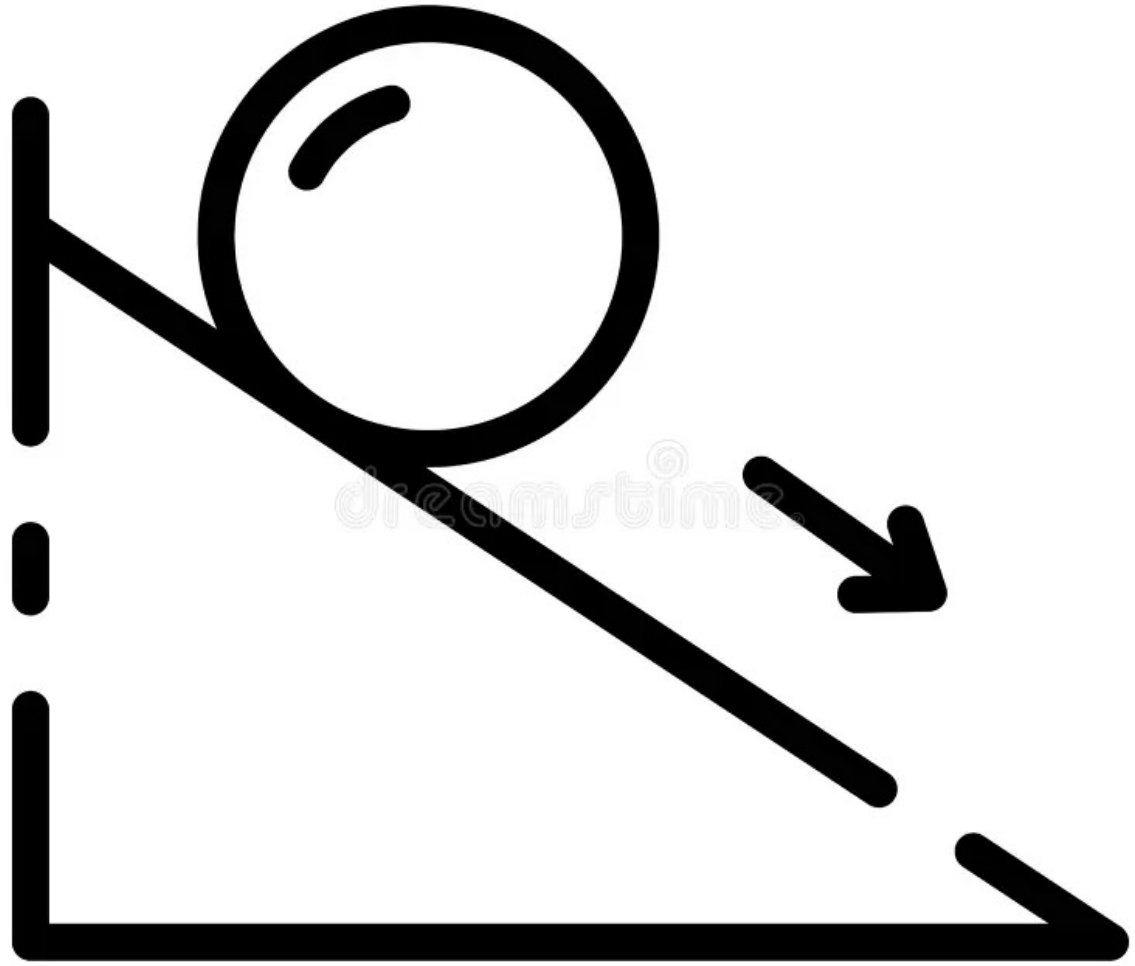
- The majority of online harms are micro targeted (victim pool of less that 10K)
- Reporting of harms is voluntary
- When little actions are taken, incentive to report is reduced
- Prosecution of online harms is global sub 2% of reported
- **The World Economic Forum's 2020 Global Risk Report states that the rate of detection (or prosecution) is as low as 0.05 percent in the U.S.** (https://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf)

CleanDNS

barrier-to-entry analysis

friction in the process

- Pricing
- Volumes at purchase
- Resale of accounts
- Migration between providers
- Friction at account creation
- Friction at deployment based on infrastructure reputation



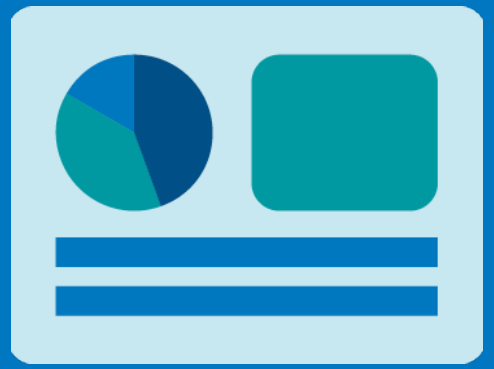
CleanDNS

Barriers

Difficult to obtain metrics

- Must purposely track/log
- Internal only in most cases
- Can be considered a competitive advantage

Discussion



Section Title Goes Here

Section subhead lorem ipsum dolor sit amet

CleanDNS